SEJM
RZECZYPOSPOLITEJ POLSKIEJ
VIII kadencja
Prezes Rady Ministrów
RM-10-64-18

Druk nr 2505 cz. II

Warszawa, 30 kwietnia 2018 r.

Pan
Marek Kuchciński
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku

Na podstawie art. 118 ust. 1 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. przedstawiam Sejmowi Rzeczypospolitej Polskiej projekt ustawy

- o krajowym systemie cyberbezpieczeństwa z projektami aktów wykonawczych.

Projekt ma na celu wykonanie prawa Unii Europejskiej.

W załączeniu przedstawiam także opinię dotyczącą zgodności proponowanych regulacji z prawem Unii Europejskiej.

Jednocześnie informuję, że do prezentowania stanowiska Rządu w tej sprawie w toku prac parlamentarnych został upoważniony Minister Cyfryzacji.

Z poważaniem

(-) Mateusz Morawiecki

RAPORT Z KONSULTACJI PUBLICZNYCH I OPINIOWANIA

PROJEKTU USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

1. Informacje ogólne

Niniejszy dokument stanowi wypełnienie obowiązku, zgodnie z którym organ wnioskujący sporządza raport z konsultacji obejmujący omówienie wyników przeprowadzonych konsultacji publicznych i opiniowania.

Na podstawie art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa projektowana ustawa została udostępniona na stronie podmiotowej Biuletynu Informacji Publicznej Ministerstwa Cyfryzacji oraz na stronie Rządowego Centrum Legislacji.

2. Przebieg konsultacji

Konsultacje odbyły się w terminie od dnia 31 października do 21 listopada 2017 r.

W ramach konsultacji publicznych projekt został przesłany do:

1. Fundacji Bezpieczna Cyberprzestrzeń
2. Fundacji ePaństwo
3. Fundacji Przedsiębiorców Polskich Archiwizjoner
4. Fundacji Instytut Mikromakro
5. Fundacji PANOPTYKON
6. Fundacji Pułaskiego
7. Instytutu Kolejnictwa
8. Instytutu Kościuszki
9. Instytutu Logistyki i Magazynowania
10. Izby Gospodarki Elektronicznej
11. Izby Gospodarcza Gazownictwa
12. Izby Gospodarcza Transportu Lądowego
13. Krajowej Izby Gospodarcza Elektroniki i Telekomunikacji
14. Krajowej Izby Gospodarki Cyfrowej
15. Krajowej Izby Gospodarki Morskiej
16. Krajowej Izby Gospodarczej
17. Krajowej Izby Komunikacji Ethernetowej
18. Krajowej Rady Radców Prawnych
19. Polskiej Izby Informatyki i Telekomunikacji
20. Polskiej Izby Radiodyfuzji Cyfrowej
21. Polskiej Izby Komunikacji Elektronicznej
22. Polskiej Izby Paliw Płynnych
23. Polskiej Izby Ubezpieczeń
24. Polskiej Organizacji Przemysłu i Handlu Naftowego
25. Polskiego Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej
26. Polskiego Towarzystwo Informatyczne
27. Stowarzyszenia Euro-Atlantyckiego
28. Towarzystwa Gospodarczego Polskie Elektrownie
29. Związku Armatorów Polskich

30. Związku Przedsiębiorców i Pracodawców
31. Związku Telewizji Kablowych w Polsce
32. Związku Banków Polskich
33. Związku Pracodawców Mediów Elektronicznych
34. Związku Pracodawców Branży Internetowej Interactive Advertising Bureau Polska

W celu wykonania obowiązku zasięgnięcia opinii projekt ustawy został przekazany do zaopiniowania do:

1) Agencji Bezpieczeństwa Wewnętrznego
2) Agencji Wywiadu
3) Banku Gospodarstwa Krajowego
4) Biblioteki Narodowej
5) Biura Bezpieczeństwa Narodowego
6) Centralnego Biura Antykorupcyjne
7) Centrum Systemów Informacyjnych Ochrony Zdrowia
8) Generalnego Inspektora Ochrony Danych Osobowych
9) Giełdy Papierów Wartościowych
10) Głównego Urzędu Statystycznego
11) Kancelarii Prezydenta Rzeczypospolitej Polskiej
12) Kancelarii Sejmu Rzeczypospolitej Polskiej
13) Kancelarii Senatu Rzeczypospolitej Polskiej
14) Kasy Rolniczego Ubezpieczenia Społecznego
15) Komendy Głównej Policji
16) Komendy Głównej Straży Granicznej
17) Krajowego Depozytu Papierów Wartościowych
18) Krajowej Izby Rozliczeniowej
19) Krajowej Rady Radiofonii i Telewizji
20) Naczelnej Rady Adwokacka
21) Naczelnej Dyrekcji Archiwów Państwowych
22) Najwyższej Izba Kontroli
23) Narodowego Centrum Badań i Rozwoju
24) Narodowego Centrum Kryptologii
25) Narodowego Centrum Nauki
26) Narodowego Banku Polskiego
27) Narodowego Funduszu Ochrony Środowiska i Gospodarki Wodnej
28) Narodowego Funduszu Zdrowia
29) Narodowego Instytutu Muzealnictwa i Ochrony Zbiorów
30) Ośrodka Przetwarzania Informacji
31) Państwowej Agencji Atomistyki
32) Polskiej Agencji Żeglugi Powietrznej
33) Polskiej Akademii Nauk
34) Polskiego Centrum Akredytacji
35) Prokuratorii Generalna Rzeczypospolitej Polskiej
36) Rady Dialogu Społecznego
37) Rady do Spraw Cyfryzacji
38) Rządowego Centrum Bezpieczeństwa
39) Sądu Najwyższego

40) Służby Kontrwywiadu Wojskowego
41) Służby Wywiadu Wojskowego
42) Trybunału Konstytucyjnego
43) Urzędu Ochrony Konkurencji i Konsumentów
44) Ubezpieczeniowego Funduszu Gwarancyjnego
45) Urzędu Regulacji Energetyki
46) Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych
47) Urzędu Lotnictwa Cywilnego
48) Urzędu Transportu Kolejowego
49) Urzędu Komisji Nadzoru Finansowego
50) Urzędu Zamówień Publicznych
51) Zakładu Ubezpieczeń Społecznych
52) Business Centre Club – Związku Pracodawców
53) Niezależnego Samorządowego Związku Zawodowego „Solidarność"
54) Ogólnopolskiego Porozumienia Związków Zawodowych
55) Forum Związków Zawodowych
56) Pracodawców Rzeczypospolitej Polskiej
57) Konfederacji Lewiatan
58) Związku Rzemiosła Polskiego

Uwagi do projektu zgłosiły następujące podmioty:
1) Fundacja Bezpieczna Cyberprzestrzeń
2) Instytut Audytorów Wewnętrznych IIA Polska
3) Instytut Kościuszki
4) Instytut Logistyki i Magazynowania
5) Izba Gospodarcza Gazownictwa
6) Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji
7) Krajowa Izba Komunikacji Ethernetowej
8) Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa
9) Krajowy Związek Banków Spółdzielczych
10) dwie osoby fizyczne
11) Polska Izba Informatyki i Telekomunikacji
12) Polska Izba Komunikacji Elektronicznej
13) Polska Izba Radiodyfuzji Cyfrowej
14) Polska Izba Ubezpieczeń
15) Polska Organizacja Przemysłu i Handlu Naftowego
16) Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej
17) Związek Banków Polskich
18) Business Centre Club - Związek Pracodawców
19) Federacja Przedsiębiorców Polskich
20) Konfederacja Lewiatan
21) Pracodawcy Rzeczypospolitej Polskiej
22) Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM
23) Biuro Bezpieczeństwa Narodowego
24) Generalny Inspektor Ochrony Danych Osobowych
25) Kancelaria Sejmu Rzeczypospolitej Polskiej

26) Kancelaria Senatu Rzeczypospolitej Polskiej
27) Komisja Nadzoru Finansowego
28) Krajowa Rada Radiofonii i Telewizji
29) Naczelny Dyrektor Archiwów Państwowych
30) Najwyższa Izba Kontroli
31) Narodowe Centrum Badań i Rozwoju
32) Narodowy Bank Polski
33) Polska Akademia Nauk
34) Prokuratoria Generalna Rzeczypospolitej Polskiej
35) Rada do Spraw Cyfryzacji
36) Rządowe Centrum Bezpieczeństwa
37) Służba Kontrwywiadu Wojskowego
38) Ubezpieczeniowy Fundusz Gwarancyjny
39) Urząd Dozoru Technicznego
40) Urząd Komunikacji Elektronicznej
41) Urząd Lotnictwa Cywilnego
42) Urząd Regulacji Energetyki
43) Zakład Ubezpieczeń Społecznych
44) Prokuratura Krajowa

Projekt w dniu 31 października 2017 r. został także skierowany do zaopiniowania przez Komisję Wspólną Rządu i Samorządu Terytorialnego i w dniu 13 grudnia 2017 r. został uzgodniony przez Komisję Wspólną Rządu i Samorządu Terytorialnego.

3. Omówienie wyników przeprowadzonych konsultacji publicznych i opiniowania

Uwagi wraz z prezentacją stanowiska Ministra Cyfryzacji wobec tych uwag omówiono w tabelach stanowiących załącznik do Raportu z konsultacji publicznych i opiniowania.

4. Przedstawienie wyników zasięgnięcia opinii, dokonania konsultacji albo uzgodnienia projektu z właściwymi organami i instytucjami Unii Europejskiej, w tym Europejskim Bankiem Centralnym

Ustawa zostanie notyfikowana Komisji Europejskiej zgodnie z art. 25 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1). Projekt ustawy nie wymaga przedłożenia innym instytucjom i organom Unii Europejskiej lub Europejskiemu Bankowi Centralnemu w celu uzyskania opinii, dokonania konsultacji lub uzgodnienia.

5. Wskazanie podmiotów, które zgłosiły zainteresowanie pracami nad projektem w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa, wraz ze wskazaniem kolejności dokonania zgłoszeń albo informację o ich braku.

Nie odnotowano zgłoszeń zainteresowanych podmiotów w trybie przepisów o działalności lobbingowej w procesie stanowienia prawa.

Zestawienie zgłoszonych uwag do projektu ustawy o krajowym systemie cyberbezpieczeństwa – OPINIOWANIE

L.p.	Art.	Podmiot	Treść uwagi	Stanowisko MC
Uwagi ogólne				
1.	ogólna	Służba Kontrwywiadu Wojskowego	SKW sugeruje doprecyzowanie w treści projektowanej ustawy kwestii związanych z zarządzaniem ryzykiem, szczególnie na poziomie krajowym. Należy także rozważyć wprowadzenie funkcji koordynatora krajowego (o stosownych uprawnieniach), w zakresie działań merytorycznych CSIRT'ów poziomu krajowego.	Uwaga częściowo uwzględniona. Sposób realizacji zadań i współpracy oraz właściwości CSIRT poziomu krajowego został określony w ustawie. Obecny model został zaproponowany przez CSIRT poziomu krajowego w ramach uzgodnień roboczych. Zasady koordynacji operacyjnej wskazują przepisy dot. CSIRT oraz Zespołu ds. Incydentów Krytycznych (m.in. art. 28 i art. 37). Projekt zostanie rozszerzony o przepisy przewidujące powołanie przy Radzie Ministrów Kolegium do spraw Cyberbezpieczeństwa w skład którego wchodzić będzie Minister Kooordynator Służb Specjalnych, MON, MSWiA, MC i RCB. W opinii projektodawcy przepisy dotyczące zarządzania ryzykiem na poziomie krajowym są wystarczające.
2.	ogólna	Rada do Spraw Cyfryzacji	Certyfikacja podmiotów świadczących usługi z zakresu cyberbezpieczeństwa Wskazane w art. 4 pkt 15 projektu ustawy „podmioty świadczące usługi z zakresu cyberbezpieczeństwa", które zostały objęte krajowym systemem cyberbezpieczeństwa, powinny być poddane certyfikacji ABW lub SKW (co najmniej mechanizm analogiczny do nadania certyfikatu bezpieczeństwa teleinformatycznego - zgodnie	Uwaga nieuwzględniona.

			z art. 50 ust. 3 ustawy o ochronie informacji niejawnych). Z uwagi na zakres zadań w obszarze cyberbezpieczeństwa operatorów usług kluczowych, który może być przekazany ww. podmiotom (art. 15 ust 2 w związku z art. 10 ust. 2, art. 11 ust. 1, art. 12 ust. 1 oraz art. 14), m.in. zbieranie informacji o zagrożeniach, zarządzanie incydentami, zarządzanie ryzykiem, objęcie monitoringiem świadczenie usług kluczowych oraz dostawców usług cyfrowych (art. 23), jak i zadania z zakresu współpracy z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań (art. 35 ust. 5) oraz dostęp do systemu teleinformatycznego, o którym mowa w art. 42 (art. 42 ust. 1 pkt 1), konieczne jest, aby ustawa w sposób literalny odnosiła się do wymogu certyfikacji podmiotów świadczących usługi z zakresu cyberbezpieczeństwa. W tym aspekcie, nadzór ministra właściwego ds. informatyzacji przewidziany w art. 47 ust. 1pkt. 1 projektu ustawy, należy uznać za model niewystarczający zarówno w kontekście ograniczonych kryteriów kontroli (zawężonych do czynników wskazanych w art. 15 ust. 2), następczego charakteru realizacji przedmiotowej kompetencji, jak i ograniczonego zakresu czynności kontrolnych (zgodnie z procedurą kontroli działalności gospodarczej przedsiębiorcy opisaną w ustawie o swobodzie działalności gospodarczej - art. 48 ust. 1 w związku z art. 47 ust. 1 pkt 1 projektu ustawy). Potrzeba literalnego ustanowienia mechanizmu certyfikacji podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, które wchodzą w skład krajowego systemu cyberbezpieczeństwa wynika zarówno z okoliczności faktycznych, dokumentów programowych Ministerstwa Cyfryzacji oraz generalnego postulatu jasności prawa (kompleksowości tekstu prawnego). Po pierwsze, z uwagi na podstawowe interesy bezpieczeństwa państwa, certyfikacja ABW zminimalizuje ryzyko wykorzystywania w ramach ochrony teleinformatycznej operatorów usług kluczowych (oraz pozostałych wskazanych powyżej sferach) rozwiązań, które przyczyniałyby się do obniżenia poziomu cyberbezpieczeństwa poprzez m.in. użytkowanie oprogramowania zawierającego celowo umieszczone luki (m.in. backdoor). Postulat udziału ABW w procesie weryfikacji producentów i usługodawców rozwiązań w ramach sieci teleinformatycznych organów administracji	

			państwowej, podnoszony był również w Założeniach strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2016 roku. Literalne odniesienie wprost do ustawy o ochronie informacji niejawnych, pozwoli także zniwelować ewentualną niejasność co do stosowania właściwych przepisów w kontekście czynności realizowanych przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa, które wchodzą w skład krajowego systemu cyberbezpieczeństwa. Umożliwi to zdjęcie z operatorów usług kluczowych obowiązku każdorazowej wykładni przepisów dotyczących informacji niejawnych w kontekście realizacji poszczególnych zadań i obowiązków przewidzianych w projekcie ustawy przy pomocy podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, co z kolei będzie miało pozytywny wpływ na stopień faktycznej ich realizacji – a zatem odporności krajowego systemu cyberbezpieczeństwa.	
3.	ogólna	Rada do Spraw Cyfryzacji	Podział zakresu odpowiedzialności za cyberbezpieczeństwo Państwa między 3 odrębne podmioty Przyjęty w projekcie ustawy ogólny kierunek podziału zakresu odpowiedzialności za cyberbezpieczeństwo Państwa między 3 odrębne podmioty jest nieracjonalny, komplikuje wytyczenie obszarów kompetencyjnych oraz znacząco pogarsza przepływ informacji i skuteczność zarządzania cyberbezpieczeństwem. Konsekwencją takiej koncepcji, jest konieczność wniesienia do ustawy całego rozdziału regulującego relacje i współpracę między poszczególnymi Centrami, a także przeniesienie części odpowiedzialności i czynności nadzorczych do branżowych ministrów. Z punktu widzenia podmiotów podlegających regulacjom, taka struktura powoduje dodatkowe komplikacje w postaci założonych w projekcie ustawy równoległych i niezależnych działań kontrolnych wszystkich uprawnionych podmiotów – poszczególnych Centrów oraz właściwych ministrów. Przyjęcie rozwiązania w postaci jednego centralnego podmiotu realizującego wszystkie wymagane zadania, nie tylko uprości cały system pozwalając przenieść większość szczegółowych regulacji na poziom statutu bądź regulaminu tego podmiotu. Przede wszystkim nie będzie powodować wzajemnej rywalizacji, sporów kompetencyjnych czy wręcz braku współpracy w poszczególnych obszarach regulowanej materii.	Uwaga nieuwzględniona. Sposób realizacji zadań i współpracy oraz właściwości CSIRT poziomu krajowego został określony w ustawie. Obecny model został zaproponowany przez CSIRT poziomu krajowego w ramach uzgodnień roboczych.

4.	ogólna	Rada do Spraw Cyfryzacji	Opisy incydentów powinny być akceptowane w języku polskim lub angielskim, w szczególności tam, gdzie jednostki zgłaszające korzystają z zagranicznych podmiotów zajmujących się bezpieczeństwem sieci lub zatrudniają międzynarodowe zespoły zajmujące się kwestiami cyfrowymi.	Uwaga nieuwzględniona.
5.	ogólna	Komisja Nadzoru Finansowego	Zgodnie z art. 15 ust. 1 oraz art. 24 ust. 1 Projektu operatorzy usług kluczowych oraz podmioty publiczne zostały zobowiązane do wyznaczenia osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług. Należałoby rozstrzygnąć, czy osoba ta ma zastąpić pełnomocnika ds. bezpieczeństwa cyberprzestrzeni (PBC), które to stanowisko określone jest w dokumencie Polityki ochrony cyberprzestrzeni RP wydanym przez Ministerstwo Administracji i Cyfryzacji oraz Agencję Bezpieczeństwa Wewnętrznego 25 czerwca 2013 r. (http://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html?search=16935). Zgodnie z przytoczonym dokumentem Polityki ochrony cyberprzestrzeni RP, osobie odpowiedzialnej za cyberbezpieczeństwo zostały przypisane określone zadania, natomiast Projekt nie precyzuje zakresu zadań dla osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług. Znacznie utrudnione, lub wręcz niemożliwe, będzie łączenie tych dwóch funkcji przez jedną osobę. Tym samym, ze względu na skalę niektórych organizacji, do których należy Urząd Komisji Nadzoru Finansowego, trzeba rozstrzygnąć zakres odpowiedzialności osoby wskazanej w Projekcie oraz PBC. Istotne jest, aby doprecyzowano minimalny katalog lub zakres kompetencji osoby, która może zostać wyznaczona przez operatora usługi kluczowej lub podmiot publiczny jako osoba odpowiedzialna za cyberbezpieczeństwo. Zarządzanie obszarem cyberbezpieczeństwa wymaga wiedzy eksperckiej zarówno z zakresu systemów teleinformatycznych jak i szeroko rozumianego bezpieczeństwa informacji. Trzeba zatem uzupełnić Projekt o upoważnienie ustawowe, albo doprecyzować art. 15 ust. 4 Projektu, które pozwoli ministrowi właściwemu do spraw informatyzacji w formie rozporządzenia dookreślić szczegółowo wymagane kompetencje.	Uwaga częściowo uwzględniona. Zmieniono brzmienie art. 15 pkt. 1 i art 24 ust. 2 wskazując, że będzie to osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Osoba ta ma być łącznikiem z innymi podmiotami krajowego systemu cyberbezpieczeństwa, natomiast nie będzie personalnie odpowiedzialna za realizację zadań danego podmiotu z zakresu cyberbezpieczeństwa; tym samym nie przewiduje się dla niej szczególnych wymogów.

6.	ogólna	Prokuratoria Generalna	Projektowana ustawa w kilku przepisach odwołuje się do decyzji wykonawczej Komisji Europejskiej, która jeszcze nie weszła w życie, oznaczając ją jedynie numerem, jako „nr 2017/…./UE”. Mając na względzie, że powyższy akt nie jest jeszcze częścią systemu prawnego, jak również w obliczu okoliczności, że jego projektowana treść nie jest jeszcze przesądzona, trudne staje się jednoznaczne odniesienie się do tych postanowień projektowanej ustawy, które do niego nawiązują. Niemniej jednak wydaje się, że zasadnym byłoby odwołanie się w projekcie ustawy do takiej decyzji poprzez wskazanie przepisu Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii , na podstawie którego decyzja zostanie wydana.	Uwaga nieuwzględniona. Planowane jest przyjęcie decyzji wykonawczej do dnia 19 grudnia 2017 r. Ministerstwo Cyfryzacji uczestniczy w pracach nad projektem przedmiotowego aktu prawnego.
7.	ogólna	Urząd Lotnictwa Cywilnego	Mając na uwadze powyższe ULC zwraca szczególną uwagę na rezygnację w obecnym projekcie ww. ustawy z regulacji przewidujących możliwość tworzenia sektorowych zespołów reagowania na incydenty bezpieczeństwa komputerowego, zwanych dalej „CSIRT” (Computer Security Incident Response Team), które w opinii ULC nadal znajdują uzasadnienie w przypadku podsektora lotniczego. Uzasadnienie: Branża lotnicza ulega w coraz większym stopniu procesowi cyfryzacji. Rośnie przez to liczba systemów, które mogą stać się potencjalnym celem cyberataku, a stopień skomplikowania incydentów, jak również ich zasięg z roku na rok rosną. Dodatkowo taki czynnik jak brak znajomości specyfiki danego sektora przez specjalistów z CSIRT na poziomie krajowym, może również mieć negatywny wpływ na prowadzone działania zapobiegawcze i naprawcze, a czas reakcji, w przypadku takich obszarów jak transport lotniczy, odgrywa kluczowe znaczenie. W opinii ULC rozwiązaniem wychodzącym naprzeciw nadmienionym wyzwaniom była proponowana we wcześniejszych projektach ustawy organizacja CSIRT-ów sektorowych, w których zatrudnieni specjaliści znaliby charakterystykę użytkowanych w danej branży systemów, a zbiorowa ochrona byłaby zapewniana już na wczesnym etapie. CSIRT o charakterze sektorowym jest również najefektywniejszą	Uwaga częściowo uwzględniona. Projekt zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa CSIRT jest zarezerwowana dla zespołów poziomu krajowego.

			formą współpracy, a przede wszystkim wymiany kluczowych informacji i dobrych praktyk pomiędzy samymi uczestnikami rynku. Bezzwłoczne przekazanie informacji o zdiagnozowaniu podatności, czy wystąpieniu incydentu w którymś z podmiotów, może pozwolić innym partnerom na podjęcie odpowiednich działań prewencyjnych, zapobiec rozprzestrzenieniu się zagrożenia oraz skierować zbiorowy wysiłek i wolne zasoby na rzecz „obsłużenia" incydentu u zaatakowanego partnera. W przypadku proponowanego w obecnym projekcie ustawy kształtu systemu krajowego, cześć podmiotów sektora lotniczego wchodzących w skład infrastruktury krytycznej państwa podlegałaby ochronie CSIRT GOV (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa ABW), podczas gdy część pozostawałaby pod ochroną CSIRT NASK (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy) – mogłoby to dotyczyć np. portów lotniczych. Taki kształt systemu mógłby skutkować istnieniem odrębnych ścieżek raportowania i kanałów współpracy, nawet w przypadku pomiotów o bardzo zbliżonym charakterze i rodzaju prowadzonej działalności (np. portów lotniczych). Proponowane rozwiązanie mogłoby ostatecznie doprowadzić do zwolnienia tempa obiegu informacji w podsektorze (co jak było podkreślone, może być kluczowym czynnikiem w zakresie skutecznej ochrony w lotnictwie), osłabiałoby możliwość koordynacji działań w ramach podsektora, a tym samym wywierałoby negatywny wpływ na efektywność systemu jako całości. W przypadku transportu lotniczego CSIRT sektorowy byłby również partnerem dla swoich zagranicznych odpowiedników oraz elementem budowanego pod egidą Europejskiej Agencji Bezpieczeństwa w Lotnictwie Cywilnym (EASA) europejskiego systemu cyberbezpieczeństwa w lotnictwie cywilnym. Ponadnarodowy charakter lotnictwa cywilnego jest również cechą charakterystyczną dla podsektora lotniczego, a wartościowe rozwiązania i europejski dorobek w zakresie cyberbezpieczeństwa lotnictwa cywilnego powinien być możliwie szybko implementowany	

			przez polski rynek lotniczy. CSIRT sektorowy może stanowić element łączący specjalistów z zakresie cyberbezpieczeństwa w danym sektorze z ekspertami zagranicznymi. Biorąc powyższe pod uwagę zdaniem ULC współpraca i rozwój podsystemów sektorowych przyczynia się nie tylko do podniesienia poziomu ochrony w samym sektorze, czy podsektorze (poprzez ścisłą współpracę podmiotów w danej branży – także na poziomie ponadnarodowym), ale również do zwiększenia odporności i potencjału całego krajowego systemu cyberbezpieczeństwa, bowiem daje szansę obsłużyć większą liczbę incydentów, a dodatkowo pozwala także na odpowiednie uwzględnienie specyfiki szczególnie wrażliwych obszarów.	
8.	ogólna	Biuro Bezpieczeństwa Narodowego	Projekt ustawy ma na celu wdrożenie do polskiego porządku prawnego unijnej dyrektywy NIS i zasadniczo reguluje tylko sprawy w niej poruszone. Nie można zatem stwierdzić, że ustawa kształtuje krajowy system cyberbezpieczeństwa. Reguluje ona jedynie fragment systemu cyberbezpieczeństwa. Tym samym, tytuł projektowanej ustawy nie odzwierciedla jej treści. Należałoby zatem rozważyć jego zmianę.	Uwaga nieuwzględniona. Ustawa ma szerszy zakres niż tylko implementację dyrektywy 2016/1148. Jest to implementacja minimalna, a projekt traktuje materię szerzej.
9.	ogólna	Biuro Bezpieczeństwa Narodowego	Treść projektu ustawy nie jest zgodna z zapisami Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, stanowiących załącznik do uchwały Nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. Nie reguluje bowiem spraw związanych z koordynacją systemu na poziomie ponadresortowym. Zgodnie z zapisami Krajowych Ram Polityki, do zadań organów państwowych należy „określenie zakresu odpowiedzialności podmiotu koordynującego krajowy system cyberbezpieczeństwa (...) oraz sposób oddziaływania koordynatora na uczestników systemu". Rozumiejąc powody, dla których takie przepisy nie znalazły się w projekcie ustawy, a także akceptując, iż „przyjęty w ustawie model regulacyjny zakłada poszerzenie kompetencji organów sektorowych w zakresie cyberbezpieczeństwa, zamiast ustanowienia jednego krajowego podmiotu ds. cyberbezpieczeństwa na poziomie centralnym" (jak wskazano w uzasadnieniu do projektu), proponuję jednak mieć na uwadze potrzebę odniesienia się w przyszłości do kwestii koordynacji	Uwaga uwzględniona. Projekt zostanie rozszerzony o przepisy przewidujące powołanie przy Radzie Ministrów Kolegium do spraw Cyberbezpieczeństwa w skład którego wchodzić będzie Minister Koordynator Służb Specjalnych, MON, MSWiA, MC i RCB.

			całości systemu cyberbezpieczeństwa na poziomie ponadresortowym.	
10.	ogólna	Biuro Bezpieczeństwa Narodowego	Należałoby rozważyć, czy katalog operatorów usług kluczowych (wykaz sektorów i podsektorów wymienionych w załączniku do ustawy) nie powinien pokrywać się z wykazem systemów infrastruktury krytycznej określonym w Narodowym Programie Ochrony Infrastruktury Krytycznej. Zaproponowany w załączniku do projektu ustawy wykaz sektorów i podsektorów pokrywa się wprawdzie z wykazem zawartym w załączniku do dyrektywy NIS, jednakże zgodnie z art. 3 tej dyrektywy, państwa członkowskie mogą przyjmować lub utrzymywać przepisy mające na celu osiągnięcie wyższego poziomu bezpieczeństwa sieci i systemów informatycznych (tzw. harmonizacja minimalna).	Uwaga częściowo uwzględniona. Zostaną przeredagowane przepisy w zakresie obowiązków operatorów usług kluczowych będących jednocześnie operatorami infrastruktury krytycznej, które wykluczy powielanie obowiązków wynikających z obu ustaw. W przypadku spełniania obowiązków wynikających z ustawy o zarządzaniu kryzysowym, obowiązki wynikające z projektu niniejszej ustawy będą uznane za spełnione.
11.	ogólna	Kancelaria Senatu RP	Projekt wymaga poprawek usuwających błędy techniczno-legislacyjne, np.: a) skrót „usługa kluczowa" występuje przed przepisem, który wprowadza ten skrót (art. 5 ust. 2 pkt 1), b) przepis art. 5 ust. 4 zdanie drugie jest powtórzeniem treści art. 61 § 1 K.p.a., c) zwroty, które nie zostały zdefiniowane (np. „wczesne ostrzeżenia", „dynamiczna analiza"), d) określenia potoczne (np. „ćwiczenia uruchamiane"), e) przepisy powtarzające normy zawarte w innych przepisach ustawy (np. art. 3 ust. 2 i art. 36 ust. 5), f) odesłania do „odrębnych przepisów" (np. art. 43 ust. 1), g) podkreślanie, ze organ kolegialny wyraża swoje stanowisko w formie uchwały (np. art. 56 ust. 1), h) ustawa posługuje się niestanowczymi wyrażeniami (np. „powinien"), i) używanie wyrażeń w znaczeniu innym niż nadaje im ustawa podstawowa dla danej dziedziny spraw (np. wyraz „otrzymać" w Kodeksie postpowania administracyjnego jest używany tylko w przypadku otrzymania pisma przez organ, natomiast w stosunku do stron postpowania Kodeks posługuje się wyrazem „doręczać").	Uwagi częściowo uwzględnione.
12.	ogólna	Narodowy Bank Polski	Narodowy Bank Polski nie jest i nie może zostać uznany za operatora usługi kluczowej w rozumieniu przepisów dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (zwaną dalej w treści dyrektywą) jak i przepisów niniejszego	Wyjaśnienie. NBP nie będzie operatorem usługi kluczowej, co nie oznacza jednak, że nie powinien być objęty obowiązkiem zgłaszania incydentów podobnie jak inne podmioty publiczne.

			projektu ustawy o krajowym systemie cyberbezpieczeństwa. Przyjęcie tej konstrukcji w ramach prac nad projektem ustawy jest o tyle istotne, że zgodnie z art. 227 Konstytucji RP, centralnym bankiem państwa jest Narodowy Bank Polski o określonej roli i zadaniach ustawowych, nad którymi nie jest sprawowany merytoryczny nadzór. Co więcej, zadania te nie są możliwe do przypisania do żadnego z sektorów wskazanych w załączniku projektu ustawy, tudzież w załączniku do dyrektywy. Udział NBP w krajowym systemie cyberbezpieczeństwa powinien zatem odbywać się – uwzględniając odpowiednie postanowienia rozdziału 4 projektu ustawy - na zasadach równorzędnej i swobodnie kreowanej współpracy z pozostałymi podmiotami zaliczanymi do tego systemu, co zdecydowanie zwiększa efektywność i elastyczność działania na rzecz podnoszenia poziomu cyberbezpieczeństwa Rzeczypospolitej Polskiej. Wprowadzanie odmiennej roli i zadań NBP w ramach krajowego systemu cyberbezpieczeństwa może skutkować naruszeniem ustawowej zasady niezależności centralnego banku państwa. Powyższe stanowisko wydaje się być spójne także z samym projektem ustawy, zwłaszcza z rozdziałem 8, w którym wskazano zakres podmiotowy nad którym sprawowany jest nadzór, do którego zaliczono podmioty świadczące usługi z zakresu cyberbezpieczeństwa (art. 47 ust. 1 pkt 1 projektu), operatorów usług kluczowych (art. 47 ust. 2 pkt 2 lit. a projektu) i dostawców usług cyfrowych (art. 47 ust. 2 pkt 2 lit. b projektu). Kwestia ta będzie podnoszona także w poniższych uwagach szczegółowych.	
13.	ogólna	Najwyższa Izba Kontroli	Przedstawiony do konsultacji projekt pozwala na wdrożenie do polskiego porządku prawnego Dyrektywy Parlamentu Europejskiego i Rady (UE) z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (tzw. Dyrektywa NIS). Szczegółowa analiza projektu oraz doświadczenia z kontroli NIK wskazują jednak, ze istnieje istotne ryzyko, ze proponowane w ww. regulacji rozwiązania będą mało skuteczne i tylko w ograniczonym stopniu mogą wpływać na poprawę poziomu bezpieczeństwa polskiej cyberprzestrzeni. Wbrew deklaracjom autorów projektu, którzy podkreślają	Wyjaśnienie. Projekt ustawy wprowadza rozwiązania systemowe w zakresie zapewnienia cyberbezpieczeństwa i włącza różnych interesariuszy (służby, sektor prywatny, infrastrukturę krytyczną, administrację publiczną) w krajowy system cyberbezpieczeństwa.

			znaczenie i dynamikę zagrożeń w cyberprzestrzeni, przedłożona do konsultacji regulacja nie kreuje w praktyce nowych, kompleksowych rozwiązań, a tylko przenosi na grunt prawny funkcjonujące już struktury (np. zespoły CSIRT) oraz „zapożycza" rozwiązania z zakresu zarządzania kryzysowego, które w świetle kontroli NIK należy uznać za nieskuteczne (np. identyfikacja operatorów usług kluczowych przez poszczególnych ministrów). Brak usystematyzowanego i kompleksowego podejścia do kwestii cyberbezpieczeństwa może skutkować kolizją proponowanej regulacji z obowiązującymi już w tym obszarze aktami prawnymi, takimi jak ustawa z dnia 26 kwietnia 2007 r, o zarzadzaniu kryzysowym, czy ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, które określają konkretne obowiązki i uprawnienia wielu istotnych podmiotów w tym obszarze (operatorzy infrastruktury krytycznej, organy administracji publicznej zarządzające istotnymi z punktu widzenia ciągłości funkcjonowania państwa systemami teleinformatycznymi, Szef ABW).	
14.	ogólna	Najwyższa Izba Kontroli	Rozproszony charakter krajowego systemu cyberbezpieczeństwa. Ustalenia wcześniejszych kontroli NIK wskazują, że poszczególni ministrowie, którym przypisano zadania organów właściwych do spraw cyberbezpieczeństwa (nawet po otrzymaniu niewielkiego wzmocnienia etatowego, o którym mowa w ocenie skutków regulacji) nie będą posiadać adekwatnych kompetencji i zasobów do realizacji przypisanych im obowiązków dot., m.in. identyfikacji operatorów usług kluczowych, nadzoru i kontroli nad tymi podmiotami, rekomendowania im działań wzmacniających bezpieczeństwo, czy tez udziału w ćwiczeniach. Bardziej efektywnym rozwiązaniem byłoby, zdaniem NIK, wyznaczenie jednego krajowego organu właściwego ds. cyberbezpieczeństwa, wyposażonego w adekwatne zasoby do realizacji tych specjalistycznych zadań. Podobna uwaga dotyczy wskazanej w ustawie struktury krajowych zespołów CSIRT, która nie przewiduje powołania narodowego zespołu CSIRT koordynującego działania innych podmiotów w zakresie obsługi incydentów. Podział zadań między poszczególne zespoły CSIRT wymienione w projekcie ustawy jest niejasny i dodatkowo koliduje on z zadaniami Zespołu CSIRT w ABW ustanowionymi na podstawie ustawy z dnia 10	Wyjaśnienie. W celu stworzenia systemowych rozwiązań, sposób realizacji zadań i współpracy oraz właściwości CSIRT poziomu krajowego został określony w ustawie. Obecny model został zaproponowany przez CSIRT poziomu krajowego w ramach uzgodnień roboczych.

			czerwca 2016 r. o działaniach antyterrorystycznych (wątpliwe jest czy w momencie zaistnienia incydentu możliwe będzie szybkie rozstrzygniecie, czy ma on charakter zdarzenia terrorystycznego). Wprawdzie koordynacja działań poszczególnych zespołów CSIRT została przypisana obsługiwanemu przez RCB Zespołowi do spraw Incydentów Krytycznych, to jednak, jak wskazują wyniki kontroli NIK, istnieje wysokie ryzyko, ze podmiot ten nie będzie w stanie realizować przypisanego mu zadania szybko i efektywnie (m.in. w kontekście powierzania RCB kolejnych zadań bez wzmocnienia kadrowego urzędu podlegającego Dyrektorowi RCB);	
15.	ogólna	Najwyższa Izba Kontroli	Tworzenie wskazu operatorów usług kluczowych równolegle do istniejącego już wykazu infrastruktury krytycznej oraz powielanie rozwiązań z ustawy o zarzadzaniu kryzysowym służącym identyfikacji operatorów usług kluczowych. Zdaniem NIK nie jest zasadne powielanie „reżimów ochronnych" ustanowionych przez ustawę o zarzadzaniu kryzysowym oraz ustawę o krajowym systemie cyberbezpieczeństwa, które to regulacje w znacznym stopniu będą dotyczyć tych samych obiektów i operatorów (większość obiektów IK ma istotne komponenty teleinformatyczne). NIK wielokrotnie podkreślała, że warunkiem skutecznego planowania działań w zakresie ochrony cyberprzestrzeni jest pełna inwentaryzacja komponentów teleinformatycznych infrastruktury krytycznej państwa. W tym kontekście postulowano modyfikację istniejących kryteriów identyfikacji infrastruktury krytycznej oraz wskazywano na zasadność zmiany nieefektywnego modelu identyfikacji tej infrastruktury, która jest prowadzona przez ministrów i kierowników urzędów centralnych. Zaproponowano przypisanie tych zadań wyspecjalizowanemu organowi, który posługując się obiektywnymi kryteriami i właściwą metodyką będzie aktywnie zbierał z wielu źródeł i weryfikował informacje pozwalające na identyfikacji infrastruktury kluczowej dla funkcjonowania państwa;	Uwaga częściowo uwzględniona. Zostaną przeredagowane przepisy w zakresie obowiązków operatorów usług kluczowych będących jednocześnie operatorami infrastruktury krytycznej, które wykluczy powielanie obowiązków wynikających z obu ustaw. W przypadku spełniania obowiązków wynikających z ustawy o zarządzaniu kryzysowym, obowiązki wynikające z projektu niniejszej ustawy będą uznane za spełnione.
16.	ogólna	Najwyższa Izba Kontroli	Nieuzasadnione ograniczenie obowiązków przypisanych podmiotom publicznym w zakresie ochrony ich własnych systemów teleinformatyczny w porównaniu do podmiotów komercyjnych;	Wyjaśnienie. Podmioty publiczne są zobowiązane jedynie do zgłaszania incydentów. Inne obowiązki w zakresie zapewnienia bezpieczeństwa systemów

				teleinformatycznych dla organów administracji rządowej nałożone są przez ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne. Nierealizowanie tych obowiązków może spowodować odpowiedzialność kierownika jednostki, co wydaje się wystarczające.
17.	ogólna	Najwyższa Izba Kontroli	Brak rzetelnego oszacowania zasobów niezbędnych w celu budowy efektywnego krajowego systemu cyberbezpieczeństwa i ustanowienia przejrzystego systemu finansowania tych zadań - wyniki kontroli NIK pozwalają stwierdzić, ze przewidziana w ocenie skutków regulacji kwota wydatków 236,96 min zł na sfinansowanie budowy i utrzymania krajowego systemu cyberbezpieczeństwa w okresie kolejnych 10 lat jest zdecydowanie nieadekwatna. Powyższe wynika m.in. z faktu, ze wynagrodzenia informatyków w sferze komercyjnej znacznie przewyższają stawki pracowników sfery budżetowej, co może uniemożliwić zatrudnienie odpowiedniej liczby specjalistów posiadających kwalifikacje w obszarze ochrony cyberprzestrzeni;	Wyjaśnienie. Środki niezbędne na realizację zadań wynikających z ustawy zostały oszacowane w sposób adekwatny. Należy zauważyć, że podmioty będące operatorami usług kluczowych w przeważającej większości z uwagi na ochronę świadczonych usług już mają wdrożone systemy bezpieczeństwa, a podmioty publiczne są zobowiązane je posiadać zgodnie z przepisami wykonawczymi wydanymi na podstawie ustawy o informatyzacji podmiotów realizujących zadania publiczne.
18.	ogólna	Najwyższa Izba Kontroli	Brak uwzględnienia w projekcie ustawy obecnej i deklarowanej przez Kierownictwo MON aktywności resortu w zakresie ochrony cyberprzestrzeni.	Wyjaśnienie. Rozwiązania w tym zakresie mogą być wprowadzone po przekazaniu propozycji przez MON.
Uwaga szczegółowe				
19.	art. 2	Rada do Spraw Cyfryzacji	1. Brak definicji Incydent Bezpieczeństwa Komputerowego - w ramach którego rozróżnione zostaną systemy IT od systemów OT (technologicznych); 2. Brak definicji systemu IT i OT /Brak jasnego zdefiniowania zakresu cyberbezpieczeństwa, który zmienia się ze względu na implementację rozporządzenia NIS w tym dokumencie, powoduje, że podmioty będące adresatem tej ustawy nie będą w 100% pewne zakresu ochrony usług i procesów, szczególnie, że definiuje się systemy informatyczne, które inaczej są nazywane w świecie IT a inaczej w świecie sieci technologicznych. Przykładem może tu być branża energetyczna, gdzie w przypadku systemów i sieci technologicznych mówi się o „łączności" i „systemach SCADA. Należy pamiętać, że będzie to	Wyjaśnienie. Definicja systemu teleinformatycznego obejmuje zarówno systemy IT jak i systemy OT – nie ma konieczności rozróżniania tych dwóch definicji. Warto zaznaczyć, że w automatyce przemysłowej mówi się jeszcze o wielu innych kwestiach, a nie tylko o łączności. IACS to nie tylko SCADA, ale też PLC, przetworniki wielkości nieelektrycznych na elektryczne, serwomechanizmy, transmisja danych w specjalizowanych sieciach (np. RS 422/485, CANBus, ARING 429, mil-std-1553b, a także Ethernet).

			pierwsze poważne zderzenie świata z unormowanymi i ustandaryzowanymi protokołami ze światem, gdzie prawie każdy z liczących się producentów automatyki i systemów do sterowania sieciami technologicznymi „stworzył" swój własny protokół transmisyjny/	
20.	art. 2	Prokuratoria Generalna	Projektowana ustawa posługuje się wielokrotnie pojęciem usługi krytycznej podczas, gdy w art. 2, regulującym znaczenie określeń użytych w ustawie, brak jest definicji tego pojęcia. Prokuratoria Generalna dostrzega przy tym, że definicja usługi kluczowej zawarta została w art. 5 ust. 2 pkt 1 projektu ustawy, co jednak wydaje się niewystarczające zważywszy na fakt, że termin ten jest w projekcie ustawy wielokrotnie używany w artykułach poprzedzających art. 5, w którym go zdefiniowano. Tym samym zasadne jest rozważanie zamieszczenia definicji tego pojęcia w art. 2 projektowanej ustawy.	Uwaga uwzględniona. Termin „usługa kluczowa" zostanie zdefiniowany w słowniczku do ustawy po uzgodnieniu z RCL.
21.	art. 2	Prokuratoria Generalna	Odnośnie do wyodrębnionych i zdefiniowanych w projektowanej ustawie czterech rodzajów incydentów powstaje pytanie o to jak w świetle tych definicji rozumieć termin „incydentu mającego istotny skutek zakłócający dla świadczenia usługi kluczowej", o którym stanowi art. 5 ust. 2 pkt 3 projektowanie ustawy. Wydaje się, że zasadnym byłoby opisanie tego rodzaju incydentu przy wykorzystaniu występujących w projekcie ustawy kategorii incydentów zdefiniowanych w jej słowniczku, w szczególności powstaje pytanie o stosunek tego pojęcia do terminu „incydent istotny" ujętego w art. 2 pkt 12 projektu ustawy.	Uwaga częściowo uwzględniona. Art. 5 określa sposób identyfikacji operatorów usług kluczowych, w którym jednym z warunków uznania za operatora jest sytuacja, w której incydent miałby istotny skutek zakłócający dla świadczenia usługi przez tego operatora. Nie jest to kategoria incydentu – zostały one zdefiniowane w art. 2. W celu większej przejrzystości, definicje incydentów zostaną częściowo przeredagowane.
22.	art. 2 pkt 1-4 [w piśmie z uwagami określony błędnie jako art 1 ust. 1	Rada do Spraw Cyfryzacji	Niezrozumiałe jest zachowanie skrótów od nazwy angielskiej CSIRT (Computer Security Incident Response Team); czy nie jest to w kolizji z ustawą o języku polskim z dnia 7 października 1999 r.?	Wyjaśnienie. Niniejszy przepis nie narusza ustawy o języku polskim z dnia 7 października 1999 r. Wyraz CSIRT został zdefiniowany w projekcie.

	pkt 1-4]			
23.	art. 2 pkt 5	Centralne Biuro Antykorupcyjne	W art. 2 proponujemy dostosować definicję do już funkcjonujących w dyrektywie NIS lub normach związanych z bezpieczeństwem teleinformatycznym (szczególnie normy z rodziny ISO/IEC 27000), poprzez nadanie następujących brzmień: pkt 5: cyberbezpieczeństwo – działania realizowane w celu osiągnięcia lub utrzymania zakładanej odporności systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informatyczne;	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy.
24.	art. 2 pkt 5	Służba Kontrwywiadu Wojskowego	W słowniku pojęć sugerujemy doprecyzowanie pojęcia: cyberbezpieczeństwo – termin ten wykracza poza systemy teleinformatyczne, problem wymaga systemowego podejścia do istniejących pojęć np. bezpieczeństwo teleinformatyczne i nowych pojęć z przedrostkiem cyber, np. cyberobrona, cyberatak ale również bezpieczeństwo cyberprzestrzeni - obrona/atak w cyberprzestrzeni.	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy.
25.	art. 2 pkt 5	Rada do Spraw Cyfryzacji	„Dany poziom zaufania” - w ustawie nie definiuje się co oznacza dany poziom zaufania. Nie ma też odniesienia do definicji, która byłaby w innych dokumentach. Brak takiego zapisu może nie być istotną przeszkodą w działaniu ustawy, ale pozwala na różną interpretacją czy dane procesy wymagają dbałości w obszarze cyberbezpieczeństwa, czy też nie. Elastyczność w określaniu „danego poziomu zaufania”, może być wykorzystane do bagatelizowania kwestii zaistniałych incydentów poprzez np. nieklasyfikowanie zdarzenia do incydentu zwykłego (Art. 2.11) a przez to innych incydentów.	Wyjaśnienie. Zgodnie z definicją, cyberbezpieczeństwo jest stanem systemów informacyjnych, jednak nie jest to stan dowolny, a taki który oznacza „odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne”. W związku z tym przepis jest jednoznaczny.
26.	art. 2 pkt 5	Ubezpieczeniowy Fundusz Gwarancyjny	Ustawodawca stosuje termin Cyberbezpieczeństwo, natomiast Dyrektywa NIS stosuje termin Bezpieczeństwo/Bezpieczeństwo Sieci i Systemów Informacyjnych (w Dyrektywie NIS występuje tylko raz hasło cybersecurity). Termin bezpieczeństwo ma szersze	Wyjaśnienie. Użyty w projekcie termin „systemy informacyjne” zawiera w sobie zarówno część infrastrukturalną

			znaczenie niż cyberbezpieczeństwo i obejmuje również zapobieganie incydentom nie związanych bezpośrednio z cyberbezpieczeństwem np. Awaria infrastruktury IT, brak zasilania skutkujących brakiem dostępności usługi kluczowej etc. Ograniczenie się do sformułowania Cyberbezpieczeństwo może wprowadzić mylne przekonanie, że raportowaniu podlegają tylko określone Incydenty (poważne) związane z zagrożeniami cybernetycznymi.	(elementem systemu teleinformatycznego jest również sieć) wraz z przetwarzanymi w nich danymi w postaci elektronicznej. Jest to podejście szersze (obejmujące również dane), zatem definicja z art. 2 pkt 5 nie dotyczy wyłącznie kwestii sieci teleinformatycznych. Konieczność zapewnienia cyberbezpieczeństwa dotyczy ww. systemów informacyjnych i ich atrybutów (triada CIA – Confidentiality, Integrity, Availability). Ustawa nie reguluje tylko kwestii bezpieczeństwa teleinformatycznego, ale też m.in. ciągłości działania.
27.	art. 2 pkt 8	Centralne Biuro Antykorupcyjne	W art. 2 proponujemy dostosować definicję do już funkcjonujących w dyrektywie NIS lub normach związanych z bezpieczeństwem teleinformatycznym (szczególnie normy z rodziny ISO/IEC 27000), poprzez nadanie następujących brzmień: pkt 8: incydent – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, które wpływają na określony stan systemu informatycznego, usługi lub sieci, wskazując na możliwe naruszenie obowiązujących przepisów, błąd zabezpieczeń lub nieznaną dotychczas sytuację, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrożenia cyberbezpieczeństwa; jako alternatywę, zastosować można uproszczoną definicję wprost z dyrektywy NIS: incydent – każde zdarzenie, które ma rzeczywisty niekorzystny skutek dla bezpieczeństwa sieci i systemów informatycznych;	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy. Jeśli chodzi o definicję incydentu, jest ona celowo szersza niż w dyrektywie 2016/1148, gdyż obejmuje również możliwy, a nie tylko rzeczywisty, skutek.
28.	art. 2 pkt 8	Ubezpieczeniowy Fundusz Gwarancyjny	Ustawodawca wprowadza inną definicje Incydentu w odniesieniu do dyrektywy NIS. Sugeruje się aby wszystkie definicje (tam gdzie jest to zasadne) a w szczególności dotyczące "Incydentu" były zbieżne z definicjami użytymi przez twórców Dyrektywy NIS.	Wyjaśnienie. Dyrektywa 2016/1148 wymaga harmonizacji minimalnej – projekt ustawy reguluje kwestie szerzej, a nie ściśle z dyrektywą.
29.	art. 2 pkt 8-12	Krajowa Rada Radiofonii i Telewizji	definicje pojęcia incydent wskazane w projektowanym art. 2 pkt 8-12 nie są precyzyjne, a w treści projektu ustawy używa się tego pojęcia w sposób niekonsekwentny ;	Wyjaśnienie. Definicje incydentów zostaną przeredagowane dla większej przejrzystości.

30.	art. 2 pkt 8-12	Rada do Spraw Cyfryzacji	W przedstawionym projekcie występuje niejaki „mętlik" definicyjny, który może poważnie rzutować na stosowanie tej ustawy w praktyce. Chodzi o definicję zasadniczego pojęcia, jakim jest „incydent". Z podanych w art. 2. definicji wynika, że: 1. Pojęcie to obejmuje różne kategorie incydentów: Krytyczny Poważny Istotny Zwykły 2. Mają miejsce następujące relacje: K jest zawarte w P K jest zawarte w I K jest zawarte w Z 3. Dalej: P jest zawarte w Z 4. Natomiast Z jest definiowane jako dowolne zdarzenie o niekorzystnym wpływie na cyberbezpieczeństwo. 5. Dodatkowo I jest definiowane przez odniesienie do dokumentu zawierającego odnośną decyzję Komisji Europejskiej. Przy tak sformułowanych definicjach można postawić szereg pytań, na które nie ma jednoznacznej odpowiedzi, np.: Czy incydent typu I jest również incydentem typu Z? Czy incydent typu P jest również incydentem typu I? Czy Ustawa celowo dopuszcza możliwość, że incydent istotny (typu I) może nie być ani Zwykły, ani Poważny, ani Krytyczny? Taki stan definicyjny może przysporzyć wielu kłopotów, np. w zakresie ustalania, kto jest za co odpowiedzialny i czego dotyczą przepisy szczegółowe tej ustawy. „Incydent krytyczny, poważny, istotny albo zwykły"– definicje incydentów są nieprecyzyjne co może skutkować trudnościami w klasyfikacji przez podmioty podlegające ustawie, w szczególności przedsiębiorców. Niektóre z parametrów służących do zdefiniowania kategorii incydentu są niemierzalne lub też mierzalne dopiero po zdarzeniu w sposób statystyczny np. „zaufanie do instytucji publicznych". Podmiot komercyjny będzie mieć problem z klasyfikacją zdarzenia. Wydaje się że w takiej formie dopiero po zakończeniu trwania incydentu będzie możliwe	Uwaga częściowo uwzględniona. Definicje incydentów zostaną przeredagowane dla większej przejrzystości.

			w sposób jednoznaczny (ale być może negocjacyjny) określenie jego przyporządkowania. Zbyt szeroka jest definicja „incydentu zwykłego” - przykładowo: każde wydarzenie prowadzące do ujawnienia informacji związanych z systemem informatycznym lub hierarchią władzy w jednostce może mieć niekorzystny wpływ na cyberbezpieczeństwo.	
31.	art. 2 pkt 8-12	Narodowy Bank Polski	Ze względu na brzmienie definicji znajdujących się w art. 2 pkt 8 – 12 projektu, pod rozwagę projektodawcy przedkładamy wprowadzenie jednolitej definicji incydentu (podobnie jak to jest w dyrektywie), jak również dookreślenie, że incydenty odnoszą się do incydentów cyberbezpieczeństwa. Dodatkowo, przedmiotowa definicja powinna wskazywać kryteria klasyfikacji zdarzenia do konkretnego typu incydentu. Zasadnym wydaje się również ujednolicenie przepisów dotyczących poszczególnych incydentów wskazanych w projektowanej ustawie, bądź też ewentualne bardziej precyzyjne podkreślenie różnic w przedmiocie ich stosowania. W przypadku zwiększenia przejrzystości w klasyfikacji incydentów, poddajemy pod rozwagę, aby uspójnić zasady ich zgłaszania na podstawie projektu ustawy. Wskazać chociażby należy, że w art. 12 projektu wprowadzony został obowiązek zgłaszania incydentu poważnego w określonym przedziale czasu, podczas, gdy brak jest zasad procedowania w przypadku incydentu krytycznego, który – ze względu na skutki – jest niezwykle istotny i zasady jego obsługi powinny być określone w sposób zrozumiały.	Uwaga częściowo uwzględniona. Definicje incydentów zostaną przeredagowane dla większej przejrzystości.
32.	art. 2 pkt 9	Kancelaria Sejmu RP	W art. 2 w pkt 9 w definicji pojęcia „incydent krytyczny” użyto nieostrego sformułowania: „skutkujący znaczną szkodą dla (…) zaufania do instytucji publicznych”. Oznacza to możliwość, nieprzewidzianą przez projektodawców w uzasadnieniu i Ocenie Skutków Regulacji, objęcia przepisami projektowanej ustawy w zakresie takich instytucji prawnych jak „usługa kluczowa” czy „operator usługi kluczowej” – Sejmu lub Kancelarii Sejmu.	Wyjaśnienie. Ani Sejm ani Kancelaria Sejmu nie będą operatorami usług kluczowych.

33.	art. 2 pkt 9	Kancelaria Sejmu RP	W art. 2 w pkt 9 znajduje się użyte pojęcie „instytucji publicznej". Należy zwrócić uwagę, iż sposób posługiwania się terminologią dotyczącą szeroko pojętej administracji publicznej jest niezgodny z § 10 załącznika do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad Techniki Prawodawczej" (Dz. U. 2016 r. poz. 283- zwanego dalej „Zasadami Techniki Prawodawczej"), tzn. używane są zamiennie różne pojęcia na określenie tego samego zakresu znaczeniowego w różnych przepisach, np.: „podmiot publiczny" w art. 2 pkt 10, „organy publiczne oraz organy je obsługujące" w art. 4 pkt 6, „jednostki podległe i nadzorowane przez organy administracji rządowej" w art. 4 pkt 11. Przypomnieć wypada, że w ustawie należy posługiwać się określeniami, które zostały użyte w ustawie podstawowej dla danej dziedziny spraw, w szczególności w ustawie określanej jako „kodeks" lub „prawo". W tym kontekście należałoby się odnieść do definicji „organów administracji publicznej" zawartej w art. 5 ustawy z dnia 14.06.1960 r. Kodeks postępowania administracyjnego (Dz.U. z 2017 r. poz. 1257), bądź też do „organów władzy publicznej", o których mowa w art. 7 Konstytucji Rzeczpospolitej Polskiej.	Uwaga częściowo uwzględniona.
34.	art. 2 pkt 9	Prokuratoria Generalna	Definicja pojęcia incydentu krytycznego ujęta w art. 2 pkt 9 projektu ustawy jest w dużym stopniu zbieżna z pojęciem incydentu poważnego, zawartym w rozdziale 11 pkt 7 uchwały Rady Ministrów nr 52/2017 z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022. Jednocześnie projekt ustawy zawiera własną definicję pojęcia incydentu poważnego odmienną od znaczenia, jakie nadały temu pojęciu Krajowe Ramy Polityki Cyberbezpieczeństwa. W tym kontekście wątpliwości budzi celowość występujących rozbieżności terminologicznych. Racjonalnym wydaje się ujednolicenie definicji poszczególnych kategorii incydentów występujących w Krajowych Ramach Polityki Cyberbezpieczeństwa oraz w projektowanej ustawie.	Wyjaśnienie. Definicje zawarte w ustawie są stworzone na potrzeby funkcjonowania krajowego systemu cyberbezpieczeństwa. Będą one obowiązywały podmioty stosujące ustawę.
35.	art. 2 pkt 10 i 12	Służba Kontrwywiadu Wojskowego	W słowniku pojęć sugerujemy doprecyzowanie pojęcia: kategorie incydentów – w projekcie ustawy incydent poważny pokrywa się w swej definicji z incydentem istotnym. Dodatkowo w art. 29 projektowanej ustawy jest mowa o incydencie związanym	Uwaga częściowo uwzględniona. Definicje incydentów zostaną przeredagowane.

			ze zdarzeniami o charakterze terrorystycznym, dla którego definicja nie istnieje. Proponuje się ograniczenie do trzech kategorii incydentów. Zwykłego, nieobsługiwanego na poziomie krajowym. Niezwykłego, obligatoryjnie zgłaszanego na poziom krajowy oraz ciężkiego, który ma znaczenie dla całego kraju (obsługiwanego na poziomie krajowym).	
36.	art. 2 pkt 12	Ubezpieczeniowy Fundusz Gwarancyjny	Ustawodawca wprowadza termin : Incydent istotny dla Dostawców usług cyfrowych . Dyrektywa NIS nie wprowadza takiego terminu i ogranicza się jedynie do "Poważny Incydent". W chwili obecnej mamy sformułowanie Incydent poważny w odniesieniu do podmiotów świadczących usługę kluczową oraz Incydent istotny odnoszący się do Dostawców usługi cyfrowej.	Uwaga częściowo uwzględniona. Projekt ustawy implementuje dyrektywę 2016/1148, dostosowując ją do warunków polskich i nie musi przenosić literalnie definicji z dyrektywy. Dla przejrzystości, definicje incydentów zostaną przeredagowane. Incydent istotny jest zdefiniowany zgodnie z art. 16 dyrektywy.
37.	art. 2 pkt 13	Prokuratoria Generalna	Prokuratoria Generalna dostrzega, że definiując pojęcie internetowej platformy handlowej w art. 2 pkt 13 projektu ustawy posłużono się terminem „usługa” podczas, gdy Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii definiująca to samo pojęcie w jej art. 4 pkt 17 wskazuje wyraźnie, że jest to usługa cyfrowa. Jakkolwiek w dalszej części definicji internetowej platformy handlowej zaznaczono, że usługa ta umożliwia zawieranie umów drogą elektroniczną to wydaje się, że koniecznym jest doprecyzowanie, że sama usługa, nie tylko zawierane za jej pomocą umowy, jest świadczona drogą elektroniczną, tj. jest usługą cyfrową.	Wyjaśnienie. Tą wątpliwość rozstrzyga zawarta w projekcie ustawy definicja usługi cyfrowej.
38.	art. 2 pkt 14	Służba Kontrwywiadu Wojskowego	W słowniku pojęć sugerujemy doprecyzowanie pojęcia: obsługa incydentu – zaproponowana definicja nie wyczerpuje pojęcia „obsługi incydentu” (m.in. wyszukiwanie powiązań, usuwanie przyczyn, rejestrację). Ponadto lepszym pojęciem wydaje się być „zarządzanie incydentem”.	Wyjaśnienie. Projekt ustawy celowo reguluje tylko obsługę incydentu jako niezbędne dla bezpieczeństwa minimum podjętych działań związanych z incydentem. Zarządzanie incydentem jest terminem szerszym i nie ma konieczności jego definiowania na potrzeby niniejszego projektu.

39.	art. 2 pkt 16	Centralne Biuro Antykorupcyjne	W art. 2 proponujemy dostosować definicję do już funkcjonujących w dyrektywie NIS lub normach związanych z bezpieczeństwem teleinformatycznym (szczególnie normy z rodziny ISO/IEC 27000), poprzez nadanie następujących brzmień: pkt 16 ryzyko – wielkość charakteryzująca prawdopodobieństwo oraz skutek wystąpienia incydentu w systemie informatycznym lub mającego wpływ na system informatyczny, w szczególności służący do świadczenia usług kluczowych lub usług cyfrowych;	Uwaga nieuwzględniona. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy.
40.	art. 2 pkt 16	Narodowy Bank Polski	Proponujemy także rozważenie doprecyzowania określenia „wielkość charakteryzująca prawdopodobieństwo" zawartego w art. 2 pkt 16 projektu lub ewentualnie zastąpienie innym, które w sposób bardziej przystępny określi, jak należy rozumieć ryzyko na gruncie projektu tejże ustawy.	Wyjaśnienie. „Wielkość charakteryzująca prawdopodobieństwo" jest poprawnym terminem, albowiem w szacowaniu ryzyka zwykle nie posługujemy się prawdopodobieństwem w sensie jakim nadaje mu matematyczna teoria prawdopodobieństwa.
41.	art. 2 pkt 18-19	Centralne Biuro Antykorupcyjne	Proponujemy usunięcie podziału na system informacyjny i teleinformatyczny (pkt 18 i 19) i wprowadzenie określenia: system informatyczny – system, o którym mowa w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570) wraz z przetwarzanymi w nim danymi w postaci elektronicznej; pojęcie system informacyjny jest znacznie bliższe dziedzinom związanym z zarządzaniem – ponadto w dyrektywie NIS używane jest pojęcie „sieć i system informatyczny";	Wyjaśnienie. „Sieć i system informatyczny" to nic innego jak „system teleinformatyczny". „System informacyjny" natomiast jest pojęciem szerszym – obejmuje również dane w nim. W cyberbezpieczeństwie chodzi o ochronę informacji, ochrona systemu TI jest tylko środkiem do takiej ochrony.
42.	art. 2 pkt 20	Kancelaria Sejmu RP	W art. 2 w pkt 20 stanowiącym definicję „usługi przetwarzanej w chmurze" użyto, niezgodnie z § 8 ust. 2 pkt 1 Zasad Techniki Prawodawczej niezrozumiałego powszechnie pojęcia specjalistycznego: „skalowalnego (…) zbioru zasobów obliczeniowych".	Wyjaśnienie. Posłużono się definicją z dyrektywy 2016/1148.
43.	art. 2 pkt 22	Rada do Spraw Cyfryzacji	RdC sugeruje uproszczenie definicji wyszukiwarki internetowej przez zastąpienie określenia „wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie" określeniem „wyszukiwanie publicznie dostępnych stron internetowych"	Wyjaśnienie. Posłużono się definicją z dyrektywy 2016/1148. Proponowana definicja uwzględniałaby strony opatrzone robots.txt, czego uniknięto stosując definicję z dyrektywy.

44.	art. 3 ust. 1	Kancelaria Sejmu RP	W art. 3 w ust. 1 wydaje się, iż w celu zwiększenia przejrzystości przepisów, wyrazy „w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi Incydentów" należałoby przenieść do definicji „cyberbezpieczeństwa" zawartej w art. 2 pkt 5.	Wyjaśnienie. Projekt ustawy obejmuje nie tylko cyberbezpieczeństwo, ale i ciągłość działania.
45.	art. 3 ust. 1	Narodowy Bank Polski	W art. 3 ust. 1 projektu zawarto nieprecyzyjne określenie „odpowiedniego poziomu bezpieczeństwa". Proponujemy rozważyć jego doprecyzowanie bądź zastąpienie innym, zgodnym z intencją projektodawcy. Pod rozwagę pozostawiamy kwestię, czy nie należy wprowadzić precyzyjnej gradacji poziomów bezpieczeństwa. Podobnie proponujemy doprecyzować zwrot „określonym zakresie", zawarty w art. 3 ust. 2 projektu. Biorąc pod uwagę, że przepis dotyczy przekazywania informacji do publicznej wiadomości, to jednoznaczne jego brzmienie wydaje się być zasadne.	Uwaga częściowo uwzględniona. W art. 3 ust. 1 przedstawiono cele i założenia krajowego systemu cyberbezpieczeństwa. Tym samym nie ma powodu wprowadzać gradacji poziomów bezpieczeństwa. Natomiast w art. 3 ust. 2 wprowadzono ten zwrot świadomie, aby informacje nie były przekazywane w pełnym zakresie. Zostanie on doprecyzowany poprzez uściślenie, że będzie to „niezbędny zakres".
46.	art. 3 ust. 2	Kancelaria Sejmu RP	W art. 3 w ust. 2 należałoby rozważyć doprecyzowanie niejasnego zwrotu „w określonym zakresie" użytego w celu opisania sytuacji przekazywania niepełnej informacji o incydentach, podatności na nie, o zagrożeniach cyberbezpieczeństwa, oraz o poziomie ryzyka występowania incydentów. Doprecyzowanie powinno nastąpić także w zakresie określenia podmiotu decydującego o zakresie przekazywanych informacji.	Uwaga częściowo uwzględniona. W art. 3 ust. 2 wprowadzono ten zwrot świadomie, aby informacje nie były przekazywane w pełnym zakresie. Zostanie on doprecyzowany poprzez uściślenie, że będzie to „niezbędny zakres".
47.	art. 3 ust. 2	Centralne Biuro Antykorupcyjne	W art. 3 ust. 2 proponujemy nadać brzmienie: „2. Informacje o podatnościach, zagrożeniach oraz o ryzykach wystąpienia incydentów gromadzone przez podmioty krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4, mogą być przekazywane przez te podmioty w określonym zakresie do publicznej wiadomości w przypadku, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę trwającego incydentu lub w przypadku gdy ujawnienie incydentu z innych względów jest w interesie publicznym, w tym również, jeśli przyczyni się do zwiększenia cyberbezpieczeństwa. Przekazywanie niezbędnych informacji do publicznej wiadomości nie może naruszać przepisów o ochronie tajemnic oraz o ochronie danych osobowych";	Uwaga nieuwzględniona. Proponuje się pozostawić możliwość przekazywania informacji o incydentach.

48.	art. 3 ust. 2	Służba Kontrwywiadu Wojskowego	W art. 3 ust. 2 treści wyrażonej w ostatnim zdaniu, proponuje się nadanie następującego brzmienia: „Przekazywanie niezbędnych informacji do publicznej wiadomości nie może naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic ustawowo chronionych.”. Zdaniem SKW zaproponowane brzmienie w lepszy sposób zabezpieczy interes ochrony informacji niejawnych. Należy zauważyć, że ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2016 r. poz. 1167, z późn. zm.) stanowi lex specialis w stosunku do „tajemnic ustawowo chronionych”, co potwierdza przepis art. 1 ust. 3, gdzie określono, iż „Przepisy ustawy o ochronie informacji niejawnych nie naruszają przepisów innych ustaw o ochronie tajemnicy zawodowej lub innych tajemnic prawnie chronionych (…)”. Powyższe, w ocenie SKW, uzasadnia jednoznaczne wskazanie w komentowanym przepisie na pierwszym miejscu przepisów o ochronie informacji niejawnych, a następnie innych tajemnic ustawowo chronionych. Wydaje się także, że w przypadku przedłożonego brzmienia nie ma potrzeby, aby wymieniać dodatkowo przepisy o ochronie danych osobowych, które stanowią jedną z „innych tajemnic ustawowo chronionych”	Uwaga uwzględniona.
49.	art. 3 ust. 3	Generalny Inspektor Ochrony Danych Osobowych	W projekcie wyłączono stosowanie przepisów ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2016 r. poz. 1764) w sytuacji przekazywania do publicznej wiadomości informacji o podatnościach na incydenty, incydentach, zagrożeniach cyberbezpieczeństwa itp. Może to powodować rozproszenie metod udostępniania komunikatów dla użytkowników usług, którym mają służyć w celu poprawy cyberbezpieczeństwa. Generalny Inspektor postuluje, by przynajmniej w zakresie podmiotów objętych w/w ustawą o dostępie do informacji publicznej, pozostawić stosowanie przepisów o metodach udostępniania informacji, w szczególności art. 8 ustawy – zamieszczania informacji w Biuletynie Informacji Publicznej. Ewentualnie projektodawca powinien rozważyć wskazanie, w jaki sposób ma się odbywać przekazywanie do publicznej wiadomości niezbędnych informacji. Analogiczną uwagę należy zgłosić do treści art. 30 ust. 4, 31 ust. 2 oraz 36 ust. 5 projektu.	Uwaga częściowo uwzględniona. Projekt zostanie uzupełniony poprzez wskazanie kanału komunikacji.

50.	art. 3 ust. 3	Kancelaria Sejmu RP	W art. 3 w ust. 3 zawarty jest przepis o niestosowaniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, wydaje się, iż właściwszym rozwiązaniem, ze względu na spójność i przejrzystość systemu prawnego, byłaby zamiana tego przepisu na stosowną nowelizację ww. ustawy.	Do uzgodnienia z RCL.
51.	art. 4	Rada do Spraw Cyfryzacji	W ustawie brakuje jasno określonego stałego organu koordynacyjno – kontrolnego w zakresie nadzoru nad efektywnością pracy zespołów CSIRT i pozostałych elementów Krajowego Systemu Cyberbezpieczeństwa, który na poziomie KRM w sposób stały koordynowałby system.	Uwaga nieuwzględniona. Sposób realizacji zadań i współpracy oraz właściwości CSIRT poziomu krajowego został określony w ustawie. Obecny model został zaproponowany przez CSIRT poziomu krajowego w ramach uzgodnień roboczych.
52.	art. 4	Polska Akademia Nauk	Brak definicji podmiotu świadczącego usługi z zakresu cyberbezpieczeństwa.	Wyjaśnienie. W opinii projektodawcy, definicja ta nie jest potrzebna do zapewnienia właściwego funkcjonowania ustawy.
53.	art. 4 pkt 6	Kancelaria Sejmu RP	W art.4 w pkt 6 wydaje się, iż wyrazy „organy publiczne” należałoby zastąpić pojęciem „organy władzy publicznej” albo „organy administracji publicznej”.	Uwaga uwzględniona.
54.	art. 4 pkt 6-14	Narodowe Centrum Badań i Rozwoju	W ocenie NCBR do jak najszerszej pomocy w zakresie cyberbezpieczeństwa, warto poddać pod rozwagę rozszerzenie katalogu podmiotów uprawnionych do zwrócenia się do CSIRT o wsparcie w obsłudze lub obsługę poważnych incydentów o ww. podmioty publiczne. W przypadku uwzględnienia tej uwagi stosownej zmianie powinna ulec treść art. 28 ust. 2 oraz 3 Projektu ustawy.	Uwaga uwzględniona.
55.	art. 4 pkt 7	Kancelaria Sejmu RP	W art. 4 w pkt 7 należałoby rozważyć dodanie analogicznego sformułowania jak w art. 4 pkt 6 tj. „jednostki je obsługujące”.	Uwaga może zostać uwzględniona po jej wyjaśnieniu.
56.	art. 4 pkt 11	Narodowe Centrum Badań i Rozwoju	Artykuł wskazuje, że krajowy system cyberbezpieczeństwa obejmuje jednostki podległe i nadzorowane przez organy administracji rządowej, a Rozdział 4 Projektu ustawy w związku z tym faktem przewiduje obowiązki podmiotów publicznych, należy w tym miejscu zaakcentować szczególną rolę rekomendacji i	Wyjaśnienie. Wystarczający wydaje się być przepis zawarty w art. 41 pkt 7.

			wytycznych, o których mowa w art. 39 ust. 1 pkt 4) Projektu ustawy oraz udostępniania informacji i dobrych praktyk, a także prowadzenia szkoleń, o których mowa w art. 41 pkt 6) i 7) Projektu ustawy, które wydatnie wspierałyby podmioty publiczne w należytym wykonywaniu obowiązków określonych w Projekcie ustawy.	
57.	art. 4 pkt 11	Polska Akademia Nauk	Użyte w pkt 11 określenie „jednostki podległe i nadzorowane przez organy administracji rządowej" jest niejasne. Jednostkami nadzorowanymi przez organy administracji rządowej są np. także publiczne szkoły wyższe i sądy, te zaś zostały wymienione w odrębnych punktach.	Uwaga uwzględniona. Intencją było objęcie regulacją publicznych szkół wyższych. Tym samym projekt ustawy zostanie zmieniony poprzez usunięcie „uczelni publicznych" z art. 4 pkt 13 oraz zostaną jednoznacznie wskazane jednostki podległe i nadzorowane w rozumieniu art. 33 ust. 1d ustawy o Radzie Ministrów.
58.	art. 4 pkt 12	Rada do Spraw Cyfryzacji	W przypadku samorządów, ustawa (odmiennie niż w pkt 11 dla administracji rządowej) nie obejmuje jednostek podległych. Część z nich stanowi elementy infrastruktury krytycznej (np. woda).	Uwaga uwzględniona.
59.	art. 4 pkt 12	Kancelaria Sejmu RP	W art. 4 w pkt 12 należałoby rozważyć użycie zwrotu zastosowanego w art. 28 ust. 6 w pkt 1 lit e i f: „jednostki samorządu terytorialnego i ich związki" oraz „związki metropolitalne".	Wyjaśnienie. W terminie „związki" mieszczą się „związki metropolitarne".
60.	art. 4 pkt 14	Kancelaria Sejmu RP	W art. 4 w pkt 14 należałoby rozważyć skreślenie zwrotu „utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych", gdyż wydaje się, iż nie ma państwowych osób prawnych utworzonych bez podstawy prawnej i nie wykonujących zadań publicznych.	Uwaga zostanie omówiona z RCL.
61.	art. 4 pkt 14	Polska Akademia Nauk	Ze sformułowania w pkt 14 wynika, że z systemu cyberbezpieczeństwa wyłączone są spółki prawa handlowego. Co wobec tego z takimi spółkami, jak np. Telewizja Polska S.A. czy Polskie Radio S.A., które dysponują rozwiniętymi sieciami i systemami informatycznymi.	Wyjaśnienie. Intencją projektodawcy było wyłączenie spółek, w których JST lub Skarb Państwa posiada udziały, o ile nie będą operatorami usług kluczowych.

62.	art. 4 pkt 14	Kancelaria Sejmu RP	W art. 4 w pkt 14 konstruując wyłączenie niektórych państwowych osób prawnych z systemu cyberbezpieczeństwa należałoby rozważyć doprecyzowanie bardzo ogólnego sformułowania „przedsiębiorstw".	Uwaga zostanie omówiona z RCL.
63.	art. 5	Rada do Spraw Cyfryzacji	Ustawodawca „zgubił" podmioty, które jako spółki samorządowe lub podmioty – spółki prawa handlowego funkcjonują w obszarze samorządowym i są operatorami usług kluczowych – np. gminne spółki wodnokanalizacyjne, elektrociepłownie. Należy uszczegółowić zakres operatorów usług kluczowych w zakresie struktur samorządowych.	Uwaga uwzględniona.
64.	art. 5 ust. 2	Urząd Regulacji Energetyki	Proponuję zdefiniowanie „usługi kluczowej", o której mowa w art. 5 ust. 2 projektu ustawy o cyberbezpieczeństwie (dalej: u.c.) w art. 2 u.c.	Uwaga zostanie omówiona z RCL.
65.	art. 5 ust. 2 pkt 2	Urząd Regulacji Energetyki	Należy doprecyzować brzmienie art. 5 ust. 2 pkt 2 u.c., tak aby jego treść była zrozumiała. Obecne brzmienie nie pozwala na określenie zależności pomiędzy usługą kluczową a systemem informacyjnym.	Wyjaśnienie. Sposób identyfikacji operatorów usług kluczowych został określony przez dyrektywę 2016/1148. Spełnianie warunków kwalifikujących podmioty jako operatorów usług kluczowych będzie przedmiotem postepowania administracyjnego prowadzonego przez organy właściwe.
66.	art. 5 ust. 2 pkt 3	Zakład Ubezpieczeń Społecznych	Określenie jako jednej z przesłanek wydania decyzji skutków wystąpienia incydentu może budzić wątpliwości z uwagi na fakt, że nie można z góry przewidzieć charakteru incydentu oraz jego skutków. Każde zakłócenie świadczenia usługi kluczowej stanowi bowiem konsekwencję określonego zdarzenia, które staje się automatycznie incydentem. Wydaje się, że decyzja może być podjęta na podstawie znaczenia i charakterystyki świadczenia danej usługi przez podmiot, czyli według kryteriów określonych w ust. 3 pkt 1, 2, 4 i 6. Ewentualnie podstawą decyzji może być w jakiś sposób skalkulowane prawdopodobieństwo zakłócenia świadczonej usługi. Jednocześnie należy zauważyć, że Zakład będąc organem publicznym świadczy usługi mające istotne znaczenie dla funkcjonowania systemu ubezpieczeń społecznych oraz ochrony zdrowia. Mając powyższe na uwadze, a w szczególności, określone	Wyjaśnienie. Zgodnie z art. 7 projektu zostaną opracowane progi istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej, na podstawie których będą identyfikowani operatorzy usług kluczowych. Operatorami usług kluczowych będą mogły być podmioty należące do jednego z sektorów, podsektorów oraz rodzajów podmiotów wymienionych w załączniku do projektu ustawy. Wydaje się, że ZUS nie zostanie zakwalifikowany jako operator usługi kluczowej, natomiast będzie podlegał obowiązkom określonym w rozdziale 4 dotyczącym podmiotów publicznym.

			w ust. 3, czynniki istotne skutku zakłócającego incydentu, tj.: - liczba milionów płatników składek oraz ubezpieczonych, którzy są zależni od usług Zakładu, - zależność służby zdrowia oraz innych instytucji publicznych od działalności Zakładu, - potencjalnego wpływu incydentów na funkcjonowanie systemu ubezpieczeń społecznych, - zasięgu całego kraju, którego mógłby dotyczyć incydent, - unikalność świadczonych usług o zasięgu krajowym oraz brak usług alternatywnych, należy stwierdzić, że Zakład spełnia kryteria umożliwiające za uznanie go za operatora usługi kluczowej. Mając na uwadze powyższe, kierując się znaczeniem usług świadczonych przez Zakład dla utrzymania krytycznej działalności systemu ubezpieczeń społecznych, należy wpisać Zakład do załącznika do projektu ustawy jako operatora usługi kluczowej.	
67.	art. 5 ust. 2, 4 i 5	Rada do Spraw Cyfryzacji	„Decyzja i konsekwencje określenia, że dany podmiot jest operatorem usługi kluczowej" – decyzja taka ma wpływ na prowadzoną działalność gospodarczą, a więc po wydaniu decyzji powinien być czas na dostosowanie jej działalności z ewentualną zmianą modelu biznesowego związanego z tą usługą. Z zapisów ustawy wynika natychmiastowe żądanie wykonalności (Art. 5. punkt 5), co może powodować problem z realizacją wymogów nałożonych w ustawie.	Wyjaśnienie. Natychmiastowa wykonalność wiąże się z zakwalifikowaniem podmiotu jako operatora usługi kluczowej. Natomiast na dostosowanie się do wymogów operator będzie miał sześć miesięcy.
68.	art. 5 ust. 3	Ubezpieczeniowy Fundusz Gwarancyjny	Wydaje się zasadne, aby każdy operator usługi kluczowej dla każdej ze świadczonych usług kluczowych zdefiniował bazowe parametry wyszczególnione w pkt. 1-5. Na tej podstawie w odniesieniu do zdefiniowanych (przez Minister właściwy do spraw informatyzacji we współpracy z organami właściwymi oraz dyrektorem Rządowego Centrum Bezpieczeństwa) progów , podmiot świadczący usługę kluczową w przypadku "zakłócenia" w świadczeniu usługi będzie w stanie szybko określić czy Incydent przekracza zdefiniowane progi.	Wyjaśnienie. Art. 5 dotyczy identyfikacji operatorów usług kluczowych, a nie progów dla kwalifikacji incydentów.
69.	art. 5 ust. 3 pkt 6	Narodowy Bank Polski	W art. 5 ust. 3 pkt 6 projektu zawarto nieprecyzyjne określenie „wystarczający poziom usługi", proponujemy rozważyć jego doprecyzowanie bądź zastąpienie innym, zgodnym z intencją projektodawcy.	Wyjaśnienie. Projekt ustawy dotyczy wielu usług w różnych sektorach. Nie jest pożądane precyzowanie tego terminu, aby nie wyłączyć lub nie zawężyć zbytnio

				regulacji.
70.	art. 7	Centralne Biuro Antykorupcyjne	Treść art. 7 proponujemy przenieść do rozdziału I. Zasadne wydaje się także zmiana delegacji, tak aby umożliwiała opracowanie wspólnych kryteriów dla wszystkich użytkowników cyberprzestrzeni (operatorzy usług kluczowych, dostawcy usług cyfrowych, podmioty publiczne oraz wyznaczone CSIRT-y), na podstawie których klasyfikowane byłyby incydenty do ustawowo nazwanych w tym artykule klas (mogą być zaproponowane: zwykłe poważne i krytyczne). Jednocześnie wskazane byłoby usunięcie „incydentu istotnego", ze względu na fakt, że różnica pomiędzy poważnym a istotnym incydentem sprowadza się wyłącznie do tego, że istotny występuje wyłącznie w obszarze świadczenia usług cyfrowych. Wydaje się, że intencją autorów, było wprowadzenie nazwy wynikającej z konwencji stosowanej w dyrektywie NIS, gdzie używane jest sformułowanie „incydent mający istotny wpływ na świadczenie usługi" co nie jest równoznaczne z wprowadzeniem nazwy własnej „incydent istotny". (Konsekwencją tej propozycji jest objęcie zakresem artykułu 7 także obecnych art. 10 ust. 2 pkt 2, art. 12 ust. 1 pkt 3 – 6 i ust. 3, art. 12 ust. 4 i 5, art. 25 pkt 4-6, art. 28 ust. 3 pkt 6, 7 i 9, a także art. 41 pkt 6 i 8, art. 42 ust. 2 pkt 4 oraz ust. 5;	Uwaga uwzględniona. Przepisy dotyczące incydentów zostaną częściowo zmienione.
71.	art. 7	Polska Akademia Nauk	Wielu skutków prawnych ustawy nie da się ustalić, ze względu na brak projektu rozporządzenia określającego progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.	Wyjaśnienie. Progi zostaną przyjęte w drodze uchwały.
72.	art. 7 ust. 1	Kancelaria Sejmu RP	Art. 7 ust. 1 stanowi podstawę do wydania w formie uchwały Rady Ministrów aktu wykonawczego mającego bardzo doniosłe znaczenie, dla wykonania przepisów ustawy, gdyż ww. akt wykonawczy określi „progi istotności", które stanowią najważniejsze kryterium określania „usług kluczowych" w rozporządzeniu wydanym na podstawie art. 6. Należy zwrócić uwagę, iż uchwała Rady Ministrów nie jest aktem normatywnym, który art. 87 Konstytucji przewiduje jako akt normatywny stanowiący źródło powszechnie obowiązującego prawa. Ponadto wytyczne do wydania ww. uchwały poprzez użycie sformułowania „co najmniej", mają charakter otwarty, co oznacza, że Rada Ministrów przyjmując ww. akt wykonawczy może kierować się nie tylko przesłankami określonymi w art. 5 ust. 3, ale także innymi	Uwaga nieuwzględniona.

			bliżej nie sprecyzowanymi kryteriami.	
73.	art. 7 ust. 3	Rada do Spraw Cyfryzacji	„Niejawność Progów istotności skutku zakłócającego” - wydaje się że progi istotności powinny być jawne, będąc częścią legislacji w zakresie cyberbezpieczeństwa. Niejawność może powodować ograniczenie liczby podmiotów decydujących się na działanie w obszarach biznesowych wymienionych w załączniku do uchwały, gdyż firmy te nie będą mogły ocenić wpływu legislacji na planowany model biznesowy i plan biznesowy. Przemyślana pod kątem cyberbezpieczeństwa decyzja związana z wejściem w działalność w danym obszarze, pozwoli na wcześniejsze uniknięcie problemów związanych z potencjalną nieprofesjonalną działalnością nowego podmiotu.	Uwaga nieuwzględniona. Operatorzy usług kluczowych w istotnej mierze będą również operatorami infrastruktury krytycznej, gdzie to zgodnie z ustawą o zarządzaniu kryzysowym kryteria identyfikujące są określone w załączniku do NPOIK, będącym dokumentem zawierającym informacje niejawne o klauzuli „zastrzeżone”. Upublicznienie progów w drodze rozporządzenia mogłoby pośrednio wpłynąć na ujawnienie kryteriów identyfikujących operatorów infrastruktury krytycznej.
74.	Art. 8	Rządowe Centrum Bezpieczeństwa	art. 8 projektowanej ustawy przewiduje prowadzenie przez ministra właściwego do spraw informatyzacji wykazu operatorów usług kluczowych, uwzględniający podział na sektory, podsektory i rodzaje podmiotów. W sytuacji ujednolicenia kryteriów oraz biorąc pod uwagę, że dyrektor RCB, zgodnie z art. 5b ust. 7 pkt 1, sporządza i prowadzi wykaz infrastruktury krytycznej (IK) powstaną dwa tożsame wykazy.	Uwaga uwzględniona. Obowiązek prowadzenia rejestru zostanie przeniesiony na dyrektora RCB.
75.	art. 8 ust. 1	Ubezpieczeniowy Fundusz Gwarancyjny	Wydaje się zasadne aby wykaz operatorów usług kluczowych zawierał również informacje, czy usługa kluczowa świadczona jest tylko na terenie RP czy może również ma charakter transgraniczny (dotyczy wymagania: informowanie innych państw członkowskich Unii Europejskiej o incydentach istotnych, które dotyczą dwóch lub większej liczby państw członkowskich). Wprowadzenie takiej Informacji do wykazu może ułatwić proces raportowania Incydentów pomiędzy CSIRTami narodowymi w ramach UE.	Uwaga uwzględniona.
76.	art. 8 ust. 6	Służba Kontrwywiadu Wojskowego	W treści art. 8 ust. 6 proponuje się ujednolicenie określenia przywołanych tam podmiotów poprzez wpisanie w odpowiednich punktach „Agencji Bezpieczeństwa Wewnętrznego” oraz „Agencji Wywiadu” oraz wpisanie „Służby Kontrwywiadu Wojskowego” i „Służby Wywiadu Wojskowego” w oddzielnych punktach.	Uwaga uwzględniona.

77.	art. 8 ust. 6	Rada do Spraw Cyfryzacji	Wykaz podmiotów uprawnionych do uzyskania informacji z wykazu operatorów usług kluczowych, pokazuje że nie może tej informacji uzyskać organ samorządu terytorialnego, którego podmiot zostanie wpisany na listę. Konsekwencją jest fakt, że prezes spółki/szef podmiotu nie może nawet poinformować burmistrza o tym fakcie i wynikających z tego obowiązkach. „Udostępnianie informacji o wykazie operatorów usług kluczowych" - informacje te powinny być udostępniane oprócz wymienionych także wszystkim podmiotom wchodzącym w skład krajowego systemu cyberbezpieczeństwa. Dzięki tej informacji podmioty te mogą świadomie podejmować decyzje o wyborze partnera biznesowego, co może przekładać się na świadczoną usługę końcową.	Wyjaśnienie. Wykaz operatorów nie jest informacją niejawną. W przedstawionym przykładzie, prezes spółki może poinformować burmistrza o tym, że znajduje się na wykazie – w ramach nadzoru właścicielskiego.
78.	art. 8 ust. 6	Kancelaria Sejmu RP	W art. 8 w ust. 6, ze względu na zasadę trójpodziału władzy, a także projekt ustawy o Straży Marszałkowskiej (druk nr 1971) rozszerzający dotychczasowe kompetencje Straży Marszałkowskiej, należałoby rozważyć dodanie tej formacji do wykazu podmiotów uzyskujących informacje z wykazu operatorów usług kluczowych.	Uwaga nieuwzględniona.
79.	art. 8 ust. 6	Biuro Bezpieczeństwa Narodowego	W art. 8 ust. 6 należałoby przyjąć jednolicie, że informacje udostępnia się wskazanym w nim służbom, a nie ich szefom (w pkt 6 jest wymieniona Służba Kontrwywiadu Wojskowego, a w pkt 7 Szef Agencji Bezpieczeństwa Wewnętrznego).	Uwaga uwzględniona.
80.	art. 8 ust. 6	Najwyższa Izba Kontroli	Ponadto należy także zwrócić uwagę na zapisy art. 8 ust. 6 oraz art. 46 ust. 10 projektowanej ustawy. Konstrukcja tych przepisów, które wymieniają w sposób zamknięty listę podmiotów uprawnionych do uzyskania informacji z wykazu operatów usług kluczowych lub z systemu teleinformatycznego, może budzić wątpliwości interpretacyjne w zakresie możliwości uzyskania takich informacji przez Najwyższą Izbę Kontroli w ewentualnych postpowaniach kontrolnych. Zgodnie z art. 29 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli nie ma potrzeby, aby przy każdej ustawowej tajemnicy uwzględniać NIK wśród podmiotów uprawnionych do dostępu do niej, jednakże ww. przepisy projektowanej ustawy wymieniają wśród uprawnionych podmiotów m.in. sądy, prokuraturę, CBA, ABW, SKW czy SWW. Wydaje się, że wymienienie ww. podmiotów w szczególności sadow, prokuraturę, czy służb, jako uprawnione podmioty, które	Wyjaśnienie. NIK będzie miał dostęp do wykazu operatorów usług kluczowych na podstawie odrębnych ustaw.

			mogą uzyskać informacje w zakresie niezbędnym do realizacji ich ustawowych zadań albo jest zbędne, ponieważ i tak mocą przepisów szczególnych w ramach prowadzonych postpowań mogłyby uzyskać takle informacje albo służy do wyłączenia innych niewymienionych podmiotów z ww. uprawnień np. naczelnego organu kontroli państwowej, jakim jest Najwyższa Izba Kontroli. Samo wpisanie w listę uprawnionych podmiotów „organów właściwych" nie rozwiązuje problemu, ponieważ jako „organy właściwe", na poziomie projektowanej ustawy, traktowane są określone ministerstwa, stosownie do zapisów art. 4 pkt 16 w zw. z art. 38. W konsekwencji może to powodować spory interpretacyjne co do zakresu kompetencji kontrolnych NIK,	
81.	art. 10 ust. 1	Rządowe Centrum Bezpieczeństwa	2. art. 10 ust. 1 przewiduje, że operatorzy usług kluczowych zapewniają bezpieczeństwo świadczonych przez nich usług kluczowych oraz ciągłość świadczenia tych usług. Taki zapis jest zbieżny, w sensie celu, z obowiązkiem narzuconym art. 6 ust. 5 ustawy o zarządzaniu kryzysowym oraz oznacza, że będą oni musieli całościowo zabezpieczyć świadczenie usługi kluczowej – wg definicji zawartej w art. 5 ust. 1 pkt 1 przez usługę kluczową należy rozumieć usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej. W tym kontekście zostało to już ujęte w Narodowym Programie Ochrony Infrastruktury Krytycznej jako 6 rodzajów zapewnienia bezpieczeństwa tj. a. zapewnienie bezpieczeństwa fizycznego (w tym wskazane w projekcie ustawy systemy kontroli dostępu), b. zapewnienie bezpieczeństwa technicznego (w tym wskazane w projekcie ustawy bezpieczeństwo środowiskowe), c. zapewnienie bezpieczeństwa osobowego, d. zapewnienie bezpieczeństwa teleinformatycznego (zawierające wszystkie elementy, o których mowa w projekcie ustawy), e. zapewnienie bezpieczeństwa prawnego, f. plany odbudowy i ciągłości działania (w tym wskazane w projekcie ustawy plany utrzymania działania usług).	Uwaga uwzględniona. Podmioty będące infrastrukturą krytyczną i operatorami usług kluczowych będą zwolnione z obowiązków z art. 10 ust. 2 (system zarządzania bezpieczeństwem informacji), art. 11 (obowiązek sporządzenia planów) oraz art. 15 ust. 1 (wyznaczenie osoby odpowiedzialnej).
82.	art. 10 ust. 2	Ubezpieczeniowy Fundusz Gwarancyjny	"Wydaje się zasadne, aby uwzględnić również poniższe wymagania: -stosowanie wewnętrznych procedur zapewniających Bezpieczeństwo Informacji;	Uwaga nieuwzględniona. Przedstawione propozycje mieszczą się w obecnej treści art. 10 ust. 2.

			-zapewnienie rozdzielności obowiązków związanych z utrzymaniem, rozwojem i bezpieczeństwem Systemów Teleinformatycznych; -budowanie świadomości bezpieczeństwa wśród Pracowników podmiotu świadczącego usługę kluczową i Użytkowników usługi kluczowej; -ciągłe doskonalenie obszaru bezpieczeństwa, w szczególności podejmowanie działań mitygujących ryzyko ponownego wystąpienia danego Incydentu poważnego; -utrzymanie i bezpieczną eksploatacją systemów informacyjnych (zapis obecnie uwzględniony) +w tym zarządzanie usługami IT."	
83.	art. 10 ust. 2	Polska Akademia Nauk	Proponuje się dodać zapis, że przedsiębiorcy posiadający dla swych systemów certyfikat normy ISO 27001 spełniają wymagania określone w art. 10 ust. 2 projektu ustawy (wzorem zapisu w Krajowych Ramach Interoperacyjności w § 20 ust. 3)	Uwaga nieuwzględniona. Przedsiębiorcy posiadający certyfikat zgodności z SZBI w rozumieniu ISO 27000 będą spełniać większość wymagań określonych dla usług kluczowych lub usług cyfrowych, pod warunkiem że certyfikacją były objęte te usługi.
84.	art. 10 ust. 2 pkt 1	Rada do Spraw Cyfryzacji	Konieczne jasne i konkretne podanie, że dotyczy to zarówno sieci IT jak i OT (technologicznych) - jeżeli takie istnieją, inaczej będzie to ustawa rozwiązująca problem częściowo – w tym zakresie należy bardziej uszczegółowić zakres procesów i usług jakie będą objęte regulacją już na poziomie ustawy ze względu na istotę problemu.	Wyjaśnienie. Systemy OT zawierają się w definicji systemów informacyjnych.
85.	art. 10 ust. 2 pkt 2	Rada do Spraw Cyfryzacji	Czy CSIRT będą mieć specjalistów od analizy wszystkich incydentów - trzeba pamiętać, że ile technologii produkcyjnych tyle protokołów na świecie, co oznacza, że nie ma standaryzacji protokołów transmisyjnych w sieciach technologicznych – sugeruje się utworzenie pojęcia CERT'ów sektorowych specjalizujących się w technologiach sieci produkcyjnych	Wyjaśnienie. Projekt nie wyklucza możliwości tworzenia CERT sektorowych.
86.	art. 10 ust. 2 pkt 3	Rada do Spraw Cyfryzacji	Odpowiednie i proporcjonalne środki techniczne, a w Ocenach Skutków Regulacji zakłada się : - 5-10 tys na pracownika SOC - Koszt SOC - 1 mln - Audyt 50 tys To nie są koszty realne i proporcjonalne. Dlatego też sugeruje się utworzenie CERT'ów sektorowych i sugerowanie operatorom usług kluczowych oraz CERT'om sektorowym wykorzystywanie specjalistycznych narzędzi audytowych do sieci technologicznych i do stałego monitorowania tych sieci.	Wyjaśnienie. Projekt nie wyklucza możliwości tworzenia CERT sektorowych.

87.	art. 10 ust. 2 pkt 5	Ubezpieczeniowy Fundusz Gwarancyjny	Czy Ustawodawca wymaga aby system monitorowania, a dokładnie alarmy/zdarzenia z narzędzi monitorujących były obsługiwane przez zewnętrzny/wewnętrzny personel również w trybie ciągłym ? Czy Ustawodawca dopuszcza sytuację, w której System monitorowania pracuje w trybie ciągłym natomiast personel odpowiedzialny za podejmowanie reakcji jest dostępny w dni robocze?	Wyjaśnienie. Intencją projektodawcy było zapewnienie monitoringu bezpieczeństwa w trybie ciągłym, a sposób realizacji tego zadania zależy już od operatora.
88.	art. 10 ust. 2 pkt 11	Kancelaria Sejmu RP	W art. 10 w ust. 2 w pkt 11 i w ust. 3 należałoby rozważyć zastąpienie pojęcia „prawidłowa komunikacja” innym zwrotem, np. „niezakłócona komunikacja”.	Uwaga nieuwzględniona. Celowo użyto terminu „prawidłowa” jako zawierającego w sobie „niezakłócona”.
89.	art. 10 ust. 3	Kancelaria Sejmu RP	W art. 10 w ust. 3 należałoby dodać przesłankę "prawidłowej komunikacji", ze względu na konieczność spójności z treścią pkt 11 ust. 2.	Uwaga uwzględniona.
90.	art. 11	Rada do Spraw Cyfryzacji	„Opracowanie dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych używanych do świadczenia usług kluczowych”. Wydaje się że czas 6 miesięcy może być trudny dla podmiotów które dopiero rozpoczną dostosowywanie się do zapisów uchwały po decyzji, iż jest on operatorem usługi kluczowej. W takim przypadku czas ten z realnych powodów działania rynku (zatrudnienie specjalistów, opracowanie procesów itp.) może być nierealny	Uwaga nieuwzględniona. W opinii projektodawcy, termin sześciu miesięcy od wyznaczenia jako operatora jest wystarczający.
91.	art. 11 ust. 1	Zakład Ubezpieczeń Społecznych	Wydaje się, że okres przechowywania dokumentacji powinien być liczony od momentu zakończenia świadczenia usługi kluczowej, ponieważ powinna być ona dostępna przez cały okres świadczenia usługi. Należy też wprowadzić wymóg aktualizacji dokumentacji, w przypadku zmiany systemu informatycznego wykorzystywanego do świadczenia usługi kluczowej. Jednocześnie należy zauważyć, że proces dojścia do obsługi incydentów w sposób opisany w ustawie jest w dużym stopniu uzależniony od spójności założeń przyjętych do jego realizacji w poszczególnych podmiotach, których dotyczy. Dlatego też Zakład proponuje rozważanie wydania rozporządzenia określającego standardy w zakresie definiowania ryzyk, zasad komunikacji i obsługi incydentów, co powinno prowadzić do ujednolicenia stosowania przepisów ustawy. Dodatkowo poddajemy pod	Uwaga uwzględniona. Przepis zostanie zmieniony.

			rozwagę możliwość koordynowania w ramach instytucji publicznych projektów dotyczących budowy systemu teleinformatycznego cyberbezpieczeństwa.	
92.	art. 11 ust. 1	Naczelny Dyrektor Archiwów Państwowych	Artykuł przewiduje, że operatorzy usług kluczowych przechowują przez 5 lat dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych. Nie wiadomo natomiast, co z tą dokumentacją ma się stać po upływie okresu przechowywania. Należy zauważyć, że operatorami usług kluczowych mogą być zarówno podmioty ze sfery publicznej (np. spółki Skarbu Państwa, przedsiębiorstwa państwowe), wytwarzające materiały archiwalne wchodzące do państwowego zasobu archiwalnego, jak i podmioty prywatne. Nie można oczywiście wykluczyć, że założeniem projektodawcy jest stosowanie w odniesieniu do podmiotów publicznych odpowiednich przepisów ustawy o narodowym zasobie archiwalnym i archiwach oraz aktów wykonawczych do niej, regulujących postępowanie z dokumentacją. Jednakże nie wynika to wprost z projektowanych przepisów.	Uwaga uwzględniona. Przepis zostanie zmieniony.
93.	art. 11 ust. 1	Centralne Biuro Antykorupcyjne	W art. 11 ust. 1 przechowywanie dokumentacji proponujemy powiązać z datą zakończenia eksploatacji systemów informatycznych, których dotyczy zamiast daty jej wytworzenia;	Uwaga uwzględniona. Przepis zostanie zmieniony.
94.	art. 11 ust. 1	Urząd Regulacji Energetyki	W przepisie tym jest mowa o obowiązku opracowania dokumentacji dotyczącej cyberbezpieczeństwa oraz o obowiązku przechowywania tej dokumentacji przez okres 5 lat. Oznacza to, że po upływie tego okresu dokumentacja może zostać zniszczona co nie znajduje uzasadnienia ze względu na okoliczność, że ustawa nie określa terminu obowiązywania decyzji o uznaniu za operatora usługi kluczowej.	Uwaga uwzględniona. Przepis zostanie zmieniony.
95.	art. 11 ust. 2	Generalny Inspektor Ochrony Danych Osobowych	Wskazano 5-letni okres przechowywania dokumentacji dotyczącej cyberbezpieczeństwa licząc ten okres od momentu jej wytworzenia, co może spowodować, że dla usług długoterminowych, po upływie 5 lat od chwili wytworzenia dokumentacji nie ma obowiązku jej przechowywania, pomimo, że usługa dalej jest świadczona. Sugeruję się wskazanie tego okresu na np. minimum przez 5 lat od chwili jej wytworzenia i nie krócej	Uwaga uwzględniona. Przepis zostanie zmieniony.

			niż do czasu, kiedy świadczenie usługi zostanie zakończone.	
96.	art. 11 ust. 3	Kancelaria Sejmu RP	Na podstawie art. 11 ust. 3 Rada Ministrów określi w drodze rozporządzenia zakres informacji zawartych w dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, co może stanowić, iż przedmiotowe rozporządzenie w tym zakresie ma charakter blankietowy i reguluje materię o charakterze ustawowym.	Uwaga zostanie skonsultowana z RCL.
97.	art. 11 ust. 3	Kancelaria Senatu RP	Na podstawie art. 11 ust. 1 operatorzy usług kluczowych opracowują dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych, oraz przechowują te dokumentację przez okres 5 lat liczonych od początku roku następującego po roku jej wytworzenia. Wobec obecnego brzmienia przepisu nie można jednoznacznie stwierdzić, czy rzeczona dokumentacja ma określać procedury postpowania, czy być dowodem (rejestrem) dokonanych czynności. Zakres dokumentacji ma być określony w rozporządzeniu wydanym na podstawie art. 11 ust. 3, którego projekt na obecnym etapie prac nie jest jeszcze dołączony do projektu ustawy. Jeżeli celem projektodawcy było odniesienie się do dokumentacji rozumianej, jako procedura postpowania, to termin 5 lat, o którym mowa w przepisie, powinien odnosić się do terminu zaprzestania wykorzystania dokumentacji, a nie do roku jej wytworzenia.	Uwaga uwzględniona. Przepis zostanie zmieniony.
98.	art. 12. ust. 1	Ubezpieczeniowy Fundusz Gwarancyjny	Wydaje się zasadne aby Ustawodawca potwierdził, że podmiot świadczący usługę kluczową niezależnie od zgłoszenia Incydentu do właściwego CSIRT w przypadku: - Incydentu dotyczącego Danych Osobowych zgłosił Incydent również do GIODO - Incydentu noszącego znamiona przestępstwa zgłosił Incydent do właściwych organów ścigania	Uwaga nieuwzględniona.
99.	art.12. ust. 1. pkt 4	Ubezpieczeniowy Fundusz Gwarancyjny	Dyrektywa NIS nie określa maksymalnego czasu zgłoszenia Incydentu znaczącego, jest użyte sformułowanie "bez zbędnej zwłoki". Wydaje się zasadne, aby wprowadzić jednolity maksymalny termin	Uwaga nieuwzględniona.

			zgłoszenia Incydentu analogicznie do RODO/GDPR - 72h. Dodatkowo w przypadku braku dostępności personelu IT w trybie 24h , zgłoszenie Incydentu w ciągu 24h od momentu wykrycia, może nie być fizycznie możliwe.	
100.	art.12. ust. 1 pkt 6	Ubezpieczeniowy Fundusz Gwarancyjny	Wydaje się zasadne, aby dodać to pojęcie do Rozdziału 1, Artykuł 2 i podać definicję.	Uwaga niejasna.
101.	art. 12 ust. 2	Służba Kontrwywiadu Wojskowego	W ocenie SKW oprócz kar dla podmiotów zobowiązanych do informowania o incydentach należałoby także przewidzieć szerszą ochronę ich interesów w kontekście zwiększonej odpowiedzialności wynikającej ze zgłoszenia incydentu. Celowym byłoby stworzenie takich regulacji, aby podmioty nie próbowały ukrywać informacji o incydentach we własnej infrastrukturze w obawie przed poniesieniem strat. Przepisy zaproponowane w projekcie ustawy mogą być niewystarczające, tj.: art. 12 ust. 2, który stanowi: „Zgłoszenie o którym mowa w ust.1 pkt 4, nie może narażać operatora usługi kluczowej na zwiększoną odpowiedzialność”. Powodzenie działania krajowego systemu cyberbezpieczeństwa zależy w dużej mierze od zaufania pomiędzy podmiotami oraz odpowiednich gwarancji, że żaden podmiot biorący udział w systemie nie poniesie dodatkowych strat wynikających z udostępnienia wrażliwych informacji o stanie swoich systemów informacyjnych;	Uwaga nieuwzględniona.
102.	art. 12 ust. 2	Kancelaria Senatu RP	Przepis zawarty w art. 12 ust. 2 stanowi, ze zgłoszenie incydentu poważnego przez operatora usług kluczowych nie może narażać tego operatora na zwiększoną odpowiedzialność. Przepis jest powtórzeniem normy z art. 14 ust. 3 zdanie trzecie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, która jest skierowana do państw członkowskich i nakłada obowiązek takiego ukształtowania wewnętrznego porządku prawnego, aby nie pogarszać sytuacji prawnej zgłaszającego podmiotu. Takie ogólne sformułowanie wymaga doprecyzowania podczas implementacji	Uwaga nieuwzględniona. Przepis dotyczy wyłączenia zwiększonej odpowiedzialności za zgłoszenie incydentu, a nie innej.

			do prawa krajowego. Przepis art. 12 ust. 2 w projektowanym brzmieniu nie daje jednoznacznej odpowiedzi, CO do konsekwencji zgłoszenia incydentu poważnego. Z jednej strony, przepis mógłby oznaczać, ze zwiększenie odpowiedzialności odnosi się jedynie do zgłoszenia incydentu. Ponieważ projekt nie wprowadza odpowiedzialności za zgłoszenie, przepis w takim znaczeniu nie niesie w sobie żadnej treści, gdyż odpowiedzialność na zasadach ogólnych jest konsekwencji zachowań, które doprowadziły do wystąpienia incydentu - a nie jego zgłoszenia. Z drugiej strony, przepis mógłby oznaczać całkowite zwolnienie operatora z wszystkich typów odpowiedzialności (karnej, cywilnej, administracyjnej), za działania, które doprowadziły do incydentu (na zasadach podobnych do czynnego żalu określonego np. wart. 15 § 1 Kodeksu karnego). Wydaje się, że takie rozwiązanie jest zbyt daleko idące, szczególnie w zakresie odpowiedzialności cywilnej. Dlatego należy odrzucić koncepcję zwolnienia operatora z wszelkich konsekwencji prawnych incydentu, w sytuacji, gdy operator dokonał zgłoszenia. Wobec powyższego, projektodawca winien precyzyjnie wskazać pułap odpowiedzialności operatora, który nie może być powiększony w przypadku zgłoszenia incydentu. Analogiczny problem jest związany z art. 19 ust. 4. Podobnie należy potraktować zakaz nakładania dodatkowych obowiązków na podmioty inne niż operatorzy usług kluczowych i dostawcy usług cyfrowych, które zgłaszają incydenty (art. 33 ust. 3 zdanie drugie). Należy podkreślić, ze działania organów administracji publicznej muszą znaleźć podstawę w przepisach prawa (art. 6 Kodeksu postpowania administracyjnego). Wobec tego wdrożenie art. 20 ust. 2 ww. dyrektywy, powinno polegać na nienakładaniu przez ustawę dodatkowych obowiązków na zgłaszającego oraz nieprzyznawaniu organom takiej kompetencji. Przy spełnieniu tych warunków przepis z art. 33 ust. 3 zdanie drugie jest niepotrzebny.	
103.	art. 12 ust. 2	Urząd Regulacji Energetyki	Należy doprecyzować, co należy rozumieć poprzez pojęcie „zwiększonej odpowiedzialności” wskazane w art. 12 ust. 2 u.c. oraz art. 19 ust. 4 u.c. Obecne brzmienie tych przepisów może powodować wątpliwości interpretacyjne.	Uwaga nieuwzględniona.

104.	art. 12 ust. 2	Ubezpieczeniowy Fundusz Gwarancyjny	Co Ustawodawca rozumie pod pojęciem "nie może narażać operatora usługi kluczowej na zwiększoną odpowiedzialność"?	Uwaga nieuwzględniona.
105.	art. 12. ust. 3	Ubezpieczeniowy Fundusz Gwarancyjny	Wydaje się zasadne, aby Ustawodawca doprecyzował pojęcie zakłócenie działania systemu teleinformatycznego	Uwaga nieuwzględniona.
106.	art. 12. ust. 3	Polska Akademia Nauk	Art. 12 ust. 3 – proponuje się zastąpić słowa „za pomocą dostępnych środków komunikacji elektronicznej” słowami „ za pomocą dostępnych środków komunikacji, w pierwszej kolejności komunikacji elektronicznej”	Uwaga nieuwzględniona.
107.	art. 12 ust. 3 i 4 oraz art. 13 ust. 1	Rada do Spraw Cyfryzacji	Artykuł 12 ust. 3, ust. 4 oraz artykuł 13 ust. 1 odwołują się do incydentu poważnego (stopnień niższy niż incydent krytyczny). Artykuł 12 ust. 1 pkt 6 rozróżnia incydent poważny i incydent krytyczny. Czy to pociąga za sobą brak obowiązku zgłaszania incydentu krytycznego?	Wyjaśnienie. Klasyfikację incydentu jako krytycznego przeprowadza CSIRT.
108.	art. 13	Polska Akademia Nauk	Ustawodawca pomija fakt, że incydent może być na tyle poważny, że odcina zgłaszającego od możliwości komunikowania za pomocą środków komunikacji elektronicznej, i w momencie zgłoszenia incydentu niekoniecznie będzie możliwe ustalenie wszystkich wymaganych w art. 13 danych.	Uwaga nieuwzględniona.
109.	art. 13 ust. 1	Ubezpieczeniowy Fundusz Gwarancyjny	Zgłoszenie powinno również zawierać takie informacje jak : Data wystąpienia Incydentu, Data wykrycia Incydentu. Dodatkowo należy jednoznacznie określić, że podmiot świadczący usługi kluczowe w przypadku wystąpienia Incydentu poważnego archiwizuje, zabezpiecza logi, inne elektroniczne dowody na okres minimum 6 miesięcy. Ustawodawca wymaga zgłoszenia Incydentu poważnego spełniającego określone kryteria w określonym terminie. Należy mieć na uwadze, że nie wszystkie Informacje wymagane w zgłoszeniu będą możliwe do przekazania w początkowym zgłoszeniu. Wydaje się zasadne, aby uwzględnić konieczność aktualizacji brakujących informacji (w zgłoszeniu początkowym) w terminie do 14 dni od daty zgłoszenia Incydentu do CSIRT.	Uwaga nieuwzględniona.

110.	art. 13 ust. 1 pkt 2 i 3	Generalny Inspektor Ochrony Danych Osobowych	W artykule wymaga się podawania, obok imienia i nazwiska osoby zgłaszającej lub uprawnionej do składania wyjaśnień, także numeru telefonu i adresu poczty elektronicznej. Organ ds. ochrony danych osobowych postuluje doprecyzowanie, iż powinny być to numery i adresy służbowe oraz być przetwarzane tylko, jeżeli osoba takowe posiada. Analogiczną uwagę należy zgłosić art. 21 projektu.	Uwaga uwzględniona.
111.	art. 13 ust. 1 pkt 4 lit. e	Polska Akademia Nauk	Art. 13 ust.1 pkt 4 lit. e – proponuje się dodać słowa „o ile skutki takie są mu znane w chwili zgłoszenia”, czyli podobnie jak w pkt 7; uwaga odnosi się także (ogólnie) do wszystkich elementów zgłoszenia, np. lit. F.	Uwaga nieuwzględniona.
112.	art. 15 ust.1 pkt 1	Rządowe Centrum Bezpieczeństwa	Art. 15 ust. 1 pkt 1 projektowanej ustawy przewiduje wyznaczenie osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług kluczowych. W procedowanej aktualnie zmianie ustawy o zarządzaniu kryzysowym zaproponowano funkcję pełnomocnika ds. ochrony IK, którego zakres obowiązków obejmuje m.in. a. koordynowanie opracowywania i wdrażania planów ochrony infrastruktury krytycznej; b. monitorowanie działalności operatora infrastruktury krytycznej w zakresie ochrony infrastruktury krytycznej, w tym sporządzanie raportu o stanie ochrony infrastruktury krytycznej; c. utrzymywanie kontaktów z administracją publiczną, w tym dyrektorem Rządowego Centrum Bezpieczeństwa, poprzez przekazywanie i odbieranie informacji o zdarzeniach zakłócających funkcjonowanie infrastruktury krytycznej, które można utożsamiać z obowiązkami pełnomocnika ds. IK.	Uwaga uwzględniona.
113.	art. 15 ust. 1 pkt 1	Centralne Biuro Antykorupcyjne	Art. 15 ust. 1 pkt 1 powinien zostać włączony do rozdziału I, z uwzględnieniem połączenia wyznaczania osoby odpowiedzialnej za cyberbezpieczeństwo z pełnomocnikiem, o którym mowa w § 5 uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022, oraz ustanawiając przepisy dotyczące wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo, o których mowa w ust. 2 i 4.	Uwaga nieuwzględniona.
114.	art. 15. ust.1 pkt. 2	Rada do Spraw Cyfryzacji	Zgodnie z art. 15 ust. 1 pkt 2 operatorzy usług kluczowych zobowiązani są do zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń	Uwaga nieuwzględniona.

			cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową. Pominąwszy nieprecyzyjny charakter przepisu, warto wskazać, iż jest on również pozbawiony sankcji (art. 57), co w znacznym stopniu może przyczynić się do braku realizacji dyspozycji ustanowionej nim normy. Operatorzy usług kluczowych, jako podmioty realizujące zadania o podstawowym znaczeniu dla funkcjonowania współczesnego społeczeństwa i gospodarki, powinni być zobowiązani do uczestnictwa w budowaniu świadomości użytkowników w obszarze cyberbezpieczeństwa. Warto w tym kontekście rozważyć nałożenie obowiązku przesyłania okresowej informacji (nie tylko „zapewniania dostępu do wiedzy") dotyczącej aktualnych zagrożeń cybernetycznych mogących wiązać się z korzystaniem z danej usługi kluczowej (np. na zasadzie aktualizacji polityki prywatności udostępnianych użytkownikom przez platformy cyfrowe lub działań edukacyjnych). Będzie to też miało korzystny wpływ na cyberbezpieczeństwo operatorów usług kluczowych, którzy mogą dzięki temu uzyskiwać bieżącą informację od użytkowników na temat wykrytych podatności i incydentów (zidentyfikowanych dzięki ostrzeżeniom operatorów). Warto również rozważyć, aby obowiązek ten dotyczył także innych podmiotów krajowego systemu cyberbezpieczeństwa, np. przedsiębiorstw telekomunikacyjnych (art. 4 pkt 5), organów administracji publicznej (art. 4 pkt 6), jednostek samorządu terytorialnego (art. 4 pkt 12).	
115.	art. 15. ust.1 pkt. 2	Ubezpieczeniowy Fundusz Gwarancyjny	Wydaje się zasadne, aby podmiot świadczący usługę kluczową również zapewnił Użytkownikowi usługi kluczowej odpowiedni kanał komunikacji np. Formularz na stronie www umożliwiający zgłoszenie Incydentu.	Uwaga nieuwzględniona.
116.	art. 15. ust.1 pkt 2	Polska Akademia Nauk	Ustawodawca pomija fakt, że ze względu na rosnącą w szybkim tempie liczbę zagrożeń, wiedza na temat skutecznych sposobów zabezpieczenia może nie być dostępna. Obowiązek dostarczenia wiedzy o skutecznych sposobach zabezpieczenia jest więc niemożliwy do zrealizowania w każdym przypadku. Zwłaszcza jeżeli uwzględnić fakt różnorodności posiadanych przez użytkowników systemów i ich funkcjonalności;	Wyjaśnienie. Wskazane jest, aby działania tego typu były prowadzone zgodnie z zasadą należytej staranności. Wystarczające będzie, zgodnie z literalnym brzmieniem przepisu, podawanie adekwatnych i zrozumiałych informacji, dostosowanych do

				przeciętnego użytkownika i dotyczących danej usługi. Przykładowo, może to być przystępnie przedstawiona polityka bezpiecznych haseł, ogólne zasady bezpiecznego korzystania z serwisu przedsiębiorcy czy też wysyłanie ostrzeżeń antyphishingowych.
117.	art. 15 ust. 2	Rada do Spraw Cyfryzacji	Artykuł rodzący wiele pytań i wątpliwości. Czy na pewno każdy operator usługi kluczowej powinien korzystać z usług zewnętrznego podmiotu świadczącego usługi cyberbezpieczeństwa, jeżeli tak to w jakim zakresie i kto określi standardy takiego podmiotu. Uważam, że tego typu podmioty powinny być certyfikowane w swoim zakresie przez CSIRT ABW lub MON lub NASK w zakresie takim, dla jakiego podmiotu usług kluczowych będą świadczyć usługi.	Uwaga nieuwzględniona.
118.	art. 15 ust. 2	Komisja Nadzoru Finansowego	W art. 15 ust. 2 Projektu wskazano, że w celu realizacji wymienionych tam zadań, operatorzy usług kluczowych powołują wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawierają umowy z podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa. Trzeba doprecyzować, jaka jest relacja pomiędzy wspomnianą wewnętrzną strukturą odpowiedzialną za cyberbezpieczeństwo, a osobą odpowiedzialną za cyberbezpieczeństwo świadczonych usług, wymienioną w art. 15 ust. 1 Projektu.	Uwaga nieuwzględniona.
119.	art. 15 ust. 3	Ubezpieczeniowy Fundusz Gwarancyjny	Czy w przypadku umów serwisowych na świadczenie utrzymania (zapewnienie dostępności) Systemów, infrastruktury świadczącej usługę kluczową. Czy Ustawodawca również wymaga przekazania o tym Informacji do właściwego CSIRT ?	Wyjaśnienie. Jeśli usługa serwisowa dotyczy bezpieczeństwa i ciągłości świadczenia usługi kluczowej to spełnia wymogi z art. 15 ust 3.
120.	art. 15 ust. 4	Rządowe Centrum Bezpieczeństwa	Dodatkowo chciałbym poinformować Panią Minister, że w ramach Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych powołany został „Zespół zadaniowy do spraw opracowania standardów zabezpieczeń antyterrorystycznych dla infrastruktury krytycznej”, w ramach którego opracowywane są m.in. standardy zapewnienie bezpieczeństwa teleinformatycznego, co potencjalnie może stanowić kolizję z wymogami, o których mowa w art. 15 ust. 4 oraz art. 42 ust. 16 pkt 3. Wymienione obszary stanowią przykłady potencjalnego nakładania	Wyjaśnienie. Minister Cyfryzacji uczestniczy w posiedzeniach Zespołu zadaniowego do spraw opracowania standardów zabezpieczeń antyterrorystycznych dla infrastruktury krytycznej i zapewnia spójność regulacji, o których mowa. Wymagania zostaną do siebie dostosowane tak, aby się nie powielały.

			się celów i podwójność (jeśli nie potrójność, jeśli weźmiemy pod uwagę prace MZZT) obowiązków nakładanych na przedsiębiorców i instytucje. W związku z tym proponuję kontynuować prace nad usunięciem nadmiarowości rozwiązań.	
121.	art. 15 ust. 4	Polska Akademia Nauk	Brak możliwości określenia skutków prawnych regulacji, ze względu na brak projektu rozporządzenia. Treść rozporządzenia będzie przesądzać o tym jak duży będzie zbiór podmiotów uprawnionych do świadczenia takich usług.	Wyjaśnienie. Projekt rozporządzenia zostaną przygotowane na etap SKRM.
122.	art. 16	Rada do Spraw Cyfryzacji	Ustawa nakłada obowiązek audytu procedur, brakuje obowiązku przeprowadzenia rzeczywistych testów bezpieczeństwa. RdC sugeruje wprowadzenie obowiązku przeprowadzenia co określony czas audytu bezpieczeństwa przez zewnętrznych certyfikowanych pentesterów.	Uwaga nieuwzględniona.
123.	art. 16	Polska Akademia Nauk	Pojęcie jednostki akredytowanej użyte w art. 16 ust. 2 nie zostało sprecyzowane. Nie wiadomo jakie jednostki i w jakim trybie będą uznawane za akredytowane. Brak jest także delegacji ustawowej do wydania aktu wykonawczego w tym zakresie.	Uwaga nieuwzględniona.
124.	art. 16 ust. 1	Rada do Spraw Cyfryzacji	Zgodnie z art. 16 ust. 1 projektu ustawy, operatorzy usług kluczowych są zobowiązani do przeprowadzenia co najmniej raz na dwa lata audytu bezpieczeństwa teleinformatycznego. Z uwagi na bezprecedensową dynamikę rozwoju liczby i zaawansowania zagrożeń w cyberprzestrzeni oraz fundamentalną rolę operatorów usług kluczowych dla funkcjonowania współczesnego społeczeństwa i gospodarki, audyty bezpieczeństwa teleinformatycznego powinny być realizowane co pół roku. Tym samym ustawa powinna doprecyzować procedurę wyboru (prawdopodobnej certyfikacji jak w przypadku podmiotów świadczących usługi z zakresu cyberbezpieczeństwa) oraz organ dokonujący akredytacji (art. 16 ust. 2) podmiotów uprawnionych do realizacji audytów.	Uwaga nieuwzględniona.
125.	art. 16 ust. 1	Biuro Bezpieczeństwa Narodowego	W art. 16 ust. 1 ustanawia się obowiązek przeprowadzania audytów bezpieczeństwa teleinformatycznego. Dokonują tego, zgodnie z ust. 2, akredytowane jednostki. Nie jest jasne, o jakich jednostkach jest mowa w tym przepisie.	Uwaga nieuwzględniona.

126.	art. 16 ust. 1	Komisja Nadzoru Finansowego	W art. 16 ust. 1 Projektu wspomina się o audycie bezpieczeństwa teleinformatycznego, zwanego dalej „audytem". Audyt, zgodnie z ust. 2 tego artykułu, będzie przeprowadzany przez stosowną jednostkę, która oceniać ma „zgodność systemu zarządzania bezpieczeństwem". Podkreślić trzeba, że pojęcia „bezpieczeństwo teleinformatyczne" oraz „system zarządzania bezpieczeństwem" nie są tożsame. Audyt systemu zarządzania bezpieczeństwem jest pojęciem dużo szerszym niż audyt bezpieczeństwa teleinformatycznego, które (bezpieczeństwo teleinformatyczne) jest jednym z obszarów systemu zarządzania bezpieczeństwem informacji. Trzeba także rozstrzygnąć, czy przez audyt systemu zarządzania bezpieczeństwem (art. 16 ust. 2 Projektu) należy rozumieć audyt Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w rozumieniu przyjętym przez ogólnoświatowy standard, czyli zbiór norm ISO z grupy 27000 dot. bezpieczeństwa informacji (polska norma PN-ISO 27000:2014) oraz wskazanym w rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 526 z późn. zm.), zwane dalej „rozporządzeniem z dnia 12 kwietnia 2012 r.". Powyższe rozporządzenie z dnia 12 kwietnia 2012 r. stanowi: „§ 20. ust. 1 Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność." SZBI zarówno w rozumieniu normy ISO 27000, jak i rozporządzenia z dnia 12 kwietnia 2012 r. jest zbiorem dużo szerszym, niż tylko zarządzanie bezpieczeństwem teleinformatycznym (bezpieczeństwem systemów informatycznych), obejmując całość bezpieczeństwa informacji m.in. obszary bezpieczeństwa fizycznego, środowiskowego oraz bezpieczeństwa osobowego.	Uwaga uwzględniona odnośnie uzupełnienia ust. 2 poprzez wskazanie, że chodzi o audyty bezpieczeństwa informacji. Odnośnie drugiej części uwagi, wprowadzono możliwość audytu systemu bezpieczeństwa w oparciu o wytyczne sektorowe wydawane przez organy właściwe.

127.	art. 16 ust. 1	Ubezpieczeniowy Fundusz Gwarancyjny	Czy Ustawodawca wymaga przeprowadzenia testów penetracyjnych w ramach "audytu" ?	Wyjaśnienie. Szczegółowe metody przeprowadzania audytów nie są materią ustawową. Co do zasady jednak, wyniki testów penetracyjnych mogą być elementem oczekiwanym w ramach dokumentacji bezpieczeństwa, o której mowa w art. 11.
128.	art. 16 ust. 2	Komisja Nadzoru Finansowego	W art. 16 ust. 2 Projektu używa się pojęcia „audytu zgodności systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania”, jednakże przepisy Projektu nie określają szczegółowych kryteriów tej zgodności. Doprecyzowanie kryteriów może nastąpić poprzez przyjęcie polskich norm jako kryteriów zgodności, podobnie jak to ma miejsce w przytoczonym powyżej rozporządzeniu z dnia 12 kwietnia 2012 r., czy też dokumencie Ministerstwa Cyfryzacji „Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych” z dnia 15 grudnia 2015 r. Warto także zauważyć, że art. 16 ust. 2 Projektu posługuje się pojęciem „akredytowanej” jednostki oceniającej zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania. Należałoby rozważyć wyraźne zdefiniowanie terminu „jednostka akredytowana”. Jeżeli pojęcie „akredytacji” jest związane z akredytacją przez Polskie Centrum Akredytacji, zwane dalej „PCA”, które jako krajowa jednostka akredytująca jest upoważnione do akredytacji jednostek oceniających zgodność na podstawie ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398), to biorąc pod uwagę liczbę podmiotów, na które oddziałuje Projekt wyszczególnionych w „Ocenie skutków regulacji” wydaje się niemożliwe przeprowadzenie przez akredytowane jednostki certyfikujące w podmiotach objętych regulacją Projektu takiej liczby audytów, która umożliwiłaby późniejszą ocenę poziomu realizacji jej wymogów. Z danych publikowanych na stronie PCA wynika, że w przypadku jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji zgodnie z normą PN-ISO/IEC 27006 akredytację uzyskało tylko 7 podmiotów	Uwaga częściowo uwzględniona. Wprowadzono możliwość audytu systemu bezpieczeństwa w oparciu o wytyczne sektorowe wydawane przez organy właściwe. W oparciu o te wytyczne będą mogły być realizowane audyty przez podmioty oceniające zgodność, przy założeniu rozszerzenia możliwości prowadzenia tego audytu na inne podmioty zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) NR 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93. Przepisy zostaną przeredagowane w zakresie doprecyzowania, że chodzi o jednostki posiadające akredytację PCA lub równoważnych ciał w UE.

			(https://www.pca.gov.pl/akredytowane-podmioty/akredytacje-aktywne/jednostki-certyfikujace-systemy/), a mianowicie: a)Polski Rejestr Statków SA (w jego ramach Biuro Certyfikacji Systemów Zarządzania); b)Polskie Centrum Badań i Certyfikacji SA (w jej ramach Zakład Certyfikacji Systemów Zarządzania); c)Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego (w jej ramach Centrum Certyfikacji Jakości); d)Bureau Veritas Polska Sp. z o.o. (w jej ramach Bureau Veritas Certification Polska); e)TUV Nord Polska Sp. z o.o.; f)TUV Rheinland Polska Sp. z o.o.; g)ISOCERT Sp. z o.o. sp.k.	
129.	art. 16 ust. 2	Rada do Spraw Cyfryzacji	W projekcie ustawy brakuje informacji o warunkach koniecznych do spełnienia w celu otrzymania odpowiedniej akredytacji oraz o instytucji odpowiedzialnej za przydzielanie takich akredytacji. Problem rodzi zapis „akredytowana jednostka". CO to ma być za akredytacja i jakie wymagania ma spełniać ta jednostka? Problem w tym, że nie ma standaryzacji tych jednostek a dodatkowo ograniczamy się do np. jednostek dużych bądź specjalizowanych typu PwC, Ey, KPMG, wykluczając mniejsze polskie firmy realizujące takie audyty. Dlaczego CSIRT albo CERT sektorowe nie mogą przeprowadzać samodzielnie audytów przy użyciu powszechnie znanych i często dostępnych narzędzi dla tych operatorów?	Uwaga częściowo uwzględniona. Wprowadzono możliwość audytu systemu bezpieczeństwa w oparciu o wytyczne sektorowe wydawane przez organy właściwe. Do dyskusji w trakcie posiedzenia czy zasadnym byłoby poszerzenie kompetencji CSIRT poziomu krajowego o realizację obowiązków z zakresu audytu.
130.	art. 16 ust. 2	Ubezpieczeniowy Fundusz Gwarancyjny	Czy akredytacja dotyczy tylko norm ISO27001 I ISO22301?	Wyjaśnienie. Audyt ma dotyczyć zgodności z ustawą. Te normy mogą być podstawą, natomiast dla poszczególnych sektorów mogą być dodatkowe normy.
131.	art. 16 ust. 2	Kancelaria Sejmu RP	Należy rozważyć, czy wobec prawdopodobnie znacznej liczby operatorów usług kluczowych, cele audytu powinny sprowadzać się jedynie do sprawdzenia wymogów prawnych? Czy w celu efektywniejszego stosowania przepisów projektowanej ustawy nie należałoby rozważyć dodania przepisów stwierdzających, iż celem audytu byłoby także udzielenie porad, wskazówek bądź też nie wiążących zaleceń w zakresie podnoszenia poziomu cyberbezpieczeństwa? Doprecyzowania wymaga wskazanie	Uwaga nieuwzględniona.

			podmiotu odpowiedzialnego za akredytację jednostek przeprowadzających audyt, o czym stanowi art. 16 ust.2 projektu ustawy.	
132.	art. 16 ust. 2	Narodowy Bank Polski	W art. 16 ust. 2 projektu proponuje się wprowadzenie obowiązku polegającego na przeprowadzaniu audytu przez akredytowaną jednostkę oceniającą zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania. Projektodawca nie zawarł jednak doprecyzowania, co rozumiemy pod pojęciem „akredytowana jednostka przeprowadzająca audyt", która w trakcie trwania audytu będzie miała dostęp do wrażliwych informacji o operatorach usług krytycznych. Ponadto, zgodnie z art. 16 ust. 6 projektu organ właściwy na podstawie analizy wyników audytu może wydawać wiążące polecenia wprowadzenia środków zaradczych w odniesieniu do stwierdzonych w audycie uchybień. W przypadku, o którym mowa w ust. 5 pkt 2 projektu, polecenia wydawane są po zasięgnięciu opinii dyrektora Rządowego Centrum Bezpieczeństwa (RCB). Niezależnie od niespójności pomiędzy art. 4 i art. 27 projektu, która została przedstawiona w uwagach szczegółowych do art. 27, zwracamy uwagę, że ze względu na fakt, iż NBP nie jest i nie może zostać uznany za operatora usługi kluczowej nie sposób zastosować do niego wymagań zawartych w rozdziale 2 projektowanej ustawy.	Wyjaśnienie. Operator usługi kluczowej wybiera jednostkę, która przeprowadzi audyt i jest odpowiedzialny za wskazanie jednostki, która rzetelnie przeprowadzi audyt.
133.	art. 16 ust. 5	Ubezpieczeniowy Fundusz Gwarancyjny	Wydaje się zasadne, aby operator usługi kluczowej (w celach kontrolnych) przekazywał Informację o fakcie, że audyt się odbył.	Uwaga nieuwzględniona.
134.	art. 16 ust. 6	Kancelaria Sejmu RP	W art. 16 w ust. 6 przewiduje się, iż organ właściwy na podstawie analizy wyników audytu może wydawać „wiążące polecenia". Należałoby rozważyć, czy wiążące polecenie nie powinno mieć formy decyzji administracyjnej? Czy w związku z tym, analogicznie do art. 48 ust. 1, nie powinny znaleźć w tym przypadku zastosowanie przepisy dotyczące przeprowadzania kontroli z ustawy o swobodzie działalności gospodarczej?	Uwaga częściowo uwzględniona.

135.	art. 16 ust. 6	Kancelaria Senatu RP	Na podstawie art. 16 ust. 6 i art. 39 ust. 2 organy właściwe będą mogiły wydawać operatorom usług kluczowych wiążące polecenia, a na podstawie art. 39 ust. 2 będą mogły dodatkowo żądać przekazania określonych informacji. Wydaje się, ze celem przepisu było takie ukształtowanie procedury, aby wiążące polecenia i żądanie informacji następowały w drodze innej niż decyzje administracyjne. Egzekucja woli organu oraz możliwość obrony operatora miałyby być realizowane w trakcie postpowania w sprawie nałożenia kary administracyjnej (Wydaje się, ze wśród deliktów administracyjnych zawartych w art. 57 ust. 1 zabrakło niewykonania obowiązków wynikających z art. 39 ust. 2. Świadczy o tym fakt, ze podobne naruszenia przepisów art. 16 ust. 6 i art. 47 ust. 2 zostały wymienione w art. 57 ust. 1.). Ponieważ omawiane przepisy dotyczą postpowania przed organami administracji publicznej w należących do właściwości tych organów sprawach indywidualnych, należy wyraźnie wyłączyć możliwość wydania decyzji w rozumieniu Kodeksu postępowania administracyjnego, chyba ze celem projektodawców jest wydawanie decyzji administracyjnych w tych sprawach - w takim przypadku, ze względu na wyraźne podkreślenie formy wydania rozstrzygnięcia w innych przepisach ustawy (np. art. 5 ust. 1), wart. 16 ust. 6 i art. 39 ust. 2 również należałoby wyraźnie wskazać decyzję, jako tryb załatwienia sprawy.	Uwaga częściowo uwzględniona.
136.	art. 16 ust. 6	Polska Akademia Nauk	Ustawa nie przewiduje żadnych mechanizmów ochrony prawnej przed zaleceniami organu właściwego, które będą nieadekwatne do uchybienia, np. będą pociągać za sobą znaczne wydatki finansowe, w kontekście niewielkiego ryzyka wywołanego uchybieniem (stwierdzonego przez audytora).	Uwaga nieuwzględniona.
137.	art. 18 ust. 3	Kancelaria Sejmu RP	W art. 18 w ust. 3 należy rozważyć skreślenie wyrazów „dotyczących bezpieczeństwa ich systemów informacyjnych” ze względu na definicje zawarte w art. 2 pkt 8-12, które przewidują, iż incydent zawsze dotyczy bezpieczeństwa systemów informacyjnych.	Uwaga nieuwzględniona.
138.	art. 19 ust. 4	Urząd Regulacji Energetyki	Należy doprecyzować, co należy rozumieć poprzez pojęcie „zwiększonej odpowiedzialności” wskazane w art. 12 ust. 2 u.c. oraz art. 19 ust. 4 u.c. Obecne brzmienie tych przepisów może powodować wątpliwości interpretacyjne.	Uwaga nieuwzględniona.

139.	art. 21	Generalny Inspektor Ochrony Danych Osobowych	Wyciąg analogicznie do uwagi nr … w związku z art. 13 ust. 1 pkt 2 i 3	Uwaga częściowo uwzględniona. Projekt zostanie uzupełniony poprzez wskazanie kanału komunikacji.
140.	art. 24 [uwaga do rozdz. 4]	Rada do Spraw Cyfryzacji	Brakuje możliwości zlecenia zadań związanych z cyberbezpieczeństwem podmiotom zewnętrznym (taką możliwość dostawcom usług elektronicznych daje art. 23). Efektem takiego ograniczenia jest spadek jakości ochrony cybernetycznej lub wzrost jej kosztów.	Uwaga uwzględniona. Zostanie dodany przepis analogiczny do art. 23.
141.	Art. 24 ust. 1 w zw. Z art. 25 pkt 8	Krajowa Rada Radiofonii i Telewizji	Wątpliwości interpretacyjne może budzić pojęcie świadczenia usług użyte w art. 24 ust. 1 oraz art. 25 pkt 8), które odnosi się do podmiotów publicznych, w tym zgodnie z projektowanym art. 4 pkt 6 do organów publicznych. Przedmiotowy projekt ustawy nie definiuje, co należy rozumieć pod pojęciem świadczenia usługi w kontekście proponowanych w projekcie rozwiązań dotyczących organów publicznych. Warto zauważyć, że obowiązująca ustawa z dnia z dnia 4 marca 2010 r. o świadczeniu usług na terytorium Rzeczypospolitej Polskiej (Dz.U. z 2016 r. poz. 893, z późn. zm.) definiuje usługę jako „świadczenie wykonywane przez usługodawcę na własny rachunek, zwykle za wynagrodzeniem, w szczególności usługi budowlane, handlowe oraz usługi świadczone w ramach wykonywanego zawodu”, co nie odpowiada większości kompetencji organów publicznych. Zatem w naszej ocenie należałoby doprecyzować art.24 ust.1 oraz 25 pkt 8) projektu w kontekście pojęcia świadczenia usług przez ograny publiczne.	Uwaga uwzględniona.
142.	art. 24 ust. 1 i 2	Kancelaria Sejmu RP	W art. 24 w ust. 1 i 2 należy ujednolicić terminologię w zakresie użycia zwrotów „osoby” (ust. 1) oraz „jedną osobę” (ust. 2).	Uwaga nieuwzględniona. W ust. 2 celowo użyto sformułowania „jedna osoba” dla podkreślenia, że JST nie muszą wyznaczać osób odpowiedzialnych za cyberbezpieczeństwo w każdej ze swoich jednostek organizacyjnych.

143.	art. 24 ust. 2	Biuro Bezpieczeństwa Narodowego	Wydaje się, że zapewnienie cyberbezpieczeństwa jednostek samorządu terytorialnego zostało potraktowane zbyt powierzchownie. W art. 24 ust. 2 wskazuje się, że jednostki samorządu terytorialnego mogą wyznaczyć jedną osobę odpowiedzialną za cyberbezpieczeństwo usług świadczonych przez ich jednostki organizacyjne. Proponuje się, aby wyznaczenie było obligatoryjne i aby nie ograniczać jednostek samorządu co do liczby osób zajmujących się cyberbezpieczeństwem usług. Ponadto należy wskazać, że jednostki samorządu terytorialnego objęte są zapisami art. 24 ust. 1 Gest o nich bowiem mowa w art. 4 pkt 12), a zatem istnieją wątpliwości co do potrzeby istnienia ust. 2 omawianego art. 24.	Uwaga nieuwzględniona. JST mają obowiązek powołania osoby odpowiedzialnej za cyberbezpieczeństwo, przy czym, zgodnie z ust. 2 mogą powołać jedną osobę dla wszystkich swoich jednostek organizacyjnych.
144.	art. 25 ust. 8	Narodowy Bank Polski	W art. 25 pkt 8 projektu zawarto przepis określający konieczność zapewnienia „użytkownikowi usługi dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami”, ze względu na brak określenia kto to jest „użytkownik” i jakiego systemu informatycznego jest użytkownikiem, sugerujemy doprecyzowanie powyższego przepisu. Ponadto zwracamy również uwagę, że posłużenie się przez projektodawcę nieprecyzyjnie zdefiniowanymi pojęciami, jak „wiedza”, „zapewnianie dostępu do wiedzy”, może spowodować wzrost zapytań kierowanych do NBP (niekoniecznie merytorycznych) dotyczących kwestii związanych z cyberbezpieczeństwem w NBP, na które – zgodnie ze wspomnianymi przepisami – NBP będzie zobligowany do udzielenia odpowiedzi. W skrajnych przypadkach może to generować dla NBP ryzyko związane z koniecznością poświęcania znacznej ilości czasu na obsługę ww. zapytań, jak również ryzyko, że podmioty zewnętrzne będą oczekiwać od NBP udzielania informacji, które z punktu widzenia centralnego banku państwa mogą być uznawane za wrażliwe (potencjalnie może to dotyczyć również „wiedzy” NBP w zakresie funkcjonowania nadzorowanych podmiotów i systemów tworzących infrastrukturę systemu finansowego). Wymaganie to jest także ujęte w art. 15 ust. 1 pkt 2 projektu w odniesieniu do operatorów usług kluczowych, w związku z czym każdy użytkownik usługi kluczowej miałby zapewniony, zgodnie z projektowaną	Uwaga nieuwzględniona.

			ustawą, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa.	
145.	art. 25 pkt 8	Polska Akademia Nauk	Z przyczyn opisanych wyżej w pkt 6 obowiązek zapewnienia skutecznych sposobów zabezpieczenia przed zagrożeniami nie zawsze będzie możliwy do zrealizowania nawet z zachowaniem profesjonalnej staranności.	Wyjaśnienie. Wskazane jest, aby działania tego typu były prowadzone zgodnie z zasadą należytej staranności. Wystarczające będzie, zgodnie z literalnym brzmieniem przepisu, podawanie adekwatnych i zrozumiałych informacji, dostosowanych do przeciętnego użytkownika i dotyczących danej usługi. Przykładowo, może to być przystępnie przedstawiona polityka bezpiecznych haseł, ogólne zasady bezpiecznego korzystania z serwisu przedsiębiorcy czy też wysyłanie ostrzeżeń antyphishingowych.
146.	art. 27	Komisja Nadzoru Finansowego	Projekt nakazuje aby do podmiotu publicznego, wobec którego wydana została decyzja o uznaniu za operatora usługi kluczowej, stosować przepisy rozdziału 2 Projektu. Tym samym, do tych podmiotów zastosowanie znajdzie dyspozycja art. 16 ust. 1 Projektu, nakazująca przeprowadzenia co najmniej raz na dwa lata audytu bezpieczeństwa teleinformatycznego. Wejście w życie regulacji Projektu (ustawowej) może powodować konieczność wyjaśnienia relacji pomiędzy nakazem ustawowym a dyspozycją rozporządzenia z dnia 12 kwietnia 2012 r. lub ewentualnej zmiany tego ostatniego. Rozporządzenie z dnia 12 kwietnia 2012 r. nakazuje bowiem, w przypadku podmiotów realizujących zadania publiczne w minimalnych wymaganiach dla systemów teleinformatycznych, przeprowadzanie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.	Uwaga uwzględniona. Zostanie dodany przepis, który pozwoli na uznanie, że audyt z § 20 rozporządzenia o KRI spełnia wymogi określone w art. 16 ust. 2 projektu w odniesieniu do podmiotu publicznego, który jest operatorem usługi kluczowej.
147.	art. 27	Kancelaria Sejmu RP	Należy rozważyć skreślenie art. 27 jako oczywistego.	Wyjaśnienie. Ze względu na liczne uwagi zgłaszane w trakcie konsultacji do tego przepisu jak i szerzej do statusu operatorów usług kluczowych będących podmiotami publicznymi, zasadnym wydaje się utrzymanie tego przepisu celem wyjaśnienia ewentualnych sytuacji spornych.

148.	art. 27	Narodowy Bank Polski	Przepis art. 27 projektu stanowi, że „Do podmiotu publicznego, o którym mowa w art. 4 pkt 6-14, wobec którego wydana została decyzja o uznaniu za operatora usługi kluczowej, stosuje się przepisy rozdziału 2". Taka konstrukcja budzi zastrzeżenia, bowiem nie są zrozumiałe ewentualne potencjalne okoliczności uzasadniające wydanie takiej decyzji wobec NBP. Co więcej, podtrzymanie takiej konstrukcji prawnej może oddziaływać na niezależność NBP, co zostało zasygnalizowane w uwadze ogólnej. Proponujemy zatem modyfikację przepisu w taki sposób, aby wyłączyć NBP z podmiotów decyzji o uznaniu za operatora usługi kluczowej. Wydaje się to zasadne mając na uwadze, iż to organ właściwy, zgodnie z art. 39 ust. 1 pkt 2 projektu, wydaje decyzję o uznaniu za operatora usługi kluczowej, co oznaczałoby, że wobec centralnego banku państwa ustawa wprowadzałaby konstrukcję swoistego nadzoru kompetencyjnego, co może budzić wątpliwości natury konstytucyjnej. Dodatkowo, zgodnie z art. 4 projektu, bank centralny został explicite wskazany jako podmiot będący elementem krajowego systemu cyberbezpieczeństwa, a zatem wprowadzenie możliwości zmiany statusu NBP na podstawie art. 27 projektu budzi poważne wątpliwości.	Wyjaśnienie. NBP nie będzie operatorem usługi kluczowej.
149.	art. 28 [uwaga do rozdz. 5]	Rada do Spraw Cyfryzacji	Znaczna cześć regulacji w tym rozdziale jest konsekwencją przyjętej koncepcji 3 różnych ośrodków CSIRT. Skutkuje to koniecznością regulowania ich wzajemnych relacji oraz szczegółowego podziału kompetencji. Przewidziano np. sytuacje zgłoszeń do niewłaściwego CSIRT i przekazywania ich dalej, co wydłuży procedurę. Niejasne jest forsowanie koncepcji 3 odrębnych struktur, przy jednoczesnym zapisaniu możliwości wzajemnego powierzania sobie zadań – art. 28 ust. 10. Art. 36 uwypukla inny aspekt rozproszenia obszarów kompetencji między 3 ośrodki – w przypadku poważnego incydentu na styku wszystkich ośrodków, powstaną 3 niezależne analizy potencjalnych skutków incydentu. Art. 37 explicite pokazuje niewydolność takiego rozwiązania, ustanawiając strukturę nadrzędna nad trzema CSIRT, o niesprecyzowanych ostro kompetencjach - szczególnie wobec poszczególnych CSIRT; a także rozbudowując procedury	Uwaga nieuwzględniona. Sposób realizacji zadań i współpracy oraz właściwości CSIRT poziomu krajowego został określony w ustawie. Obecny model został zaproponowany przez CSIRT poziomu krajowego w ramach uzgodnień roboczych.

			uzgadniania stanowisk, decyzji i działań. Jednocześnie proponowane są rozwiązania blokujące, które mogą doprowadzić do paraliżu tego ciała – np. „Zespół na posiedzeniu: 1) wyznacza jednomyślnie CSIRT koordynujący obsługę incydentu”.	
150.	art. 28	Prokuratoria Generalna	Projektowana ustawa wprowadza regulację Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego określane również jako CSIRT. Wyróżnia trzy takie zespoły prowadzone odpowiednio przez Ministerstwo Obrony Narodowej (CSIRT MON), Państwowy Instytut Badawczy (CSIRT NASK) oraz Szefa Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV). Mając na względzie regulację powyższych zespołów, obsługa lub koordynacja obsługi zgłoszeń Prokuratorii Generalnej powinny być objęta zadaniami CSIRT GOV (art. 28 ust. 7 projektowanej ustawy). Niemniej jednak regulacja podmiotów, których zgłoszenia są obsługiwane i koordynowane przez CSIRT NASK (art. 28 ust. 6 projektowanej ustawy) jest na tyle szeroka, że również obejmuje podmioty takie, jak Prokuratoria Generalna. Otóż kwalifikację podmiotu wskazaną art. 28 ust. 6 pkt 1 lit. d projektowanej ustawy obejmuje m.in. Prokuratorię Generalną, z tego względu, że Prezes Rady Ministrów sprawuje nadzór nad działalnością administracji rządowej nieobjętą zakresem działów administracji rządowej, wykonywaną przez Prokuratorię Generalną Rzeczypospolitej Polskiej (art. 33a ust. 1 pkt 17 ustawy z dnia 4 września 1997 r. o działach administracji rządowej). Tym samym wskazane byłoby wprowadzenie odpowiednich zmian do projektu ustawy celem przypisania obsługi i koordynacji obsługi incydentów zgłaszanych przez Prokuratorię Generalną wyłącznie do zadań CSIRT GOV.	Wyjaśnienie. Podział podmiotowy został określony przez CSIRT w drodze uzgodnień roboczych poprzedzających projekt ustawy. Podział wynika z dotychczasowych doświadczeń CSIRT w zakresie obsługi incydentów i zakłada optymalizację obsługi incydentów.
151.	art. 28. ust. 2	Kancelaria Sejmu RP	W art. 28 w ust. 2 w zdaniu drugim zabrakło podmiotu tego zdania, zapewne chodzi o „CSIRT MON, CSIRT NASK i CSIRT GOV”, analogicznie jak w zdaniu pierwszym.	Uwaga do uzgodnienia z RCL.
152.	art. 28. ust. 3. pkt 9	Ubezpieczeniowy Fundusz Gwarancyjny	Wydaje się zasadne, aby Ustawodawca doprecyzował w jakich okolicznościach, przy uwzględnieniu jakich kryteriów CSIRT może dokonać zmiany klasyfikacji Incydentów.	Wyjaśnienie. Zmiana klasyfikacji incydentów będzie wynikać z informacji pozyskanych w drodze analizy incydentu. Kryteria klasyfikacji incydentów są określone w ustawie.

153.	art. 28. ust. 5. pkt 2	Prokuratoria Generalna	Wątpliwości Prokuratorii Generalnej w szerszej perspektywie budzi regulacja zakresu obsługi i koordynacji obsługi incydentów przez CSIRT MON. Zespół ten zobowiązany jest bowiem obsługiwać incydenty zgłaszane przez podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane (art. 28 ust. 5 pkt 1 projektu ustawy). Projekt ustawy wyszczególnia jednak dodatkowo w art. 28 ust. 5 pkt 2 określoną grupę podmiotów podległych MON lub przez niego nadzorowanych, których zgłoszenia również obsługuje CSIRT MON. Z analizy przepisu wynika, że zbiór podmiotów ujętych art. 28 ust. 5 pkt 2 jest w całości zawarty w zbiorze podmiotów wymienionych w art. 28 ust. 5 pkt 1, skutkiem czego art. 28 ust. 5 pkt 2 wydaje się zbędny.	Uwaga nieuwzględniona. Art. 28 ust. 5 pkt 2 ma na celu stworzenie przepisu wyodrębniającego infrastrukturę krytyczną będącą w zarządzie MON (por. art. 28 ust. 7 pkt 12).
154.	art. 28 ust. 5-7	Generalny Inspektor Ochrony Danych Osobowych	Odnosząc się do wyliczeń z art. 28 ust. 5-7 projektu należy poddać w wątpliwość, czy wszystkie organy administracji publicznej są objęte obsługą lub koordynacją obsługi incydentów. W szczególności dotyczy to organów administracji publicznej niezależnych od administracji rządowej. Wyczerpujące określenie tych katalogów pozwoli uniknąć wątpliwości przy przekazywaniu zgłoszeń do właściwego CSIRT, czego dotyczy ust. 8 komentowanego artykułu	Uwaga nieuwzględniona. Podział obowiązków i właściwości CSIRT wynika z ustaleń CSIRT poziomu krajowego poczynionych w czasie uzgodnień roboczych.
155.	art. 28 w ust. 6 w pkt 1 w lit. a	Kancelaria Sejmu RP	Należy rozważyć zsynchronizowanie treści zawartej w art. 28 w ust. 6 w pkt 1 w lit. a z brzmieniem art. 4 pkt 14. W tym ostatnim przepisie mamy do czynienia z wyłączeniem z sytemu cyberbezpieczeństwa państwowych osób prawnych będących przedsiębiorstwami, bankami lub spółkami prawa handlowego, natomiast w art. 28 w ust. 6 w pkt 1 w lit. a, są one objęte zadaniami CSIRT NASK polegającymi na obsłudze lub koordynacji obsługi incydentów.	Uwaga uwzględniona. Art. 28 ust 6 pkt 1 lit a zostanie zmieniony tak, aby był zgodny z art. 4 pkt 14.
156.	art. 28. ust. 6. pkt 1 lit. p	Ubezpieczeniowy Fundusz Gwarancyjny	Jakie inne podmioty zostały uwzględnione przez Ustawodawcę w tym zakresie?	Wyjaśnienie. Zgodnie z literalnym brzmieniem przepisu, będą to wszelkie podmioty, niewymienione w art. 28 ust. 6 pkt 1 lit. a-o oraz ust. 5 i 7.

157.	art. 28 ust. 7	Biuro Bezpieczeństwa Narodowego	W art. 28 ust. 7 do listy podmiotów zgłaszających incydenty do CSIRT GOV należałoby dopisać- obok Kancelarii Prezydenta RP - także Biuro Bezpieczeństwa Narodowego.	Uwaga uwzględniona.
158.	art. 28 ust. 7 pkt 12	Narodowy Bank Polski	Z projektowanego art. 28 ust. 7 pkt 12 wynika, że „Do zadań CSIRT GOV należy obsługa lub koordynacja obsługi incydentów zgłaszanych przez inne niż wymienione w pkt 1-11 oraz ust. 5 pkt 2 i 3 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne są wpisane do jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym”. Z przepisu tego nie wynika jednoznacznie, co miałaby oznaczać „obsługa” zgłaszanych incydentów oraz w jaki sposób miałaby być realizowana. Jest to istotne ze względu na fakt, że przepis ten odnosiłby się również do incydentów zgłaszanych do NBP przez podmioty podlegające nadzorowi systemowemu przez Prezesa NBP na mocy przepisów ustawy z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami (Dz. U. z 2016 r., poz. 1224). W efekcie tej ustawy, incydenty w systemach płatności są analizowane przez NBP w ramach sprawowania nadzoru systemowego w zakresie systemu płatniczego, a mając na uwadze art. 28 ust. 7 pkt 12 projektu, powstałaby konstrukcja w której istniałyby 2 ośrodki, NBP i CSIRT GOV, które niezależnie od siebie analizowałyby incydenty i ich skutki. W efekcie, sytuacja ta mogłaby powodować powstanie niejednolitego podejścia obu instytucji w zakresie oceny skutków incydentów, co byłoby niepożądane.	Wyjaśnienie. Obsługa incydentu świadczona przez CSIRT będzie się odnosiła wyłączenie do kondycji systemów informacyjnych w rozumieniu projektu ustawy, a nie do systemu płatności w rozumieniu ustawy o ostateczności rozrachunku.
159.	art. 28 ust. 9	Kancelaria Sejmu RP	W art. 28 w ust. 9 użyto sformułowania nieznanego ustawie z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077) „umowa dotacji podmiotowej”, w związku z powyższym należałoby raczej posłużyć się odesłaniem do właściwego przepisu tej ostatniej ustawy.	Uwaga uwzględniona Mając na uwadze art. 126 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2070), zauważyć należy, że tryb oraz zasady udzielania i rozliczania dotacji, określane są w umowie zawartej z beneficjentem.

				Zadania będą finansowane ze środków budżetu państwa w formie dotacji udzielanej przez ministra właściwego do spraw informatyzacji. Odpowiednio modyfikacja art. 28 ust. 9 i 43 ust.2 projektu ustawy.
160.	art. 28 ust. 9	Prokuratoria Generalna	Odnośnie do zadań CSIRT NASK art. 28 ust. 9 projektowanej ustawy przewiduje, że zadania CSIRT NASK są finansowane z części budżetu, której dysponentem jest minister właściwy do spraw informatyzacji na podstawie dotacji podmiotowej. Zgodnie z art. 131 ustawy o finansach publicznych „[d]otacje podmiotowe obejmują środki dla podmiotu wskazanego w odrębnej ustawie lub w umowie międzynarodowej, wyłącznie na dofinansowanie działalności bieżącej w zakresie określonym w odrębnej ustawie lub umowie międzynarodowej". W konsekwencji dotacja podmiotowa ma taki charakter, że jest skonkretyzowana tylko podmiotowo, nie zaś przedmiotowo – otrzymane środki dany podmiot może wykorzystać na cele przez siebie wybrane w granicach własnej działalności. Mając na względzie zasady odpowiedzialności za naruszenie dyscypliny finansów publicznych, obowiązkiem otrzymującego dotację jest jej rozliczenie, zaś udzielający dotacji ma obowiązek żądać od beneficjenta przedstawienia rozliczenia udzielonej dotacji. Nierozliczenie przekazanej dotacji lub nieterminowe jej rozliczenie przez udzielającego dotację stanowi naruszenie dyscypliny finansów publicznych (art. 8 ustawy z 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych). W konsekwencji Prokuratoria Generalna zwraca uwagę na potrzebę rozważania uregulowania dotacji, o której mowa w projekcie ustawy, jako dotacji podmiotowo-przedmiotowej, a następnie uregulowania w umowie dotacji z CSIRT NASK (art. 28 ust. 9 projektu ustawy) zasad rozliczenia dotacji i wyposażenie ministra właściwego do spraw informatyzacji, z którego części budżetu dotacja jest udzielana, w narzędzia służące egzekucji i kontroli poprawności dokonanych rozliczeń.	Uwaga uwzględniona Mając na uwadze art. 126 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2070), zauważyć należy, że tryb oraz zasady udzielania i rozliczania dotacji, określane są w umowie zawartej z beneficjentem. Zadania będą finansowane ze środków budżetu państwa w formie dotacji udzielanej przez ministra właściwego do spraw informatyzacji. Odpowiednio modyfikacja art. 28 ust. 9 i 43 ust.2 projektu ustawy.

161.	art. 28 ust. 10	Narodowy Bank Polski	W proponowanym art. 28 ust. 10 wskazano, że „CSIRT MON, CSIRT NASK i CSIRT GOV mogą w drodze porozumienia powierzyć sobie wzajemnie wykonywanie zadań, w stosunku do niektórych rodzajów podmiotów, o których mowa w ust. 5-7. O zawarciu porozumienia CSIRT, który powierzył wykonywanie zadań, informuje podmioty, w stosunku do których nastąpiła zmiana CSIRT”. Należy zauważyć, iż zakres ten obejmuje NBP oraz m.in. Krajową Izbę Rozliczeniową, nad którą nadzór sprawuje NBP w ramach systemów płatności, co generuje ryzyko wzajemnego przekazywania - bez wiedzy i zgody NBP - informacji wrażliwych, za jakie należałoby uznać szczegóły poważnych, istotnych oraz krytycznych incydentów odnotowywanych przez NBP lub Krajową Izbę Rozliczeniową. Jest to o tyle istotne, że zgodnie z art. 36 ust. 5 projektu „CSIRT MON, CSIRT NASK i CSIRT GOV mogą przekazywać do publicznej wiadomości informacje o incydentach oraz o zagrożeniach, w niezbędnym zakresie, o ile przekazywanie informacji przyczyni się do zwiększenia cyberbezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów”. W efekcie, przepis określa przesłankę do przekazywania przez CSIRT - bez porozumienia z podmiotem, którego te informacje dotyczą - do opinii publicznej informacji o incydentach, które nie zostały precyzyjnie zdefiniowane, a które – ze względu na zadania centralnego banku państwa podlegają nadzorowi systemowemu Prezesa NBP – mogą skutkować ujawnieniem informacji o istotnym znaczeniu dla stabilności systemu finansowego. Proponujemy stosowną modyfikację przepisu, aby uniknąć wskazanego powyżej ryzyka ujawnienia informacji, których skutek upublicznienia mógłby potencjalnie wpłynąć na sytuację gospodarczą Polski.	Wyjaśnienie. Wszystkie CSIRT będą stosowały podobne procedury w zakresie obsługi incydentów i będą miały te same zadania, obowiązki i ograniczenia wynikające z ustawy. Tym samym wskazane obawy wydają się nieuzasadnione.
162.	art. 28 ust. 11	Narodowy Bank Polski	W art. 28 ust. 11 projektu zawarto odesłanie do „ust. 8” zamiast do „ust. 10”.	Uwaga uwzględniona.

163.	art. 29 ust. 1 i 2	Służba Kontrwywiadu Wojskowego	W art. 29 ust. 1 i 2 nie uwzględniono uprawnień zarezerwowanych dla SKW zgodnie z art. 5 ust. 1 pkt 2a ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2017 r. poz. 1978). SKW proponuje dopisać tę treść do projektowanego brzmienia art. 29 ust. 1 i 2.	Uwaga może zostać uwzględniona po przekazaniu propozycji uzgodnionej z ABW (kwestie podziału kompetencji z art. 29).
164.	art. 30 ust. 4	Generalny Inspektor Ochrony Danych Osobowych	Wyciąg analogicznie do uwagi nr … w związku z art. 3 ust. 3.	Uwaga częściowo uwzględniona. Projekt zostanie uzupełniony poprzez wskazanie kanału komunikacji.
165.	art. 30 ust. 4	Kancelaria Senatu RP	Przesłanką publikacji przez właściwe organy informacji niezbędnej, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę trwającego incydentu albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym, jest przeprowadzenie konsultacji z operatorem usługi kluczowej albo dostawcą usług cyfrowych (art. 30 ust. 4 i art. 31 ust. 2). W przypadku braku współpracy ze strony operatora lub dostawcy usługi, publikacja będzie niemożliwa. Dlatego należy zmodyfikować procedurę w sposób, który uniemożliwi blokowanie publikacji informacji ze względu na bierność podmiotów (np. wyznaczając termin na odpowiedz).	Uwaga nieuwzględniona. Konsultacja nie jest wiążąca.
166.	art. 31 ust. 2	Generalny Inspektor Ochrony Danych Osobowych	Wyciąg analogicznie do uwagi nr … w związku z art. 3 ust. 3.	Uwaga częściowo uwzględniona. Projekt zostanie uzupełniony poprzez wskazanie kanału komunikacji.
167.	art. 34. ust. 5	Ubezpieczeniowy Fundusz Gwarancyjny	Czy oznacza to, że w przypadku Incydentów zgłoszonych do CSIRT i noszących znamiona przestępstwa, podmiot świadczony usługę kluczową której dotyczy Incydent nie musi zgłaszać tego faktu do organów ścigania, a zgłoszeniem zajmie się CSIRT?	Wyjaśnienie. Niniejszy przepis nie zastępuje zawiadomienia o popełnieniu przestępstwa.
168.	art. 34. ust. 6	Ubezpieczeniowy Fundusz Gwarancyjny	Czy oznacza to, że w przypadku Incydentów zgłoszonych do CSIRT I dotyczących Danych Osobowych, podmiot świadczony usługę kluczową której dotyczy Incydent nie musi zgłaszać tego faktu do GIODO, a zgłoszeniem zajmie się CSIRT?	Wyjaśnienie. Niniejszy przepis nie znosi obowiązku notyfikacji do GIODO.

169.	art. 35	Generalny Inspektor Ochrony Danych Osobowych	W artykule zaproponowano, by CSIRT MON, CSIRT GOV i CSIRT NASK oraz dyrektor Rządowego Centrum Bezpieczeństwa oraz minister właściwy do spraw informatyzacji mogli przetwarzać szczególne kategorie danych w rozumieniu art. 9 ust. 1 tzw. ogólnego rozporządzenia o ochronie danych[1]. Należy poddać w wątpliwość konieczność przetwarzania takich informacji w związku z obsługą zgłoszeń incydentów przez podmioty zobowiązane. W uzasadnieniu na s. 25 wskazano jedynie, że w/w podmioty będą mieć uprawnienia do przetwarzania danych. Z dotychczasowej treści projektu nie wynika, by niezbędne było przetwarzanie innych niż zwykłe dane osobowe. W projekcie wskazano jedynie podstawowe dane identyfikacyjne i kontaktowe podmiotów zobowiązanych oraz ich pracowników. Propozycja jest zatem nieuzasadniona i nadmierna z punktu widzenia planowanych do realizacji zadań.	Uwaga nieuwzględniona. Co do zasady nie przewiduje się przetwarzania danych wrażliwych, jednak w przypadku sektora ochrony zdrowia może dojść do przetwarzania takich danych w związku z obsługą incydentu.
170.	art. 36 ust. 1	Kancelaria Sejmu RP	W art. 36 w ust. 1 należałoby rozważy określenie terminu na przekazywanie informacji o incydencie, który może spowodować wystąpienie sytuacji kryzysowej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.	Uwaga uwzględniona. Dodano termin „niezwłocznie”.
171.	art. 36 ust. 5	Generalny Inspektor Ochrony Danych Osobowych	Wyciąg analogicznie do uwagi nr … w związku z art. 3 ust. 3.	Uwaga częściowo uwzględniona. Projekt zostanie uzupełniony poprzez wskazanie kanału komunikacji.
172.	art. 36 ust. 5	Narodowy Bank Polski	W art. 36 ust. 5 projektu zawarto nieprecyzyjne określenie wskazujące na „niezbędny zakres”. Proponujemy rozważyć jego doprecyzowanie bądź zastąpienie innym, zgodnym z intencją projektodawcy.	Uwaga nieuwzględniona.
173.	art. 37 ust. 1	Polska Akademia Nauk	Z punktu widzenia kompetencji przypisanych w ust. 6, zwłaszcza w pkt 1 i pkt 2, nazywanie Zespołu „organem pomocniczym” nie jest zasadne. Zespół ten ma bowiem istotne i wyłączne kompetencje decyzyjne.	Uwaga do omówienia z RCL.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1), dalej zwane RODO.

174.	art. 37 ust. 6 pkt 1	Kancelaria Senatu RP	W art. 37 znalazły się przepisy dotyczące Zespołu ds. Incydentów Krytycznych. Zgodnie z art. 37 ust. 6 pkt 1 zespól wyznacza jednomyślnie jeden z Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) do koordynowania obsługi incydentu. Przyjęcie zasady jednomyślności może doprowadzić do paraliżu decyzyjnego. Praktyczniejszym rozwiązaniem jest stosowanie zasady większości przy podejmowaniu decyzji. Inną metodą jest wskazanie organu, który w przypadku braku jednomyślności ma glos rozstrzygający.	Uwaga nieuwzględniona. Zaproponowany model został wskazany jako preferowany przez CSIRT poziomu krajowego w drodze wspólnych ustaleń roboczych.
175.	art. 37. ust. 6 pkt 1	Polska Akademia Nauk	Wątpliwości budzi co będzie w sytuacji, gdy Zespół nie uzyska jednomyślności? Przyjęcie zasady jednomyślności wydaje się nieracjonalne.	Uwaga nieuwzględniona. Zaproponowany model został wskazany jako preferowany przez CSIRT poziomu krajowego w drodze wspólnych ustaleń roboczych.
176.	art. 37 ust. 6 pkt 3	Kancelaria Senatu RP	W art. 37 ust. 6 pkt 3 posłużono się wyrazem „decyzja" w kontekście, który jednoznacznie wskazuje na akt niebędący decyzji administracyjną. Ponieważ w ustawie wyraz „decyzja" występuje w znaczeniu nadawanym mu przez Kodeks postpowania administracyjnego, należy zastąpić go innym wyrazem. Ponadto przepis zdaje się sugerować, ze wystąpienie z wnioskiem w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego jest obowiązkiem Zespołu ds. Incydentów Krytycznych. Aby uniknąć wątpliwości, przepis należy sformułować w jednoznaczny sposób, rozstrzygając, czy wystąpienie jest obowiązkiem, czy uprawnieniem Zespołu ds. Incydentów Krytycznych.	Uwaga nieuwzględniona. Nie jest to decyzja administracyjna.
177.	art. 37 ust. 8	Kancelaria Senatu RP	W art. 37 ust. 8 zawarto przepis przyznający Zespołowi ds. Incydentów Krytycznych oraz Rządowemu Zespołowi Zarządzania Kryzysowego prawo wydawania „wiążących decyzji", dotyczących obsługi incydentu krytycznego. Wymaga wyjaśnienia, czy decyzje, o których mowa, są decyzjami w znaczeniu Kodeksu postpowania administracyjnego. Jeżeli nie są, należy użyć innego wyrazu niż rzeczownik „decyzja". W przypadku, gdy rozstrzygnięcia mają mieć charakter decyzji administracyjnych, niepotrzebne jest podkreślanie, ze są wiązce, gdyż ten przymiot wynika z istoty decyzji. Regulacja zawarta w art. 37 ust. 8 jest sprzeczna z charakterem Rządowego Zespołu Zarządzania Kryzysowego, który jest ciałem opiniodawczo-doradczym działającym przy Radzie	Uwaga nieuwzględniona. Nie jest to decyzja administracyjna.

			Ministrów (art. 8 ust. 1 i art. 9 ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarzadzaniu kryzysowym). Wobec czego Rządowy Zespól Zarządzania Kryzysowego nie powinien mieć władczych uprawnień, które mogłyby przysługiwać Prezesowi Rady Ministrów lub Radzie Ministrów. Ponadto przypadek, gdy dwa organy (tzn. Zespól ds. Incydentów Krytycznych oraz Rządowy Zespół Zarządzania Kryzysowego) mają identyczną właściwość rzeczową i miejscową nie jest optymalny ze względu na efektywność zarządzania oraz zasady postpowania administracyjnego.	
178.	art. 38 ust. 1	Kancelaria Sejmu RP	Należy rozważyć, czy organy właściwe wskazane w art. 38 ust. 1 obejmują wszystkie obszary cyberbezpieczeństwa? Zachodzą wątpliwości np. jaki organ będzie właściwym dla Sejmu lub Kancelarii Sejmu, w przypadku objęcia jednego z tych podmiotów statusem operatora usługi kluczowej? Czy w związku z powyższym w pkt 7 nie powinien obejmować zakresu niewymienionego w pkt 1-6?	Wyjaśnienie. Nie wszystkie obszary cyberbezpieczeństwa będą objęte ustawą, gdyż jest to niemożliwe. Ani Sejm, ani Kancelaria Sejmu nie będą operatorami usług kluczowych.
179.	art. 38 ust. 1	Biuro Bezpieczeństwa Narodowego	Brzmienie art. 38 ust. 1 i tytuł rozdziału 6 sugerują, że określono w nim katalog organów właściwych do spraw cyberbezpieczeństwa. W takim przypadku należałoby przyjąć, że pominięto w nim, w szczególności Ministra Obrony Narodowej i Szefa Agencji Bezpieczeństwa Wewnętrznego, a więc organy, którym podlega CSIRT MON i CSIRT GOV. Rozumiejąc intencję zapisów zawartych w rozdziale 6 projektu ustawy, zgodnie z którą przedmiotowe regulacje dotyczą jedynie ministrów odpowiedzialnych za sektory, w ramach których działają operatorzy infrastruktury krytycznej, proponuje się zmienić tytuł rozdziału 6 oraz treść art. 38 ust. 1, tak aby odpowiadały intencji projektodawcy.	Uwaga nieuwzględniona. Zadania organów właściwych dotyczą tylko operatorów usług kluczowych. MON ani ABW nie będą nadzorować ani kontrolować operatorów usług kluczowych.
180.	art. 39 ust. pkt 2	Rządowe Centrum Bezpieczeństwa	art. 39 ust. pkt 2 przewiduje, że organy właściwe wydają decyzję o uznaniu podmiotu za operatora usługi kluczowej. Zgodnie z art. 5b ust. 7 pkt 4 ustawy o zarządzaniu kryzysowym dyrektor RCB informuje o ujęciu w wykazie IK obiektów, instalacji lub urządzeń - ich właścicieli, posiadaczy samoistnych i zależnych, co powoduje powstanie obowiązków, o których mowa w art. 6 ust. 5 i 5a tej ustawy. Zakładane wykorzystanie usług krytycznych do identyfikacji usług kluczowych spowoduje podwójne działania podmiotów administracji w stosunku do tych samych podmiotów, będących operatorami IK i usług kluczowych.	Uwaga uwzględniona. Obowiązek prowadzenia rejestru zostanie przeniesiony na dyrektora RCB.

181.	art. 39 ust. 2	Kancelaria Senatu RP	Na podstawie art. 16 ust. 6 i art. 39 ust. 2 organy właściwe będą mogiły wydawać operatorom usług kluczowych wiążące polecenia, a na podstawie art. 39 ust. 2 będą mogły dodatkowo żądać przekazania określonych informacji. Wydaje się, ze celem przepisu było takie ukształtowanie procedury, aby wiążące polecenia i żądanie informacji następowały w drodze innej niż decyzje administracyjne. Egzekucja woli organu oraz możliwość obrony operatora miałyby być realizowane w trakcie postpowania w sprawie nałożenia kary administracyjnej (Wydaje się, ze wśród deliktów administracyjnych zawartych w art. 57 ust. 1 zabrakło niewykonania obowiązków wynikających z art. 39 ust. 2. Świadczy o tym fakt, ze podobne naruszenia przepisów art. 16 ust. 6 i art. 47 ust. 2 zostały wymienione w art. 57 ust. 1.). Ponieważ omawiane przepisy dotyczą postpowania przed organami administracji publicznej w należących do właściwości tych organów sprawach indywidualnych, należy wyraźnie wyłączyć możliwość wydania decyzji w rozumieniu Kodeksu postępowania administracyjnego, chyba ze celem projektodawców jest wydawanie decyzji administracyjnych w tych sprawach - w takim przypadku, ze względu na wyraźne podkreślenie formy wydania rozstrzygnięcia w innych przepisach ustawy (np. art. 5 ust. 1), wart. 16 ust. 6 i art. 39 ust. 2 również należałoby wyraźnie wskazać decyzję, jako tryb załatwienia sprawy.	Uwaga częściowo uwzględniona.
182.	art. 39 ust. 3	Urząd Dozoru Technicznego	W obecnym brzmieniu projekt ustawy, zgodnie z art. 39 ust. 3, umożliwia powierzenie realizacji niektórych zadań w imieniu organu właściwego jedynie jednostkom podległym lub nadzorowanym przez ten organ. Wydaje się jednak, że ograniczenie katalogu jednostek, którym organ właściwy mógłby powierzyć na podstawie porozumienia realizację niektórych zadań tworzy niepotrzebną barierę dla organów właściwych. Obecny zapis uniemożliwia organom właściwym wykorzystanie potencjału i możliwości jednostek, także będących podmiotami publicznymi, które mogłyby realizować niektóre zadania, a które nie są jednostkami nadzorowanymi lub podległymi, takim jak Urząd Dozoru Technicznego. Proponuje się zatem rozszerzyć organom właściwym możliwość na podstawie porozumienia delegowanie uprawnień innym	Uwaga nieuwzględniona.

			podmiotów publicznych posiadających wiedzę i doświadczenie z zakresu bezpieczeństwa, w tym z zakresu cyberbezpieczeństwa i zainteresowanych zapewnieniem ustanowienia kompleksowego, niezakłóconego systemu bezpieczeństwa teleinformatycznego państwa.	
183.	art. 42	Prokuratoria Generalna	Artykuł 42 projektu ustawy, w zamierzeniu jej projektodawców „zawiera regulacje dotyczące systemu teleinformatycznego prowadzonego przez ministra właściwego do spraw informatyzacji" (str. 27 uzasadnienia projektu ustawy). Określa on funkcjonalności tego systemu, jak również wskazuje, że zakresu uprawnień użytkowników określony zostanie w drodze rozporządzenia (por. art. 42 ust. 16 pkt 2 projektu ustawy). Powyższe jednak nie rozstrzyga kwestii dotyczących możliwości używania systemu teleinformatycznego, a dokładnie praw autorskich majątkowych do przedmiotów (utworów) składających się na ten system przez Skarb Państwa. Z projektu ustawy, jak również z jej uzasadnienia, nie wynika czy system teleinformatyczny będzie tworzonym we wysłanym zakresie przez Skarb Państwa, czy będzie systemem tworzonym na zamówienie. Z uwagi na konieczność zapewnienia maksymalnie swobodnego korzystania przez Skarb Państwa, reprezentowany przez ministra właściwego do spraw informatyzacji, z systemu teleinformatycznego zasadnym byłoby rozważanie, wprowadzania do projektu ustawy przepisów regulujących kwestię przynależności autorskich praw majątkowych do systemu teleinformatycznego po stronie Skarbu Państwa. Tytułem przykładu należy wskazać na regulację art. 74 ust. 3 ustawy o prawie autorskim i prawach pokrewnych , która przesądza, że autorskie prawa majątkowe do programu komputerowego stworzonego przez pracownika w wyniku wykonywania obowiązków ze stosunku pracy przysługują pracodawcy (o ile umowa z pracownikiem nie stanowi inaczej). W kierunku powyższych rozwiązań, tj. przyznających autorskie prawa majątkowe do programu komputerowego stworzonego nakładem określonego podmiotu i na rzecz tego podmiotu pozostaje przepis art. 175 f ustawy z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych , regulujący przyznanie Skarbowi Państwa uprawnień do programów komputerowych obsługujących sądowe systemy informatyczne. W analizowanym przypadku, przepis	Uwaga do dyskusji na konferencji uzgodnieniowej.

			projektowanej ustawy nie byłby tak daleko idący, gdyż odnosiłby się do konkretnego systemu teleinformatycznego (ewentualnie składających się na niego przedmiotów praw autorskich) w incydentalnym, opisanym w ustawie przypadku, a nie względem każdego programu komputerowego.	
184.	art. 42 ust. 7	Generalny Inspektor Ochrony Danych Osobowych	Wprowadzono wyjątek zwalniający administratora danych osobowych z obowiązków, o których mowa w art. 12-22 RODO. W opinii Generalnego Inspektora zwolnienie to bez wcześniejszego przeprowadzenia analizy skutków dla ochrony danych, o której mowa w art. 35 w związku z art. 23 ust. 2 RODO jest nieuzasadnione. Bez przeprowadzenia takiej analizy i wypełnienia pozostałych wymogów z art. 23 trudno jest przewidzieć, czy w systemie tym nie pojawią się dane osobowe w kontekście i sytuacji, o których osobę, której dotyczą nie należałoby poinformować. Kierunkowo, zauważyć należy, że przepis art. 23 RODO nie stanowi podstawy prawnej do całkowitego zwolnienia z obowiązków i praw w tym akcie wskazanych, a jedynie daje możliwość ich ograniczenia z zachowaniem zasad wynikających z tego przepisu. Powinno to być przedmiotem głębokiej analizy projektodawcy. W art. 42 ust. 8 projektu wskazano, iż w związku z funkcjonowaniem systemu teleinformatycznego dochodzić będzie do przetwarzania danych osobowych. W związku z tym Generalny Inspektor przyjmuje, iż w toku udostępniania upoważnionym podmiotom informacji, będzie dochodziło do przekazywania informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach. Z tego powodu konieczne jest precyzyjne wskazanie zakresu przetwarzanych danych oraz okresu ich retencji. Należy tutaj zauważyć, iż tzw. dyrektywa NIS[2] zawiera w motywie nr 72 oraz art. 2 postanowienia dotyczące stosowania przepisów o przetwarzaniu danych osobowych. Będzie to oznaczało stosowanie przepisów ustawy oraz w dalszej kolejności przepisów ustawy o ochronie danych i ogólnego rozporządzenia o ochronie danych. Koniecznym jest zatem precyzyjne wskazanie, jakie dane i jak długo będą w systemie przechowywane. Użycie określenia, iż są	Wyjaśnienie. Zostanie przeprowadzona analiza skutków dla ochrony danych w OSR. Zostanie także uzupełnione uzasadnienie oraz częściowo zostaną przeredagowane przepisy.

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. U. UE L z 2016 r. Nr 194, s. 1–30).

			„przechowywane wyłącznie przez okres niezbędny do realizacji zadań” nie jest prawidłowe.	
185.	art. 42. ust. 7	Ubezpieczeniowy Fundusz Gwarancyjny	Czy poprzez objęcie tym zakresem art. 22 projektodawca chciał wyłączyć możliwość profilowania? Jeśli tak to uwagę można uznać za niebyłą.	Wyjaśnienie. Projektodawca nie zakładał, że CSIRT będą profilować.
186.	art. 42. ust. 7	Prokuratoria Generalna	Prokuratoria Generalna dostrzega nieprawidłowości w treści art. 42 ust. 7 projektowanej ustawy, który stanowi, że przetwarzanie danych osobowych w systemie teleinformatycznym, o którym mowa w tym przepisie, nie wymaga realizacji obowiązków określonych w art. 12-22 rozporządzenia 2016/679. Odnośnie do treści tego przepisu Prokuratoria Generalna w pierwszej kolejności wskazuje na wadliwe powołanie aktu prawnego, jakim jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) . Ponadto Prokuratoria Generalna zwraca uwagę, że art. 23 ust. 1 rozporządzenia 2016/679 zezwala na ograniczenie aktem prawnym zakresu obowiązków i praw przewidzianych m. in. w jego art. 12–22. Powyższe oznacza, że ustawodawca nie jest uprawniony do wyłączenia w przepisach krajowych określonych obowiązków wynikających z rozporządzenia, ma jedynie prawo je ograniczyć. Tym samym zwolnienie ze wskazanych w wyżej przywołanym rozporządzeniu obowiązków w przypadku przetwarzania danych w systemie teleinformatycznym, o jakim mowa w art. 42 projektowanej ustawy, należy uznać za rozwiązania prawne zbyt daleko idące.	Uwaga nieuwzględniona. Zgodnie z zasadami techniki prawodawczej, nie jest konieczne powtórne przywoływanie pełnej nazwy aktu prawnego. Rozporządzenie 2016/679 pojawia się wcześniej w tekście projektu (art. 35). Jeśli pojawił się inny błąd, konieczne jest wskazanie, na czym polega wadliwe wskazanie aktu prawnego. Druga część uwagi do dyskusji na konferencji uzgodnieniowej.
187.	art. 42 ust. 10	Służba Kontrwywiadu Wojskowego	W treści art. 42 ust. 10 proponuje się ujednolicenie określenia przywołanych tam podmiotów poprzez wpisanie w odpowiednich punktach „Agencji Bezpieczeństwa Wewnętrznego” oraz „Agencji Wywiadu” oraz wpisanie „Służby Kontrwywiadu Wojskowego” i „Służby Wywiadu Wojskowego” w oddzielnych punktach.	Uwaga uwzględniona.

188.	art. 42 ust. 10	Urząd Regulacji Energetyki	Sugeruję rozważenie dodania do wykazu podmiotów, którym udostępnia się informacje również Prezesa Urzędu Regulacji Energetyki. Nie uwzględnienie Regulatora w tym przepisie powodować może utrudnienia w realizacji ustawowych zadań tego organu.	Uwaga nieuwzględniona. URE nie posiada zadań ustawowych określonych w projekcie.
189.	art. 42 ust. 13	Rada do Spraw Cyfryzacji	RdC sugeruje zmianę „mogą być udostępniane" na „są udostępniane na wniosek".	Uwaga uwzględniona.
190.	art. 42 ust. 14	Rada do Spraw Cyfryzacji	Dostęp do systemu teleinformatycznego służącego do zgłaszania incydentów powinien być udostępniany każdemu podmiotowi związanemu Ustawą.	Wyjaśnienie. Projekt przewiduje, że dostęp do systemu teleinformatycznego służącego do zgłaszania incydentów mają wszystkie podmioty krajowego systemu cyberbezpieczeństwa.
191.	art. 43 ust. 2	Kancelaria Sejmu RP	W art. 43 w ust. 2 użyto sformułowania „umowa dotacji", wydaje się, iż należałoby raczej posłużyć się odesłaniem do właściwego przepisu ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych.	Uwaga uwzględniona. Mając na uwadze art. 126 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2070), zauważyć należy, że tryb oraz zasady udzielania i rozliczania dotacji, określane są w umowie zawartej z beneficjentem. Zadania będą finansowane ze środków budżetu państwa w formie dotacji udzielanej przez ministra właściwego do spraw informatyzacji. Odpowiednio modyfikacja art. 28 ust. 9 i 43 ust.2 projektu ustawy.
192.	art. 47 [uwaga do rozdz. 8]	Ubezpieczeniowy Fundusz Gwarancyjny	Rozdział 8 szczegółowo opisuje zagadnienia związane z czynnościami kontrolnymi wobec podmiotów będących przedsiębiorcami. Brakuje opisu (tak jak w przypadku podmiotu będącego przedsiębiorcą) zagadnienia związanego z czynnościami kontrolnymi wobec podmiotów nie będących przedsiębiorcami.	Wyjaśnienie. Zgodnie z art. 48 ust. 2 pkt 2 wobec podmiotów niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. poz. 1092).
193.	art. 47 [uwaga do rozdz.	Kancelaria Sejmu RP	W związku z treścią rozdziału 8 „Nadzór i kontrola" zachodzi wątpliwość, czy w przypadku gdy Kancelaria Sejmu albo Sejm będą operatorami usług kluczowych, a będzie to rozstrzygane w rozporządzeniu, nie dojdzie do naruszenia zasady trójpodziału	Wyjaśnienie. Ani Sejm, ani Kancelaria Sejmu nie będą operatorami usług kluczowych, gdyż nie mieszczą się w żadnym

	8]		władzy, poprzez to, iż organ administracji rządowej będzie nadzorował i kontrolował władzę ustawodawczą, a także np. zobowiązywał do usunięcia nieprawidłowości i nakładał kary pieniężne.	sektorze określonym w załączniku do projektu.
194.	art. 49	Ubezpieczeniowy Fundusz Gwarancyjny	Czy Ustawodawca przewiduje (w przypadku podejrzenia wystąpienia, wykrycia nieprawidłowości) podczas kontroli zabezpieczenie elektronicznego materiału dowodowego przez osobę kontrolującą? Jeśli tak, to wydaje się zasadne aby Ustawodawca zdefiniował zasady na jakich taka czynność może się odbyć?	Uwaga nieuwzględniona. Nie jest zasadne szczegółowe określanie praktycznych zasad przeprowadzania poszczególnych czynności podczas kontroli.
195.	art. 49 pkt 1	Rada do Spraw Cyfryzacji	„Zapewnienie osobie prowadzącej czynności kontrolne swobodnego wstępu i poruszania się bez przepustki po terenie podmiotu kontrolowanego" – w wielu przypadkach nie wydaje się to realne. W firmach istnieją systemy kontroli dostępu, dodatkowo działanie kontrolowanego podmiotu może dotyczyć branży, w której do samodzielnego poruszania po terenie zakładu, wymagana jest znaczna wiedza i znajomość prowadzonej działalności wraz z przeszkoleniem (np. petrochemia, przedsiębiorstwa energetyczne itp.). Powinno być zapisane, że podmiot kontrolowany zapewni swobodny wstęp, a to w jakiej to zrobi formie (np. pracownik merytoryczny opiekujący się osobą kontrolującą) to kwestia organizacyjna. Prawo do swobodnego poruszania się po kontrolowanym obiekcie jest sprzeczne z podstawowymi wymogami bezpieczeństwa serwerowni.	Wyjaśnienie. Przepis nie wyklucza stosowania wewnętrznych procedur obowiązujących w firmach. Ma on jedynie zapewnić kontrolerowi swobodny wstęp i zapobiec sytuacji, w której zostanie odmówiony wstęp osobie kontrolującej ze względu na brak posiadania przepustki.
196.	art. 49. pkt 1	Ubezpieczeniowy Fundusz Gwarancyjny	Poruszanie się po terenie podmiotu kontrolowanego i podejmowanie czynności kontrolnych tak jak w przypadku innych kontroli, audytów powinno być realizowane przy udziale przedstawiciela kontrolowanego podmiotu (domyślnie może to być Pracownik odpowiedzialny za cyberbezpieczeństwo świadczonych usług kluczowych). Poruszanie się po obiekcie i podejmowanie działań kontrolnych bez przepustki, identyfikatora, asysty przedstawiciela podmiotu kontrolowanego nie jest zgodne z wymogami bezpieczeństwa fizycznego i środowiskowego np. zgodnie z normą ISO27001:2013. Dodatkowo, obecny zapis w praktyce może nie być skuteczny w związku ze stosowaniem przez większość podmiotów Systemu	Wyjaśnienie. Przepis nie wyklucza stosowania wewnętrznych procedur obowiązujących w firmach. Ma on jedynie zapewnić kontrolerowi swobodny wstęp i zapobiec sytuacji, w której zostanie odmówiony wstęp osobie kontrolującej ze względu na brak posiadania przepustki.

			Kontroli Dostępu (SKD) oraz kart dostępowych i ograniczeń w dostępie do wybranych pomieszczeń i przestrzeni biurowej poprzez wydzielenie stref dostępowych.	
197.	art. 49. pkt 1	Polska Akademia Nauk	Prawo wstępu bez wydania przepustki nie jest akceptowalne, zważywszy na fakt istnienia zabezpieczeń systemów, zarówno formalnych, jak i techniczno-organizacyjnych.	Wyjaśnienie. Przepis nie wyklucza stosowania wewnętrznych procedur obowiązujących w firmach. Ma on jedynie zapewnić kontrolerowi swobodny wstęp i zapobiec sytuacji, w której zostanie odmówiony wstęp osobie kontrolującej ze względu na brak posiadania przepustki.
198.	art. 49 pkt 6	Ubezpieczeniowy Fundusz Gwarancyjny	Ustawodawca wprowadza termin oględzin urządzeń, nośników oraz systemów informacyjnych, jednak zakres czynności w ramach ""oględzin"" nie został doprecyzowany. Wydaje się zasadne aby Ustawodawca doprecyzował ten termin. Czy w sformułowaniu oględziny zawiera się również dostęp do Systemu na poziomie administratora (co wiąże się z założeniem konta dla osoby prowadzącej czynności kontrolne i nadanie uprawnień zgodnie z obowiązującą w danej organizacji Procedury)? Należy mieć na uwadze, że założenie konta i nadanie uprawnień będzie wymagało stosownych zgód po stronie podmiotu kontrolowanego.	Uwaga nieuwzględniona. Termin „oględziny” wydaje się dobrze ukonstytuowany w polskim prawie i nie ma potrzeby jego doprecyzowania. Co do zasady, czynności na samym systemie wykonuje pracownik jednostki kontrolowanej, który przekazuje informacje kontrolującemu.
199.	art. 50 ust. 1	Rada do Spraw Cyfryzacji	Konieczne jest wprowadzenie ograniczenia informacji pozyskiwanych na nośnikach cyfrowych do informacji związanych bezpośrednio z bezpieczeństwem danego systemu informatycznego.	Wyjaśnienie. Dostęp do informacji ma być zapewniony w zakresie niezbędnym do przeprowadzenia kontroli.
200.	art. 50 ust. 1	Ubezpieczeniowy Fundusz Gwarancyjny	Co Ustawodawca rozumie pod pojęciem udostępniania niezbędnych urządzeń technicznych, w jakim zakresie ma nastąpić udostępnienie? Podmiot kontrolowany powinien mieć możliwość (w uzasadnionych przypadkach np. związanych z ochroną tajemnicy przedsiębiorstwa) na odmowę wykonania kopii informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach informacyjnych. Pisemna odmowa wraz z uzasadnieniem powinna zostać przekazana kontrolującymi w terminie do końca trwania bieżącej kontroli.	Wyjaśnienie. Urządzenia techniczne mają być udostępnione, zgodnie z treścią przepisu, w zakresie niezbędnym do wykonania kontroli. Podobna zasada dotyczy dostępu do informacji – dostęp do nich ma być zapewniony w zakresie niezbędnym do przeprowadzenia kontroli.

			Przygotowanie kopii Informacji może również wymagać anonimizacji Danych Osobowych jeśli nie ma uzasadnienia (cel i zakres) do udostępnienia, powierzenia Danych Osobowych.	
201.	art. 53 ust. 2	Ubezpieczeniowy Fundusz Gwarancyjny	Wydaje się zasadne, aby Ustawodawca uwzględnił ograniczenie w angażowaniu specjalistów (zakładamy, że chodzi o specjalistów "z rynku") w stosunku do których istnieje konflikt interesów np. są/byli zaangażowani w świadczenie usługi cybebezpieczeństwa dla kontrolowanego podmiotu, brali udział w audytach bezpieczeństwa w kontrolowanym podmiocie, są byłymi Pracownikami kontrolowanego podmiotu etc. O potencjalnym konflikcie interesów może poinformać podmiot kontrolowany lub wyznaczony do kontroli Specjalista.	Wyjaśnienie. Organy właściwe odpowiedzialne są za wykluczenie możliwości powstania konfliktu interesów.
202.	art. 53 ust. 2	Narodowy Bank Polski	Zgodnie z proponowanym brzmieniem art. 53 ust. 2 projektu „Jeżeli dokonanie określonych czynności kontrolnych wymaga wiedzy specjalistycznej podmiot przeprowadzający kontrolę może włączyć do kontroli specjalistów”. W ocenie NBP wątpliwości budzi fakt, iż przepis nie określa, jakimi specjalistami będzie się mógł posiłkować organ właściwy (np. czy będą to pracownicy organu właściwego czy też firmy zewnętrzne) oraz w jaki sposób zostanie nawiązana współpraca pomiędzy tymi specjalistami a kontrolowanym podmiotem, a także czy zostanie zabezpieczona poufność danych, do których specjaliści będą mieli dostęp (np. poprzez podpisanie przez nich odpowiedniej umowy o zachowaniu poufności).	Uwaga częściowo uwzględniona.
203.	art. 53 ust. 3 pkt 1	Ubezpieczeniowy Fundusz Gwarancyjny	W kontekście potencjalnej kary w wysokości do 200 000 PLN, w celu uniknięcia każdorazowej interpretacji sformułowania poważne zagrożenie, wydaje się zasadne aby Ustawodawca doprecyzował to sformułowanie	Artykuł 53 ust. 3 pkt 1 nie reguluje kwestii kar. Prawdopodobnie chodzi o art. 57 ust. 3 pkt 1. Uwaga nieuwzględniona.
204.	art. 53 ust. 3 pkt 2	Ubezpieczeniowy Fundusz Gwarancyjny	W kontekście potencjalnej kary w wysokości do 200 000 PLN, w celu uniknięcia każdorazowej interpretacji tych sformułowań po, wydaje się zasadne aby Ustawodawca doprecyzował te sformułowania	Uwaga niejasna.
205.	art. 56 ust. 4	Biuro Bezpieczeństwa Narodowego	Proponuje się uwzględnić udział Biura Bezpieczeństwa Narodowego w pracach nad Strategią Cyberbezpieczeństwa RP. W art. 56 ust. 4 należałoby dodać zdanie w brzmieniu: ,,W pracach nad projektem Strategii może uczestniczyć	Uwaga uwzględniona.

			przedstawiciel Prezydenta RP.".	
206.	art. 57 [uwaga do rozdz. 10]	Rada do Spraw Cyfryzacji	Projekt ustawy nie zawiera jednoznacznego postanowienia, iż kary pieniężne stanowią dochód budżetu państwa.	Uwaga uwzględniona.
207.	art. 57. ust. 1	Rada do Spraw Cyfryzacji	1. Problem: Nieokreślenie sankcji za naruszenie obowiązków wynikających z ustawy przez dostawców usług cyfrowych. Dyrektywy Parlamentu Europejskiego i Rady (EU) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej: Dyrektywa), określa wymagania w zakresie cyberbezpieczeństwa dotyczące operatorów usług kluczowych i dostawców usług cyfrowych. Podobnie, przedstawiony projekt ustawy określa zobowiązania operatorów usług kluczowych oraz dostawców usług cyfrowych (rozdział 3). Zgodnie z art. 21 Dyrektywy, państwa członkowskie zobowiązane są do wprowadzenia sankcji za naruszenie przepisów krajowych implementujących Dyrektywę. Przepis art. 57 ust. 1 projektu ustawy, reguluje odpowiedzialność operatorów usług kluczowych za naruszenie określonych przepisów ustawy. Projekt ustawy nie przewiduje jednak sankcji za naruszenie przepisów przez dostawców usług cyfrowych. Projekt nie przewiduje nakładania kar na dostawców usług cyfrowych. Brak sankcji za niewykonanie przez dostawców usług cyfrowych obowiązków wynikających z ustawy, prowadzić może do nienależytego wykonywania przez takie podmioty obowiązków ustawowych, a w konsekwencji do obniżenia poziomu cyberbezpieczeństwa. Zasadnym wydaje się zatem wprowadzenie sankcji (być może również kar pieniężnych) za naruszenie ustawy przez dostawców usług cyfrowych. 2. Problem: Niezgodność przepisu art. 47 ust. 2 z przepisami rozdziału X („Przepisy o karach pieniężnych), w tym art. 57 ust. 1 projektu ustawy: Art. 47. 1. Nadzór w zakresie stosowania przepisów ustawy sprawują: 1) minister właściwy do spraw informatyzacji w zakresie spełniania przez podmioty świadczące	Uwaga uwzględniona w zakresie nakładania kar finansowych na dostawców usług cyfrowych (problemy 1 i 2). W pozostałym zakresie uwagi zostaną częściowo uwzględnione.

			usługi z zakresu cyberbezpieczeństwa wymogów, o których mowa w art. 15 ust. 2; 2) organy właściwe w zakresie: a) wykonywania przez operatorów usług kluczowych wynikających z ustawy obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów, związanych ze świadczonymi usługami kluczowymi, b) spełniania przez dostawców usług cyfrowych wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych i zgłaszanie incydentów, zgodnie z decyzją wykonawczą Komisji Europejskiej 2017/…/UE. 2. W ramach nadzoru, o którym mowa w ust. 1, organ właściwy lub minister właściwy do spraw informatyzacji: 1) prowadzi kontrole w zakresie, o którym mowa w ust. 1; 2) zobowiązuje do usunięcia nieprawidłowości ustalonych w wyniku kontroli; 3) nakłada kary pieniężne. Zgodnie z przepisem art. 47 ust. 1 pkt 2 lit b) projektu ustawy, właściwy organ sprawuje nadzór nad spełnieniem przez dostawców usług cyfrowych wymogów bezpieczeństwa. Przepis art. 47 ust. 2 pkt. 3 projektu ustawy, przewiduje natomiast, że w ramach takiego nadzoru właściwy organ lub minister ds. Informatyzacji nakłada kary pieniężne. A zatem, literalne brzmienie przepisu sugeruje, że kary pieniężne mogą zostać nałożone również na dostawców usług cyfrowych (art. 47 ust. 2 odwołuje się do całego ust. 1, a nie tylko do ust. 1 pkt 2 lit a). Przepisy rozdziału X projektu ustawy (przepisy o karach pieniężnych) nie przewidują natomiast nakładania kar pieniężnych na dostawców usług cyfrowych. Należy zatem, wprowadzić redakcję przepisów nie powodująca tego rodzaju sprzeczności. 3. Problem: Niejednoznacznie (lub jak się wydaje zbyt wąsko) opisane okoliczności stanowiące podstawę naliczenia kary. a) Art. 57 ust. 1 pkt 3 projektu ustawy. Zgodnie z art. 11 ust. 2 projektu ustawy: „Operatorzy usług kluczowych opracowują dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych …”. Natomiast art. 11 ust. 3 projektu ustawy, przewiduje wydanie przez Radę Ministrów rozporządzenia określającego „sposób tworzenia, aktualizacji, oraz zakres informacji zawartych w dokumentacji (..).” Przewiduje się zatem zasady aktualizacji dokumentacji. Zgodnie z art. 57 ust. 1 pkt 3	

			projektu ustawy, kara pieniężna może zostać nałożona jeżeli operator usług kluczowych „ nie opracował dokumentacji". Przepis nie przewiduje możliwości nałożenia kary w przypadku brak „aktualizacji" dokumentacji. Jeżeli zatem operator usług kluczowych opracuje dokumentacje ale potem zaniecha jej aktualizacji, to nie będzie istnieć podstawa do nałożenia kary (wydaje się, że powinna istnieć realna sankcja również za brak wymaganej aktualizacji dokumentacji). b) Art. 57 ust. 1 pkt 4 projektu ustawy Artykuł 12 projektu ustawy przewiduje szereg obowiązków operatora usług kluczowych (6 podpunktów). Przepis art. 57 ust. 1 pkt 4 projektu ustawy, przewiduje karę, jeżeli operator usług kluczowych „nie wykonuje obowiązków wynikających z art. 12 ust. 1". Powstać może jednak wątpliwość, czy karę można nałożyć wyłącznie w przypadku, w którym operator usług kluczowych nie wykona wszystkich obowiązków opisanych w art. 12 ust. 1 projektu ustawy (a przynajmniej dwóch, bo termin – „obowiązków" użyty został w liczbie mnogiej), czy też karę można nałożyć w przypadku niewykonania, któregokolwiek z obowiązków opisanych w art. 12 ust.1 projektu ustawy. Wydaje się, że niewykonanie któregokolwiek (tj. nawet jednego) z opisanych obowiązków, skutkować powinno możliwością nałożenia kary. c) Brak kary za naruszenie obowiązku wynikającego z art. 15 ust. 1 pkt 2 projektu ustawy (zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania ..). Wydaje się, że niewykonanie tego obowiązku również powinno zostać zabezpieczone stancją w postaci kary pieniężnej.	
208.	art. 57 ust. 1 pkt 9	Rada do Spraw Cyfryzacji	Zdaniem RdC kary są nieadekwatne do rodzaju i zakresu szkód jakie może spowodować nie stosowanie się do zapisów niniejszej ustawy. Straty spowodowane incydentami cyberbezpieczeństwa mogą i będą powodować znaczne straty w mieniu, a ich efekt może spowodować realne zagrożenie dla zdrowia wielu osób /np. awaria instalacji w rafinerii na skutek ataku hakerskiego może spowodować wybuch i nie tylko śmierć osób, ale także skażenie obszaru wokół rafinerii/. RdC sugeruje uzależnienie kar od % obrotu spółek analogicznie do kar w Rozporządzeniu o Ochronie	Uwaga uwzględniona.

			Danych Osobowych, wtedy zachowamy równe obciążenie dla każdej wielkości przedsiębiorstwa. W przypadku samorządów można analogicznie ograniczyć kary po poziomu 100 tys. PLN za pojedyncze naruszenie ale włączyć odpowiedzialność karną zarządzającego jednostką samorządową. Art	
209.	art. 57 ust. 2	Rada do Spraw Cyfryzacji	1. Problem – Zbyt niska wysokość kar pieniężnych. Przepis art. 21 Dyrektywy nakazuje określenie w przepisach krajowych sankcji za naruszenie przepisów krajowych, przyjętych na podstawie Dyrektywy. Przepis art. 21 Dyrektywy przewiduje przy tym, że „Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające.” Przepis art. 57 ust. 2 przewiduje kary pieniężne w wysokości od 1 tys do 100 tys zł. Należy zauważyć, że przepis określa maksymalny wymiar kary (co podkreśla się również w uzasadnieniu ustawy). W praktyce, należy liczyć się zatem z wymierzaniem kary na niższym poziomie. RdC uważa, że generalnie dobrym rozwiązaniem jest przyjęty w projekcie ustawy model sankcji w postaci kar pieniężnych. Mając jednak na uwadze, jak istotna dla bezpieczeństwa państwa i obywateli jest kwestia zapewnienia odpowiedniego poziomu cyberbezpieczeństwa, proponowana wysokość kar pieniężnych wydaje się zbyt niska. Wątpliwym jest, czy kary pieniężne w proponowanej wysokości rzeczywiście stanowić będą „skuteczną” i „odstraszającą” sankcje. Ponadto, ustanowienie maksymalnej wysokości kary pieniężnej, uniemożliwia elastyczne dostosowanie jej do wielkości, pozycji rynkowej i sytuacji gospodarczej podmiotu, który dopuścił się naruszenia (np. kara w wysokości 10 tys. zł może być skuteczna odnośnie „niewielkiego” przedsiębiorcy, a zupełnie niezauważalna dla innego, „większego” przedsiębiorcy). RdC proponuje wprowadzenie systemu, przewidującego możliwość nałożenia kary w wysokości do określonej w ustawie kwoty lub do określonej wartości procentowej przychodów za poprzedni rok. (tj. kara do X zł lub do X % przychodów za poprzedni rok). Decydowałby przy tym wartość wyższa. Jak zostało to już wskazane, wydaje się, że kwota pieniężna (tj. kwota X) powinna zostać ustalona na wyższym poziomie niż przewidziana w projekcie ustawy. Proponowane rozwiązanie nie jest nowe w polskim systemie	Uwaga uwzględniona.

			prawnym. Podobne rozwiązanie przewiduje art. 83 Ogólnego rozporządzenia o ochronie danych. Ponadto, system kar pieniężnych kalkulowanych w oparciu o wielkość przychodu przewiduje np. Prawo Telekomunikacyjne z dnia 16 lipca 2004 r. (art. 209 – art. 210), ustawa o ochronie konkurencji i konsumentów (art. 106). Oczywiście dopracowania wymagają kwestie szczegółowe np. czy kara obliczana jest od przychodu/obrotu, za ostanie rok obrotowy/kalendarzowy itp.	
210.	art. 68 ust. 1	Kancelaria Sejmu RP	W art. 68 ust.1 należy zwrócić uwagę, iż tak sformułowany przepis nie jest przepisem zmieniającym, dostosowującym, przejściowym ani końcowym, choć został umieszczony w rozdziale pt. „Zmiany w przepisach obowiązujących, przepisy przejściowe, dostosowujące i końcowe”.	Uwaga uwzględniona.
211.	art. 69	Generalny Inspektor Ochrony Danych Osobowych	Na zakończenie należy zwrócić uwagę na przepis art. 69 projektu, zgodnie, z którym do czasu uruchomienia systemu, o którym mowa w art. 42 ust. 1, podmioty wymienione w ustawie mają korzystać z dostępnych środków komunikacji i systemów teleinformatycznych. Przypomnieć należy, iż muszą one spełniać wymogi ochrony danych osobowych ujęte w ustawie oraz od 25 maja 2018 r. RODO.	Wyjaśnienie. Podmioty krajowego systemu mają obowiązek stosować się do wymogów dotyczących ochrony danych osobowych.
212.	art. 69	Narodowy Bank Polski	Projekt ustawy przewiduje wprowadzenie obowiązku zgłaszania incydentów poważnych, istotnych oraz krytycznych oraz informacji o cyberzagrożeniach poprzez dedykowany do tego system teleinformatyczny opisany w art. 42 ust. 1 projektu. Pragniemy zauważyć, iż system ten, zgodnie z projektowanym art. 69 ust. 1 zostanie uruchomiony do dnia 1 stycznia 2021 r., a zgodnie z ust. 2, do czasu uruchomienia systemu teleinformatycznego, o którym mowa w art. 42 ust. 1, operatorzy usług kluczowych, dostawcy usług cyfrowych, CSIRT MON, CSIRT NASK oraz CSIRT GOV zgłaszają incydenty oraz wymieniają się informacjami przy pomocy dostępnych środków komunikacji elektronicznej oraz przetwarzają informacje w dostępnych systemach teleinformatycznych. W tym kontekście zwracamy uwagę na brak poprawnego zdefiniowania tychże „dostępnych środków komunikacji elektronicznej”, jak również brak sprecyzowania w jakiej formie będą zgłaszane incydenty w okresie do 2021 roku, kto będzie miał dostęp do tych zgłoszeń oraz brak sprecyzowania wymogu zabezpieczenia tej	Uwaga do dyskusji na konferencji. Konieczne wspólne stanowisko wszystkich CSIRT.

			komunikacji. Może to narażać operatorów usług kluczowych na ryzyko przechwycenia przekazywanych informacji o poważnych, istotnych oraz krytycznych incydentach, które będą przez nich zgłaszane. Obowiązek zgłaszania wynika również z art. 12 ust. 3 projektu, który stanowi, że w przypadku zakłócenia działania systemu teleinformatycznego, o którym mowa w art. 42 ust. 1, operatorzy usług kluczowych zgłaszają incydenty poważne za pomocą dostępnych środków komunikacji elektronicznej. Co ważne, także w tym przypadku projektowany przepis nie wspomina o zabezpieczeniu tejże komunikacji elektronicznej, co w ocenie NBP stanowi poważny mankament.	
213.	art.69. ust. 2	Ubezpieczeniowy Fundusz Gwarancyjny	Wydaje się zasadne określenie minimalnego wymaganego poziomu zabezpieczeń zapewniających poufność i integralność wymienianych Informacji.	Uwaga do dyskusji na konferencji. Konieczne wspólne stanowisko wszystkich CSIRT.
214.	art. 71	Kancelaria Sejmu RP	Należałoby także rozważyć dokładne oszacowanie kosztów wejścia w życie ustawy wskazanych w art. 71 i Ocenie Skutków Regulacji, z uwzględnieniem aktualnego poziomu zaawansowania adresatów projektowanego aktu, w realizację zadań objętych jej zakresem regulacji.	Wyjaśnienie. Oszacowanie kosztów wejścia w życie ustawy zostało opisane w OSR w wyniku przeprowadzonych analiz.
215.	art. 72	Kancelaria Sejmu RP	W art. 72 określono, iż ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia. Wydaje się, iż jest to zbyt krótkie vacatio legis na wdrożenie tak wielu nowych różnorodnych obowiązków nakładanych na bardzo dużą liczbę adresatów projektowanych przepisów, które przewidują także dotkliwe sankcje w postaci kar pieniężnych za nieprzestrzeganie projektowanych regulacji.	Wyjaśnienie. Vacatio legis wynosi czternaście dni, ale obowiązki wynikające z ustawy będą nakładane stopniowo.
216.	załącznik	Urząd Regulacji Energetyki	Na wstępie należy wskazać, że w załączniku do projektu ustawy „Sektory i Podsektory oraz rodzaje podmiotów” w sektorze Energetyka, w kolumnie 2 niewłaściwie wskazano podsektor „Ropa naftowa” zamiast „Paliwa ciekłe”. Zauważyć należy, że w świetle przepisów ustawy – Prawo energetyczne, uzyskania koncesji wymaga prowadzenie działalności gospodarczej w zakresie paliw ciekłych (wytwarzanie, magazynowanie lub przeładunek, przesyłanie lub dystrybucja paliw ciekłych, obrót paliwami ciekłymi, w tym obrót z zagranicą). Koncesje w tym zakresie udzielane są przez Prezesa Urzędu Regulacji Energetyki. Wobec	Uwaga uwzględniona.

			powyższego zasadnym wydaje się także, aby w opis „Rodzaju podmiotu" otrzymał brzmienie: „Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy – Prawo energetyczne, posiadające koncesję na przesyłanie lub dystrybucję paliw ciekłych, na wytwarzanie paliw ciekłych, na magazynowanie lub przeładunek paliw ciekłych, na obrót paliwami ciekłymi lub na obrót paliwami ciekłymi z zagranicą."	
217.	załącznik	Urząd Regulacji Energetyki	W podsektorze „Gaz", w opisie „Rodzaju podmiotów" skreślić należy wiersz szósty (na stronie 43, pierwszy od góry), w którym wskazani są operatorzy OSM i OSGZ, posiadający jednocześnie koncesje OPG lub OGZ. Wszystkie wymienione w tym wierszu podmioty zostały już ujęte w innych wierszach, w związku z tym zachowany zostanie zamierzony charakter wyczerpującego wyliczenia. Ponadto, podmiot będący OSM, nie może uzyskać koncesji OPG lub OGZ. Zbędne jest również powołanie OSP i OSD, wymienionych w wierszach powyżej.	Uwaga uwzględniona. Przedsiębiorstwa energetyczne posiadające te koncesje zostaną wykreślone z załącznika.
218.	załącznik	Urząd Regulacji Energetyki	Niekonsekwentnie w podsektorze „Gaz" posłużono się definicjami OSP i OSD zawartymi w ustawie o zapasach , zamiast używanymi w projekcie definicjami z ustawy – Prawo energetyczne (art. 3 pkt 24 i 25), tym bardziej, iż projektodawca odwołuje się do przepisów Prawa energetycznego, definiując OSP i OSD elektroenergetycznych.	Uwaga uwzględniona.
219.	załącznik	Urząd Regulacji Energetyki	Zbędny jest wiersz siódmy dotyczący przedsiębiorstw energetycznych posiadających koncesję SGZ. Zgodnie z art. 4e1 ustawy- Prawo energetyczne podmiot taki nie może świadczyć usług w zakresie skraplania gazu ziemnego lub regazyfikacji skroplonego gazu ziemnego jeżeli nie został wyznaczony operatorem. Natomiast operator systemu skraplania gazu ziemnego (OSGZ) został już wcześniej wymieniony w załączniku (wiersz piąty, str. 42).	Uwaga uwzględniona. Przedsiębiorstwa energetyczne posiadające tą koncesję zostaną wykreślone z załącznika.
220.	załącznik	Rada do Spraw Cyfryzacji	Podmiotem świadczącym usługi DNS jest prawie każdy dostawca internetu udostępniający swoje systemy rozwiązywania nazw klientom oraz każda kawiarnia udostępniająca swoim klientom bezpłatny dostęp do internetu (każdy router WiFi ma wbudowany serwer DNS).	Wyjaśnienie. O uznaniu danego podmiotu za operatora usługi kluczowej decydować będą także progi ustalone na mocy art. 6.

221.	załącznik	Narodowy Bank Polski	Ad Załącznika do projektu ustawy pt. „SEKTORY I PODSEKTORY ORAZ RODZAJE PODMIOTÓW” W odniesieniu do treści załącznika do projektowanej ustawy warto zwrócić uwagę, że nie jest możliwe zaklasyfikowanie NBP do żadnej z kategorii podmiotów będących operatorami usług kluczowych. Określona w załączniku do ustawy kategoryzacja rodzajów podmiotów nie przewiduje bowiem odpowiedniej dla NBP pozycji na tej liście. Potwierdza to słuszność stanowiska zawartego w uwadze ogólnej, jak również w uwagach szczegółowych (uwagi do art. 16 i 27 projektu).	Wyjaśnienie. Nie przewiduje się, aby NBP był operatorem usługi kluczowej. Będzie on za to zobowiązany do przestrzegania przepisów z art. 24, dotyczących organów publicznych.
222.	uzasadnienie	Narodowy Bank Polski	Uzasadnienie projektu ustawy w punkcie 2.3 (str. 9) jest nieprecyzyjnie sformułowane, bowiem umożliwia twierdzenie, że instytucjami kredytowymi w Polsce są jedynie banki, gdy tymczasem są nimi również spółdzielcze kasy oszczędnościowo-kredytowe, funkcjonujące w oparciu o ustawę z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo - kredytowych (Dz. U. z 2017 r., poz. 2065). Zwracamy uwagę, że zgodnie z dyrektywą, zakresem regulacji powinny zostać objęte wszystkie instytucje kredytowe. W konsekwencji, sugerujemy doprecyzowanie w uzasadnieniu, że zakresem niniejszej ustawy będzie objęty również sektor spółdzielczych kas oszczędnościowo-kredytowych i w efekcie czego zmianę zamieszczonej w tabeli wskazującej sektory i podsektory do celów identyfikacji operatorów usług kluczowych (załącznik do projektu ustawy) nazwy omawianego sektora na „Sektor instytucji kredytowych”.	Uwaga uwzględniona. Uzasadnienie zostanie uzupełnione.
223.	OSR	Komisja Nadzoru Finansowego	Zgodnie z Projektem, istnieje duże prawdopodobieństwo, że Urząd KNF, będący w chwili obecnej operatorem infrastruktury krytycznej w rozumieniu ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209, z późn. zm.) oraz rozporządzenia Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej (Dz. U. nr 83, poz. 541), zostanie uznany za operatora usług kluczowych. W OSR wskazano, że w przypadku podmiotów pełniących tę rolę uwzględnić należy koszt utworzenia operacyjnego centrum bezpieczeństwa, zwane dalej „SOC” oszacowanego na 1 mln zł oraz	Uwaga nieuwzględniona. Projekt ustawy nie obliguje do budowy SOC w podmiocie będących operatorem usługi kluczowej. W kwestii tej każdy podmiot ma pełna swobodę działania, polegająca na wyborze pomiędzy wariantami: budowa SOC we własnej organizacji, zlecenie usługi dla podmiotu świadczącego usługi w zakresie cyberbezpieczeństwa. Przyjęte w OSR szacunkowe koszty policzono na podstawie danych rynkowych dla operatora średniej wielkości. Dlatego

			jego utrzymania oszacowanego na 2 mln zł rocznie. Uwzględnione muszą być także wydatki związane z dodatkowym zatrudnieniem. Tym samym uwzględnić należy fakt, że budżet Komisji Nadzoru Finansowego w części 70 budżetu państwa musiałby zostać zwiększony o taką kwotę, co na obecnym etapie uchwalania budżetu państwa na 2018 r. wydaje się znacznie utrudnione, jako że proces ten na etapie rządowym został zakończony a projekt ustawy budżetowej został przesłany do Sejmu. Projekt w art. 71 wskazuje co prawda maksymalny limit wydatków z budżetu państwa będących skutkiem finansowym wejścia w życie ustawy, ale analizując ujęte tam kwoty, uznać należy, że nie obejmują one wydatków Urzędu KNF będących konsekwencją jej uchwalenia i wdrażania. Biorąc także pod uwagę fakt, że KNF podlega ograniczeniom nakładanym przez ministra właściwego ds. finansów publicznych na etapie planowania budżetowego, nieujęcie ww. kwot w Projekcie oznacza brak podstawy do zwiększenia wydatków w cz. 70 budżetu państwa „Komisja Nadzoru Finansowego", a co za tym idzie uniemożliwia realizację obowiązków wynikających z Projektu. Wydatki w 2018 r. musiałyby zostać pokryte z rezerwy celowej. Zasadne wydaje się więc wskazanie w OSR, a także w Projekcie, że wydatki związane z wdrażaniem jego regulacji będą wyższe. W przypadku Urzędu KNF, zgodnie z informacjami zawartymi w OSR, uwzględnić należałoby co najmniej 2 mln zł w roku 2018 (1 mln zł związany z utworzeniem SOC oraz 1 mln zł na jego utrzymanie), oraz co najmniej 2 mln zł w latach kolejnych na utrzymanie SOC. Dodatkowo biorąc pod uwagę wielkość Urzędu KNF uznać należy, że konieczne będzie zatrudnienie dodatkowych 5 – 7 osób dedykowanych do realizacji zadań przewidzianych w Projekcie dla operatorów usług kluczowych. Przy szacowanych w Projekcie kosztach zatrudnienia jednego specjalisty ds. cyberbezpieczeństwa oznacza to dodatkowe wydatki w wysokości od 600 do 840 tys. zł rocznie, jednak tak jak wspomniano wyżej, wzrost zatrudnienia oznacza konieczność zmiany projektu budżetu państwa w zakresie liczby etatów w Urzędzie KNF.	też, w OSR nie zostały przedstawione kalkulacje środków dla poszczególnych podmiotów.

224.	OSR pkt 4	Urząd Regulacji Energetyki	Należy zwrócić uwagę, że Ocena skutków regulacji w pkt 4 nieprawidłowo wskazuje na nieistniejący podmiot tj. operatora systemu przesyłowego (OSP) paliw ciekłych. W związku z tym, w pkt 4 wyraz „OSP" należy skreślić. Uwzględnić natomiast należy podmioty, które prowadzą działalność w zakresie przesyłania i dystrybucji paliw ciekłych (podmioty działające w tym zakresie to: PERN S.A. oraz Polski Koncern Naftowy ORLEN S.A.).	Uwaga uwzględniona.
225.	OSR pkt 4	Urząd Regulacji Energetyki	W punkcie 4 wskazano dla podsektora ropy naftowej 4 podmioty, na które oddziałuje projekt ustawy, natomiast w pkt 7 w dodatkowych informacjach w ppkt a) „Operatorzy usług kluczowych" w części b. „Sektor energetyka, podsektor ropa naftowa" wymieniono łącznie 5 podmiotów, w tym Polskie Górnictwo Naftowe i Gazownictwo S.A., które nie posiada koncesji w zakresie paliw ciekłych. Biorąc powyższe pod uwagę zasadnym jest skorelowanie wartości wskazanych w pkt 4 oraz w pkt 7 OSR.	Uwaga uwzględniona.
226.	uwaga ogólna	Urząd Komunikacji Elektronicznej	Z zaproponowanych przepisów nie wynika dostatecznie precyzyjnie określony sposób uczestnictwa Prezesa Urzędu Komunikacji Elektronicznej, zwanego dalej „Prezesem UKE", w systemie przekazywania informacji w ramach krajowego systemu cyberbezpieczeństwa. Zgodnie z projektowaną w art. 61 zmianą w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907), zwaną dalej „Pt", Prezes UKE ma przekazywać informacje, o których mowa w art. 175a ust. 1 Pt, za pośrednictwem systemu teleinformatycznego, o którym mowa w art. 42 ust. 1 projektowanej ustawy Zespołowi Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) właściwemu dla zgłaszającego przedsiębiorcy telekomunikacyjnego zgodnie z art. 28 ust. 5-7 tej ustawy. W odniesieniu do projektowanej regulacji należy przede wszystkim zauważyć, że nie określono z jaką częstotliwością ww. informacje miałyby być przekazywane przez Prezesa UKE (cyklicznie np. raz w tygodniu, czy może niezwłocznie po ich otrzymaniu od przedsiębiorcy telekomunikacyjnego). Ponadto, zarówno z projektowanego art. 175a ust. 1a Pt, jak i z pozostałych przepisów projektowanej ustawy nie wynika sposób w jaki informacje te mają być przekazywane przez Prezesa UKE „za pośrednictwem systemu teleinformatycznego", którego funkcjonowanie ma zapewnić	Uwaga uwzględniona. Przepisy zostaną doprecyzowane.

			minister właściwy do spraw informatyzacji. Wiedza na ten temat jest niezbędna dla potrzeb oceny możliwości realizacji planowanego przedsięwzięcia w aspekcie technicznym oraz kadrowym. Trudno bowiem w chwili obecnej stwierdzić, czy wdrożenie proponowanego modelu funkcjonowania krajowego systemu cyberbezpieczeństwa będzie wymagało zapewnienia przez Prezesa UKE całodobowej obsługi (na wzór CSIRT), czy też może nie będą potrzebne żadne zmiany w tym zakresie (kwestia personelu do realizacji obowiązków przewidzianych projektowaną ustawą i związanych z tym kosztów). Dodatkowo, w odniesieniu do projektowanego art. 42 ust. 15 (na podstawie którego minister właściwy do spraw informatyzacji, na wniosek przedsiębiorcy telekomunikacyjnego, może zapewnić dostęp do systemu teleinformatycznego w celu realizacji obowiązków, o których mowa w art. 175a ust. 1 Pt) należy podkreślić, iż w ramach ewentualnej realizacji niniejszego przepisu konieczne będzie wdrożenie takich uwarunkowań technicznych, które zapewnią, iż przekazywane przez przedsiębiorców telekomunikacyjnych informacje będą trafiały także do Prezesa UKE. Jest to szczególnie istotne dla spełnienia wymogu wynikającego z art. 13a ust. 3 dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (Dz. Urz. UE L 108 z 24.04.2002, str. 33), zgodnie z którym, państwa członkowskie zapewniają, aby przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej powiadamiały właściwy „krajowy organ regulacyjny" o każdym naruszeniu bezpieczeństwa lub utracie integralności, które miały znaczący wpływ na sieci lub usługi. Przedmiotowy projekt, pomimo postanowień art. 1 ust. 3 implementowanej dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1), zgodnie z którym, wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w niniejszej dyrektywie nie mają zastosowania do przedsiębiorstw, które podlegają wymogom art. 13a i 13b dyrektywy 2002/21/WE,	

			przewiduje udział przedsiębiorców telekomunikacyjnych, jak również Prezesa UKE w krajowym systemie cyberbezpieczeństwa. Należy jednak zaznaczyć, że przewidziane w opiniowanym projekcie regulacje są zbyt ogólne i nieprecyzyjne, powodując tym samym wątpliwości, o których mowa w powyższych uwagach. Ich rozstrzygnięcie będzie miało kluczowe znaczenie dla możliwości odniesienia się m. in. do wskazanych w części 6 („Wpływ na sektor finansów publicznych") oceny skutków regulacji projektowanej ustawy szacunkowych kosztów wynikających z zadań nakładanych na Prezesa UKE, które mogą okazać się np. zbyt niskie.	

Zestawienie zgłoszonych uwag do projektu ustawy o krajowym systemie cyberbezpieczeństwa – OPINIOWANIE (Prokuratura Krajowa)

L.p.	Art.	Podmiot	Treść uwagi	Stanowisko MC
Uwagi ogólne				
1.	art. 2	Prokuratura Krajowa	Nadesłany do zaopiniowania projekt w sposób został zmodyfikowany w sposób zasadniczy w stosunku do poprzednio opiniowanego projektu, ustosunkowywanie się do wcześniej zgłoszonych uwag do projektu należy uznać za niecelowe, choć - co należy podkreślić - w zakresie obszarów wymagających zmian w projekcie, uwagi pozostają aktualne również w odniesieniu do obecnie procedowanej wersji projektu. Analiza treści projektu wskazuje, ze projektodawca zmienił zakres podmiotowy opiniowanego projektu, włączając w obszaru regulacji projektu ustanawiającego krajowy system cyberbezpieczeństwa prokuratury (art. 4 pkt 6 - organy publiczne). Z tych względów koniecznym stała się analiza projektowanych przepisów w zakresie, w jakim kształtują prawa i obowiązki podmiotów tworzących krajowy system cyberbezpieczeństwa. Aktualnym pozostaje nadal kwestia modyfikacji słownicza projektu ustawy poprzez uzupełnienie go definicją „usługi kluczowej". Obecnie definicja „usługi kluczowej" wskazana została dopiero w rozdziale 2 art. 5 ust. 2 pkt 1 projektu, choć już we wcześniejszych artykułach projektu określenie to się pojawia. Z tych względów proponuje się przeniesienie do katalogu zawartego w art. 2 definicji pojęcia „usługa kluczowa".	Uwaga uwzględniona. Art. 2 zostanie uzupełniony o definicję usługi kluczowej.

2.	art. 2 pkt 8-12	Prokuratura Krajowa	W odniesieniu do przyjętego w projekcie ustawy aparatu pojęciowego w postaci zdefiniowanych w art. 2 pojęć zdaniem Biura na ponowną analizę w trakcie procesu legislacyjnego nadal zasługuje przyjęta definicja pojęcia incydent. Poprawne określenie zakresu tego pojęcia ma wpływ na czynności wykrywania, klasyfikacji, analizowania i podejmowania działań naprawczych. Z tych względów wątpliwości budzi proponowany w projekcie podział definicji incydentu na: incydent, incydent krytyczny, incydent poważny, incydent zwykły i incydent istotny. Definicje te nieostre i nie pozwalają na jednoznaczną klasyfikację incydentów. Z kolei blednę zakwalifikowanie incydentu może skutkować nałożeniem przez organy kontrolne kary pieniężnej na dany podmiot. Biorąc pod uwagę powyższe, a także fakt, iż wdrażana dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. posługuje się tylko jedną definicja incydentu, rozumianą jako każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na cyberbezpieczeństwa sieci i systemów informatycznych - art. 4 pkt 7 dyrektywy, należy rozważyć ponowne doprecyzowanie tego pojęcia w projektowanej ustawie. Należy również zauważyć, że przyjęty sposób definiowania pojęcia incydent w art. 2 pkt 8, w którym incydent jest zdefiniowany, jako „incydent krytyczny, poważny, istotny albo zwykły" jest przykładem definiowania ignotum per ignotum. Najpierw należy zdefiniować pojęcie incydentu, a następnie można określać jego rodzaje.	Uwaga częściowo uwzględnione. Definicje incydentów zostaną przeredagowane.

3.	art. 3 ust. 2	Prokuratura Krajowa	Niespójność zapisów projektu ujawnia się? przy zestawieniu art. 3 ust. 2 projektu ustawy, który umożliwia podmiotom krajowego systemu cyberbezpieczeństwa przekazywanie gromadzonych informacji o podatnościach na incydenty, incydentach i zagrożeniach cyberbezpieczeństwa oraz o poziomie ryzyka wystąpienia incydentów do publicznej wiadomości w przypadku, gdy ujawnienie incydentu jest w interesie publicznym, w tym jeśli przyczyni się do zwiększenia cyberbezpieczeństwa z art. 36 ust. 5, wskazującym na możliwość przekazywania do publicznej wiadomości informacji o incydentach przez CSIRT MON, CSIRT NASK i CSIRT GOV choć są to podmioty, którym tego rodzaju uprawnienie przysługuje na podstawie art. 3 ust. 2.	Uwaga częściowo uwzględniona. Intencją projektodawcy było rozróżnienie delegacji specjalnej dla CSIRT, które mają szczególne uprawnienia w tym zakresie (art. 36 ust. 5 projektu). Przepis art. 3 ust. 2 odnosi się do wszystkich uczestników krajowego systemu cyberbezpieczeństwa i przez to ma charakter bardziej ogólny. Zmieniono treść obu przepisów w ten sposób, aby mocniej zaakcentować różnice między dwoma sposobami publikowania informacji.
4.	art. 24	Prokuratura Krajowa	Odnosząc się do regulacji związanych bezpośrednio z obowiązkami nałożonymi na podmioty publiczne, w tym na prokuraturę należy wskazać na zapisy art. 24 projektu, wprowadzający obowiązek wyznaczenia osoby odpowiedzialnej za cyberbezpieczeństwa świadczonych usług. Ponieważ projekt definiuje jedynie pojęcie usług cyfrowych powstaje pytanie, o jakiego rodzaju usługach jeśli mowa w art. 24, czego konsekwencją będzie realizacja obowiązku wyznaczenia osoby odpowiedzialnej za ich bezpieczeństwa bądź tez niewyznaczanie takiej osoby. W przypadku gdyby prokuratura była zobligowania do wyznaczenia osoby powstaje pytanie, czy powszechne jednostki organizacyjne prokuratury mogą wyznaczyć jedna osobę odpowiedzialna za cyberbezpieczeństwo świadczonych usług przez wszystkie jednostki, albowiem tego rodzaju uprawnienie znalazło się w art. 24 ust. 2 jedynie w stosunku do jednostek samorządu terytorialnego. Ponadto projektowane przepisy nie	Wyjaśnienie. Zapis art. 24 ust. 2 zostanie zmieniony. Projektodawca skoryguje zapis nakładając na podmioty publiczne obowiązek wyznaczenia osoby odpowiedzialnej za kontaktowanie się z właściwym CSIRT.

			określają obowiązków takiej osoby, jej miejsca w strukturze organizacyjnej podmiotu, odpowiedzialności, a co wydaje się elementem niezbędnym i wymaga rozszerzenie regulacji w tym zakresie.	
5.	art. 35 oraz 42	Prokuratura Krajowa	Poważne wątpliwości budzi zgodność projektowanych przepisów ustawy z przepisami o ochronie danych osobowych. W szczególności, w projektowanym art. 35 ust. 1 ustawy brak jest katalogu danych osobowych, które mogą być przetwarzane w związku z realizacja zadań wynikających z ustawy, Przepis ten zakłada wzajemna wymiany danych osobowych przez CSIRT MON, CSIRT NASK oraz CSRIT GOV. Nie reguluje on natomiast jakie dane oraz na jakich zasadach będą podlegały udostępnianiu pomiędzy ww. podmiotami. Z przepisów prawa zaś powinien wprost wynikać zakres, cel oraz zasady udostępniania danych, a podstawę takiego udostepnienia powinien stanowić wyłącznie wniosek. Zasada minimalizacji danych jest jedną z podstawowych zasad przetwarzania danych osobowych na gruncie krajowych i unijnych przepisów z tego zakresu. W tym miejscu wskazać należy, że projektowana ustawa o krajowym systemie cyberbezpieczeństwa będzie wywoływać skutki prawne w czasie obowiązywania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46 WE (ogólne rozporządzenie o ochronie danych osobowych), zwanego dalej RODO. Przepisy RODO będą stosowane wprost od dnia 25 maja 2018 r. Mając na uwadze powyższe, przy pracach nad projektem ustawy należy uwzględnić wskazane regulacje z zakresu ochrony	Uwaga uwzględniona. Przepisy dotyczące ochrony danych osobowych zostaną zmienione.

			danych osobowych. Art. 35 ust. 2 projektowanej ustawy, w zakresie obejmującym wzajemną wymianę danych, wydaje się sprzeczny z przepisami o ochronie danych osobowych. Powyższy zapis powinien regulować jakie dane oraz na jakich zasadach będą podlegały udostępnianiu pomiędzy ww. podmiotami. Z przepisów prawa wynikać powinien zakres, cel oraz zasady udostępniania danych, a podstawą takiego udostępnienia stanowić może wyłącznie wniosek. Zgodnie z motywem 31 RODO, żądanie ujawnienia danych osobowych, z którym występują organy publiczne, powinno mieć zawsze formę pisemną, być uzasadnione, mieć charakter wyjątkowy i nie powinno dotyczyć całego zbioru ani prowadzić do polaczenia zbiorów. Wskazać również należy na art. 42 projektu ustawy, dotyczący wprowadzenia centralnego systemu prowadzonego przez ministra właściwego ds. informatyzacji, który wymaga doprecyzowania w zakresie dotyczącym ochrony danych osobowych. W ustępie 6 wskazano, ze administratorem danych zgromadzonych w systemie jest minister właściwy ds. informatyzacji. Nie została uregulowana natomiast kwestia jakie kategorie danych osobowych będą w powyższym systemie przetwarzane. Za niezbędne w odniesieniu do systemu centralnego U7.nac należy określenie okresu przechowywania danych, co będzie stanowić realizację przepisów art. 5 ust. 1 lit. e) RODO, który wprowadza zasadę ograniczenia czasowego przechowywania danych osobowych (dane osobowe nie powinny być przetwarzane dużej niż jest to niezbędne dla celów ich przetwarzania). Ponadto, zgodnie z motywem 39 RODO dane powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których one przetwarzane. Okres przechowywania danych ograniczony winien być do minimum. Dane osobowe	

			powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu. W art. 42 ust. 7 projektu wyłączono możliwość realizacji praw osób, których dane dotyczą oraz obowiązki ciążące na administratorze w tym zakresie. Wyłączenie takie jest dopuszczalne na gruncie przepisów RODO, jednakże wymaga wskazania określonego interesu publicznego oraz wykazania, ze jest to niezbędne i proporcjonalne do jego realizacji. W uzasadnieniu projektu ustawy nie wskazano, w jaki sposób zapewnione jest wykonanie art. 23 ust. 2 RODO. Jednocześnie, zgodnie z art. 35 RODO, jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. W OSR do ustawy nie uwzględniono oceny wpływu regulacji na prywatność osób, których dane dotyczą. Mając na uwadze powyższe, przy projektowaniu należy uwzględnić ewentualne skutki dla ochrony prywatności osób, których dane dotyczą.	
6.	OSR pkt 4	Prokuratura Krajowa	Należy również zaznaczyć, ze zmiana ta nie znalazła swojego odzwierciedlenia w załączonych do projektu ocenach skutków regulacji, gdzie w punkcie 4 zawierającym wykaz podmiotów, na które oddziałuje projekt nie znalazła się prokuratura. Nie ulega bowiem wątpliwości, że tak jak w przypadku innych organów	OSR będzie uzupełniany.

			publicznych, które zostały ujęte w wykazie (np. centralna i terenowa administracja rządowa) oddziaływanie będzie polegać na konieczności spełnienia przez prokuraturę nałożonych na nią projektem ustawy wymogów.	

Zestawienie zgłoszonych uwag do projektu ustawy o krajowym systemie cyberbezpieczeństwa – KONSULTACJE PUBLICZNE

L.p.	Art.	Podmiot	Treść uwagi	Stanowisko MC
1.	ogólna	Fundacja Bezpieczna Cyberprzestrzeń	W projekcie niejasna jest rola firm świadczących usługi cyberbezpieczeństwa w krajowym systemie cyberbezpieczeństwa. Firmy te ze względu na profil swojej działalności mogą niejednokrotnie dysponować informacjami istotnymi dla krajowego systemu cyberbezpieczeństwa. Ponadto, projekt ustawy ogranicza rolę operatorów telekomunikacyjnych w Krajowym Systemie Cyberbezpieczeństwa podczas gdy operatorzy telekomunikacyjni ze względu na zajmowaną przez siebie pozycję i poziom widoczności informacji w sieci Internet mogą odgrywać istotną rolę we wczesnym wykrywaniu nowych zagrożeń cyberbezpieczeństwa oraz w zwalczaniu i minimalizowaniu skutków trwających incydentów. W projekcie ustawy brakuje także jakiegokolwiek odniesienia do sfery operacji informacyjnych, które nierzadko „współgrają" z tradycyjnie rozumianymi cyberatakami, a zatem wymagałaby uwzględnienia. Ponadto, w projekcie występuje nadmierna ilość sformułowań nieprecyzyjnych lub takich, które stają się jasne dopiero po przeczytaniu unijnej Dyrektywy NIS.	Uwaga częściowo uwzględniona. Zostanie rozszerzone uzasadnienie w zakresie roli podmiotów świadczących usługi z zakresu cyberbezpieczeństwa. Zostanie także rozszerzony katalog informacji przekazywanych do organów właściwych przez operatorów usług kluczowych, którzy korzystają z usług podmiotów świadczących usługi z zakresu cyberbezpieczeństwa. Będą dodatkowo przekazywane informacje o zakresie usług świadczonych przez podmiot świadczący usługi z zakresu cyberbezpieczeństwa i osobie do kontaktu. Projekt uwzględnia przedsiębiorców telekomunikacyjnych w krajowym systemie cyberbezpieczeństwa, ale z uwagi na ograniczenia określone w dyrektywie 2016/1148 ustawa nie nakłada żadnych nowych obowiązków na przedsiębiorców telekomunikacyjnych dotyczących cyberbezpieczeństwa i zgłaszania incydentów.

2.	ogólna	Instytut Kościuszki	Ustawa o krajowym systemie cyberbezpieczeństwa zgodnie z postulatami przedstawionymi w Krajowych Ramach Polityki Cyberbezpieczeństwa RP na lata 2017-22, Planie Działań na rzecz wdrażania Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017 - 2022 oraz pozostałych dokumentach programowych Ministerstwa Cyfryzacji w przedmiotowym obszarze, powinna stanowić kompleksową regulację zapewniającą skuteczność systemu cyberbezpieczeństwa poprzez konsolidację i harmonizację działań wszystkich interesariuszy. Wedle diagnozy, że efektywność dotychczasowych jest obniżona z uwagi na rozproszony charakter działań w obszarze cyberbezpieczeństwa podmiotów ze sfery cywilnej, wojskowej, sektora publicznego i prywatnego oraz instytucji odpowiedzialnych za zwalczanie cyberprzestępczości, ustawa powinna w sposób całościowy obejmować podstawy ustroju i wzajemnych relacji zaangażowanych podmiotów. Przedstawiony do konsultacji projekt pozostaje w tym zakresie niekompletny, ograniczając się do uporządkowania przedmiotowych obszarów w znacznym stopniu tylko w kontekście implementacji postanowień Dyrektywy NIS. W tym kontekście projekt ustawy ignoruje m.in.: postulat utworzenia Naukowego Klastra Cyberbezpieczeństwa (szkolnictwo wyższe jest elementem systemu wyłącznie w kontekście realizacji zgłoszeń incydentów, art. 28 ust. 6 lit. l w zw. z art. 4 pkt 13 – takie zawężenie jest też wątpliwe w świetle motywu 5 dyrektywy NIS) lub budowy systemu wsparcia przedsięwzięć badawczorozwojowych w dziedzinie cyberbezpieczeństwa, rozwoju hubów innowacyjności oraz uruchomienia programu Cyberpark Enigma. Jakkolwiek do niektórych z tych kwestii odniesiono się częściowo w Ocenie Skutków Regulacji, należy podkreślić, iż brak literalnego określenia ich pozycji i zadań w ramach krajowego systemu cyberbezpieczeństwa stanowi niedociągnięcie, którego nie niwelują wskazane w art. 41 pkt. 2-3 kompetencje ministra właściwego ds. informatyzacji w zakresie realizacji Strategii Cyberbezpieczeństwa RP. W projekcie ustawy nie unormowano	Wyjaśnienie. Projekt wykracza poza implementację dyrektywy 2016/1148. Jednakże, podstawą przedsięwzięć gospodarczych i dotyczących polityki innowacyjnej z zakresu cyberbezpieczeństwa będą określone w „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej" plany działań i projekty szczegółowe. Stosowne zapisy znajdują się w aktualnie obowiązujących „Krajowych Ramach Polityki Cyberbezpieczeństwa RP na lata 2017-22". Obecnie opracowywany jest Plan działań.

			również roli Forum ds. Cyberbezpieczeństwa przy Ministerstwie Cyfryzacji, jak i Zespołu zadaniowego ds. bezpieczeństwa cyberprzestrzeni RP w ramach KRMC.	
3.	ogólna	Instytut Kościuszki	Podobnie projekt ustawy pomija zagadnienie budowy klastra bezpieczeństwa dla administracji centralnej oraz roli jaką powinien on pełnić w ramach systemu na poziomie technicznym. Priorytetowe, zgodnie z Krajowymi Ramami, wyzwanie utworzenia bezpiecznych sieci typu intranet, oferujących połączenia wewnątrz sieci, usługi bezpieczeństwa oraz bezpieczny dostęp do sieci Internet, nie zostało uwzględnione w projekcie ustawy.	Uwaga nieuwzględniona. Zagadnienie to nie jest przedmiotem projektowanej ustawy. Kwestia budowy rządowego klastra bezpieczeństwa jest przedmiotem Planu Działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa RP na lata 2017-2022.
4.	ogólna	Instytut Kościuszki	Projekt ustawy nie odnosi się także wprost do potrzeby budowania sektorowych zespołów CSIRT, która była postulowana w Krajowych Ramach. Z uwagi na specyfikę sektorów, dogodnym rozwiązaniem byłoby, aby każdy organ właściwy w rozumieniu projektu ustawy posiadał zespół CSIRT będący z jednej strony jego zapleczem eksperckim, a z drugiej – elementem pośredniczącym pomiędzy operatorami usług kluczowych a właściwym CSIRT (NASK, GOV, MON). Warto w tym kontekście wykorzystać doświadczenie oddolnych inicjatyw sektorowych (np. w sektorze energetycznym).	Uwaga częściowo uwzględniona. Projekt zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa CSIRT jest natomiast zarezerwowana dla zespołów poziomu krajowego.
5.	ogólna	Instytut Kościuszki	Zaznaczone wyraźnie w projekcie ustawy podejście sankcyjne nie zostało w dostatecznie wyraźnym stopniu uzupełnione w obszarze konkretnych zachęt oraz wsparcia administracji publicznej w przedmiocie realizacji nowych obowiązków nałożonych na podmioty objęte zakresem normowania. Zgodnie z Krajowymi Ramami, rząd powinien podejmować działania wspierające budowanie zdolności i kompetencji w zakresie cyberbezpieczeństwa wśród operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych. Poza nieprecyzyjnymi postanowieniami art. 41 pkt 3-4, 6-7, projekt ustawy nie zawiera odpowiednich mechanizmów w tej kwestii. Dobrym rozwiązaniem	Wyjaśnienie. Oprócz przepisów art. 41 pkt 3-4, 6-7 projektodawca zakłada, że działania wspierające budowanie zdolności i kompetencji w zakresie cyberbezpieczeństwa wśród operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych będą również realizowane w ramach planu działań i projektów szczegółowych wynikających ze Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej”.

			byłoby opracowanie sektorowych standardów przy wsparciu CSIRT, organów właściwych, operatorów usług kluczowych, dostawców usług cyfrowych oraz z wykorzystaniem potencjału intelektualnego ekspertów zgromadzonych w komitetach technicznych Polskiego Komitetu Normalizacyjnego, ośrodkach naukowych, akademickich i instytutach badawczych, które w oparciu o normy międzynarodowe (np. NIST) i najlepsze praktyki a także wytyczne Agencji ENISA, umożliwiłyby efektywne wzmocnienie krajowego systemu cyberbezpieczeństwa. Podobnie ustawa o krajowym systemie cyberbezpieczeństwa powinna nakładać na operatorów usług kluczowych, podmioty publiczne, organy właściwe obowiązek systematycznych szkoleń i ćwiczeń (obecnie tylko w odniesieniu do organów właściwych) podnoszących ogólny poziom świadomości i kompetencji w obszarze cyberbezpieczeństwa. Postulat, zaznaczony w Krajowych Ramach, nie znalazł swego odzwierciedlenia w projekcie ustawy.	Dodatkowo należy zwrócić uwagę, że zgodnie z art. 39 ust. 1 pkt. 4 organy właściwe będą przygotowywać we współpracy z CSIRT NASK, CSIRT GOV i CSIRT MON rekomendacje do działań mające na celu wzmocnienie cyberbezpieczeństwa, w tym w wytyczne sektorowe do zgłaszania incydentów. Rekomendacje i wytyczne będą obejmować dorobek europejskich i międzynarodowych organizacji standaryzacyjnych, Polskiego Komitetu Normalizacyjnego, najlepsze praktyki a także wytyczne Agencji ENISA, ośrodków naukowych, akademickich i instytutów badawczych.
6.	ogólna	Instytut Kościuszki	Projekt ustawy nie wykorzystuje potencjału organizacji pozarządowych (fundacji, stowarzyszeń) w budowaniu świadomości społecznej w obszarze cyberbezpieczeństwa. Szczególnie w zakresie kompetencji nadanych ministrowi właściwemu ds. informatyzacji (art. 41 pkt 7) polegających na prowadzeniu działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i podnoszenia świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników, powinna zostać podkreślona rola i możliwe modele współpracy z trzecim sektorem. Pomijając już możliwą większą efektywność tego rodzaju zadań związanych z możliwości wykorzystania nieformalnych struktur sieciowych, w ramach których funkcjonują organizacje pozarządowe, możliwość delegacji przedmiotowych zadań podmiotom z trzeciego sektora byłaby zgodna z Programem współpracy Ministra Cyfryzacji z organizacjami pozarządowymi oraz	Uwaga częściowo uwzględniona.

			podmiotami wymienionymi w art. 3 ust. 3 ustawy o działalności pożytku publicznego I o wolontariacie z 2016 roku.	
7.	ogólna	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Wdrożenie systemu cyberbezpieczeństwa w proponowanym przez Projekt modelu spowoduje wzrost popytu na usługi i produkty cyberbezpieczeństwa, w konsekwencji wzrost importu zarówno usług, jak i rozwiązań produktowych (ze względu na brak rozwiązań krajowych), co z jednej strony osłabi krajową gospodarkę, a z drugiej pogłębi uzależnienie cyberbezpieczeństwa Polski od zagranicznych rozwiązań. Aby uniknąć tej sytuacji należy zaprojektować krajowy system cyberbezpieczeństwa tak, aby stymulował rozwój innowacyjności polskiego sektora ICT oraz wprowadził na rynek możliwie największą ilość narzędzi wytworzonych przez krajowe przedsiębiorstwa. Konieczne jest, także przyspieszenie rozwoju kompetencji z zakresu cyberbezpieczeństwa w sektorze publicznym i komercyjnym. Polska nie jest obecnie przygotowana do gwałtownego rozwinięcia systemu cyberbezpieczeństwa, a projektowana ustawa powinna uwzględniać model etapowego (np. w okresie 3 letnim) jego wdrażania, tak aby paralelnie rozwijać kompetencje krajowe w tym zakresie.	Wyjaśnienie. Założeniem projektodawcy jest, że podstawą przedsięwzięć gospodarczych i dotyczących polityki innowacyjnej z zakresu cyberbezpieczeństwa będą określone w „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej” plany działań i projekty szczegółowe. Stosowne zapisy znajdują się w aktualnie obowiązujących „Krajowych Ramach Polityki Cyberbezpieczeństwa RP na lata 2017-22”. Obecnie opracowywany jest Plan działań.
8.	ogólna	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Biorąc pod uwagę potrzebę kompleksowego zmierzenia się ze zjawiskiem cyberprzestępczości, groźnym dla obywateli, przedsiębiorców, organów państwa oraz ekonomicznych interesów państwa, postulujemy pilne podjęcie prac, dzięki którym wszelkie nieautoryzowane działania przy zabezpieczeniach systemów byłyby ścigane z mocy prawa. Można byłoby, m.in. wzorować się na rozwiązaniach przyjętych w Stanach Zjednoczonych, gdzie próba naruszenia stosowanych przez przedsiębiorców zabezpieczeń jest przestępstwem federalnym.	Wyjaśnienie. Zagadnienia te były przedmiotem rozmów pomiędzy resortami w ramach prac nad ustawą o krajowym systemie cyberbezpieczeństwa. Niezbędne są analizy dotyczące przepisów karnych i przepisów z zakresu ścigania przestępczości będące w kompetencji innych resortów. Ewentualne zmiany przepisów w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty.

9.	ogólna	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Wydaje się, że zarówno wśród zadań operatorów kluczowych, jak i wśród elementów wdrażanego przez nich systemu zarządzania bezpieczeństwem większy nacisk powinien zostać położony na monitorowanie zdarzeń w sieciach i systemach teleinformatycznych. Umożliwiłoby to identyfikację potencjalnego naruszenia, które dopiero może przerodzić się w incydent. Bez takich wymogów działalność operatorów kluczowych będzie wyłącznie reaktywna, a przez to nie będzie zapewniała usługom kluczowym odpowiedniego poziomu bezpieczeństwa. Ponadto operatorzy powinni mieć obowiązek analizy zaistniałych incydentów i dostosowywania w oparciu o zebrane doświadczenia posiadanych przez siebie systemów. Wyjaśnienia ze strony Projektodawcy wymagają przepisy rozdziału 4 Projektu. Wskazać trzeba, że do obowiązków podmiotów publicznych należałoby dodać identyfikację możliwych potencjalnych ryzyk dla ich systemów - podobnie jak w przypadku operatorów usług kluczowych. Ponadto, w związku z wyspecjalizowanym charakterem nakładanych na nie wymogów, dopuścić należy możliwość zlecania prowadzenia ciążących na nich obowiązków podmiotom zewnętrznym, posiadającym odpowiednie akredytacje i doświadczenie. Odnosząc się do rozdziału 5 Projektu „Zadania CSIRT” wydaje się, że w sposób bardziej sformalizowany powinna zostać opisana współpraca wymienionych CSIRT. Rozważyć również należy dodanie do nich również CSIRT sektorowych, opisanie ich zadań i dodanie dla nich wymogów, które muszą spełniać. Zwrócić należy również uwagę, że wśród zadań CSIRT powinno zostać wymienione monitorowanie potencjalnych zagrożeń w sieci, a przez to bardziej proaktywne zapobieganie incydentom. Wymóg ten wydaje się być szczególnie uzasadniony w odniesieniu do CSIRT MON i CSIRT ABW, które będą prowadziły aktywną politykę w zakresie cyberbezpieczeństwa. Ich zadania w tym zakresie powinny zatem zostać uzupełnione. CSIRT powinny również, w uzasadnionych	Wyjaśnienie/Uwaga częściowo uwzględniona. Stosowne przepisy dotyczące obowiązku aktywnego monitorowania zdarzeń w sieciach teleinformatycznych znajdują się w przepisie art. 10 ust. 2 pkt. 5. Podmioty publiczne są zobowiązane jedynie do zgłaszania incydentów. Inne obowiązki w zakresie zapewnienia bezpieczeństwa systemów teleinformatycznych dla organów administracji rządowej nałożone są przez ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne. W kwestii CSIRT poziomu krajowego w opinii projektodawcy zasady wzajemnej współpracy są opisane w wystarczający sposób. Przepisy art. 28 ust. 1, 2 oraz ust. 3 pkt. 1 stanowią podstawę stałego monitorowania potencjalnych zagrożeń w sieci. Ustawa wprowadza konstrukcję zgłaszania poważnych i istotnych incydentów, oraz fakultatywnie incydentów zwykłych CSIRT poziomu krajowego, a nie organom właściwym.

			przypadkach, zajmować się obsługą incydentów powstałych u przedsiębiorców telekomunikacyjnych, które w nieodzowny sposób mogą się łączyć z incydentami zachodzącymi u operatorów usług kluczowych. Sporym brakiem w Projekcie jest brak wyraźnego wskazania na konieczność bezpiecznego projektowania, wdrażania i rozwijania systemów informatycznych. Pozwoliłoby to zaadresować ewentualne ryzyko kupowania przez jakieś podmioty zobowiązane ustawą do zachowania bezpieczeństwa niesprawdzonych lub narażających je na inwigilację. Wyjaśnienia ze strony projektodawcy wymaga, czy zgłoszenie incydentu do właściwego CSIRT zwalnia podmiot zobowiązany ustawą od obowiązku zgłaszania incydentu właściwym organom, a czynności z tego zakresu przeprowadzi CSIRT, czy też obowiązek ten będzie niezależnie spoczywał na poszczególnych podmiotach.	
10.	ogólna	Polska Izba Informatyki i Telekomunikacji	Brak publikacji kluczowych aktów wykonawczych. Uwzględniając, że nowe obowiązki oraz ograniczenia prowadzenia działalności gospodarczej mogą być wprowadzane wyłącznie w drodze ustawowej, wątpliwości budzi fakt, że do konsultacji nie zostały skierowane projekty obligatoryjnych rozporządzeń, których postanowienia będą bardzo istotne dla całego systemu ochrony cyberprzestrzeni, a tym samym mają kluczowy wpływ na ocenę całości proponowanych rozwiązań. W naszej ocenie, ustawa powinna być konsultowana i procedowana w pakiecie wraz ze wszystkimi (przynajmniej obligatoryjnymi) aktami wykonawczymi. Dodatkowo zwracamy uwagę, że trudno ustalić faktyczne i merytoryczne przesłanki uzasadniające decyzje o regulacji pewnych zagadnień na poziomie ustawowym, a część na poziomie aktów wykonawczych. Przykładowo, bardzo szczegółowo definiuje się wymagania funkcjonalne na system teleinformatyczny wspomagający obsługę incydentów, pozostawiając jednocześnie do regulacji w drodze rozporządzenia wydawanego przez ministra ds.	Wyjaśnienie. Należy mieć na uwadze, że materia regulowana ustawą i rozporządzeniami wykonawczymi dotyczy zagadnień o charakterze międzysektorowym, co w połączeniu z wizją przyjętego modelu regulacyjnego - poszerzenie kompetencji organów sektorowych w zakresie cyberbezpieczeństwa, zamiast ustanowienia jednego krajowego podmiotu ds. cyberbezpieczeństwa na poziomie centralnym, wymaga przeprowadzenia szeregu konsultacji dotyczących problematyki sektorowej (zagadnienia usług kluczowych, poważnych incydentów). Dodatkowo materiały robocze istotne z punktu widzenia rozporządzeń są jeszcze opracowywane przez odpowiednie podgrupy Grupy Współpracy, powołanej na podstawie Dyrektywy 2016/1148.

			informatyzacji istotne z punktu widzenia obrotu gospodarczego wymagania dla podmiotów świadczących usługi outsourcingu w zakresie cyberbezpieczeństwa. W tym kontekście, jako niespotykaną dotychczas praktykę odbieramy określenie w regulacji ustawowej (z zasady mało elastycznej i trudniejszej do zmiany) precyzyjnych wymagań dla systemu informatycznego i jego funkcjonalności (co wydaje się materią typowo wykonawczą), podczas gdy sam projekt ustawy nie określa w sposób jasny i precyzyjny podstawowego pojęcia, jakim ma być „incydent poważny".	
11.	ogólna	Polska Izba Informatyki i Telekomunikacji	Brak precyzyjnych zasad funkcjonowania jednostek zależnych od organów państwowych funkcjonujących również na rynku komercyjnym, w tym m.in. brak ograniczeń prowadzenia działalności komercyjnej przez jednostki wykonujące zadania CSIRT, w zakresie wynikającym z ustawy. W naszej ocenie podmiot pełniący funkcję CSIRT, powinien realizować wyłącznie zadania o charakterze publicznych i niekomercyjnym. Jego funkcjonowanie na rynku konkurencyjnym, budzi istotne wątpliwości, szczególnie w sytuacji, gdy możliwość pozyskiwania (z mocy prawa) informacji od innych podmiotów stawia go w uprzywilejowanej pozycji rynkowej.	Uwaga nieuwzględniona. Podmioty pełniące funkcję CSIRT realizują wyłączenie zadania o charakterze niekomercyjnym.
12.	ogólna	Polska Izba Informatyki i Telekomunikacji	Brak ograniczenia zakresu uprawnień nadzorczych organów nadzoru i kontroli wyłącznie do obszaru związanego bezpośrednio ze świadczeniem usług kluczowych.	Uwaga częściowo uwzględniona. Przepisy zostaną doprecyzowane.
13.	ogólna	Polska Izba Informatyki i Telekomunikacji	Brak określania wymagań dla „specjalistów" angażowanych przez organów nadzorczych na potrzeby prowadzonych przez te organy kontroli.	Uwaga częściowo uwzględniona. Przepisy zostaną przeredagowane.
14.	ogólna	Polska Izba Informatyki i	Bardzo szerokie uprawnienia, CSIRT-ów w zakresie możliwości żądania od operatorów telekomunikacyjnych udostępnienia informacji dot. ich działalności oraz przyjętych rozwiązań	Wyjaśnienie.

		Telekomunikacji	organizacyjno–technicznych, a także przyznania organom nadzoru prawa do wydawania wiążących zaleceń. Wprowadzenie takich rozwiązań, w szczególności z pominięciem analizy ryzyka i bez uwzględnienia zasady adekwatności stosowanych zabezpieczeń do zidentyfikowanych ryzyk, może w istotnym zakresie ograniczać swobodę działalności gospodarczej, a jednocześnie obniżać efektywność prowadzonych działań w obszarze cyberbezpieczeństwa.	Przepisy uwzględniają przedsiębiorców telekomunikacyjnych w krajowym systemie cyberbezpieczeństwa, ale z uwagi na ograniczenia określone w dyrektywie 2016/1148 ustawa nie będzie nakładać żadnych nowych obowiązków dotyczących bezpieczeństwa i zgłaszania incydentów, ponad te które są określone w Prawie telekomunikacyjnym.
15.	ogólna	Polska Izba Informatyki i Telekomunikacji	Brak jednego punktu zgłoszeń incydentów na poziomie krajowym, do którego można byłoby zgłaszać incydenty, a do którego odpowiedzialności należałoby odpowiednie przekierowanie incydentu wg właściwości. Takie rozwiązanie wydaje się efektywniejsze niż zaproponowany, dość skomplikowany model zgłaszania poszczególnych kategorii incydentów w Polsce. Warto w tym kontekście zauważyć, że liczba organów, do których przedsiębiorca powinien zgłaszać ewentualne incydenty, w ostatnim okresie, wraz ze stopniowym wprowadzaniem nowych rozwiązań legislacyjnych, znacząco wzrasta. Aktualnie obowiązki takie istnieją już w zakresie zgłoszeń do: UKE, GIODO, ministra ds. informatyzacji (odnośnie usług zaufania). Dodatkowo wprowadzony zostanie obowiązek wobec CSIRT NASK (odnośnie incydentów istotnych przy usługach cyfrowych), odpowiedni CSIRT (w zakresie incydentów poważnych przy usługach kluczowych). Liczne obowiązku sprawozdawcze, ograniczają funkcjonowanie przedsiębiorcom, a same w sobie nie przyczyniają się do zwiększenia poziomu cyberbezpieczeństwa użytkowników. Zasadnym jest utrzymanie dotychczasowego modelu zgłaszania incydentów do Urzędu Komunikacji Elektronicznej, który to urząd, pełni faktycznie rolę CSiRT dla branży telekomunikacyjnej i powinien być jedynym punktem kontaktowym do zgłaszania incydentów.	Uwaga nieuwzględniona. W opinii projektodawcy, przepisy jasno wskazują podmioty, do których zgłasza się incydenty.

16.	ogólna	Polska Izba Informatyki i Telekomunikacji	Brak jest zagwarantowania ochrony przepływu informacji wrażliwych dotyczących bezpieczeństwa, którymi będą się wymieniały poszczególne podmioty. Objęcie tych informacji (a w szczególności wymienianych za pomocą systemu teleinformatycznego który ma wdrożyć MC) ochroną prawną z założenia, w znaczący sposób podniesie poziom bezpieczeństwa przetwarzania danych. Ponadto informacje objęte poszczególnymi tajemnicami sektorowymi np. tajemnicą telekomunikacyjną czy bankową przekazywane do miejsce ich raportowań powinny być utrzymane w reżimie tej tajemnicy.	Uwaga nieuwzględniona. Projekt nie ma na celu wdrażania do systemu prawnego nowego typu tajemnicy prawnie chronionej.
17.	ogólna	Polska Izba Informatyki i Telekomunikacji	W delegacji do wydania rozporządzeń nie ma wytycznych do posługiwania się w rozporządzeniach obowiązującymi w tym zakresie normami i rekomendacjami ETSI oraz ENISA. Należało by rozważyć uzupełnienie tych delegacji o taki wymóg, analogicznie jak ma to miejsce w rozporządzeniu RM dotyczącym Krajowych Ram Interoperacyjności.	Uwaga nieuwzględniona. Nie ma potrzeby, aby powoływać się na normy i rekomendacje przy delegacjach do aktów wykonawczych.
18.	ogólna	Polska Izba Informatyki i Telekomunikacji	Incydent istotny Projekt nie definiuje incydentu istotnego, ale odsyła do przygotowywanej obecnie decyzji wykonawczej Komisji Europejskiej. Formułując definicję tego incydentu należy zapewnić, że zgłaszane powinny być wszelkiego rodzaju ataki które przerodziły się lub mogły się przerodzić w incydent i ich źródłem było nieautoryzowane działanie osób trzecich. Zgłaszanie wszystkich incydentów (np. czasowa niedostępność usługi) będzie kontrproduktywne, bo utrudni zidentyfikowanie CSIRT NASK realnych zagrożeń. Obecna wersja projektu decyzji wykonawczej stanowi: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-4460501_en Article 4 *Substantial impact of an incident* (*pominięto cytat*)	Uwaga nieuwzględniona. Na etapie incydentu nie jest zawsze możliwe określenie, czy ma on podłoże w interwencji osób trzecich, czy też nie. Zarówno dyrektywa, jak i projekt ustawy obowiązuje do obsługi incydentu niezależnie od jego przyczyny. Natomiast zgłaszanie incydentu dotyczy tylko incydentu istotnego, tj. przekraczającego wspomniane w decyzji wykonawczej progi.

19.	ogólna	Polska Izba Informatyki i Telekomunikacji	Brak jednoznacznego i nie budzącego wątpliwości określenia odpowiedzialności za obsługę incydentu poważnego – z jednej strony odpowiedzialność za obsługę incydentu spoczywa na operatorze, z drugiej strony projekt ustawy przewiduje wprost uprawnienia CSIRT w zakresie obsługi incydentów poważnych, nie wskazując przy tym zasad przejmowania przez CSIRT incydentów do obsługi oraz przyznając CSIRT pewne uprawnienia „władcze" wobec operatora (np. wezwanie za pośrednictwem organu właściwego operatora do usunięcia podatności, żądanie informacji itd.). Tym samym, CSIRT miałby możliwość ingerencji w działalność jednostkowego operatora z pominięciem jakiejkolwiek odpowiedzialności za podejmowane wobec operatora działania. Uszczegóławiając powyższe, zwracamy uwagę, że zgodnie z projektowanym art. 12 ust. 1 pkt 6 operator ma zapewnić obsługę incydentu poważnego i incydentu krytycznego we współpracy z właściwym CSIRT, w tym poinformować o usunięciu podatności, które doprowadziły lub mogły doprowadzić do poważnego incydentu. Na wniosek operatora CSIRT może zapewnić wsparcie w obsłudze lub obsługę poważnych incydentów (art. 28 ust.2), przy czym odpowiednio – zgodnie z projektowanym art. 28 ust. 2 - zadaniem CSIRT jest realizacja zadań na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewnienie koordynację obsługi poważnych incydentów. Natomiast zgodnie z projektowanym art. 28 ust. 5, 6 i 7 do zadań CSIRT należy obsługa lub koordynacja obsługi incydentów zgłaszanych przez wskazane w ustawie podmioty. Z tym uprawnieniem korelują uprawnienia CSIRT wskazane w art. 34, zgodnie z którym CSIRT może: „wykonywać niezbędne działania techniczne, związane z monitorowaniem zagrożeń, obsługa incydentów poważnych (…), a także dokonywać analiz (…)", „wystąpić do organu właściwego z wnioskiem o wezwanie	Wyjaśnienie. Założeniem projektodawcy było z jednej strony zapewnienie możliwości technicznej obsługi poważnych i krytycznych incydentów przez wyspecjalizowane do tego typu podmioty, czyli CSIRT poziomu krajowego. Z drugiej strony projektodawca chce zagwarantować, aby możliwe było zastosowanie władztwa o charakterze administracyjno-prawnym w przypadku działań na rzecz zapobiegania rozprzestrzeniania się incydentu. Przepisy art. 28 dot. uprawnień CSIRT przy koordynacji obsługi incydentów zostaną zmienione.

			operatora, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do poważnego incydentu" oraz „może wystąpić bezpośrednio do operatora o udostępnienie informacji technicznych związanych z incydentem, które będą niezbędne do przeprowadzenia analizy zdarzenia lub obsługi incydentu" W praktyce może to oznaczać, że dla jednego incydentu, właściwe będą dwa ośrodki, co w praktyce znacznie utrudni, o ile nie uniemożliwi jego właściwą obsługę. Po drugie, istnieje znaczące ryzyko, że CSIRT może definiować względem operatora nieadekwatne wymagania, które mogą generować nadmierne obciążenia kosztowe, jednocześnie nie stanowiąc najbardziej efektywnego rozwiązania zaistniałego problemu.	
20.	Ogólna	Business Centre Club	Niezależnie od treści samego Projektu, pragniemy zwrócić uwagę, iż w polskim kodeksie karnym wciąż brak jest takich pojęć jak cyberprzestępczość, przestępczość komputerowa, czy przestępczość internetowa. Biorąc pod uwagę potrzebę kompleksowego zmierzenia się ze zjawiskiem cyberprzestępczości - groźnym dla obywateli, przedsiębiorców, organów państwa oraz ekonomicznych interesów państwa - postulujemy pilne podjęcie prac, dzięki którym wszelkie nieautoryzowane działania przy zabezpieczeniach systemów byłyby ścigane z mocy prawa. Można byłoby m.in. wzorować się na rozwiązaniach przyjętych w Stanach Zjednoczonych, gdzie próba naruszenia stosowanych przez przedsiębiorców zabezpieczeń jest przestępstwem federalnym.	Wyjaśnienie. Zagadnienia te były przedmiotem rozmów pomiędzy resortami w ramach prac nad ustawą o krajowym systemie cyberbezpieczeństwa. Niezbędne są analizy dotyczące przepisów karnych i przepisów z zakresu ścigania przestępczości będące w kompetencji innych resortów. Ewentualne zmiany przepisów w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty.
21.	ogólna	Polska Izba Informatyki i Telekomunikacji	Pragniemy zwrócić uwagę, iż w polskim kodeksie karnym wciąż brak jest takich pojęć jak cyberprzestępczość, przestępczość komputerowa, czy przestępczość internetowa. Biorąc pod uwagę potrzebę kompleksowego zmierzenia się ze zjawiskiem cyberprzestępczości, groźnym dla obywateli, przedsiębiorców, organów państwa oraz ekonomicznych interesów państwa, postulujemy pilne podjęcie prac, dzięki którym wszelkie	Wyjaśnienie. Zagadnienia te były przedmiotem rozmów pomiędzy resortami w ramach prac nad ustawą o krajowym systemie cyberbezpieczeństwa. Niezbędne są analizy dotyczące przepisów karnych i przepisów z zakresu ścigania przestępczości będące w kompetencji innych

			nieautoryzowane działania przy zabezpieczeniach systemów byłyby ścigane z mocy prawa. Można byłoby, m.in. wzorować się na rozwiązaniach przyjętych w Stanach Zjednoczonych, gdzie próba naruszenia stosowanych przez przedsiębiorców zabezpieczeń jest przestępstwem federalnym.	resortów. Ewentualne zmiany przepisów w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty.
22.	ogólna	Polska Izba Informatyki i Telekomunikacji	Zgodnie z Dyrektywą ustawa ma być przyjęta do 9 maja a stosowana od 10 maja włącznie z tym, że operatorzy usług kluczowych mają być wskazani najpóźniej do 9 listopada. Ustawa ma vacatio legis tylko 14 dni. Pozostaje bardzo mało czasu na wdrożenie jakichkolwiek obowiązków wynikających z ustawy. Oczywiście niektóre podmioty mają zapewne już wdrożone wewnątrz organizacji część z obowiązków, jednak, nawet sam czas rekrutowania stanowiska specjalistycznego w cyberbezpieczeństwie, to nawet nie licząc ograniczeń finansowych, w Polsce około 6-9 miesięcy, a na świecie nawet bliżej roku. Przy obecnym vacatio legis dostosowanie się do zapisów ustawy w wymaganym terminie przez podmioty do tego zobowiązane wydaje się wątpliwym. Zasadnym jest opracowanie projektów rozporządzeń wykonawczych równolegle do rozpoczętego procesu legislacyjnego przedmiotowej ustawy oraz opracowanie terminów wejścia w życie rozporządzeń w taki sposób, aby wdrożenie wymogów ustawy było realizowalne.	Wyjaśnienie. W projekcie przewidziano że operatorzy usług kluczowych będą mieli czas na dostosowanie się do obowiązków wynikających z ustawy, w zależności od wskazanych obowiązków 3 lub 6 miesięcy od dnia otrzymania decyzji o uznaniu za operatora usługi kluczowej.
23.	ogólna	Polska Izba Radiodyfuzji Cyfrowej	Zgodnie z Dyrektywą ustawa ma być przyjęta do 9 maja a stosowana od 10 maja włącznie z tym, że operatorzy usług kluczowych mają być wskazani najpóźniej do 9 listopada. Ustawa ma vacatio legis tylko 14 dni. Pozostaje bardzo mało czasu na wdrożenie jakichkolwiek obowiązków wynikających z ustawy. Oczywiście niektóre podmioty mają zapewne już wdrożone wewnątrz organizacji część z obowiązków, jednak, nawet sam czas rekrutowania stanowiska specjalistycznego w cyberbezpieczeństwie, to nawet nie licząc ograniczeń finansowych, w Polsce około 6-9 miesięcy, a na świecie nawet bliżej roku. Przy	Wyjaśnienie. Projektodawca nie podziela powyższych zastrzeżeń, w tym faktu, że kwestie formalne i instytucjonalne nie odegrają istotnej roli prewencyjnej w zakresie cyberbezpieczeństwa. Wraz z wejściem w życie ustawy zaczną m.in. obowiązywać przepisy dotyczące CSIRT poziomu krajowego, zadań realizowanych przez ministra właściwego do spraw informatyzacji i organy właściwe. M.in. organy właściwe będą miały wskazany

			obecnym vacatio legis dostosowanie się do zapisów ustawy w wymaganym terminie przez podmioty do tego zobowiązane wydaje się wątpliwym. Jak wynika z uzasadnienia Projektu oraz uzasadnienia do niego, celem regulacji jest rozbudowa systemu cyberbezpieczeństwa państw członkowskich Unii Europejskiej. Z jednej strony stawiany jest nacisk na aspekty formalne i instytucjonalne. Chodzi m. in. o utworzenie zespołów reagowania , kwalifikację incydentów, stworzenie katalogu operatorów usług kluczowych, obowiązek wyznaczenia osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług, obowiązek stworzenia spójnego i kompletnego systemu zarządzania ryzykiem w zakresie cyberbezpieczeństwa lub wreszcie stworzenie katalogu organów właściwych do spraw cyberbezpieczeństwa. Faktem jest, że kwestie formalne i instytucjonalne nie odegrają istotnej, a może nawet żadnej, roli prewencyjnej w zakresie cyberbezpieczeństwa.	w ustawie czas na przeprowadzenie procedur administracyjnych w sprawie identyfikacji operatorów usług kluczowych – do ok. 10 listopada 2018 r. Od momentu doręczenia decyzji operatorzy usług kluczowych będą mieli natomiast 3 lub 6 miesięcy na dostosowanie do przepisów ustawy. Uwzględniając powyższe harmonogramy można założyć, że będzie to wystarczający czas na dostosowanie się do wymagań.
24.	ogólna	Polska Izba Radiodyfuzji Cyfrowej	Postulat wprowadzenia przepisów karnych penalizujących czyny zagrażające cyberbezpieczeństwu, w tym obejmujących zawinione zaniechania realizacji obowiązków nakładanych Projektem. Pragniemy zwrócić uwagę, iż w polskim kodeksie karnym wciąż brak jest takich pojęć jak cyberprzestępczość, przestępczość komputerowa, czy przestępczość internetowa. Biorąc pod uwagę potrzebę kompleksowego zmierzenia się ze zjawiskiem cyberprzestępczości, groźnym dla obywateli, przedsiębiorców, organów państwa oraz ekonomicznych interesów państwa, postulujemy pilne podjęcie prac, dzięki którym wszelkie nieautoryzowane działania przy zabezpieczeniach systemów byłyby ścigane z mocy prawa. Można byłoby, m.in. wzorować się na rozwiązaniach przyjętych w Stanach Zjednoczonych, gdzie próba naruszenia stosowanych przez przedsiębiorców zabezpieczeń jest przestępstwem federalnym.	Wyjaśnienie. Zagadnienia te były przedmiotem rozmów pomiędzy resortami w ramach prac nad ustawą o krajowym systemie cyberbezpieczeństwa. Niezbędne są analizy dotyczące przepisów karnych i przepisów z zakresu ścigania przestępczości będące w kompetencji innych resortów. Ewentualne zmiany przepisów w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty. Uwaga uwzględniona w zakresie wysokości kar pieniężnych.

			Prewencja w tym zakresie i słusznie jest realizowana zgodnie z Projektem poprzez Rozdział 10 zatytułowany „Przepisy o karach pieniężnych" (vide art. 57 i n. Projektu). Maksymalną karą pieniężną przewidzianą Projektem jest 200.000,00 (dwieście tysięcy) złotych. Maksymalna wysokość kar pieniężnych jest rażąco niska. Porównać je można chociażby z karami finansowymi przewidzianymi w projekcie ustawy o ochronie danych osobowych z 12 września 2017 roku, który odsyła do Rozporządzenia ogólnego o ochronie danych osobowych z 27 kwietnia 2016 roku, które przewiduje kary pieniężne aż do 20 mln EURO lub do 4 % światowego obrotu podmiotu dokonującego naruszenia. Zważywszy na istotę regulacji wprowadzanych Projektem, w tym dla bezpieczeństwa obywateli i Państwa, w pełni uzasadnione jest twierdzenie, że naruszenia obowiązków nakładanych Projektem, w tym przez operatorów usług kluczowych, powinny penalizowane przepisami karnymi. Szeroko rozumiane bezpieczeństwo obywateli i Państwa jest ponad wszelką wątpliwość przedmiotem ochrony Projektu. Zauważyć należy, że przewidziane w Projekcie kary pieniężne są niewielkie. Przekładać się to będzie na marginalne traktowanie omawianych regulacji przez podmioty, które powinny stać na straży cyberbezpieczeństwa. Po drugie, kary finansowe mają być nakładane na instytucje, nie zaś osoby, które sprawują w nich funkcje kierownicze. Tym samym osoby pełniące te funkcje, co do zasady, będą miały mniejszą motywację rzetelnego stosowania się do postanowień Projektu niż, gdyby przewidywał on sankcje karne, które z natury swojej dotykałyby te właśnie osoby. Wprowadzenie penalizacji działań i zaniechań, których skutkiem będzie lub może być uniemożliwienie wzrostu albo zamach na cyberbezpierzeństwo Rzeczpospolitej Polski wydaje się konieczne, zważywszy na doniosłość tego zagadnienia dla przyszłości kraju. Przepisy Kodeksu karnego, w tym dotyczące przestępstw przeciwko	

			bezpieczeństwu powszechnemu (art. 163 i n. Kodeksu karnego) w żadnym stopniu nie przystają do istniejących zagrożeń płynących z cyberprzestrzeni.	
25.	Uwaga ogólna	Pracodawcy RP	Na wstępie należy zwrócić uwagę na przyjęty model regulacji, który w bardzo wysokim stopniu ingeruje w swobodę działalności gospodarczej podmiotów rynkowych, poprzez nałożenie dodatkowych obowiązków (wypełnienie ich będzie wpływało na podstawową działalność gospodarczą przedsiębiorców). Jednocześnie nakładane obowiązki wydają się nie wyczerpywać przesłanki proporcjonalności w tym sensie, że dla wykonania założeń ustawy, czyli znacznego podniesienia poziomu cyberbezpieczeństwa, wystarczające byłyby obowiązki sformułowane w sposób mniej dotkliwy. Spełnienie obowiązków odbywałoby się z zachowaniem zasad kontroli nad działalnością wyznaczonych CSIRT-ów, w szczególności w zakresie instytucji tzw. „wiążących poleceń" i „środków zaradczych". Aktualny kształt projektu, zdaje się bowiem przyznawać podmiotom zewnętrznym prawo do ingerencji w obszar prowadzonej działalności oraz sposób organizacji przedsiębiorstwa, w zbyt daleko idącym zakresie. Represyjny charakter przyjmowanych rozwiązań zdają się potwierdzać przedstawione w OSR analizy, które z góry zakładają liczbę nakładanych rocznie kar na podmioty objęte ustawą (str. 8 OSR). Biorąc powyższe pod uwagę, przedstawiamy nasze uwagi do projektu ustawy. Zaznaczamy jednocześnie, że w całości wymaga on także dodatkowych poprawek merytorycznych i legislacyjnych. Na tym etapie odnosimy się wyłącznie do zagadnień najistotniejszych, których uwzględnienie powinno powodować istotne zmiany treści i brzmienia poszczególnych przepisów, a tym samym czynić uwagi szczegółowe bezprzedmiotowymi. Poza powyższym, zwracamy uwagę, że liczne propozycje zawarte w projekcie, odnoszące się do możliwości władczego, pozbawionego	Wyjaśnienie. Założeniem projektodawcy było z jednej strony zapewnienie możliwości technicznej obsługi poważnych i krytycznych incydentów przez wyspecjalizowane do tego typu podmioty, czyli CSIRT poziomu krajowego. Z drugiej strony projektodawca chce zagwarantować, aby możliwe było zastosowanie władztwa o charakterze administracyjno-prawnym w przypadku działań na rzecz zapobiegania rozprzestrzeniania się incydentu.

			kontroli oraz uprawnienia strony kontrolowanej/nadzorowanej do jakiejkolwiek obrony, budzą nasze istotne wątpliwości pod kątem poszanowania przynajmniej swobody działalności gospodarczej. Przede wszystkim więc wnosimy o ponowną analizę projektu pod tym kątem, aby w przyszłości rozwiązania ustawowe nie musiały być kwestionowane.	
26.	Uwaga ogólna	Pracodawcy RP	Konieczność publikacji wszystkich podstawowych aktów wykonawczych i przeprowadzenia ich konsultacji równolegle z projektem ustawy. Mamy świadomość, że formalny obowiązek przedłożenia projektów aktów wykonawczych aktualizuje się dopiero na etapie prac Rady Ministrów, jednak potencjalna wartość merytoryczna przewidzianych do wydania rozporządzeń, uzasadnia przeprowadzenie ich konsultacji społecznych na jak najwcześniejszym etapie prac. Przykładem takiego rozwiązania jest art. 11, który wprowadzić ma obowiązek opracowania dokumentacji dot. cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych. Brak tych wymagań nie pozwala na dokonanie oceny wprowadzanego w ustawie obowiązku. Dodatkowo zwracamy uwagę na to, że trudno ustalić faktyczne i merytoryczne przesłanki uzasadniające decyzje o regulacji pewnych zagadnień na poziomie ustawowym, a części na poziomie aktów wykonawczych. Przykładowo, bardzo szczegółowo definiuje się wymagania funkcjonalne na system teleinformatyczny wspomagający obsługę incydentów, pozostawiając jednocześnie do regulacji w drodze rozporządzenia wydawanego przez ministra ds. informatyzacji istotne z punktu widzenia obrotu gospodarczego wymagania dla podmiotów świadczących usługi outsourcingu w zakresie cyberbezpieczeństwa. W tym kontekście, jako niespotykaną dotychczas praktykę odbieramy określenie w regulacji ustawowej (z zasady mało elastycznej i trudniejszej do zmiany)	Wyjaśnienie. Akty wykonawcze do ustawy zostaną opublikowane na kolejnym etapie procesu legislacyjnego.

			precyzyjnych wymagań dla systemu informatycznego i jego funkcjonalności (co wydaje się materią typowo wykonawczą), podczas gdy sam projekt ustawy nie określa w sposób jasny i precyzyjny podstawowego pojęcia, jakim ma być „incydent poważny”. Postulat: Rekomendujemy przedstawienie do konsultacji wszystkich przewidzianych do wydania projektów rozporządzeń, a także wprowadzenie w projekcie ustawy odpowiednich przepisów uzależniających aktualizację obowiązków, od faktycznego wydania aktów wykonawczych. Dodatkowo należy przewidzieć odpowiednio długie okresy vacatio legis dla każdego z obowiązków, których szczegółowy zakres wykonania będzie określony w rozporządzeniu.	
27.	Uwaga ogólna	Pracodawcy RP	Rozproszony system raportowania incydentów Postulujemy uporządkowanie i scentralizowanie systemu raportowania różnych kategorii incydentów występujących w sieci. Aktualnie obowiązki takie istnieją już w zakresie zgłoszeń do: UKE, GIODO, ministra ds. informatyzacji (odnośnie usług zaufania). Dodatkowo wprowadzony zostanie obowiązek wobec CSIRT NASK (odnośnie incydentów istotnych przy usługach cyfrowych) oraz odpowiedni CSIRT (w zakresie incydentów poważnych przy usługach kluczowych). Postulat: Należy rozważyć wskazanie jednego podmiotu na poziomie centralnym, który będzie przyjmował zgłoszenia i przekierowywał je do właściwych jednostek, zgodnie z wprowadzaną w innych obszarach koncepcją jednego punktu kontaktowego, czy np. jednego numeru dla połączeń alarmowych.	Uwaga nieuwzględniona. Projektodawca jest w pełni świadomy, że pomysł centralnego mechanizmu zgłaszania różnych incydentów jest słuszny, jednak trudny do realizacji w obecnym stanie prawnym. Incydenty mają różny charakter i różne podstawy prawne, które wynikają czasami z różnych przepisów unijnych, są też związane często z konkretnymi sektorami. Wymagane są dodatkowe analizy nt. liczby i typów zgłaszanych incydentów i nie jest wykluczona realizacja tego typu projektu w przyszłości.
28.	Uwaga ogólna	Pracodawcy RP	Niewystarczająca koordynacja ze strony CSIRT-ów w zakresie profilaktyki i prewencji Zapisy projektu w niewystarczającym stopniu adresują potrzebę zapewnienia wsparcia i koordynacji ze strony CSIRT-ów w zakresie	Uwaga nieuwzględniona. W opinii projektodawcy przepisy dotyczące profilaktyki i prewencji cyberbezpieczeństwa zostały

			profilaktyki i prewencji oraz w sytuacjach kryzysowych dla podmiotów zobowiązanych do stosowania ustawy. Poprzez profilaktykę i prewencję rozumiemy współpracę i edukację prowadzoną przez CSIRT nakierunkowaną na ograniczanie liczy incydentów poważnych w ramach całego kraju. Potrzeba koordynacji w sytuacjach kryzysowych to np. jednoczesny atak cybernetyczny na wiele podmiotów w różnych sektorach, podczas którego szybki i sprawny przepływ informacji, a także decyzyjność, są kluczowe dla opanowania sytuacji. Taką rolę koordynacyjną powinien pełnić CSIRT. Postulat: Zapewnienie lepszej koordynacji w zgodzie z powyższym opisem.	wyczerpujące opisane jako zadanie ministra właściwego do spraw informatyzacji (art. 41), zadanie organu właściwego (art. 39) i CSIRT poziomu krajowego (art. 28).
29.	Uwaga ogólna	Pracodawcy RP	Różne CSIRT-y zamiast jednego ośrodka Nasze wątpliwości budzi powołanie różnych CSIRT-ów – MON, GOV, NASK. Nie negując potrzeby zachowania pewnej izolacji informacji przekazywanych w ramach różnych CSIRT-ów, np. MON – obszar obronności, GOV – obszar biznesowy, niemniej natura zagrożeń jest podobna. Nierzadko może zajść sytuacja jednoczesnego ataku na infrastrukturę podlegającą pod różne CSIRT-y, a opanowanie sytuacji będzie niepotrzebnie wydłużone o czas potrzebny na komunikację i uzgodnienia między CSIRT-ami. Postulat: Rozważenie ujednolicenia CSIRT-ów w celu usprawnienia funkcjonowania w sytuacjach kryzysowych.	Uwaga nieuwzględniona. W opinii projektodawcy przepisy dotyczące usprawnienia funkcjonowania w sytuacjach kryzysowych są wystarczające. Ustawa zawiera przepisy dotyczące Zespołu ds. Incydentów Krytycznych oraz zawiera mechanizmy uruchamiania Rządowego Zespołu Zarządzania Kryzysowego.
30.	Uwaga ogólna	Pracodawcy RP	Niejasne zasady funkcjonowania podmiotów wskazanych w ustawie na rynku komercyjnym Sygnalizujemy, że wprowadzane w ustawie rozwiązania nie zawierają ograniczeń w zakresie prowadzenia działalności komercyjnej przez wskazane w ustawie jednostki wykonujące zadania CSIRT. Z uwagi na fakt, że podmioty te będą wykorzystywać środki publiczne, a także będą uprawnione do prowadzenia kontroli, w tym bezpośredniego wpływania na działania podmiotów	Uwaga nieuwzględniona. Podmioty pełniące funkcję CSIRT realizują wyłączenie zadania o charakterze niekomercyjnym.

			gospodarczych w obszarze cyberbezpieczeństwa, znajdą się w pozycji daleko uprzywilejowanej wobec podmiotów czysto rynkowych. Wątpliwości te pogłębia fakt, że wśród podmiotów wymienionych w projekcie ustawy znajdują się podmioty obecne już dzisiaj na rynku konkurencyjnym. Dopuszczenie działalności komercyjnej w takich przypadkach wydaje się nieuzasadnione. Można byłoby je porównywać do potencjalnego uprawnienia służb np. Policji do świadczenia prywatnych usług detektywistycznych, czy chociażby Krajowej Administracji Skarbowej w zakresie doradztwa podatkowego i gospodarczego. W tych przykładowych jedynie przypadkach konflikt interesów jest naturalnie rozpoznawalny, a świadczenie takich usług nie jest dopuszczone. Postulat: Wprowadzenie do ustawy zapisu wskazującego, że podmioty wykonujące zadania określone w ustawie nie mogą wykonywać działalność komercyjnej, w tym świadczyć odpłatnych i nieodpłatnych usług dla innych podmiotów.	
31.	Uwaga ogólna	Pracodawcy RP	Brak kompleksowego podejścia do zjawiska cyberzagrożeń, w tym działalności o charakterze przestępczym Projekt ustawy, koncentrując się na systemie instytucjonalnym oraz nowych obowiązkach usługodawców, pomija zasadnicze wręcz zagadnienia penalizacji zachowań godzących w bezpieczeństwo w sieci. W tym kontekście trzeba zwrócić uwagę, że Kodeks karny pozbawiony jest kompleksowych regulacji odnoszących się do zagadnień takich jak cyberprzestępczość, przestępczość komputerowa, czy przestępczość internetowa. Tym samym aparat państwa nie posiada wystarczającego instrumentarium prawnego do walki z podmiotami celowo, a często w sposób zorganizowany i nakierowany na cele zarobkowe doprowadzają do występowania w sieci zjawisk groźnych dla całości społeczeństwa, gospodarki, a nawet funkcjonowania organów państwa. Postulat:	Wyjaśnienie. Kwestia była przedmiotem uzgodnień pomiędzy resortami w ramach prac nad ustawą o krajowym systemie cyberbezpieczeństwa. Podjęta została decyzja o uregulowaniu kwestii dotyczących przestępczości w odrębnej ustawie, która będzie w przyszłości przygotowana przez Ministerstwo Sprawiedliwości.

			Postulujemy wprowadzenie rozwiązań dotyczących penalizacji i ścigania z urzędu cyberprzestępczości, w szczególności w zakresie dokonywania naruszeń i prób naruszeń istniejących w systemach przedsiębiorców i administracji systemów zabezpieczeń. Podobne rozwiązania zostały przyjęte w Stanach Zjednoczonych.	
32.	ogólna	Związek Pracodawców Branży Internetowej IAB Polska	Niezależnie od treści samego Projektu, pragniemy zwrócić uwagę, iż w polskim kodeksie karnym wciąż brak jest takich pojęć jak cyberprzestępczość, przestępczość komputerowa, czy przestępczość internetowa. Biorąc pod uwagę potrzebę kompleksowego zmierzenia się ze zjawiskiem cyberprzestępczości - groźnym dla obywateli, przedsiębiorców, organów państwa oraz ekonomicznych interesów państwa - postulujemy pilne podjęcie prac, dzięki którym wszelkie nieautoryzowane działania przy zabezpieczeniach systemów byłyby ścigane z mocy prawa. Można byłoby m.in. wzorować się na rozwiązaniach przyjętych w Stanach Zjednoczonych, gdzie próba naruszenia stosowanych przez przedsiębiorców zabezpieczeń jest przestępstwem federalnym.	Wyjaśnienie. Zagadnienia te były przedmiotem rozmów pomiędzy resortami w ramach prac nad ustawą o krajowym systemie cyberbezpieczeństwa. Niezbędne są analizy dotyczące przepisów karnych i przepisów z zakresu ścigania przestępczości będące w kompetencji innych resortów. Ewentualne zmiany przepisów w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty.
33.	ogólna	Związek Banków Polskich	Brak szczegółowych przepisów w tzw. ustawach sektorowych	Wyjaśnienie. Poszczególne sektory nie zgłosiły potrzeb zasadniczych zmian w przepisach sektorowych.
34.	ogólna	Związek Banków Polskich	Brak faktycznego zarządcy krajowym systemem cyberbezpieczeństwa RP. W chwili obecnej kwestie cyberbezpieczeństwa są w kompetencjach: MON, MSWiA, Ministra Koordynatora ds. Służb Specjalnych. Brak podmiotu, który faktycznie sprawowałby nadzór nad funkcjonowaniem całego systemu, jego aktualizacją oraz zarządzania środkami publicznymi. Ministerstwo Cyfryzacji, jako resort cywilny nie będzie nadrozować resortów siłowych. Taki nadzór powinien być sprawowany przez	Uwaga uwzględniona. Planowane jest rozszerzenie o przepisy przewidujące powołanie przy Radzie Ministrów Kolegium do spraw Cyberbezpieczeństwa w skład którego wchodzić będzie Minister Koordynator Służb Specjalnych, MON, MSWiA, MC i RCB.

			ciało, które gromadziłoby przedstawicieli wszystkich interesariuszy odpowiedzialnych za cyberbezpieczeństwo sektora publicznego, cyberbezpieczeństwo sektora prywatnego oraz cyberbezpieczeństwo obywateli.	
35.	ogólna	Związek Banków Polskich	Cel ustawy nie jest określony jasno i właściwie zarówno w zakresie tego "co" ma być chronione oraz tego "jak" ma być chronione.	Wyjaśnienie. Cel ustawy został określony w art. 3 ust. 1.
36.	ogólna	Związek Banków Polskich	Brak jest określenia zakresu podmiotowego stosowania ustawy np. wskazując, że ustawa ma zastosowanie wobec podmiotów świadczących usługi kluczowe lub usługi cyfrowe, które są świadczone przy użyciu lub są zależne od cyberprzestrzeni Rzeczypospolitej Polskiej.	Uwaga nieuwzględniona. Zakres podmiotowy ustawy został określony w art. 4, 5 ust. 1 ustawy, natomiast w przypadku dostawców usług cyfrowych zastosowanie mają przepisy o charakterze jurysdykcyjnym wymienione w art. 17.
37.	ogólna	Związek Banków Polskich	Oprócz samego projektu ustawy o krajowym systemie cyberbezpieczeństwa z 31.10.2017 r. do opiniowania przedstawiony został jedynie Załącznik do ww. projektu, nie przedstawiono natomiast do weryfikacji treści rozporządzeń wykonawczych (dla przykładu - art. 6, art. 10 ust. 3, art. 11 ust. 3 i n.).	Wyjaśnienie. Należy mieć na uwadze, że materia regulowana ustawą i rozporządzeniami wykonawczymi dotyczy zagadnień o charakterze międzysektorowym, co w połączeniu z wizją przyjętego modelu regulacyjnego - poszerzenie kompetencji organów sektorowych w zakresie cyberbezpieczeństwa, zamiast ustanowienia jednego krajowego podmiotu ds. cyberbezpieczeństwa na poziomie centralnym, wymaga przeprowadzenia szeregu konsultacji dotyczących problematyki sektorowej (zagadnienia usług kluczowych, poważnych incydentów). Dodatkowo materiały robocze istotne z punktu widzenia rozporządzeń są jeszcze opracowywane przez odpowiednie podgrupy Grupy Współpracy, powołanej na podstawie Dyrektywy 2016/1148.

38.	ogólna	Związek Banków Polskich	W odniesieniu do kluczowych obowiązków dostawcy usług cyfrowych (choćby tych z art. 19 ust. 1) - należy wypełnić treścią (numerem) - pojawiające się w tekście projektu odwołania do decyzji wykonawczej Komisji Europejskiej 2017/.../UE (dla przykładu - art. 2 pkt 12), art. 21 ust. 1 pkt 4), art. 23 i n.).	Wyjaśnienie. Planowane jest przyjęcie decyzji wykonawczej do dnia 19 grudnia 2017 r. Ministerstwo Cyfryzacji uczestniczy w pracach nad projektem przedmiotowego aktu prawnego.
39.	ogólna	Związek Banków Polskich	Brak w projekcie potrzeby powołania przy Premierze Rządu RP organu kolegialnego sprawującego nadzór nad krajowym systemem cyberbezpieczeństwa, którego misją byłoby zapewnienie wysokiego poziomu bezpieczeństwa podmiotom z sektora publicznego, prywatnego oraz obywatelom funkcjonującym w cyberprzestrzeni RP. Nadzór nad działalnością tego ciała powinien sprawować Prezes Rady Ministrów lub wskazana przez niego osoba np. w randze Ministra – Pełnomocnika Rządu.	Uwaga uwzględniona. Planowane jest rozszerzenie o przepisy przewidujące powołanie przy Radzie Ministrów Kolegium do spraw Cyberbezpieczeństwa w skład którego wchodzić będzie Minister Koordynator Służb Specjalnych, MON, MSWiA, MC i RCB.
40.	ogólna	Związek Banków Polskich	Brak w projekcie możliwości żądania przez Operatorów usług kluczowych od swoich pracowników oraz kandydatów do pracy zaświadczeń potwierdzających ich niekaralność, o których mowa w ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym, a także przedłożenie informacji w oparciu o dane zgromadzone przez instytucje, w szczególności o których mowa w art. 105 ust. 4 ustawy - Prawa bankowego;	Uwaga nieuwzględniona. Środki bezpieczeństwa osobowego powinny być dostosowane do charakteru przetwarzanych informacji. Inne środki będą stosowane przez podmioty publiczne, które przetwarzają informacje niejawne, a inne przez podmioty prywatne, przetwarzające głównie dane osobowe albo inne informacje prawnie chronione. Ze względu na powyższe nie jest zasadne ich precyzowanie.
41.	ogólna	Związek Banków Polskich	Brak w projekcie możliwości, w przypadkach postępowań karnych o wykorzystywanie operatora usług kluczowych oraz dostawcy usług cyfrowych do celu ukrycia działań przestępczych lub dla celów mających związek z przestępstwem, w szczególności, o którym mowa w art. 165a lub art. 299 Kodeksu karnego, ochrony tożsamości pracowników tego operatora usług kluczowych lub	Wyjaśnienie. Zagadnienia te były przedmiotem rozmów pomiędzy resortami w ramach prac nad ustawą o krajowym systemie cyberbezpieczeństwa. Niezbędne są analizy dotyczące przepisów karnych i przepisów z zakresu

			dostawcy usług cyfrowych (poprzez anonimizację ich danych osobowych) występujący w tych postępowaniach w charakterze świadków są objęci ochroną prawną zapewniającą im bezpieczeństwo;	ścigania przestępczości będące w kompetencji innych resortów. Ewentualne zmiany przepisów w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty.
42.	ogólna	Związek Banków Polskich	Brak w projekcie ochrony operatora usług kluczowych lub dostawcy usług cyfrowych, a także ich pracowników - nieponoszenie odpowiedzialności cywilnej i karnej za szkodę, która może wynikać z wykonywania przez nich, właściwych państwu i na jego rzecz, ustawowych obowiązków w zakresie przeciwdziałaniu przestępstwom, gdy działając z należytą starannością i w dobrej wierze zgłosili właściwym organom zawiadomienie o podejrzeniu popełniania przestępstwa, a te po weryfikacji uznały podejrzenie za nieuzasadnione. W takich przypadkach odpowiedzialność za szkodę wynikłą z podjętych działań przez operatora usług kluczowych lub dostawcy usług cyfrowych i ich pracowników ponosi Skarb Państwa – mechanizmy stosowane już w innych rozwiązaniach prawnych;	Uwaga nieuwzględniona.
43.	ogólna	Związek Banków Polskich	Brak w projekcie ochrony operatorów usług kluczowych przed odpowiedzialnością względem użytkowników końcowych, jeżeli ci użytkownicy nie zachowali zasad bezpiecznego korzystania z usług kluczowych, a w szczególności doprowadzili do ujawnienia informacji poufnych związanych z identyfikacją i uwierzytelnieniem ich tożsamości.	Wyjaśnienie. Projektodawca zakłada w przepisie art. 15 ust. 1 pkt. 2 zapewnienie użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową. Ponadto, kwestie wyłączenia odpowiedzialności operatorów usług kluczowych wobec użytkowników, którzy sami doprowadzili do ujawnienia informacji powinna być regulowana w umowach oświadczenie danego rodzaju usług.

44.	ogólna	Związek Banków Polskich	Brak w projekcie wprowadzenia przepisu, którym operatorzy usług kluczowych będą zobowiązani do zapewnienia adekwatnych do zakresu świadczonych usług zasobów ludzkich, technicznych, organizacyjnych i finansowych. Jednocześnie te nakłady poniesione na cyberbezpieczeństwo przez operatorów usług kluczowych stanowią koszt uzyskania przychodu w rozumieniu odrębnych przepisów.	Uwaga nieuwzględniona. Stosowne rozwiązania znalazły się w art. 15 projektu.
45.	ogólna	Związek Banków Polskich	Brak w projekcie potrzeby powołania CSIRT narodowego, którego głównym zadaniem byłoby nadzorowanie, zarządzanie i wspieranie obsługi incydentów o skutku oddziaływania międzysektorowym i międzynarodowym oraz o stopniu istotności: istotnym i krytycznym. CSIRT narodowy powinien działań na zasadach istniejącego Centrum Antyterrorystycznego (CAT) i powinien skupiać przedstawicieli wszystkich interesariuszy odpowiedzialnych za cyberbezpieczeństwa RP;	Uwaga nieuwzględniona. Dyrektywa 2016/1148 nie ogranicza liczby ustanowionych CSIRT poziomu krajowego. Jednocześnie CSIRT poziomu krajowego ustanowione w projekcie ustawy realizują nadzorowanie, zarządzanie i wspieranie obsługi incydentów poważnych, istotnych i krytycznych.
46.	ogólna	Związek Banków Polskich	Brak w projekcie wprowadzenia przepisów, które umożliwią prokuraturze sprawowanie nadzoru nad pozyskiwaniem, przetwarzaniem, przechowywaniem i udostępnianiem informacji prawnie chronionych przez Policję, CSIRT GOV, CSIRT MON oraz inne instytucje uczestniczące w CSIRT narodowym odpowiedzialne za bezpieczeństwo wewnętrzne i porządek publiczny. Ponadto Prokurator Krajowy oddelegowuje do CSIRT narodowego prokuratorów zajmujących się zwalczaniem i ściganiem przestępstw popełnianych w cyberprzestrzeni RP, którzy są uprawnieni do koordynowania działań po stronie prokuratury na obszarze całego kraju, a także będą mieli dostęp do informacji prawnie chronionych;	Wyjaśnienie. Zagadnienia te były przedmiotem rozmów pomiędzy resortami w ramach prac nad ustawą o krajowym systemie cyberbezpieczeństwa. Niezbędne są analizy dotyczące przepisów karnych i przepisów z zakresu ścigania przestępczości będące w kompetencji innych resortów. Ewentualne zmiany przepisów w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty.
47.	ogólna	Związek Banków Polskich	Brak w projekcie wprowadzenia przepisów umożliwiających Komendantowi Głównemu Policji oddelegowanie do CSIRT narodowego funkcjonariuszy Policji zajmujących się zwalczaniem i ściganiem przestępstw popełnianych w cyberprzestrzeni RP w związku z realizacją zadań, o których w art. 1 ust. 2 ustawy z dnia 6	Wyjaśnienie. Zagadnienia te były przedmiotem rozmów pomiędzy resortami w ramach prac nad ustawą o krajowym systemie cyberbezpieczeństwa. Niezbędne są analizy

			kwietnia 1990 r. o Policji w obszarach: operacyjnym, rozpoznawczym oraz procesowym, a także badań i wsparcia. Funkcjonariusze ci powinni posiadać uprawnienia do koordynowania działań: operacyjnych, rozpoznawczych i procesowych po stronie Policji na obszarze całego kraju, a także do dostępu do informacji prawnie chronionych w celu ścigania i zwalczania przestępstw popełnianych w cyberprzestrzeni RP.	dotyczące przepisów karnych i przepisów z zakresu ścigania przestępczości będące w kompetencji innych resortów. Ewentualne zmiany przepisów w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty.
48.	ogólna	Związek Banków Polskich	Brak w projekcie wprowadzenia przepisów umożliwiających Szefowi Agencji Bezpieczeństwa Wewnętrznego oddelegowania do CSIRT narodowego funkcjonariuszy zajmujących się zwalczaniem i ściganiem przestępstw popełnianych w cyberprzestrzeni RP w związku z realizacją zadań, o których w art. 5 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu w obszarach: operacyjnym, rozpoznawczym oraz procesowym. Funkcjonariusze ci powinni posiadać uprawnienia koordynowania działań po stronie Agencji Bezpieczeństwa Wewnętrznego na obszarze całego kraju, a także do dostępu do informacji prawnie chronionych w celu ścigania i zwalczania przestępstw popełnianych w cyberprzestrzeni RP.	Uwaga nieuwzględniona z uwagi na przyjętą w projekcie koncepcję CSIRT poziomu krajowego.
49.	ogólna	Związek Banków Polskich	Brak w projekcie wprowadzenia przepisów umożliwiających Ministrowi Obrony Narodowej oddelegowanie do CSIRT narodowego swoich przedstawicieli zajmujących się zwalczaniem i ściganiem przestępstw popełnianych w cyberprzestrzeni RP w związku z realizacją zadań, o których w art. 3 ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej. Przedstawiciele ci powinni posiadać uprawnienia do koordynowania działań po stronie Ministra Obrony Narodowej na obszarze całego kraju, a także do dostępu do informacji prawnie chronionych w celu ścigania i zwalczania przestępstw popełnianych w cyberprzestrzeni RP.	Uwaga nieuwzględniona z uwagi na przyjętą w projekcie koncepcję CSIRT poziomu krajowego.

50.	ogólna	Związek Banków Polskich	Brak w projekcie potrzeby utworzenia CSIRT sektorowych dla sektorów i podsektorów wymienionych w załączniku nr II do dyrektywy NIS oraz sektora publicznego, w celu sprawnego koordynowania obsługi cyberincedentów. Dodatkowo powinna być przewidziana możliwość powierzenia funkcji CSIRT sektorowego CSIRT'owi komercyjnemu, w sytuacji kiedy dany sektor uznałby za nieopłacalne powołanie odrębnego własnego CSIRT.	Uwaga częściowo uwzględniona. Projekt zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa CSIRT jest zarezerwowana dla zespołów poziomu krajowego.
51.	ogólna	Związek Banków Polskich	Brak w projekcie potrzeby włączenia pośredniego CSIRT komercyjnych oraz ISAC pod warunkiem wpisania na listę prowadzoną przez pojedynczy punkt kontaktowy.	Wyjaśnienie. Projektodawca dopuszcza możliwość budowy wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo, bądź „outsourcingu" usług z zakresu cyberbezpieczeństwa. Celem zapewnienia świadczenia przez podmioty świadczące usług z zakresu cyberbezpieczeństwa na rzecz operatorów usług kluczowych na odpowiednim poziomie projekt ustawy określa wymagania dla takich podmiotów.
52.	ogólna	Związek Banków Polskich	Brak w projekcie umożliwienia CSIRT narodowemu, CSIRT sektorowym oraz CSIRT komercyjnym wytwarzania lub pozyskiwania urządzenia lub programy komputerowe, o których mowa w art. 269b Kodeksu karnego, oraz ich używania w celu określenia podatności ocenianego systemu na możliwość popełnienia przestępstw, jeżeli właściciel systemu wyraził na to zgodę.	Uwaga nieuwzględniona. Zastosowanie znajduje przepis art. 269b § 2 i art. 269c kodeksu karnego i nie ma konieczności tworzenia nowego przepisu.
53.	ogólna	Związek Banków Polskich	Brak w projekcie ochrony CSIRT narodowego lub CSIRT sektorowych przed odpowiedzialnością karną, jeśli w trakcie wykonywania obowiązków wynikających z ustawy o krajowym systemie cyberbezpieczeństwa wejdą w posiadanie materiałów lub informacji, których posiadanie jest zabronione, jeżeli: 1) niezwłocznie powiadomią o tym właściwe organy ochrony prawa i przekażą im te materiały i informacje z tym związane;	Wyjaśnienie. Z uwagi na przyjętą koncepcję CSIRT poziomu krajowego oraz uzupełnienie projektu ustawy o przepisy umocowujące organy właściwe do powoływania podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora

			2) usuną w sposób trwały te materiały i informacje, chyba, że organy ochrony prawa kierując się dobrem śledztwa postanowią inaczej. Przepis ten powinien mieć zastosowanie również wobec CSIRT komercyjnych wpisanych na listę, jeśli w trakcie świadczonych przez siebie usług wejdą w posiadanie materiałów, których posiadanie jest zabronione.	wprowadzenie takich przepisów nie znajduje uzasadnienia.
54.	ogólna	Związek Banków Polskich	Pracownicy przedstawicielstw CSIRT GOV, CSIRT MON i CSIRT sektorowych powinni być zobowiązani do posiadania poświadczeń dostępu do informacji niejawnych o klauzuli „poufne" lub wyższej.	Uwaga nieuwzględniona. Kwestie dostępu do informacji niejawnych reguluje ustawa o ochronie informacji niejawnych.
55.	ogólna	Związek Banków Polskich	Należy rozważyć wprowadzenie przepisów obligujących, w ramach krajowego system cyberbezpieczeństwa, podejmowanie następujące działania z obszaru edukacji: 1) edukacja użytkownika końcowego; 2) edukacja ekspercka; 3) obowiązki informacyjne (polityka informacyjna) o cyberincydentach.	Wyjaśnienie. Obowiązki informacyjne o incydentach zostały określone w przepisach art. 3, przepisy dotyczące wymagań operatorów usług kluczowych w zakresie kompetencji personelu i edukacji użytkownika końcowego w art. 15.
56.	ogólna	Związek Banków Polskich	Brak w projekcie wprowadzenia stosownych zmian w kodeksie karnym w zakresie ustanowienia kar oraz zwiększenia już istniejących związanych z cyberprzestępstwami popełnianymi na szkodę operatorów usług kluczowych oraz dostawców usług cyfrowych, a także ich klientów. Dodatkowo należy dostosować przepisy kodeksu postępowania karnego w przedmiotowym zakresie.	Wyjaśnienie. Zagadnienia te były przedmiotem rozmów pomiędzy resortami w ramach prac nad ustawą o krajowym systemie cyberbezpieczeństwa. Niezbędne są analizy dotyczące przepisów karnych i przepisów z zakresu ścigania przestępczości będące w kompetencji innych resortów. Ewentualne zmiany przepisów w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty.
57.	ogólna	Polska Organizacja Przemysłu i Handlu Naftowego	Dodatkowo, pragniemy wskazać, że Projekt nie precyzuje wielu obowiązków operatorów usług kluczowych, wskazując że poszczególne obowiązki lub wymagania będą określone w rozporządzeniach wykonawczych. Wobec czego treść rozporządzeń wykonawczych do Projektu, które mają znaczny wpływ na obowiązki	Wyjaśnienie. Projekt ustawy formułuje obowiązki w zakresie bezpieczeństwa teleinformatycznego operatorów usług kluczowych. Operatorzy usług kluczowych będą zobowiązani do wdrożenia i stosowania środków

			operatorów kluczowych również powinna być przedmiotem konsultacji.	technicznych i organizacyjnych, aby zapewnić bezpieczeństwo systemów informacyjnych służących do świadczenia usług kluczowych, szacowania ryzyka związanego z cyberbezpieczeństwem oraz przekazywania CSIRT poziomu krajowego informacji o zaistniałych incydentach, podejrzeniu wystąpienia incydentu oraz ich obsługi we współpracy ze wspomnianym CSIRT.
58.	ogólna	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponuje się rozważenie rozszerzenia listy podmiotów wymienionych w załączniku do projektu ustawy w podsektorze ‘energia elektryczna’ o wytwórców energii elektrycznej kluczowych z punktu widzenia bezpieczeństwa, ciągłości działania i odbudowy systemu elektroenergetycznego (o ile nie koliduje to z ustawą o zarządzaniu kryzysowym).	Uwaga uwzględniona. Załącznik zostanie poszerzony m.in. o wytwórców energii elektrycznej
59.	ogólna	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponuje się dokonać ewentualnego przeredagowania zapisów projektu ustawy bezpośrednio odnoszących się do definicji usługi kluczowej.	Uwaga uwzględniona.
60.	ogólna	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	W dokumencie występuje w kilku miejscach zapis o tym, że uzupełnieniem do ustawy będą rozporządzenia Rady Ministrów warunkujące sposób wdrożenia ustawy ukażą się znacząco późno po ogłoszeniu ustawy w skutek czego i tak krótki okres 6- ciu miesięcy dedykowany OUK a wdrożenie ustawy będzie znacząco skrócony co czyni zagrożenie dla rzetelnego wdrożenia ustawy.	Wyjaśnienie. Projektodawca nie podziela powyższych zastrzeżeń, Wraz z wejściem w życie ustawy organy właściwe będą miały wskazany w ustawie czas na przeprowadzenie procedur administracyjnych w sprawie identyfikacji operatorów usług kluczowych – do ok. 10 listopada 2018 r. Od momentu doręczenia decyzji operatorzy usług kluczowych będą miały natomiast 3 lub 6 miesięcy na dostosowanie do przepisów ustawy.

61.	ogólna	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Rozdział 2, art. 10, 11, 12 i 15 nakładają na Operatora Usług Kluczowych szereg obowiązków, spełnienie których będzie wymagało nakładów inwestycyjnych oraz organizacyjnych. Nie ma wskazanych źródeł finansowania. Jeśli obowiązki wynikające z projektu zostaną narzucone OSD, powinniśmy mieć pewność, iż będą one uwzględniane w taryfie. Np.: a) Operatorzy usług kluczowych – zwiększenie poziomu bezpieczeństwa świadczonych usług, poprzez wprowadzenie efektywnego zarządzania systemem cyberbezpieczeństwa, objęcie ochroną przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa. Nałożenie na operatorów dodatkowych obowiązków związanych z zapewnieniem bezpieczeństwa ich systemów informacyjnych, ciągłości świadczonych usług. Operatorzy usług kluczowych będą zobowiązani wskazać wśród swoich pracowników osobę odpowiedzialną za kwestie bezpieczeństwa teleinformatycznego. W przypadku konieczności zatrudnienia takiej osoby, przedsiębiorcy będą musieli się liczyć z kosztem od 5.000 zł do 10.000 zł brutto. Koszt jest zależny od kwalifikacji i obowiązków pracownika oraz od wielkości przedsiębiorcy. Koszt został policzony dla zatrudnienia 6 pracowników. Do tego należy doliczyć koszt utworzenia operacyjnego centrum bezpieczeństwa (SOC) – szacunkowo 1 mln zł oraz jego utrzymania – szacunkowo 2 mln zł, przy czym kwota ta może się zmienić w przypadku utworzenia sektorowego SOC albo skorzystania z komercyjnych usług podmiotu działającego na rynku. Operatorzy usług kluczowych będą zobowiązani m.in. ponieść koszty audytu zewnętrznego raz na dwa lata. Szacuje się, że koszt jednostkowy wykonania audytu wyniesie 50 tys. zł. Audyt po raz pierwszy będzie przeprowadzony w roku 2019 a następnie co 2 lata. a. Sektor energetyka, podsektor energia elektryczna Podsektor tworzą duże przedsiębiorstwa obsługujące wiele podmiotów, korzystające z systemów informacyjnych w znacznym stopniu. Wdrożenie regulacji przyczyni się do zapewnienia ciągłości dostaw	Wyjaśnienie. Środki niezbędne na realizację zadań wynikających z ustawy zostały oszacowane w sposób adekwatny. Należy zauważyć, że podmioty będące operatorami usług kluczowych w przeważającej większości z uwagi na ochronę świadczonych usług już mają wdrożone systemy bezpieczeństwa, a podmioty publiczne są zobowiązane je posiadać zgodnie z przepisami wykonawczymi wydanymi na podstawie ustawy o informatyzacji podmiotów realizujących zadania publiczne. Ponadto przeredagowano przepisy, wskazując na obowiązek wskazania osoby do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, co nie będzie uzasadniało konieczności zatrudniania dodatkowej osoby.

			prądu, zwiększy odporność przedsiębiorstw na ataki na infrastrukturę teleinformatyczną.	
62.	ogólna	Konfederacja Lewiatan	Brak precyzyjnych zasad funkcjonowania jednostek zależnych od organów państwowych funkcjonujących również na rynku komercyjnym, w tym m.in. brak ograniczeń prowadzenia działalności komercyjnej przez jednostki wykonujące zadania CSIRT, w zakresie wynikającym z ustawy. W naszej ocenie podmiot pełniący funkcję CSIRT, powinien realizować wyłącznie zadania o charakterze publicznych i niekomercyjnym. Jego funkcjonowanie na rynku konkurencyjnym, budzi istotne wątpliwości, szczególnie w sytuacji gdy możliwość pozyskiwania (z mocy prawa) informacji od innych podmiotów stawia go w uprzywilejowanej pozycji rynkowej.	Uwaga nieuwzględniona. CSIRT nie będą prowadziły działalności o charakterze komercyjnym.
63.	ogólna	Konfederacja Lewiatan	Brak ograniczenia zakresu uprawnień nadzorczych organów nadzoru i kontroli wyłącznie do obszaru związanego bezpośrednio ze świadczeniem usług kluczowych.	Uwaga nieuwzględniona.
64.	ogólna	Konfederacja Lewiatan	Brak określania wymagań dla „specjalistów” angażowanych przez organów nadzorczych na potrzeby prowadzonych przez te organy kontroli.	Uwaga częściowo uwzględniona. Przepisy zostaną przeredagowane.
65.	ogólna	Konfederacja Lewiatan	Bardzo szerokie uprawnienia, CSIRT-ów w zakresie możliwości żądania od operatorów telekomunikacyjnych udostępnienia informacji dot. ich działalności oraz przyjętych rozwiązań organizacyjno–technicznych, a także przyznania organom nadzoru prawa do wydawania wiążących zaleceń. Wprowadzenie takich rozwiązań, w szczególności z pominięciem analizy ryzyka i bez uwzględnienia zasady adekwatności stosowanych zabezpieczeń do zidentyfikowanych ryzyk, może w istotnym zakresie ograniczać swobodę działalności gospodarczej, a jednocześnie obniżać efektywność prowadzonych działań w obszarze cyberbezpieczeństwa.	Wyjaśnienie. Przepisy uwzględniają przedsiębiorców telekomunikacyjnych w krajowym systemie cyberbezpieczeństwa, ale z uwagi na ograniczenia określone w dyrektywie 2016/1148 ustawa nie będzie nakładać żadnych nowych obowiązków dotyczących bezpieczeństwa i zgłaszania incydentów, które są określone w Prawie telekomunikacyjnym.

66.	ogólna	Konfederacja Lewiatan	Brak publikacji kluczowych aktów wykonawczych. Uwzględniając, że nowe obowiązki oraz ograniczenia prowadzenia działalności gospodarczej mogą być wprowadzane wyłącznie w drodze ustawowej, wątpliwości budzi fakt, że do konsultacji nie zostały skierowane projekty obligatoryjnych rozporządzeń, których postanowienia będą bardzo istotne dla całego systemu ochrony cyberprzestrzeni, a tym samym mają kluczowy wpływ na ocenę całości proponowanych rozwiązań. W naszej ocenie, ustawa powinna być konsultowana i procedowana w pakiecie wraz ze wszystkimi (przynajmniej obligatoryjnymi) aktami wykonawczymi. Dodatkowo zwracamy uwagę, że trudno ustalić faktyczne i merytoryczne przesłanki uzasadniające decyzje o regulacji pewnych zagadnień na poziomie ustawowym, a część na poziomie aktów wykonawczych. Przykładowo, bardzo szczegółowo definiuje się wymagania funkcjonalne na system teleinformatyczny wspomagający obsługę incydentów, pozostawiając jednocześnie do regulacji w drodze rozporządzenia wydawanego przez ministra ds. informatyzacji istotne z punktu widzenia obrotu gospodarczego wymagania dla podmiotów świadczących usługi outsourcingu w zakresie cyberbezpieczeństwa. W tym kontekście, jako niespotykaną dotychczas praktykę odbieramy określenie w regulacji ustawowej (z zasady mało elastycznej i trudniejszej do zmiany) precyzyjnych wymagań dla systemu informatycznego i jego funkcjonalności (co wydaje się materią typowo wykonawczą), podczas gdy sam projekt ustawy nie określa w sposób jasny i precyzyjny podstawowego pojęcia, jakim ma być „incydent poważny”.	Wyjaśnienie. Należy mieć na uwadze, że materia regulowana ustawą i rozporządzeniami wykonawczymi dotyczy zagadnień o charakterze międzysektorowym, co w połączeniu z wizją przyjętego modelu regulacyjnego - poszerzenie kompetencji organów sektorowych w zakresie cyberbezpieczeństwa, zamiast ustanowienia jednego krajowego podmiotu ds. cyberbezpieczeństwa na poziomie centralnym, wymaga przeprowadzenia szeregu konsultacji dotyczących problematyki sektorowej (zagadnienia usług kluczowych, poważnych incydentów). Dodatkowo materiały robocze istotne z punktu widzenia rozporządzeń są jeszcze opracowywane przez odpowiednie podgrupy Grupy Współpracy, powołanej na podstawie Dyrektywy 2016/1148.
67.	ogólna	Konfederacja Lewiatan	Brak jednego punktu zgłoszeń incydentów na poziomie krajowym, do którego można byłoby zgłaszać incydenty, a do którego odpowiedzialności należałoby odpowiednie przekierowanie incydentu wg właściwości. Takie rozwiązanie wydaje się efektywniejsze, niż zaproponowany, dość skomplikowany model	Uwaga nieuwzględniona. Projektodawca jest w pełni świadomy, że pomysł centralnego mechanizmu zgłaszania różnych incydentów jest słuszny, jednak trudny do realizacji w

			zgłaszania poszczególnych kategorii incydentów w Polsce. Warto w tym kontekście zauważyć, że liczba organów, do których przedsiębiorca powinien zgłaszać ewentualne incydenty, w ostatnim okresie, wraz ze stopniowym wprowadzaniem nowych rozwiązań legislacyjnych, znacząco wzrasta. Aktualnie obowiązki takie istnieją już w zakresie zgłoszeń do: UKE, GIODO, ministra ds. informatyzacji (odnośnie usług zaufania). Dodatkowo wprowadzony zostanie obowiązek wobec CSIRT NASK (odnośnie incydentów istotnych przy usługach cyfrowych), odpowiedni CSIRT (w zakresie incydentów poważnych przy usługach kluczowych). Liczne obowiązku sprawozdawcze, ograniczają funkcjonowanie przedsiębiorcom, a same w sobie nie przyczyniają się do zwiększenia poziomu cyberbezpieczeństwa użytkowników.	obecnym stanie prawnym. Incydenty mają różny charakter i różne podstawy prawne, które wynikają czasami z różnych przepisów unijnych, są też związane często z konkretnymi sektorami. Wymagane są dodatkowe analizy nt. liczby i typów zgłaszanych incydentów i nie jest wykluczona realizacja tego typu projektu w przyszłości.
68.	ogólna	Konfederacja Lewiatan	Brak jednoznacznego i nie budzącego wątpliwości określenia odpowiedzialności za obsługę incydentu poważnego – z jednej strony odpowiedzialność za obsługę incydentu spoczywa na operatorze, z drugiej strony projekt ustawy przewiduje wprost uprawnienia CSIRT w zakresie obsługi incydentów poważnych, nie wskazując przy tym zasad przejmowania przez CSIRT incydentów do obsługi oraz przyznając CSIRT pewne uprawnienia „władcze" wobec operatora (np. wezwanie za pośrednictwem organu właściwego operatora do usunięcia podatności, żądanie informacji itd.). Tym samym, CSIRT miałby możliwość ingerencji w działalność jednostkowego operatora z pominięciem jakiejkolwiek odpowiedzialności za podejmowane wobec operatora działania. Uszczegóławiając powyższe, zwracamy uwagę, że zgodnie z projektowanym art. 12 ust. 1 pkt 6 operator ma zapewnić obsługę incydentu poważnego i incydentu krytycznego we współpracy z właściwym CSIRT, w tym poinformować o usunięciu podatności, które doprowadziły lub mogły doprowadzić do poważnego incydentu.	Wyjaśnienie. Założeniem projektodawcy było z jednej strony zapewnienie możliwości technicznej obsługi poważnych i krytycznych incydentów przez wyspecjalizowane do tego typu podmioty, czyli CSIRT poziomu krajowego. Z drugiej strony projektodawca chce zagwarantować, aby możliwe było zastosowanie władztwa o charakterze administracyjno-prawnym w przypadku działań na rzecz zapobiegania rozprzestrzeniania się incydentu. Przeredagowane zostaną przepisy art. 28 dotyczące CSIRT.

			Na wniosek operatora CSIRT może zapewnić wsparcie w obsłudze lub obsługę poważnych incydentów (art. 28 ust.2), przy czym odpowiednio – zgodnie z projektowanym art. 28 ust. 2 - zadaniem CSIRT jest realizacja zadań na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewnienie koordynację obsługi poważnych incydentów. Natomiast zgodnie z projektowanym art. 28 ust. 5, 6 i 7 do zadań CSIRT należy obsługa lub koordynacja obsługi incydentów zgłaszanych przez wskazane w ustawie podmioty. Z tym uprawnieniem korelują uprawnienia CSIRT wskazane w art. 34, zgodnie z którym CSIRT może: „wykonywać niezbędne działania techniczne, związane z monitorowaniem zagrożeń, obsługa incydentów poważnych (…), a także dokonywać analiz (…)”, „wystąpić do organu właściwego z wnioskiem o wezwanie operatora, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do poważnego incydentu” oraz „może wystąpić bezpośrednio do operatora o udostępnienie informacji technicznych związanych z incydentem, które będą niezbędne do przeprowadzenia analizy zdarzenia lub obsługi incydentu” W praktyce może to oznaczać, że dla jednego incydentu, właściwe będą dwa ośrodki, co w praktyce znacznie utrudni, o ile nie uniemożliwi jego właściwą obsługę. Po drugie, istnieje znaczące ryzyko, że CSIRT może definiować względem operatora nieadekwatne wymagania, które mogą generować nadmierne obciążenia kosztowe, jednocześnie nie stanowiąc najbardziej efektywnego rozwiązania zaistniałego problemu.	
69.	ogólna	Konfederacja Lewiatan	Pragniemy zwrócić uwagę, iż w polskim kodeksie karnym wciąż brak jest takich pojęć jak cyberprzestępczość, przestępczość komputerowa, czy przestępczość internetowa. Biorąc pod uwagę potrzebę kompleksowego zmierzenia się ze zjawiskiem	Wyjaśnienie. Zagadnienia te były przedmiotem rozmów pomiędzy resortami w ramach prac nad ustawą o krajowym

			cyberprzestępczości, groźnym dla obywateli, przedsiębiorców, organów państwa oraz ekonomicznych interesów państwa, postulujemy pilne podjęcie prac, dzięki którym wszelkie nieautoryzowane działania przy zabezpieczeniach systemów byłyby ścigane z mocy prawa. Można byłoby, m.in. wzorować się na rozwiązaniach przyjętych w Stanach Zjednoczonych, gdzie próba naruszenia stosowanych przez przedsiębiorców zabezpieczeń jest przestępstwem federalnym.	systemie cyberbezpieczeństwa. Niezbędne są analizy dotyczące przepisów karnych i przepisów z zakresu ścigania przestępczości będące w kompetencji innych resortów. Ewentualne zmiany przepisów w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty.
70.	ogólna	A.K. (uwagi osoby prywatnej)	Ustawa stanowi konglomerat rzeczy ważnych i mało istotnych, często o charakterze operacyjnym, których wprowadzenie do regulacji ustawowej przesłania cel ustawowy oraz pozostaje w sprzeczności z zasadami poprawnej legislacji, w tym m.in. zasadą dostatecznej określoności przepisów prawa oraz zasadą bezpieczeństwa prawnego i pewności prawa. W obecnej postaci Ustawa jest bardzo nierówna. Są fragmenty napisane bardzo dobrze, są fragmenty, które zdecydowanie w dokumencie na takim poziomie znaleźć się nie powinny. Niestety znając rynek łatwo widać, kto lub z czyjej inspiracji, pisał poszczególne fragmenty Ustawy. Nietrudno zgadnąć co np. jest z inspiracji NASK ("chciejstwa" w zakresie zadań NASK), a co dopisał zespół dyr. (np. specyfikacja systemu teleinformatycznego wpisana wprost w Ustawę, a nie w SIWZ - bo nawet Rozporządzenie to za wysoki dokument na taką specyfikację - to nowum - nie spotkałem się z taką konstrukcją w żadnej z Ustaw).	Wyjaśnienie. Projekt ustawy powstawał w Ministerstwie Cyfryzacji. Ministerstwo prowadziło prace z ministerstwami, które uczestniczyły w pracach międzyresortowego zespołu roboczego ds. przygotowania ustawy (skład osobowy bazował na zespole ds. opracowania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022). Przeprowadzono również konsultacje wewnątrz resortu Ministerstwa Cyfryzacji i prekonsultacje. Zgodnie z Regulaminem pracy Rady Ministrów w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny w dniu 2 listopada br. udostępniony został projekt ustawy o krajowym systemie cyberbezpieczeństwa. Został wyznaczony 14-dniowy termin na zgłaszanie uwag w ramach uzgodnień międzyresortowych, konsultacji publicznych i opiniowania.

71.	ogólna	A.K. (uwagi osoby prywatnej)	W obecnej formie Ustawa nie przyczyni się niestety do podniesienia poziomu cyberbezpieczeństwa krajowego. Ustawa nie sprzyja budowaniu zaufania do państwa przewidując niekontrolowany wpływ państwa na podmioty gospodarcze, rozszerzając uprawnienia władcze organów państwowych wobec podmiotów gospodarczych oraz wpływając negatywnie na konkurencyjność gospodarczą i uczciwą konkurencję w kraju w szczególności poprzez: - brak precyzyjnych zasad funkcjonowania jednostek zależnych od organów państwowych na rynku komercyjnym, w tym m.in. brak zakazu prowadzenia działalności komercyjnej w zakresie wynikającym z ustawy dla jednostek wykonujących zadania CSIRT; Żaden podmiot CSIRT nie powinien świadczyć usług komercyjnych, o których mowa w Ustawie, ponieważ stawia to go w uprzywilejowanej pozycji rynkowej z racji pozyskiwania informacji od innych podmiotów (ryzyko nieuczciwej konkurencji); - niedookreślenie zakresu uprawnień nadzorczych organów nadzoru i kontroli wyłącznie do obszaru związanego bezpośrednio ze świadczeniem usług kluczowych; - brak wymagań dla specjalistów wykorzystywanym przez organy nadzorcze na potrzeby prowadzonych przez organ kontroli; - zapewnienia CSIRT-om prawa do niekontrolowanego żądania od operatorów udostępnia informacji dot. ich działalności oraz przyjętych rozwiązań organizacyjno – technicznych oraz prawa organom nadzoru do wydawania wiążących zaleceń (z pominięciem analizy ryzyka i bez uwzględnienia zasady adekwatności stosowanych zabezpieczeń do zidentyfikowanych ryzyk).	Wyjaśnienie. Projektodawca nie podziela powyższych zastrzeżeń, w tym faktu, że kwestie formalne i instytucjonalne nie odegrają istotnej roli prewencyjnej w zakresie cyberbezpieczeństwa. Wraz z wejściem w życie ustawy zaczną m.in. obowiązywać przepisy dotyczące CSIRT poziomu krajowego, zadań realizowanych przez ministra właściwego do spraw informatyzacji i organy właściwe. Zostaną doprecyzowane przepisy dotyczące zasad współpracy operatorów z właściwym CSIRT w taki sposób, by zapewnić ochronę interesów handlowych operatora. CSIRT nie będą prowadziły działalności o charakterze komercyjnym.
72.	ogólna	A.K. (uwagi osoby prywatnej)	Znaczna część istotnej materii regulacyjnej została wyłączona do uregulowania w drodze aktów niższego rzędu bez wskazania terminu, w jakim akty wykonawcze zostaną wydane. Ustawa powinna wejść w pakiecie wraz z aktami wykonawczymi. Poza tym projektodawca nie wykazuje konsekwencji przyjmując określone obszary do regulacji ustawowej, a część wyłączając do regulacji w	Wyjaśnienie. Należy mieć na uwadze, że materia regulowana ustawą i rozporządzeniami wykonawczymi dotyczy zagadnień o charakterze międzysektorowym, co w połączeniu z wizją przyjętego modelu regulacyjnego -

			drodze rozporządzeń, tzn. np. bardzo szczegółowo definiuje się wymagania funkcjonalne na system teleinformatyczny wspomagający obsługę incydentów, pozostawiając jednocześnie do regulacji w drodze rozporządzenia wydawanego przez ministra ds. informatyzacji istotne z punktu widzenia biznesu wymagania bezpieczeństwa dla podmiotów świadczących usługi outsourcingu w zakresie cyberbezpieczeństwa. Warto zaznaczyć, że niespotykaną dotychczas praktyką jest to, że w regulacji ustawowej precyzyjnie opisuje się wymagania dla systemu informatycznego i jego funkcjonalności (materia typowo wykonawcza), podczas gdy z uwagi na brak informacji, co będzie uznane za incydent poważny, nie wiadomo nawet w jakim zakresie będzie wykorzystywany i czy jest faktycznie potrzebny. Czytając zawartą w Ustawie definicję potrafiłbym wdrożyć taki system w mniej niż rok czasu z budżetem poniżej 1 mln zł. Pytanie, czy o taki system chodzi, czy zaproponowane zapisy są nieadekwatne.	poszerzenie kompetencji organów sektorowych w zakresie cyberbezpieczeństwa, zamiast ustanowienia jednego krajowego podmiotu ds. cyberbezpieczeństwa na poziomie centralnym, wymaga przeprowadzenia szeregu konsultacji dotyczących problematyki sektorowej (zagadnienia usług kluczowych, poważnych incydentów). Dodatkowo materiały robocze istotne z punktu widzenia rozporządzeń są jeszcze opracowywane przez odpowiednie podgrupy Grupy Współpracy, powołanej na podstawie Dyrektywy 2016/1148.
73.	ogólna	A.K. (uwagi osoby prywatnej)	Zaproponowano niespójny i skomplikowany model zgłaszania poszczególnych kategorii incydentów w Polsce – brak jednego punktu zgłoszeń incydentów na poziomie krajowym, do którego można zgłaszać incydenty, a do którego odpowiedzialności należałoby odpowiednie przekierowanie incydentu wg właściwości. Liczba organów, do których przedsiębiorca powinien zgłaszać ewentualne incydenty wzrasta wraz z każdą Ustawą. A miała maleć - po to koordynacja i system! Aktualnie mamy zgłaszać incydenty do: UKE, GIODO, ministra ds. informatyzacji (odnośnie usług zaufania), teraz dochodzi CSIRT NASK (odnośnie incydentów istotnych przy usługach cyfrowych), odpowiedni CSIRT (w zakresie incydentów poważnych przy usługach kluczowych). Nie ułatwia to funkcjonowania przedsiębiorcom, a co ważniejsze nie przyczynia się do zwiększenia poziomu cyberbezpieczeństwa użytkowników. Zróżnicowanie zasad zgłaszania poszczególnych kategorii incydentów, różnorodność terminów notyfikacji incydentów, różny	Uwaga nieuwzględniona. Projektodawca jest w pełni świadomy, że pomysł centralnego mechanizmu zgłaszania różnych incydentów jest słuszny, jednak trudny do realizacji w obecnym stanie prawnym. Incydenty mają różny charakter i różne podstawy prawne, które wynikają czasami z różnych przepisów unijnych, są też związane często z konkretnymi sektorami. Wymagane są dodatkowe analizy nt. liczby i typów zgłaszanych incydentów i nie jest wykluczona realizacja tego typu projektu w przyszłości.

			poziom obowiązków w zakresie raportowania poincydentalnego nie ułatwia realizacji przez przedsiębiorców tych zadań, a w kontekście wdrożenia systemu teleinformatycznego wspomagającego zgłaszania i obsługę incydentów dopiero od 1.01.2021 r. nie wygląda optymistycznie.	
74.	ogólna	A.K. (uwagi osoby prywatnej)	Ustawa skupia się tak naprawdę na systemie zgłaszania incydentów związanych z cyberbezpieczeństwem. Mało mówi o prewencji, monitorowaniu stanu normalnego i wyszukiwaniu incydentów na podstawie anomalii (arrakis? sondy? sandboxy?). Nic nie mówi o obowiązkach operatorów w zakresie usługi infrastruktury krytycznej i abonentów.	Wyjaśnienie. Stosowne przepisy dotyczące obowiązku aktywnego monitorowania zdarzeń w sieciach teleinformatycznych znajdują się w przepisie art. 10 ust. 2 pkt. 5.
75.	ogólna	A.K. (uwagi osoby prywatnej)	Na dziś projekt głównie nakłada obowiązki, nie bardzo precyzując profity i obowiązki administracji centralnej. A takie powinno być przesłanie: tworzymy system, w ramach tego systemu przekazujecie dane, te dane przetwarzamy, w zamian dajemy wam informacje o istotnych zdarzeniach wynikających z tych danych, korelacji zdarzeń pomiędzy podmiotami czy wręcz sektorami, informacje od służb zagranicznych, informacje podane do rozpowszechnienia przez ABW. Wspieramy was w rozwiązywaniu problemów, zdejmujemy z was wybrane problemy prawne, np. występując w waszym imieniu do sprawnie działających sądów czy jednostek policji w celu podjęcia działań. Na dziś zgłoszenie cyberprzestępstwa przez ISP do organów jest drogą przez mękę.	Wyjaśnienie. Przepisy precyzujące zachęty dla operatorów usług kluczowych i dostawców usług cyfrowych znalazły się głównie w art. 41 i art. 42. Projektodawca zakłada, że działania wspierające budowanie zdolności i kompetencji w zakresie cyberbezpieczeństwa wśród operatorów usług kluczowych, operatorów infrastruktury krytycznej oraz dostawców usług cyfrowych będą również realizowane w ramach planu działań i projektów szczegółowych wynikających ze Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej”.
76.	ogólna	A.K. (uwagi osoby prywatnej)	Słabo opisana jest rola współpracy międzysektorowej, np. operatorów telekomunikacyjnych z sektorem bankowym czy energetycznym (taka współpraca już występuje), i jej koordynacja czy też wspieranie przez MC/NASK/ABW. Będziemy mieli coraz więcej incydentów międzysektorowych, zwłaszcza w kontekście spodziewanego boomu na IoT.	Uwaga częściowo uwzględniona. Projekt zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa

				CSIRT jest zarezerwowana dla zespołów poziomu krajowego.
77.	ogólna	Instytut Logistyki i Magazynowania	Podział odpowiedzialności krajowych CSIRT Jeżeli intencją ustawodawcy było odseparowanie zagadnień cyberbezpieczeństwa związanych z obronnością państwa to wydzielenie CSIRT MON wydaje się słuszne. Jednak podział odpowiedzialności za pozostałe elementy pomiędzy CSIRT GOV i CSIRT NASK jest już prawdopodobnie nadmiarowe. Będzie komplikowało organizację całego systemu przez co ograniczy skuteczność reakcji na incydenty i zidentyfikowane ryzyka.	Wyjaśnienie. Wszyscy operatorzy usług kluczowych będący jednocześnie operatorami infrastruktury krytycznej są zobowiązani zgłaszać incydenty do CSIRT GOV.
78.	ogólna	Instytut Logistyki i Magazynowania	Wspólny system teleinformatyczny Jeżeli założeniem wydzielenia CSIRT MON od pozostałych krajowych CSIRT jest specjalna ochrona wrażliwego obszaru bezpieczeństwa kraju to wykorzystywanie do zarządzania incydentami wspólnego systemu teleinformatycznego może stwarzać ryzyko niezachowania poufności danych MON. Mimo zapisów art.42 ust.16 wskazane jest fizyczne rozdzielenie teleinformatycznych systemów wsparcia dla uczestników nadzorowanych przez CSIRT MON i dla pozostałych uczestników (to mogą być dwie instancje tego samego systemu).	Wyjaśnienie. Bezpieczeństwo funkcjonowania systemu jest zagadnieniem o fundamentalnym znaczeniu. Dlatego też Minister Cyfryzacji, projektując system, dokłada najwyższej staranności w aspekcie bezpieczeństwa. Przewiduje się, że architektura bezpieczeństwa systemu będzie konsultowana z CSIRT GOV i CSIRT MON. W systemie zakłada się realizację zasady wiedzy koniecznej i projekt ustawy w tym zakresie zostanie zmodyfikowany. Administrator systemu będzie zarządzał uprawnieniami administracyjnymi zgodnie z ww. zasadą wiedzy koniecznej. Dokumentacja bezpieczeństwa systemu zostanie skonsultowana z CSIRT GOV i CSIRT MON. W ocenie projektodawcy zapewnienie jednego narzędzia, w którym gromadzone będą dane z trzech CSIRT jest jednym z mechanizmów koordynacji na poziomie krajowym i umożliwi uzyskanie pełnego obrazu cyberbezpieczeństwa państwa i

				przeprowadzenie bieżącej analizy ryzyka na poziomie kraju. Nie jest zasadne regulowanie na poziomie ustawy szczegółowych funkcjonalności systemu, które to kwestie będą omawiane na spotkaniach roboczych trzech CSIRT.
79.	ogólna	Instytut Logistyki i Magazynowania	Informacje o audytach bezpieczeństwa teleinformatycznego Projekt zobowiązuje operatorów usług kluczowych do przeprowadzania audytów zgodności wdrożonego systemu zarządzania bezpieczeństwem z przepisami ustawy. Dostawcy usług cyfrowych świadczonych na rzecz operatorów usług kluczowych powinni być zobowiązani do przekazywania wyników audytów bezpieczeństwa teleinformatycznego do właściwych CSIRT.	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE.
80.	ogólna	Instytut Logistyki i Magazynowania	Współpraca CSIRT z firmami komercyjnymi Należy rozważyć możliwość wprowadzenia zapisów umożliwiających wymianę informacji o incydentach również z centrami cyberbezpieczeństwa firm komercyjnych nie będących uczestnikami systemu.	Wyjaśnienie. Projekt dopuszcza dobrowolne zgłaszanie incydentów art. 28 ust. 6 pkt. 5.
81.	ogólna	Instytut Logistyki i Magazynowania	Zgłaszanie incydentów. W obowiązkach uczestników zapisano zgłoszenia: • operatorzy usług krytycznych – zgłaszają incydenty poważne (w ciągu 24 h) • dostawcy usług cyfrowych – zgłaszają incydenty istotne (w ciągu 24h) • podmioty publiczne – zgłaszają incydenty poważne (w ciągu 24h) Incydenty zwykłe są zgłaszane opcjonalnie ale nie wiadomo co operatorzy i podmioty publiczne są zobowiązani robić z incydentami istotnymi a dostawcy z incydentami poważnymi. Uczestnicy systemu powinni mieć możliwość zgłaszania incydentów bezpieczeństwa każdej z klas. Natomiast sposób ich obsługi (w tym	Uwaga częściowo uwzględniona. Przepisy dotyczące incydentów zostaną częściowo zmienione.

			KPI) będzie dostosowany do klasy incydentu i uwzględniać specyfikę procesu obsługi po stronie uczestnika. Ogólnie parametry KPI (np. czasy zgłoszenia, reakcji, naprawy, itp.) nie powinny być definiowane na poziomie ustawy, ponieważ np. konieczność ich ewentualnego skrócenia w warunkach zagrożenia będzie trwało zbyt długo. Na liście zadań CSIRT nie ma samodzielnego rejestrowania i zgłaszania incydentów, dlaczego?	
82.	ogólna	Instytut Logistyki i Magazynowania	Zakres informacyjny zgłoszenia incydentu (dla operatora art.13 ust.1 dla dostawcy art.21.1 dla podmiotów publicznych nie określono) Dla podmiotów publicznych nie określono zakresu informacyjnego zgłoszenia. Jeżeli definicja ma być taka sama jak dla operatora usługi kluczowej to trzeba to ująć w art.13 ust.1. Uczestnicy mogą zgłaszać incydenty zwykłe ale dla nich nie zdefiniowano zakresu informacyjnego. Definicje zakresu informacyjnego zgłoszeń dla incydentów różnych klas powinny poprzedzać opis obowiązków uczestników.	Uwaga częściowo uwzględniona. Przepisy dotyczące incydentów zostaną częściowo zmienione.
83.	ogólna	J.K. (uwaga od osoby prywatnej)	Ustawa skupia się na reagowaniu na zaistniałe zdarzenia. Brakuje instytucji, która zajmowałaby się opracowaniem specyfikacji dla sprzętu i oprogramowania zwiększającej odporność na ingerencję z zewnątrz. W obecnej praktyce nie wykorzystuje się twardych zabezpieczeń jakie są możliwe przy odpowiedniej konfiguracji sprzętu. Chyba dla wygody, obecnie zrezygnowano z zabezpieczeń które były stosowane w początkach stosowania PC.	Wyjaśnienie. Projekt ustawy formułuje obowiązki w zakresie bezpieczeństwa teleinformatycznego operatorów usług kluczowych. Szczegółowe obowiązki dotyczące bezpieczeństwa, w tym potencjalnie specyfikacji dla sprzętu i oprogramowania mogą zostać określone w przygotowywanych przez organy właściwe rekomendacjach do działań mających na celu wzmocnienie cyberbezpieczeństwa.
84.	ogólna	Federacja Przedsiębiorców Polskich	Wskazać należy, że incydenty bezpieczeństwa w systemach informacyjnych, takie jak ujawnienie, przejęcie lub utrata danych, wywołują w przeważającej mierze skutki niemożliwe do usunięcia. Jest to o tyle istotne, że w dzisiejszych czasach przetwarza się w ten	Uwaga nieuwzględniona. Charakter prewencyjny ustawy, o którym mowa w uwadze objawia się w wymogach art. 10 ust. 2 pkt 7-9.

			sposób zdecydowaną większość danych. Poufność raz przejętych lub ujawnionych danych nigdy nie zostanie przywrócona. Dlatego też najważniejsze jest położenie nacisku na prewencyjny charakter ustawy.	
85.	ogólna	Federacja Przedsiębiorców Polskich	W projekcie ustawy widoczne są rozbudowane przepisy dotyczące kwestii formalnych i instytucjonalnych. Faktem jest, że kwestie formalne i instytucjonalne nie odegrają istotnej, a może nawet żadnej, roli prewencyjnej w zakresie cyberbezpieczeństwa. W tym celu należy wprowadzić surowe przepisy sankcjonujące naruszenia, włącznie z przepisami karnymi (prewencja poprzez odstraszenie) oraz doprecyzować przepisy dotyczące wymaganych zabezpieczeń systemów informacyjnych (prewencja poprzez techniczne zabezpieczenie).	Wyjaśnienie. Projektodawca nie podziela powyższych zastrzeżeń, w tym faktu, że kwestie formalne i instytucjonalne nie odegrają istotnej roli prewencyjnej w zakresie cyberbezpieczeństwa. Wraz z wejściem w życie ustawy zaczną m.in. obowiązywać przepisy dotyczące CSIRT poziomu krajowego, zadań realizowanych przez ministra właściwego do spraw informatyzacji i organy właściwe. Ponadto, ewentualne zmiany przepisów karnych i przepisów dotyczących ścigania w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty.
86.	ogólna	Instytut Audytorów Wewnętrznych IIA Polska	Projekt nie uwzględnia istniejących aktów prawnych, które określają istotne kryteria w zakresie kwalifikacji i kompetencji oraz podstaw niezbędnych dla prawidłowego i rzetelnego zapewnienia o stanie bezpieczeństwa IT. Są to: Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych (Dz.U. nr 177 poz. 1195), oraz Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2012 poz. 526 z późn. zm.). Tym samym, określona w art. 16. ust 1. projektu, perspektywa fakultatywnego przeprowadzania audytu bezpieczeństwa teleinformatycznego co najmniej raz na dwa lata, jest nie tylko niespójna z wymogiem zapewnienia okresowego audytu	Uwaga częściowo uwzględniona.

			wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok (§ 20 ust. 2. pkt. 14 rozporządzenia Rady Ministrów z dn. 12 kwietnia 2012 r. w sprawie KRI...), ale rodzi wysokie ryzyko powstania nieprawidłowości skutkujących istotnymi naruszeniami systemu cyberbezpieczeństwa. Z kolei art. 16. ust 2. projektu przewiduje przeprowadzanie audytu przez akredytowaną jednostkę oceniającą zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłości działania. Istniejący porządek prawny przewiduje możliwość akredytacji wyłącznie dla akredytacji bezpieczeństwa teleinformatycznego systemów teleinformatycznych przeznaczonych do przetwarzania krajowych informacji niejawnych. Tym samym, projekt ustawy wprowadza rozwiązanie, dla którego brak jakichkolwiek odniesień prawnych, a także nie uwzględnia wymogu posiadania stosownych kwalifikacji i kompetencji, potwierdzonych certyfikatami uprawniającymi do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych. Ponadto, pojęcia użyte w ust. 1 i 2 nie tożsame, ponieważ wdrożenie systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania nie gwarantuje dostatecznego poziomu bezpieczeństwa teleinformatycznego. „Art. 16. 1. Operatorzy usług kluczowych przeprowadzają, co najmniej raz na dwa lata audytu bezpieczeństwa teleinformatycznego, zwany dalej „audytem". 2. Audyt jest przeprowadzany przez akredytowaną jednostkę oceniającą zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania." Jednocześnie zwracamy uwagę na nierealne terminy raportowania zgłoszeń o incydentach, w szczególności o ich rozwiązaniu, przyczynach oraz skutkach. Wyrażamy pogląd, iż raportowanie o wystąpieniu incydentu w określonym czasie jest słuszne, jednakże przekazywanie jednocześnie pełnej informacji o przyczynach i sposobach rozwiązania incydentu, wydaje się zadaniem wątpliwym z praktycznego i rzeczywistego punktu widzenia. Oczywiście	

			popieramy przekazanie takiej informacji, jednakże w momencie zebrania takich danych i po przeprowadzeniu wnikliwej analizy.	
87.	art. 2 [w piśmie z uwagami błędnie określone jako art. 1]	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Brak definicji pojęcia „incydent" i „usługa kluczowa" „podmiotu świadczącego usługi z zakresu cyberbezpieczeństwa" – do których odnoszą się dalsze przepisy i wynikają z nich określone obowiązki.	Uwaga uwzględniona. Zmieniono definicję incydentu i zrezygnowano z wyodrębnienia incydentu zwykłego. Posłużenie się różnymi kategoriami incydentów wynika z konieczności rozróżnienia incydentów dla operatorów usług kluczowych (incydenty poważne) oraz dostawców usług cyfrowych (incydenty istotne). Termin „usługa kluczowa" zostanie zdefiniowany.
88.	art. 2	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Proponuje się rozszerzenie o definicję usługi kluczowej (podejście analogiczne do zastosowanego np. w odniesieniu do usługi cyfrowej).	Uwaga uwzględniona.
89.	art. 2	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	W art. 2 zawierającym definicje wskazujemy na brak definicji Incydentu Bezpieczeństwa Komputerowego - w ramach którego rozróżnione zostaną systemy IT od systemów OT (technologicznych), a także brak definicji systemu IT i OT. Brak jasnego zdefiniowania zakresu cyberbezpieczeństwa, który zmienia się ze względu na implementację rozporządzenia NIS w tym dokumencie, powoduje, że podmioty będące adresatem tej ustawy nie będą w 100% pewne zakresu ochrony usług i procesów, szczególnie, że definiuje się systemy informatyczne, które inaczej są nazywane w świecie IT a inaczej w świecie sieci technologicznych. Przykładem może tu być branża energetyczna, gdzie w przypadku systemów i sieci technologicznych mówi się o „łączności" i „systemach SCADA. Należy pamiętać, że będzie to pierwsze	Wyjaśnienie. Definicja systemu teleinformatycznego obejmuje zarówno systemy IT jak i systemy OT – nie ma konieczności rozróżniania tych dwóch definicji. Warto zaznaczyć, że w automatyce przemysłowej mówi się jeszcze o wielu innych kwestiach, a nie tylko o łączności. IACS (*Industrial Automation and Control Systems*) to nie tylko SCADA, ale też PLC, przetworniki wielkości nieelektrycznych na elektryczne, serwomechanizmy, transmisja danych w

			poważne „zderzenie” świata z unormowanymi i ustandaryzowanymi protokołami ze światem, gdzie prawie każdy z liczących się producentów automatyki i systemów do sterowania sieciami technologicznymi „stworzył” swój własny protokół transmisyjny.	specjalizowanych sieciach (np. RS 422/485, CANBus, ARING 429, mil-std-1553b, a także Ethernet).
90.	art. 2	Izba Gospodarcza Gazownictwa	Brak definicji usługi kluczowej, pojawia się definicja usług cyfrowych, operatora usług cyfrowych, operatora usługi kluczowej a nie ma definicji co rozumie się pod „usługa kluczowa”	Uwaga uwzględniona.
91.	art. 2	A.K. (uwagi osoby prywatnej)	W ustawie stosujemy skrót CSIRT, który nie jest literalnie nigdzie rozwinięty. Należy dopisać angielskie brzmienie, lub zmienić skrót.	Wyjaśnienie. Określenie CSIRT zostało zdefiniowane w art. 2 pkt, 1 jako Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego. W treści ustawy nie stanowi to skrótu z języka obcego z uwagi na przepisy ustawy o języku polskim z dnia 7 października 1999 r.
92.	art. 2 w zw. art. 56 ust. 3 pkt 5 i dalsze	Izba Gospodarcza Gazownictwa	Wyrażamy wątpliwość czy podejście do oceny ryzyka wskazane w art. 56 pkt ust. 3 pkt 5 należy rozumieć jako metodykę według której będzie odbywać się systematyczne szacowanie ryzyka.	Wyjaśnienie. Powyższe należy rozumieć jako podejście do oceny ryzyka na poziomie krajowym. Stosowne zapisy znalazły się w Krajowych Ramach Polityki Cyberbezpieczeństwa.
93.	art. 2. + art.5 ust. 2. pkt 1	Związek Banków Polskich	De facto brak definicji usługi kluczowej. Tytuł rozdziału 2 "Usługi kluczowe i dostawcy usług kluczowych" Definicja usług kluczowych jest najistotniejszą kwestią, gdyż od nie zależy uznanie przedsiębiorcy świadczącego usług za podmiot świadczący usługi kluczowe. Zaproponowany przepis jest lakoniczny i który daje duże pole do nadużyć interpretacyjnych. Za usługę kluczową należy uznać usługę, która spełnia łącznie następujące warunki: 1) świadczenie jej ma istotne znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej; 2) świadczona jest przy użyciu	Uwaga częściowo uwzględniona. Termin „usługa kluczowa” zostanie zdefiniowany. Dyrektywa nie przesądza o konieczności stosowania kryteriów jakościowych i ilościowych w zakresie usług kluczowych, ponieważ obowiązki są nakładane na operatora, a proces identyfikacji odnosi się do operatora, a nie usługi. Dyrektywa 2016/1148 nie

			cyberprzestrzeni albo sieci i systemów informatycznych; 3) cyberincydent miałby istotny skutek zakłócający dla świadczenia tej usługi; 4) spełnia kryteria jakościowe i ilościowe - tzw. progi odcięcia. Należy opracować kryteria ilościowe i jakościowe, dzięki którym na małych przedsiębiorców nie zostaną narzucone takie same wymogi jak na dużych dostawców. To będą ostre kryteria decydujące o ponoszeniu dodatkowych obciążeń związanych z realizacją wymagań określonych w ustawie o KSC.	zawiera żadnych ograniczeń ustanawiania obowiązków względem operatorów usług kluczowych, będących małymi przedsiębiorcami.
94.	art. 2 pkt 1	Instytut Logistyki i Magazynowania	CSIRT na poziomie krajowym nie jest odrębną jednostką dlatego w definicji trzeba wymienić wszystkie dalej zdefiniowane, czyli CSIRT MON, CSIRT NASK, CSIRT GOV.	Wyjaśnienie. CSIRT MON, CSIRT NASK, CSIRT GOV są umiejscowione na poziomie krajowym. Pojęcie CSIRT nie odnosi się do poziomu innego niż krajowy.
95.	art. 2 pkt 3	Związek Banków Polskich	Ustawa nie dookreśla roli CSIRT NASK w zakresie działalności komercyjnej. Czy w związku z ustawowymi obowiązkami NASK będzie dalej świadczył komercyjne usługi reagowania incydenty. W jaki sposób zostanie zapewniona transparentność procesu (możliwe konflikty interesów). Wyodrębnienie części NASK do spółki celowej nadal może budzić wątpliwości co do stoswanie uczciwych zasad i zgodności.	Uwaga nieuwzględniona. CSIRT nie będą prowadziły działalności o charakterze komercyjnym.
96.	art. 2 pkt 5	Business Centre Club	W zakresie definicji zawartych w Projekcie wskazujemy również, że w ramach definicji „cyberbezpieczeństwa" pojawia się sformułowanie „danego poziomu zaufania" użyte w kontekście odporności systemów informacyjnych na ataki. Powyższe sformułowanie powinno uzyskać swoją definicję w ramach przyszłej ustawy, tak, aby ułatwić ocenę, czy stan cyberbezpieczeństwa został osiągnięty.	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy. Zgodnie z definicją, cyberbezpieczeństwo jest stanem systemów informacyjnych, jednak nie jest to stan

				dowolny, a taki który oznacza „odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne”. W związku z tym przepis jest jednoznaczny.
97.	art. 2. pkt 5	Związek Banków Polskich	Proponuje się definicję cyberbezpieczeństwa w brzmieniu: „cyberbezpieczeństwo – bezpieczeństwo sieci i systemów informatycznych oznacza odporności 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 dostepnych przez te systemy informatyczne”;	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy.
98.	art. 2 pkt 5	Związek Pracodawców Branży Internetowej IAB Polska	W zakresie definicji zawartych w Projekcie wskazujemy również, że w ramach definicji „cyberbezpieczeństwa” pojawia się sformułowanie „danego poziomu zaufania” użyte w kontekście odporności systemów informacyjnych na ataki. Powyższe sformułowanie powinno uzyskać swoją definicję w ramach przyszłej ustawy, tak, aby ułatwić ocenę, czy stan cyberbezpieczeństwa został osiągnięty.	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy. Zgodnie z definicją, cyberbezpieczeństwo jest stanem systemów informacyjnych, jednak nie jest to stan dowolny, a taki który oznacza „odporność tych

				systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne”. W związku z tym przepis jest jednoznaczny.
99.	art. 2 pkt 5	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	W art. 2 pkt 5 Projektu wnosimy o doprecyzowanie definicji w następujący sposób (zmiany kursywą i podkreślone): „cyberbezpieczeństwo – stan systemów informacyjnych i elektronicznych oznaczający odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne.” Postulujemy także, aby jasno zdefiniować „dany poziom zaufania” oraz w art.2 pkt 8-12 wprowadzić definicje incydentów umożliwiające dokładną ich klasyfikację.	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy. Zgodnie z definicją, cyberbezpieczeństwo jest stanem systemów informacyjnych, jednak nie jest to stan dowolny, a taki który oznacza „odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne”. W związku z tym przepis jest jednoznaczny.
100.	art. 2 pkt 5	Konfederacja Lewiatan	Art. 2 pkt 5 – należy dodać definicję ‘danego poziomu zaufania’.	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy.

				Zgodnie z definicją, cyberbezpieczeństwo jest stanem systemów informacyjnych, jednak nie jest to stan dowolny, a taki który oznacza „odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne”. W związku z tym przepis jest jednoznaczny.
101.	art. 2 pkt 5 [w piśmie z uwagami i błędnie oznaczne jako art. 1 pkt 5]	Fundacja Bezpieczna Cyberprzestrzeń	W projekcie zwarto: „Cyberbezpieczeństwo – stan systemów (…) integralność lub poufność przetwarzanych danych (…)”, a naszym zdaniem powinno być: „integralność lub poufność przechowywanych, przekazywanych i przetwarzanych danych”.	Uwaga nieuwzględniona.
102.	art. 2 pkt 5	Polska Izba Informatyki i Telekomunikacji	Art. 2 punkt 5 – należy dodać definicję ‘danego poziomu zaufania’, oraz wyraz „stan” zastąpić wyrazami „bezpieczeństwo i integralność” - uzasadnienie: należy posługiwać się pojęciami znanymi i używanymi w prawie w prawie polskim (np. Rozdział VIIA Pt).	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy. Zgodnie z definicją, cyberbezpieczeństwo jest stanem systemów informacyjnych, jednak nie jest to stan dowolny, a taki który oznacza „odporność tych systemów, przy danym poziomie zaufania, na wszelkie

				działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne". W związku z tym przepis jest jednoznaczny.
103.	art. 2 pkt 5	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Proponuje się rozszerzenie definicji cyberbezpieczeństwa o „poziom organizacyjno-technicznej dojrzałości i skuteczności działania organizacji oraz jednostek organizacyjnych powołanych w celu zapewnienia dostępności, autentyczności, integralności i poufności danych przetwarzanych w systemach informatycznych lub związanych z nimi usług oferowanych przez te systemy".	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy. Zgodnie z definicją, cyberbezpieczeństwo jest stanem systemów informacyjnych, jednak nie jest to stan dowolny, a taki który oznacza „odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne". W związku z tym przepis jest jednoznaczny.
104.	art. 2 pkt 5	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 2."cyberbezpieczeństwo – stan systemów informacyjnych oznaczający odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne;" – Definicja wydaje się zawężająca w stosunku do przyjętego na rynku rozumienia tego pojęcia, które zwykle rozumiane jest jako obejmujące nie tylko stan systemów informacyjnych, ale także stan organizacji i jej procesów, w tym	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy. Zgodnie z definicją, cyberbezpieczeństwo jest stanem systemów informacyjnych, jednak nie jest to stan

			świadomości/poziomu wiedzy ludzi budujących tę organizację, realizujących te procesy i wchodzących w dowolną interakcję z systemami. To te właśnie elementy w dużej mierze decydują o odporności organizacji i systemów na najbardziej aktualnie rozpowszechnione zagrożenia oparte o działania socjotechniczne.	dowolny, a taki który oznacza „odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne”. W związku z tym przepis jest jednoznaczny.
105.	art. 2 pkt 5	Instytut Kościuszki	Należy rozważyć czy zaproponowana w projekcie ustawy definicja cyberbezpieczeństwa (art. 2 pkt 5 w związku z art. 2 pkt 18-19 projektu ustawy oraz art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne) odpowiada zakresowi pojęciu bezpieczeństwa sieci i systemów informatycznych zgodnie z art. 4 pkt 2 Dyrektywy NIS. Na podstawie wykładni literalnej przedmiotowego przepisu można postawić wniosek, iż projekt ustawy zawężą zakres normowania wyłącznie do bezpieczeństwa systemów informatycznych w rozumieniu dyrektywy NIS. Nawet jeżeli przyjąć przychylną projektodawcy wykładnię, iż postulat Dyrektywy NIS jest realizowany poprzez zawarte w art. 2 pkt 19 odniesienie do definicji systemu teleinformatycznego z art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, należy stwierdzić niekonsekwencję terminologiczną, ponieważ w innych przepisach, projektodawca odnosi się literalnie do sieci teleinformatycznej (np. art. 28 ust. 5 pkt 2, art. 28 ust. 6 pkt 1 lit. a, art. 28 ust. 7 pkt 12). W związku z powyższym, w celu uniknięcia niejasności w odniesieniu do prawidłowej implementacji Dyrektywy NIS, należy dokonać jednoznacznego określenia definicji cyberbezpieczeństwa w kontekście pojęcia bezpieczeństwa sieci i systemów informatycznych.	Uwaga nieuwzględniona. Termin „systemy informacyjne” używany w projekcie zawiera w sobie zarówno część infrastrukturalną (elementem systemu teleinformatycznego jest również sieć) wraz z przetwarzanymi w nich danymi w postaci elektronicznej. Jest to podejście szersze (obejmujące również dane), zatem definicja z art. 2 pkt 5 nie pomija kwestii sieci teleinformatycznych.
106.	art. 2 pkt 5 [w piśmie z	Polska Izba Radiodyfuzji Cyfrowej	Należy dodać definicję „danego poziomu zaufania”.	Wyjaśnienie.

	uwagami błędnie oznaczne jako art. 2 ust. 5]			Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy. Zgodnie z definicją, cyberbezpieczeństwo jest stanem systemów informacyjnych, jednak nie jest to stan dowolny, a taki który oznacza „odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne”. W związku z tym przepis jest jednoznaczny.
107.	art. 2 pkt 5	Izba Gospodarcza Gazownictwa	Dokument Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 –2022, przyjęty uchwałą Rady Ministrów nr 52/2017 z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022 – posługuje się nieco inną definicją „cyberbezpieczeństwa”. Zauważamy, że projektowana definicja jest szersza. Stan ten może zmniejszać komunikatywność powiązanych ze sobą dokumentów. Przypuszczamy, że zmiany są wynikiem innego zdefiniowania systemu informacyjnego w stosunku do ww. Krajowych Ram Polityki Cyberbezpieczeństwa.	Wyjaśnienie. Przedstawione w projekcie definicje nie stoją w sprzeczności z pojęciami z norm z obszaru bezpieczeństwa informacji. Konieczne było zapewnienie zgodności z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy. Zgodnie z definicją, cyberbezpieczeństwo jest stanem systemów informacyjnych, jednak nie jest to stan dowolny, a taki który oznacza „odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne”. W związku z tym przepis jest jednoznaczny.

108.	art. 2 pkt 6	Business Centre Club	W pierwszej kolejności wskazujemy, że dostawca usług cyfrowych został zdefiniowany w Projekcie jako podmiot świadczący usługi cyfrowe, z wyłączeniem mikroprzedsiębiorstw i małych przedsiębiorstw (art. 2 pkt 6 Projektu). Z kolei w definicji usługi cyfrowej wskazano, że jest to usługa świadczona drogą elektroniczną w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219), będącą internetową platformą handlową, wyszukiwarką internetową, lub usługą przetwarzania w chmurze (art. 2 pkt 21 Projektu). Takie uregulowanie wydaje się być zgodne z treścią dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej jako „Dyrektywa NIS"), której Projekt ma stanowić implementację.	Uwaga częściowo uwzględniona. Definicja dostawcy usług cyfrowych uwzględni osobowość prawną takiego dostawcy, zgodnie z definicją w dyrektywie 2016/1148.
109.	art. 2 pkt 6 w zw. z art. 2 pkt 21	Krajowa Izba Komunikacji Ethernetowej	Dostawcą usługi cyfrowej jest podmiot świadczący usługę świadczoną drogą elektroniczną, będącą internetową platformą handlową, wyszukiwarką internetową lub usługą przetwarzania w chmurze. Z definicji nie będzie to, zatem przedsiębiorca telekomunikacyjny. (…) Naszym zdaniem nie jest to usługa telekomunikacyjna, a zatem tym bardziej nie jest zrozumiała przyczyna, dla której projekt ustawy włącza przedsiębiorców telekomunikacyjnych do krajowego systemu cyberbezpieczeństwa. W opinii KIKE art. 4 pkt 5 projektu ustawy należy wykreślić.	Wyjaśnienie. Przepisy uwzględniają przedsiębiorców telekomunikacyjnych w krajowym systemie cyberbezpieczeństwa, ale z uwagi na ograniczenia określone w dyrektywie 2016/1148 ustawa nie nakłada żadnych nowych obowiązków na przedsiębiorców telekomunikacyjnych dotyczących bezpieczeństwa i zgłaszania incydentów.
110.	art. 2 pkt 6	Krajowa Izba Komunikacji Ethernetowej	Wyrażamy zdecydowane poparcie dla rozwiązania ujętego w art. 2 pkt 6 projektu ustawy, zgodnie z którym definicja dostawcy usługi cyfrowej, a zatem i reżim projektu ustawy dotyczący takich dostawców – nie obejmuje mikro i małych przedsiębiorców w rozumieniu ustawy o swobodzie działalności gospodarczej. Obowiązki spoczywające na dostawcach usług cyfrowych określone w ustawie mogą przekraczać możliwości mikro i małych przedsiębiorców. Należy przy tym pamiętać, że szereg dodatkowych	Wyjaśnienie. Ministerstwo Cyfryzacji uczestniczy w pracach nad decyzją wykonawczą Komisji Europejskiej dotyczącą dostawców usług cyfrowych. Decyzja zostanie wydana w 2017 r. i stosowne odniesienie znajdzie się w kolejnym projekcie ustawy.

			obowiązków zostanie jeszcze w przyszłości nałożonych na te podmioty, gdy Komisja Europejska wyda decyzję wykonawczą, do czego jest upoważniona na podstawie dyrektywy NIS.	
111.	art. 2 pkt 6	Związek Pracodawców Branży Internetowej IAB Polska	W pierwszej kolejności wskazujemy, że dostawca usług cyfrowych został zdefiniowany w Projekcie jako podmiot świadczący usługi cyfrowe, z wyłączeniem mikroprzedsiębiorstw i małych przedsiębiorstw (art. 2 pkt 6 Projektu). Z kolei w definicji usługi cyfrowej wskazano, że jest to usługa świadczona drogą elektroniczną w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219), będącą internetową platformą handlową, wyszukiwarką internetową, lub usługą przetwarzania w chmurze (art. 2 pkt 21 Projektu). Takie uregulowanie wydaje się być zgodne z treścią dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej jako „Dyrektywa NIS"), której Projekt ma stanowić implementację.	Uwaga częściowo uwzględniona. Definicja dostawcy usług cyfrowych uwzględni osobowość prawną takiego dostawcy, zgodnie z definicją w dyrektywie 2016/1148.
112.	art. 2 pkt 8-12	Business Centre Club	Wskazujemy również, że definicje poszczególnych incydentów wymienionych w Projekcie powinny umożliwiać dokładną ich klasyfikację, czego obecna treść Projektu nie zapewnia. Wskazujemy w szczególności, że przy obecnych definicjach, podmiot komercyjny dokonujący klasyfikacji incydentów będzie miał ogromny problem, aby ocenić, czy np. dany incydent skutkuje „znaczną szkodą dla (…), zaufania do instytucji publicznych". W ramach definicji incydentów należy zwrócić uwagę na definicję „incydentu istotnego" zawartą w Projekcie (art. 2 pkt 12 Projektu), do którego zgłaszania do NASK mają być zobowiązani dostawcy usług cyfrowych. W ramach tej definicji nie zostało zawarte odwołanie do cyberbezpieczeństwa, co – tak, jak w przypadku definicji „internetowej platformy handlowej" – może doprowadzić do nieuzasadnionego poszerzenia stosowania Projektu. Zgodnie z	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.

			art. 4 pkt 7 Dyrektywy NIS, „incydent” oznacza każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych. Dla właściwiej implementacji zapisów Dyrektywy NIS, należałoby więc w definicjach każdego z incydentów wyszczególnionych w Projekcie zawrzeć zapis odwołujący się wprost do kwestii cyberbezpieczeństwa, czego jak wskazano wyżej, w przypadku definicji „incydentu istotnego” brakuje. Formułując definicję tego incydentu należy zapewnić, że zgłaszane powinny być wszelkiego rodzaju ataki które przerodziły się lub mogły się przerodzić w incydent i ich źródłem było nieautoryzowane działanie osób trzecich. Zgłaszanie wszystkich incydentów (np. czasowa niedostępność usługi) będzie kontrproduktywne, bo utrudni zidentyfikowanie CSIRT NASK realnych zagrożeń.	
113.	art. 2 pkt 12	Business Centre Club	W kontekście definicji „incydentu istotnego” podkreślenia wymaga także, że wprawdzie nastąpiło w niej odwołanie do decyzji wykonawczej Komisji Europejskiej (jeszcze niewydanej), która ma zgodnie z Dyrektywą NIS doprecyzować elementy brane pod uwagę przy stosowaniu środków technicznych i organizacyjnych w celu zarządzania ryzykiem oraz parametry brane pod uwagę przy ocenie, czy wpływ incydentu jest istotny, to jednak w Projekcie powinien być zawarty szerszy opis takich incydentów. Przedmiotowa definicja ogranicza się bowiem jedynie do wskazania, że incydent istotny, to zdarzenie mające istotny wpływ na świadczenie usługi cyfrowej w rozumieniu wymienionej decyzji wykonawczej Komisji Europejskiej. W art. 16 ust. 4 Dyrektywy NIS wskazano, że w celu określenia, czy wpływ incydentu jest istotny (a więc, czy dostawca usług cyfrowych jest zobowiązany do poinformowania o jego wystąpieniu), uwzględnia się liczne, ale wymienione jedynie przykładowo parametry. Wśród nich w Dyrektywie NIS wskazano na: a) liczbę użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych	Uwaga częściowo uwzględniona.

			od usługi na potrzeby świadczenia ich własnych usług; b) czas trwania incydentu; c) zasięg geograficzny, którego dotyczy incydent; d) zasięg zakłócenia funkcjonowania usługi; e) zasięg wpływu na działalność gospodarczą i społeczną. Zawarcie podobnego wyliczenia wprost w Projekcie z pewnością ułatwiłoby zobowiązanym podmiotom właściwą i adekwatną ocenę występujących incydentów, a w konsekwencji właściwe na nie reakcje. Ponadto, właściwa klasyfikacja incydentów przez zobowiązane podmioty zapobiegałaby nadmiernym obciążeniom NASK, w sytuacji, gdzie incydent nie jest na tyle poważny, aby został on zaklasyfikowany jako istotny, a w konsekwencji nie wymaga on podjęcia działań właściwych dla tego typu incydentów.	
114.	art. 2 pkt. 8-11	Związek Banków Polskich	Źle zbudowana gradacja, głównym kryterium powinno być zasięg incydentu (skutek oddziaływania: lokalny, sektorowy, międzysektorowy i międzynarodowy) oraz istotność - wpływ na bezpieczeństwo sieci lub systemów informatycznych (niska, średnia, istotna i krytyczna). Szczegółowe kwestie dotyczące klasyfikacji incydentów powinny być zaadresowane w akcie wykonawczym do niniejszej ustawy.	Wyjaśnienie. Przepisy dotyczące incydentów zostaną przeredagowane. Szczegółowe progi uznania incydentu za poważny (dla operatorów usług kluczowych) będą określone w rozporządzeniu, a kryteria incydentu istotnego (dla dostawców usług cyfrowych) wynikają z decyzji wykonawczej KE.
115.	art. 2 pkt 8-12 [w piśmie z uwagami błędnie oznaczne jako	Fundacja Bezpieczna Cyberprzestrzeń	W jaki sposób można rozróżnić incydent poważny od zwykłego? Czy incydent istotny może być równocześnie incydentem krytycznym? Zaproponowana gradacja incydentów jest wprawdzie zgodna z tym, co jest stosowane powszechnie (low/moderate/major/critical), ale brakuje 1) odpowiedniej kolejności ich wymienienia a przede wszystkim 2) rozróżnienia poprzez właściwy opis. Zupełnie niejasne jest sformułowanie: np. „incydent poważny - incydent zwykły, który powoduje lub może spowodować krytyczne obniżenie jakości (…)” a z kolei „incydent krytyczny – skutkujący znaczną szkodą”. Potrzeba	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.

	art. 1 pkt 8-12]		zmiany nazw incydentów, by były bardziej intuicyjne i bardziej precyzyjnych objaśnień. Dodatkowo warto rozważyć ograniczenie gradacji do trzech poziomów, co czyniłoby ją bardziej zrozumiałą dla odbiorców.	
116.	art. 2 pkt 8-12	Polska Izba Informatyki i Telekomunikacji	Art. 2 punkty 8-12 – definicje incydentów powinny umożliwiać dokładną ich klasyfikację. Przy obecnie podanych definicjach, podmiot komercyjny dokonujący klasyfikacji będzie miał ogromny problem, aby ocenić, czy dany incydent skutkuje 'znaczną szkodą dla [..], zaufania do instytucji publicznych […]'. Definicje należy doprecyzować i stworzyć ich spójny i mierzalny katalog.	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.
117.	art. 2 pkt 8-12	Konfederacja Lewiatan	Art. 2 punkty 8-12 – definicje incydentów powinny umożliwiać dokładną ich klasyfikację. Przy obecnie podanych definicjach, podmiot komercyjny dokonujący klasyfikacji będzie miał ogromny problem, aby ocenić, czy dany incydent skutkuje 'znaczną szkodą dla [..], zaufania do instytucji publicznych […]'.	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.
118.	art. 2 pkt 8-12	Polska Izba Radiodyfuzji Cyfrowej	Definicje incydentów powinny umożliwiać dokładną ich klasyfikację. Przy obecnie podanych definicjach, podmiot komercyjny dokonujący klasyfikacji będzie miał ogromny problem, aby ocenić, czy dany incydent skutkuje 'znaczną szkodą dla [..], zaufania do instytucji publicznych […].	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.
119.	art. 2 pkt 8-12	Związek Pracodawców Branży Internetowej IAB Polska	Wskazujemy również, że definicje poszczególnych incydentów wymienionych w Projekcie powinny umożliwiać dokładną ich klasyfikację, czego obecna treść Projektu nie zapewnia. Wskazujemy w szczególności, że przy obecnych definicjach, podmiot komercyjny dokonujący klasyfikacji incydentów będzie miał ogromny problem, aby ocenić, czy np. dany incydent skutkuje „znaczną szkodą dla (…), zaufania do instytucji publicznych".	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.

120.	art. 2 pkt 8-12	Izba Gospodarcza Gazownictwa	Definicje incydentów nie są jednoznaczne, mogą wprowadzać problem w klasyfikacji incydentu.	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.
121.	art. 2 pkt 8-12	Instytut Logistyki i Magazynowania	Zaproponowane definicje klas incydentów (w art.2) są mało precyzyjne, tylko w art.12 ust.4 opisano progi (a nie kryteria) uznania incydentu za poważny. Zadanie klasyfikacji incydentów bezpieczeństwa znajduje się w obowiązkach potencjalnie wielu zgłaszających – potrzebna jest ich precyzyjna definicja. Również w związku z tym, że od klasy incydentu zależą czasy obsługi, użyte zasoby, zakres raportowania. Proponuję zapisać, że kryteria klasyfikacji incydentów zostaną doprecyzowane w rozporządzeniu.	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.
122.	art. 2 pkt 9-12	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Zaproponowane definicje incydentów nie są precyzyjne i spójne. Proponuje się przeredagowanie opisów poszczególnych kategorii incydentów.	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.
123.	art. 2 pkt 10, w zw. art. 12 ust. 4-5	Izba Gospodarcza Gazownictwa	Projektodawca posługuje się w obrębie projektowanej ustawy pojęciem „krytyczne obniżenie jakości”. Rekomendujemy o jego zdefiniowanie w słowniku wyrażeń ustawowych lub wydanie stosownych wytycznych dot. oceny.	Uwaga nieuwzględniona.
124.	art. 2 pkt 11	Pracodawcy RP	Brak jednoznacznej definicji incydentu. Proponuje się przywołanie definicji zawartej w Art.4. pkt 7 Dyrektywy NIS.	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.
125.	art. 2 pkt 11	Związek Banków Polskich	Brak jednoznacznej definicji incydentu. Proponuje się przywołanie definicji zawartej w Art.4. pkt 7 Dyrektywy NIS.	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.

126.	art. 2 pkt 12	Związek Pracodawców w Branży Internetowej IAB Polska	W ramach definicji incydentów należy zwrócić uwagę na definicję „incydentu istotnego" zawartą w Projekcie (art. 2 pkt 12 Projektu), do którego zgłaszania do NASK mają być zobowiązani dostawcy usług cyfrowych. W ramach tej definicji nie zostało zawarte odwołanie do cyberbezpieczeństwa, co – tak, jak w przypadku definicji „internetowej platformy handlowej" – może doprowadzić do nieuzasadnionego poszerzenia stosowania Projektu. Zgodnie z art. 4 pkt 7 Dyrektywy NIS, „incydent" oznacza każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych. Dla właściwiej implementacji zapisów Dyrektywy NIS, należałoby więc w definicjach każdego z incydentów wyszczególnionych w Projekcie zawrzeć zapis odwołujący się wprost do kwestii cyberbezpieczeństwa, czego jak wskazano wyżej, w przypadku definicji „incydentu istotnego" brakuje. Formułując definicję tego incydentu należy zapewnić, że zgłaszane powinny być wszelkiego rodzaju ataki które przerodziły się lub mogły się przerodzić w incydent i ich źródłem było nieautoryzowane działanie osób trzecich. Zgłaszanie wszystkich incydentów (np. czasowa niedostępność usługi) będzie kontrproduktywne, bo utrudni zidentyfikowanie CSIRT NASK realnych zagrożeń.	Uwaga nieuwzględniona. Definicja incydentu istotnego jest ściśle powiązana z Dyrektywą NIS i decyzja wykonawczą.
127.	art. 2 pkt 12	Związek Pracodawców w Branży Internetowej IAB Polska	W kontekście definicji „incydentu istotnego" podkreślenia wymaga także, że wprawdzie nastąpiło w niej odwołanie do decyzji wykonawczej Komisji Europejskiej (jeszcze niewydanej), która ma zgodnie z Dyrektywą NIS doprecyzować elementy brane pod uwagę przy stosowaniu środków technicznych i organizacyjnych w celu zarządzania ryzykiem oraz parametry brane pod uwagę przy ocenie, czy wpływ incydentu jest istotny, to jednak w Projekcie powinien być zawarty szerszy opis takich incydentów. Przedmiotowa definicja ogranicza się bowiem jedynie do wskazania, że incydent istotny, to zdarzenie mające istotny wpływ na świadczenie usługi cyfrowej w rozumieniu wymienionej decyzji wykonawczej Komisji Europejskiej. W art. 16 ust. 4 Dyrektywy NIS	Uwaga częściowo uwzględniona. Przepisy zostaną częściowo przeredagowane.

			wskazano, że w celu określenia, czy wpływ incydentu jest istotny (a więc, czy dostawca usług cyfrowych jest zobowiązany do poinformowania o jego wystąpieniu), uwzględnia się liczne, ale wymienione jedynie przykładowo parametry. Wśród nich w Dyrektywie NIS wskazano na: a) liczbę użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług; b) czas trwania incydentu; c) zasięg geograficzny, którego dotyczy incydent; d) zasięg zakłócenia funkcjonowania usługi; e) zasięg wpływu na działalność gospodarczą i społeczną. Zawarcie podobnego wyliczenia wprost w Projekcie z pewnością ułatwiłoby zobowiązanym podmiotom właściwą i adekwatną ocenę występujących incydentów, a w konsekwencji właściwe na nie reakcje. Ponadto, właściwa klasyfikacja incydentów przez zobowiązane podmioty zapobiegałaby nadmiernym obciążeniom NASK, w sytuacji, gdzie incydent nie jest na tyle poważny, aby został on zaklasyfikowany jako istotny, a w konsekwencji nie wymaga on podjęcia działań właściwych dla tego typu incydentów.	
128.	art. 2 pkt 12	Izba Gospodarki Elektronicznej	Projekt nie definiuje incydentu istotnego, ale odsyła do przygotowywanej obecnie decyzji wykonawczej Komisji Europejskiej. Formułując definicję tego incydentu należy zapewnić, że zgłaszane powinny być wszelkiego rodzaju ataki, które przerodziły się lub mogły się przerodzić w incydent i ich źródłem było nieautoryzowane działanie osób trzecich. Zgłaszanie wszystkich incydentów (np. czasowa niedostępność usługi) będzie kontrproduktywne. Utrudni bowiem zidentyfikowanie CSIRT NASK realnych zagrożeń. Podkreślić trzeba, że czasowa niedostępność usługi może być spowodowana przez takie przyczyny, jak błąd spowodowany aktualizacją oprogramowania. Zgłaszanie takich błędów nie przyczyni się do zwiększenia cyberbezpieczeństwa, a wręcz może odwrócić uwagę CSIRT NASK od naprawdę poważnych zagrożeń.	Uwaga nieuwzględniona. Definicja incydentu istotnego jest ściśle powiązana z Dyrektywą NIS i decyzja wykonawczą.

129.	art. 2 pkt 13	Związek Pracodawców Branży Internetowej IAB Polska	Wątpliwości budzi jednak w tym kontekście definicja „internetowej platformy handlowej" jako jednej z trzech rodzajów usług zaliczających się do usług cyfrowych w rozumieniu Projektu. Zgodnie bowiem z art. 4 pkt 17 Dyrektywy NIS, „internetowa platforma handlowa" oznacza usługę cyfrową, która umożliwia konsumentom lub przedsiębiorcom zawieranie online umów dotyczących sprzedaży lub usług z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który używa usług komputerowych świadczonych przez internetową platformę handlową. Z kolei definicja „internetowej platformy handlowej" zawarta w Projekcie jest bardziej ogólna, gdyż rozumie się przez nią usługę, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów z przedsiębiorcami drogą elektroniczną. Przy tak szerokiej definicji w jej zakresie będzie mieścić się przykładowo każde narzędzie/serwis do sprzedaży treści na stronach (np. subskrypcje gazet), czy serwisy VOD. Należy więc wskazać na uzasadnione wątpliwości, czy taki właśnie był zamiar projektodawcy przy tworzeniu przedmiotowej definicji, która prowadzi do uznania, że wymienione wyżej przykładowo usługi powinny być objęte regulacjami dotyczącymi cyberbezpieczeństwa.	Uwaga uwzględniona. W wyniku zgłoszonej uwagi zmieniono definicję, dostosowując ją precyzyjnie do definicji z NIS.
130.	art. 2 pkt 13	Business Centre Club	Wątpliwości budzi jednak w tym kontekście definicja „internetowej platformy handlowej" jako jednej z trzech rodzajów usług zaliczających się do usług cyfrowych w rozumieniu Projektu. Zgodnie bowiem z art. 4 pkt 17 Dyrektywy NIS, „internetowa platforma handlowa" oznacza usługę cyfrową, która umożliwia konsumentom lub przedsiębiorcom zawieranie online umów dotyczących sprzedaży lub usług z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który używa usług komputerowych świadczonych przez internetową platformę handlową. Z kolei definicja „internetowej platformy handlowej" zawarta w Projekcie jest bardziej ogólna, gdyż rozumie się przez nią	Uwaga uwzględniona. W wyniku zgłoszonej uwagi zmieniono definicję, dostosowując ją precyzyjnie do definicji z NIS.

			usługę, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów z przedsiębiorcami drogą elektroniczną. Przy tak szerokiej definicji w jej zakresie będzie mieścić się przykładowo każde narzędzie/serwis do sprzedaży treści na stronach (np. subskrypcje gazet), czy serwisy VOD. Należy więc wskazać na uzasadnione wątpliwości, czy taki właśnie był zamiar projektodawcy przy tworzeniu przedmiotowej definicji, która prowadzi do uznania, że wymienione wyżej przykładowo usługi powinny być objęte regulacjami dotyczącymi cyberbezpieczeństwa.	
131.	art. 2 pkt 13	Polska Organizacja Przemysłu i Handlu Naftowego	Projekt posługuje się pojęciem „internetowej platformy handlowej” – jako jednej z usług cyfrowych świadczonych przez dostawców usług cyfrowych, zdefiniowanej jako „usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów z przedsiębiorcami droga elektroniczną” (art. 2 pkt. 13) Projektu). Przyjęta w Projekcie definicja może budzić wątpliwości czy określone platformy stanowią „internetowe platformy handlowe”. Projekt w szczególności nie określa jakie umowy mają być zawierane przez platformę zdefiniowaną w Projekcie. W tym zakresie mogą powstać wątpliwości czy np. platformy służące do obsługi programów lojalnościowych, benefitów dostarczanych pracownikom oraz krótkotrwałych konkursów i promocji powinny być kwalifikowane jako „internetowe platformy handlowe” w rozumieniu Projektu. Natomiast Dyrektywa w preambule wskazuje również, że „Internetowa platforma handlowa umożliwia konsumentom i przedsiębiorcom handlowym zawieranie umów sprzedaży lub umów o świadczenie usług online z przedsiębiorcami handlowymi i jest ostatecznym miejscem zawierania tych umów”. Wobec tego w celu wyeliminowania wątpliwości czy określona platforma będzie spełniała kryteria określone w Projekcie, proponujemy posłużenie się w Projekcie definicją „platformy” przyjętą w Dyrektywie tj.: „Internetowa platforma handlowa –	Uwaga uwzględniona. W wyniku zgłoszonej uwagi zmieniono definicję, dostosowując ją precyzyjnie do definicji z NIS.

			platforma internetowa, która umożliwia konsumentom i przedsiębiorcom zawieranie umów sprzedaży lub umów o świadczenie usług drogą elektroniczną z przedsiębiorcami”.	
132.	art. 2 pkt 14	Związek Banków Polskich	Proponuje się definicję w brzmieniu: 14) obsługa incydentu – oznacza wszelkie procedury i działania umożliwiające wykrywanie i analizowanie incydentu, ograniczenie jego skutków oraz reagowanie na niego.	Uwaga częściowo uwzględniona.
133.	art.2. pkt 15	Związek Banków Polskich	Błędne podejście do określenia kto jest operatorem usługi kluczowej. Decyzja techniczna administracyjna powoduje uznanie danego przedsiębiorcy za OUK lub nie. Operatorem usługi kluczowej powinien być przedsiębiorca, który faktycznie świadczący usługę kluczową a nie ten, który zostanie przez organ państwowy wpisany na jakąś listę. W ten sposób pozbawiamy prawnej możliwości oddziaływania na podmioty, które faktycznie świadczą usługi kluczowe a nie zostały uznane za OUK. W rzeczywistości nie jest to definicja tylko określenie, że dany operator zostanie uznany za operatora usługi kluczowej wyłącznie na podstawie administracyjnej decyzji. Dotyczy to kwestii nie tylko pojawienia się nowego podmiotu na wykazie ale także podmiotów, które przestają świadczyć tego typu usługi (zasady zarządzania listami operatorów usług kluczowych).	Uwaga nieuwzględniona. Po pierwsze dyrektywa 2016/1148 nie ogranicza kręgu potencjalnych podmiotów, które mogłyby zostać uznane za operatorów usług kluczowych do przedsiębiorców. Podstawą wpisania na listę operatorów usług kluczowych jest decyzja administracyjna o uznaniu za operatora usługi kluczowej, a w więc przejrzysta forma regulowania obowiązków a stroną, zobowiązaną do wypełniania tych obowiązków.
134.	art. 2 pkt 15	Izba Gospodarcza Gazownictwa	Proponujemy doprecyzowanie definicji operatora usługi kluczowej: Operator usługi kluczowej – podmiot działający w jednym z sektorów wymienionych w załączniku Ustawy, w stosunku do którego została wydana decyzja o uznaniu za operatora usługi kluczowej.	Uwaga nieuwzględniona. Zdaniem projektodawcy proponowana definicja operatora usługi kluczowej jest właściwa.
135.	art. 2. pkt 16	Związek Banków Polskich	Brak jednoznacznej definicji ryzyka. Proponujmey wykorzystanie definicji zawartej w Art.4. pkt 9 Dyrektywy NIS.	Uwaga częściowo uwzględniona.

136.	art.2. pkt 18	Związek Banków Polskich	Nieostra definicja, która może budzić wątpliwości interpretacyjne. Proponujemy zgodnie z dyrektywą NIS, a więc: „sieci i systemy informatyczne" oznaczają łącznie: a) sieci łączności elektronicznej w rozumieniu art. 2 lit. a) dyrektywy 2002/21/WE; b) wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych; c) dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony i utrzymania;	Uwaga nieuwzględniona. Zapis przyjęty w projekcie jest zgodny z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy. Użyta w projekcie ustawy definicja systemu informacyjnego obejmuje systemy teleinformatyczne wraz z przetwarzanymi w nich danymi. Jest to definicja przyjęta na potrzeby niniejszej ustawy. Intencją projektodawcy jest przyjęcie szerokiego podejścia obejmującego zarówno systemy teleinformatyczne jak i dane w tych systemach.
137.	art. 2 pkt 20 [w piśmie z uwagami błędnie oznaczne jako art. 1 pkt 20]	Polska Izba Radiodyfuzji Cyfrowej	Postulat rozbudowania Projektu o techniczne środki służące do wzrostu cyberbezpieczeństwa, w tym poprzez szyfrowanie. W art. 1 pkt 20 Projektu zdefiniowano usługę przetwarzania w chmurze. W art. 1 pkt 21 Projektu zaliczono ją do usług cyfrowych, co spowodowało, że w dalszej części projektu występuje już tylko definicja usługi cyfrowej. W dzisiejszym świecie usługi cyfrowe, w tym usługi chmurowe, mają kluczowe znaczenie praktycznie we wszystkich sektorach gospodarki, w tym m. in. w sektorze bankowym, na rynkach finansowych, w sektorze energetycznym, w usługach konsumpcyjnych B2C oraz B2B, w sektorze ubezpieczeń. Mówiąc cyberbezpieczeństwo, myślimy bezpieczeństwo danych znajdujących się w systemach informatycznych. Systemy informatyczne służą przecież do przetwarzania danych. Wszelkie dane dotyczące klientów, transakcji, finansów i tak dalej, są przechowywane w systemach informatycznych, a co raz częściej w chmurach obliczeniowych. Społeczeństwo i bezpieczeństwo oparte są dziś w dużej mierze na tych właśnie danych. Dlatego dane te wymagają szczególnej ochrony i wskazania jak to robić. Powoli jest to dostrzegane. Przykładem może być tutaj	Wyjaśnienie. Definicja usługi przetwarzania w chmurze jest zaczerpnięta z dyrektywy 2016/1148. Było to motywowane potrzebą zapewnienia jak największej zbieżności dostawców świadczących tego typu usługi w Unii Europejskiej. Należy tutaj dodać, że wymagania bezpieczeństwa dla takich dostawców będą zharmonizowane i uregulowane na poziomie unijnym, w decyzji wykonawczej Komisji Europejskiej, która zostanie wydana do końca 2017 r. Ministerstwo uczestniczy w tych pracach. W świetle projektu tej decyzji dostawca może celem zapewnienia bezpieczeństwa świadczonych usług zapewnić również szyfrowanie.

			„Wytyczne Komisji Nadzoru Finansowego dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w zakładach ubezpieczeń i zakładach reasekuracji" wydane przez Komisję Nadzoru Finansowego w grudniu 2014 roku. Wciąż brakuje jednak skonkretyzowanych regulacji na poziomie ustawowym. Nie chodzi o ograniczanie środków ochrony do systemów produkowanych przez konkretnych producentów ani nawet o wskazywanie konkretnego sposobu ochrony, ale o informowanie podmiotów jak mają się zachować, aby spełnić nakładane na nich obowiązki. Samo sformułowanie „odpowiednie środki techniczne", które występuje w Projekcie jest tak ogólne, że ciężko ustalić co się za nim kryje. Tym samym nie wiadomo jak należy się zachować, aby spełnić obowiązek ustawowy. Mając na uwadze rozwój technologiczny i złożoność zagrożeń występujących w systemach informatycznych, podkreśla się, że najodpowiedniejszym środkiem technicznym ochrony danych przetwarzanych w systemach informatycznych jest szyfrowanie. W przypadku zastosowania tego środka ochrony, dane są niemożliwe do odczytania przez osoby postronne, nawet jeżeli zostaną przechwycone. Dlatego też należy postulować dodanie katalogu otwartego środków technicznych zapewniających cyberbezpieczeństwo, w którym znajdzie się szyfrowanie. Zapewnienie cyberbezpieczeństwa powinno następować poprzez uniemożliwienie odczytania danych na żadnym z pośrednich etapów przetwarzania danych (przesył i przechowywanie). Co się tyczy usług przechowywania danych, to co raz popularniejsze są usługi chmurowe, zarówno w sektorze prywatnym jak i publicznym. Usługi te powinny być świadczone w sposób bezpieczny, z użyciem systemów kontroli dostępu do danych i ich zabezpieczenia, nie tylko hasłami, ale również poprzez szyfrowanie. Przesył każdorazowo powinien następować w sposób bezpieczny, co ma fundamentalne znaczenie dla cyberbezpieczeństwa.	

			Przesyłane dane powinny być np. zaszyfrowane. Jeszcze lepszym rozwiązaniem byłoby, aby dane nie były przesyłane, ale były przechowywane w konkretnym miejscu, np. chmurze, i bez przesyłu były udostępniane wybranym osobom. Rozwiązanie takie wyłącza ekspozycję danych na zagrożenia w trakcie przesyłu w sieci, co czyni je wyjątkowo bezpiecznym.	
138.	art. 2 pkt 20	Polska Organizacja Przemysłu i Handlu Naftowego	W Projekcie należy doprecyzować, że wewnętrzne podmioty zapewniające usługi przetwarzania danych w chmurze (cloud computing), takie jak spółki należące do tej samej grupy kapitałowej, które świadczą usługi przetwarzania danych w chmurze wyłącznie na rzecz innych spółek należących do tej samej grupy kapitałowej, nie są dostawcami usług cyfrowych zdefiniowanych w Projekcie. Podmiot świadczący usługi przetwarzania danych w chmurze powinien być uznany za dostawcę usług cyfrowych (w rozumieniu Projektu) wyłącznie w przypadku gdy podmiot ten jest operatorem świadczącym usługi kluczowe. W przeciwnym razie może dojść do niezamierzonego poszerzenia zakresu obowiązywanie przepisów o wielu usługodawców wewnętrznych.	Uwaga uwzględniona. Zmieniono definicję usługi cyfrowej, aby wyłączyć chmury prywatne.
139.	art. 2 pkt 20 [w piśmie z uwagami błędnie oznaczone jako art. 1 pkt 20]	Krajowy Związek Banków Spółdzielczych	Proponujemy uzupełnienie definicji usługa przetwarzania w chmurze tak, aby uwzględniała ona nie tylko dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników, ale także przetwarzanie tych zasobów.	Uwaga nieuwzględniona. Zapis przyjęty w projekcie jest zgodny z dyrektywą 2016/1148/UE. Zastosowane definicje są przygotowane na potrzeby niniejszej ustawy.

140.	art. 2 pkt 21 [w piśmie z uwagami błędnie oznaczne jako art. 1 pkt 21]	Krajowy Związek Banków Spółdzielczych	Zwracamy uwagę, iż definicja usługi cyfrowej została zawężona do internetowej platformy handlowej, wyszukiwarki internetowej lub usługi przetwarzania w chmurze, nie uwzględnia w związku z tym np. usługi poczty elektronicznej bądź usługi bankowości elektronicznej, mogących mieć istotne znaczenie z punktu widzenia celów krajowego systemu cyberbezpieczeństwa, wśród których znajduje się zapewnienie niezakłóconego świadczenia usług cyfrowych.	Wyjaśnienie. Projektowane przepisy uwzględniają wymogi określone w dyrektywie 2016/1148 i dotyczą usług cyfrowych objętych wymogami z zakresu cyberbezpieczeństwa.
141.	art. 2 pkt 21	Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM	Odnosząc się do nałożenia ustawą obowiązków na podmioty świadczące usługi cyfrowe, które zdefiniowane zostały jako usługi świadczone drogą elektroniczną, będące internetową platformą handlową, wyszukiwarką internetową lub usługą przetwarzania w chmurze – MEDIAKOM zaniepokoiło włączenie do kategorii tych podmiotów internetowych platform handlowych niezależnie od tego, czy działalność taka jest główną, czy też uboczną działalnością przedsiębiorcy. MEDIAKOM zwraca uwagę, że prowadzenie działalności w postaci platformy internetowej może być głównym przedmiotem działalności, bądź jedynie ubocznym, służącym ułatwieniu zawierania umów o świadczenie usług stanowiących podstawowy trzon aktywności przedsiębiorcy. Tak dzieje się w przypadku m.in. przedsiębiorców telekomunikacyjnych, którzy przede wszystkim świadczą usługi telekomunikacyjne i to jest ich podstawowy przedmiot działalności, jednak by sprawnie dotrzeć do klienta mogą oferować zawieranie umów za pośrednictwem formularza elektronicznego. Z tego tylko powodu mieszczą się w pojęciu internetowych platform handlowych – bo udostępniają usługę umożliwiającą konsumentom zawieranie umów drogą elektroniczną. Jednocześnie jest to ich działalność całkowicie	Uwaga częściowo uwzględniona. W wyniku zgłoszonej uwagi zmieniono definicję, która zostanie dostosowana precyzyjnie do definicji z NIS.

			uboczna i nie wiąże się z uzyskiwaniem dochodu, który zapewnia przecież świadczenie usług telekomunikacyjnych. W takich przypadkach, gdy usługa zwierania umów drogą elektroniczną nie jest podstawowym przedmiotem działalności i źródłem przychodu przedsiębiorcy, brak jest podstaw do stosowania do podmiotów tego rodzaju wymogów wynikających z ustawy, a dotyczących dostawców usług cyfrowych. Stąd propozycja MEDIAKOM, by ograniczyć zastosowanie przepisów Rozdziału 3 do takich podmiotów, dla których handel internetowy jest podstawowym źródłem przychodu – definiując te podmioty przykładowo poprzez wskazanie procenta przychodów uzyskiwanych z takiej działalności.	
142.	art. 3 ust. 2	Fundacja Bezpieczna Cyberprzestrzeń	Brakuje definicji pojęć „podatność" i „zagrożenie" w Art. 1	Uwaga uwzględniona.
143.	art. 3. ust. 2	Związek Banów Polskich	2. Informacje o podatnościach na incydenty, incydentach i zagrożeniach cyberbezpieczeństwa oraz o poziomie ryzyka wystąpienia incydentów gromadzone przez podmioty krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4, mogą być przekazywane przez te podmioty w określonym zakresie do publicznej wiadomości w przypadku, jedynie gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę trwającego incydentu lub w przypadku gdy ujawnienie incydentu z innych względów jest w interesie publicznym, w tym również, jeśli przyczyni się do zwiększenia cyberbezpieczeństwa. Przekazywanie niezbędnych informacji do publicznej wiadomości nie może naruszać przepisów o ochronie informacji prawnie chronionych.	Uwaga uwzględniona. Art. 3 ust. 2 ograniczono podmioty informujące do CSIRT i organów właściwych. Zmieniono termin „określony zakres" na „niezbędny zakres".
144.	art. 3. ust. 2	Krajowy Związek Banków	W art. 3 ust. 2 przewidziano możliwość przekazywania informacji o podatnościach na incydenty, incydentach i zagrożeniach cyberbezpieczeństwa oraz o poziomie ryzyka wystąpienia	Uwaga uwzględniona. Przepis zostanie zmieniony.

		Spółdzielczych	incydentów gromadzone przez podmioty krajowego systemu cyberbezpieczeństwa, w określonym zakresie do publicznej wiadomości. Proponujemy, by ze względu na istotne znaczenie tej kwestii dla funkcjonowania poszczególnych podmiotów narażonych na tego typu incydenty, zakres informacji przekazywanych do publicznej wiadomości został precyzyjnie zdefiniowany.	
145.	art. 3. ust. 2	Krajowy Związek Banków Spółdzielczych	W art. 3 ust. 2 wskazane byłoby doprecyzowanie, iż zastrzeżenie, że przekazywanie niezbędnych informacji do publicznej wiadomości nie może naruszać przepisów o ochronie tajemnic, dotyczy w szczególności tajemnicy bankowej.	Uwaga uwzględniona. Przepis zostanie zmieniony.
146.	art. 3 ust. 3	Instytut Kościuszki	Zgodnie z art. 3 ust. 3 projektu ustawy do udostępniania informacji o podatnościach na incydenty, incydentach, zagrożeniach cyberbezpieczeństwa, poziomie ryzyka wystąpienia incydentów, nie ma zastosowania ustawa o dostępie do informacji publicznej. Biorąc pod uwagę rygorystyczne kryteria wskazane w projekcie ustawy, uregulowania ustawy o ochronie informacji niejawnych, jak i proponowane rozwiązania w tym zakresie w projekcie ustawy o jawności życia publicznego (np. art. 2 ust. 1 pkt 2, art. 7 pkt 2 lit. b-d, art. 7 pkt 3 lit. a-b, art. 7 pkt 4) oraz wymogi art. 31 ust. 3 Konstytucji RP, należy stwierdzić, że takie ograniczenie stanowi nieproporcjonalną ingerencję w prawo informacji o działalności organów władzy publicznej (art. 61 Konstytucji RP). Z uwagi na okoliczność, iż nie każda informacja z zakresu określonego w art. 3 ust. 2, która mogłaby być potencjalnie przedmiotem wniosku o udostępnienie informacji publicznej, stanowi informację istotną z punktu widzenia bezpieczeństwa lub porządku publicznego państwa, sankcjonowanie wyłączenia na zasadzie klauzuli generalnej jest rozwiązaniem zbytnio naruszającym istotę prawa do informacji publicznej. Należy też zaznaczyć, że organ, wobec którego obywatel wystąpi z wnioskiem o udostępnienie informacji publicznej w przedmiotowym zakresie i tak dysponuje (w związku z	Wyjaśnienie. Przedmiotowa kwestia zostanie uzgodniona z RCL.

			przytoczonymi powyżej regulacjami, jak i warunkami z art. 3 ust. 2 projektu ustawy) istotnym zakresem uznania administracyjnego.	
147.	art. 4	Business Centre Club	Ponadto, należy wskazać, że w art. 4 Projektu należy dodać policję jako element systemu cyberbezpieczeństwa. Pominięcie policji jako istotnego elementu systemu cyberbezpieczeństwa wydaje się niedopatrzeniem, ponieważ to właśnie policja prowadzi sprawy, w których poszkodowanymi z uwagi na cyberprzestępczość są obywatele, czy przedsiębiorcy. Policja jest co najmniej źródłem informacji o typach zgłaszanych cyberprzestępstw, gdzie one występują oraz jaka jest ich skala. W ramach art. 4 Projektu zostali wskazani za to przedsiębiorcy telekomunikacyjni (art. 4 pkt 5 Projektu). Nie zostali oni jednak wymienieni w Dyrektywie NIS, której Projekt ma stanowić implementację. Przedsiębiorcy telekomunikacyjni nie powinni zatem być wymienieni też w Projekcie. W konsekwencji powyższego należy także wykreślić art. 61 Projektu.	Wyjaśnienie. Formacja, jaką jest Policja regulowana ustawą szczególną z dn. 6 kwietnia 1990 r., wpisuje się w ujęte w art. 4 pkt 11 projektu ustawy „jednostki podległe i nadzorowane przez organy administracji rządowej”. W kwestii przedsiębiorców telekomunikacyjnych - ustawa ma szerszy zakres niż tylko implementację dyrektywy 2016/1148. Jest to implementacja minimalna, a projekt traktuje materię szerzej.
148.	art. 4	Instytut Kościuszki	Zgodnie z Krajowymi Ramami, do krajowego systemu cyberbezpieczeństwa, poza podmiotami wskazanymi bezpośrednio w Dyrektywie NIS, zaliczają się także operatorzy infrastruktury krytycznej. W związku z powyższym, katalog wskazany w art. 4 nie jest wyczerpujący w świetle art. 3 pkt 2 ustawy o zarządzaniu kryzysowym, ponieważ nie odnosi się on literalnie do wszystkich systemów infrastruktury krytycznej wskazanej w niniejszej ustawie. Oznacza to, że proponowany w ustawie krajowy system cyberbezpieczeństwa może być niekompletny (np. w zakresie zaopatrzenia w żywność, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych). Zalecanym rozwiązaniem byłoby zatem odpowiednie poszerzenie katalogu z art. 4 lub odwołanie do przedmiotowych przepisów ustawy o zarządzaniu kryzysowym.	Uwaga częściowo uwzględniona.

149.	art. 4	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	W art. 4 Projektu wymienione zostały podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa. Izba zwraca uwagę, na brak wskazania wprost w Projekcie na jednostki organizacyjne policji, które dysponują wieloma wydziałami ds. walki z cyberprzestępczością. Zrezygnowano również z wyróżniania w Projekcie i wskazywania z nazwy CSIRT sektorowych, które istnieją lub w najbliższej przyszłości mają być utworzone w sektorach takich jak, bankowość czy energetyka. Projektodawca powinien wyjaśnić czym kierował się wskazując na podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa, kwestii tej nie wyjaśniono bowiem w sposób dogłębny w uzasadnieniu Projektu. Ponadto w art. 4 ust. pkt wnosimy o doprecyzowanie: Uczelnie publiczne, Polską Akademię Nauk i instytuty badawcze". Ponadto w Projekcie brakuje jasno określonego stałego organu koordynacyjno – kontrolnego w zakresie nadzoru nad efektywnością pracy zespołów CSIRT i pozostałych elementów Krajowego Systemu Cyberbezpieczeństwa, który na poziomie KRM w sposób stały koordynowałby system.	Wyjaśnienie. Formacja, jaką jest Policja regulowana ustawą szczególną z dn. 6 kwietnia 1990 r., wpisuje się w ujęte w art. 4 pkt 11 projektu ustawy „jednostki podległe i nadzorowane przez organy administracji rządowej". Projekt zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa CSIRT jest natomiast zarezerwowana dla zespołów poziomu krajowego. Projekt zostanie rozszerzony o przepisy przewidujące powołanie przy Radzie Ministrów Kolegium do spraw Cyberbezpieczeństwa w skład którego wchodzić będzie Minister Koordynator Służb Specjalnych, MON, MSWiA, MC i RCB.
150.	art. 4	Polska Izba Informatyki i Telekomunikacji	Art. 4 - Należy dodać Policję, jako element systemu cyberbezpieczeństwa Pominięcie Policji, jako elementu systemu cyberbezpieczeństwa, wydaje się niedopatrzeniem, ponieważ to właśnie Policja prowadzi sprawy, w których poszkodowanymi z uwagi na cyberprzestępczość są obywatele czy przedsiębiorcy. Policja jest co najmniej źródłem informacji o typach cyberprzestępstw zgłaszanych, gdzie występują, jaka jest ich skala.	Wyjaśnienie. Formacja, jaką jest Policja regulowana ustawą szczególną z dn. 6 kwietnia 1990 r., wpisuje się w ujęte w art. 4 pkt 11 projektu ustawy „jednostki podległe i nadzorowane przez organy administracji rządowej".
151.	art. 4	Polska Izba Radiodyfuzji Cyfrowej	W art. 4. należy dodać Policję jako element systemu cyberbezpieczerństwa. Pominięcie Policji jako istotnego elementu systemu cyberbezpieczeństwa wydaje się niedopatrzeniem, ponieważ to właśnie Policja prowadzi sprawy, w których poszkodowanymi z uwagi na cyberprzestępczość są obywatele czy	Wyjaśnienie. Formacja, jaką jest Policja regulowana ustawą szczególną z dn. 6 kwietnia 1990 r., wpisuje się w ujęte

			przedsiębiorcy. Policja jest co najmniej źródłem informacji o typach cyberprzestępstw zgłaszanych, gdzie występują, jaka jest ich skala.	w art. 4 pkt 11 projektu ustawy „jednostki podległe i nadzorowane przez organy administracji rządowej”.
152.	art. 4	Konfederacja Lewiatan	W Art. 4 Należy dodać Policję jako element systemu cyberbezpieczeństwa. Pominięcie Policji jako istotnego elementu systemu cyberbezpieczeństwa wydaje się niedopatrzeniem, ponieważ to właśnie Policja prowadzi sprawy, w których poszkodowanymi z uwagi na cyberprzestępczość są obywatele czy przedsiębiorcy. Policja jest co najmniej źródłem informacji o typach cyberprzestępstw zgłaszanych, gdzie występują, jaka jest ich skala.	Wyjaśnienie. Formacja, jaką jest Policja regulowana ustawą szczególną z dn. 6 kwietnia 1990 r., wpisuje się w ujęte w art. 4 pkt 11 projektu ustawy „jednostki podległe i nadzorowane przez organy administracji rządowej”.
153.	art. 4	Związek Pracodawców w Branży Internetowej IAB Polska	Ponadto, należy wskazać, że w art. 4 Projektu należy dodać policję jako element systemu cyberbezpieczeństwa. Pominięcie policji jako istotnego elementu systemu cyberbezpieczeństwa wydaje się niedopatrzeniem, ponieważ to właśnie policja prowadzi sprawy, w których poszkodowanymi z uwagi na cyberprzestępczość są obywatele, czy przedsiębiorcy. Policja jest co najmniej źródłem informacji o typach zgłaszanych cyberprzestępstw, gdzie one występują oraz jaka jest ich skala. W ramach art. 4 Projektu zostali wskazani za to przedsiębiorcy telekomunikacyjni (art. 4 pkt 5 Projektu). Nie zostali oni jednak wymienieni w Dyrektywie NIS, której Projekt ma stanowić implementację. Przedsiębiorcy telekomunikacyjni nie powinni zatem być wymienieni też w Projekcie. W konsekwencji powyższego należy także wykreślić art. 61 Projektu.	Wyjaśnienie. Formacja, jaką jest Policja regulowana ustawą szczególną z dn. 6 kwietnia 1990 r., wpisuje się w ujęte w art. 4 pkt 11 projektu ustawy „jednostki podległe i nadzorowane przez organy administracji rządowej”. W kwestii przedsiębiorców telekomunikacyjnych - ustawa ma szerszy zakres niż tylko implementację dyrektywy 2016/1148. Jest to implementacja minimalna, a projekt traktuje materię szerzej.
154.	art. 4	Związek Banków Polskich	Brak podmiotu centralnego, faktycznego zarządcy nadzorującego krajowy system cyberbezpieczeństwa. Brak w KSC CSIRT Sektorowych - co zaprzecza potrzebie integrowania OUK w ramach danych sektorów. Brak Policji, Prokuratury i innych organów ścigania powoduje brak skutecznej możliwości obsługi cyberincydentu i zwalczania cyberprzestępczości. Brak jest GIODO, który jest instytucją nadzorczą w zakresie ochrony danych	Wyjaśnienie. Projekt zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa

			osobowych, a wycieki danych osobowych u OUK to także incydenty, które mogą być istotne lub krytyczne dla prawidłowego świadczenia usług i ochrony interesów użytkowników końcowych korzystających z ich usług. Brak jest CSIRT komercyjnych oraz ISAC, które mogą i wspierają niektórych OUK w zapewnieniu cyberbezpieczeństwa. Natomiast wprowadzono: 6) organy publiczne oraz jednostki je obsługujące; 7) sądy i trybunały; 8) Narodowy Bank Polski; 9) Bank Gospodarstwa Krajowego; 11) jednostki podległe i nadzorowane przez organy administracji rządowej; 12) jednostki samorządu terytorialnego oraz ich związki i zrzeszenia; 13) uczelnie publiczne i Polską Akademię Nauk; 14) państwowe osoby prawne, utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, banków i spółek prawa handlowego; Są to tzw. użytkownicy końcowi (zinstytucjonalizowani ale użytkownicy końcowi). Inna kwestia bardzo istotna, to dlaczego krajowy system cyberbezpieczeństwa nie obejmuje innych użytkowników końcowych jakimi są obywatele? A przecież to dla nich świadczone są usługi kluczowe i cyfrowe i ich należy chronić! Wymieniono BGK, który jest bankiem i podlega ustawie – Prawo bankowe, a więc jest OUK. Wątpliwości rodzi udział RCB w KSC, które zajmuje się infrastrukturą krytyczną i zarządzaniem kryzysowym. Zgodnie z dyrektywą NIS banki są operatorami usług kluczowych. Ministerstwo Cyfryzacji wskazało w dokumencie "Ocena Skutków Regulacji" w części nr 4 "Podmioty, na które oddziałuje projekt" w wierszu odnoszącym się do "Podmioty świadczące usługi kluczowe w sektorze bankowości i infrastruktury rynków finansowych", że "Szacunki oparte na załączniku do projektu ustawy oraz danych KNF (dwadzieścia największych banków, dziesięć największych banków spółdzielczych, Krajowa SKOK, dziesięć największych SKOK, dwa banki państwowe, jedna giełda, dwaj operatorzy systemu obrotu i jeden kontrahent centralny)". Takie podejście jest wadliwe, gdyż ustawa w równym zakresie powinna obejmować wszystkie banki z jednoczesnym zachowaniem	CSIRT jest natomiast zarezerwowana dla zespołów poziomu krajowego. Ustawa dopuszcza dowolność w tworzeniu komercyjnych podmiotów zajmujących się obsługą incydentów jak też centrów wymiany informacji. Formacja, jaką jest Policja regulowana ustawą szczególną z dn. 6 kwietnia 1990 r., wpisuje się w ujęte w art. 4 pkt 11 projektu ustawy „jednostki podległe i nadzorowane przez organy administracji rządowej”. Prokuratura jest organem publicznym i elementem krajowego systemu na mocy art. 4 pkt 6 projektu. Obywatele jako użytkownicy końcowi nie zostali wymienieni w art. 4, gdyż nie nakłada się na nich żadnych szczególnych obowiązków, ale daje im się możliwość m.in. zgłaszania (dobrowolnego) incydentów. Planowane jest rozszerzenie o przepisy przewidujące powołanie przy Radzie Ministrów Kolegium do spraw Cyberbezpieczeństwa w skład którego wchodzić będzie Minister Koordynator Służb Specjalnych, MON, MSWiA, MC i RCB. Ustawa wzorem dyrektywy zawiera przepisy dotyczące obowiązków informacyjnych względem użytkowników usług kluczowych i cyfrowych. Zawiera również przepisy umożliwiające zgłaszanie incydentów przez osoby fizyczne do CSIRT NASK. Ustawa tworzy wymagania w zakresie podmiotowym dotyczące sektora finansowego. Podstawą wydania decyzji o uznaniu za operatora usług kluczowych jest świadczenie przez dany podmiot usług kluczowych (określonych w rozporządzeniu), za pomocą systemów informacyjnych, gdzie incydent ma istotny skutek zakłócający (próg istotności określony przez

			"zasady proporcjonalności". Brak wszystkich banków w KSC tworzy naturalną podatność dla całego systemu, i w ten sposób go osłabia.	Radę Ministrów w drodze uchwały). Nie wyklucza to włączenia wszystkich banków do KSC.
155.	art. 4	A.K. (uwagi osoby prywatnej)	Kogo właściwie obejmuje ustawa - tu jest problem, bo zgodnie z podanymi definicjami nie wiadomo czy ustawą objęty jest np. Plus. Nie prowadzi usług DNS, nie prowadzi węzła wymiany ruchu IXP. Rozumiem ograniczenia narzucone przez dyrektywę NIS, natomiast w zakresie telco jest jasne jakie podmioty świadczą tego typu usługi, czyli jakich podmiotów ustawa o systemie cyber dotyczy. Zostawcie proszę te nieszczęsne IXP w spokoju!	Wyjaśnienie. Dyspozycję do objęcia obowiązkami z zakresu bezpieczeństwa teleinformatycznego także podmiotów prowadzących punktu wymiany ruchu internetowego (IXP), wynikają z dyrektywy 2016/1148, a dokładnie z załącznika 2 do tej dyrektywy.
156.	art. 4	A.K. (uwagi osoby prywatnej)	Zagadnienia cyber w życiu codziennym najczęściej dotyczą przestępczości pospolitej. Pominięto w ogóle rolę Policji w zapewnieniu obsługi cyberbezpieczeństwa obywateli. To wyspecjalizowane jednostki policji są pierwszym miejscem kontaktu w przypadku oszustw internetowych. To pierwszy i podstawowy element systemu cyberbezpieczeństwa. Zgodnie z projektem ustawy obywatele mają zgłaszać incydenty do NASK, i co dalej? NASK zajmie się ściganiem oszustów na Allegro?	Wyjaśnienie. Policja, jako formacja porządku publicznego, regulowana ustawą szczególną z dn. 6 kwietnia 1990 r., wpisuje się w ujęte w art. 4 pkt 11 projektu ustawy „jednostki podległe i nadzorowane przez organy administracji rządowej”. Projekt ustawy o krajowym systemie cyberbezpieczeństwa dotyka wyłącznie problematyki określonej w dyrektywie 2016/1148, tj. zgłaszania i obsługi incydentów teleinformatycznych, nie ingerując w przepisy karne oraz proces ścigania cyberprzestępców. Przepisy projektowanej ustawy nie przekładają się na pracę Policji regulowaną odrębną ustawą szczególną oraz szeregiem aktów wykonawczych, regulujących działania dochodzeniowo-śledcze lub operacyjne, ani nie ingerują w pracę komórek Policji zajmujących się rozpoznawaniem, zapobieganiem i zwalczaniem cyberprzestępczości oraz ujawnianiem i ściganiem jej sprawców.

157.	art. 4 pkt 1	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu: Proponowane brzmienie „operatorów usług kluczowych i dostawców usług cyfrowych oraz jednostki je obsługujące”	Uwaga nieuwzględniona. Obowiązki wynikające z dyrektywy dotyczą operatorów usług kluczowych i dostawców usług cyfrowych, niezależnie czy są realizowane samodzielnie bądź poprzez „outsourcing”.
158.	art. 4 pkt 5	Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM	Choć w art. 4 ustawy w punkcie 5 wymienia się jako element krajowego systemu cyberbezpieczeństwa przedsiębiorców telekomunikacyjnych, to w ustawie brak jest przepisów nakładających na tych przedsiębiorców szczególne obowiązki. Jest to rozwiązanie całkowicie prawidłowe, biorąc pod uwagę szereg obowiązków obciążających przedsiębiorców telekomunikacyjnych, wynikających z ustawy Prawo telekomunikacyjne i wydawanych na ich postawie rozporządzeń, które to obowiązki zdają się realizować zamierzenia ustawy. Zwracamy uwagę na rozbieżność, jaka powstanie po wejściu w życie ustawy, z treścią art. 175a ustawy Prawo telekomunikacyjne. Zgodnie z tym przepisem przedsiębiorcy telekomunikacyjni są zobowiązani niezwłocznie informować Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług. W ocenie MEDIAKOM tak sformułowany zapis, posługujący się pojęciem integralności sieci i ocennym kryterium istotności naruszenia, prowadzi do sytuacji, gdy przedsiębiorca telekomunikacyjny powinien zawiadamiać Prezesa UKE o wszystkich incydentach, które miały miejsce i naruszyły integralność sieci – jak choćby przecięcie kabla na klatce schodowej. Jednocześnie po wejściu w życie projektowanej ustawy powstanie rozbieżność w terminach, którymi posługuje się ustawa Prawo telekomunikacyjne i nowa ustawa. Pojęcie „integralności i bezpieczeństwa sieci i usług” jest całkowicie oderwane od zdefiniowanych w projektowanej ustawie pojęcia „incydentu”. W ocenie MEDIAKOM w związku z planowanym wejściem w życie	Wyjaśnienie. Dyrektywa 2016/1148 nie pozwala na nakładanie żadnych nowych obowiązków na przedsiębiorców telekomunikacyjnych dotyczących cyberbezpieczeństwa i zgłaszania incydentów. Przedsiębiorcy telekomunikacyjni, nawet po wejściu w życie ustawy, zgłaszają incydenty w sposób określony w Prawie telekomunikacyjnym. Niniejszy projekt nie zmienia tego zakresu ani nie nakłada na przedsiębiorców telekomunikacyjnych nowych obowiązków w tym zakresie.

			ustawy o cyberbezpieczeństwie warto zadbać o po pierwsze lepszą redakcję art. 175a PT, usuwającą wątpliwości co do rodzaju i wagi zdarzeń, które winny być raportowane Prezesowi UKE przez przedsiębiorców telekomunikacyjnych, po drogie zaś ujednolicić terminologię ustaw. Zasadne wobec tego byłoby odwołanie się w art. 175a PT do pojęcia incydentu istotnego – a więc takiego, który mógł mieć istotny wpływ na świadczenie publicznie dostępnej usługi telekomunikacyjnej (w tym celu należałoby zmienić także definicję incydentu istotnego – art. 1 pkt. 12 projektu ustawy, dodając do wymienionych tam usług także publicznie dostępną usługę telekomunikacyjną). Dzięki temu przedsiębiorcy telekomunikacyjni raportowaliby tylko takie zdarzenia, które realnie i istotnie wpłynęły na cyberbezpieczeństwo. MEDIAKOM postuluje o doprecyzowanie tych projektowanych zapisów ustawy, które niepotrzebnie mogą nałożyć dodatkowe obowiązki na małych i średnich operatorów telekomunikacyjnych, co z pewnością spowoduje wzrost kosztów działalności. W ocenie MEDIAKOM zapisy rozdziałów VIIa i VIII PT, oraz wydane na ich postawie rozporządzenia wykonawcze wystarczająco, a nawet nadmiernie (kancelarie tajne i certyfikaty ABW), regulują działalność operatorów telekomunikacyjnych w zakresie bezpieczeństwa i cyberbezpieczeństwa.	
159.	art. 4 pkt 5 [w piśmie z uwagami błędnie oznaczne jako art. 4 ust. 5]	Polska Izba Radiodyfuzji Cyfrowej	W art. 4. skreślić ust. 5 przedsiębiorców telekomunikacyjnych. Brak jest wymienienia przedsiębiorców telekomunikacyjnych w przywoływanej Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148. Przedsiębiorcy telekomunikacyjni nie powinni zatem być wymienieni też w Ustawie. W konsekwencji należy zatem także wykreślić art. 61.	Uwaga nieuwzględniona. W kwestii przedsiębiorców telekomunikacyjnych - ustawa ma szerszy zakres niż tylko implementację dyrektywy 2016/1148. Jest to implementacja minimalna, a projekt traktuje materię szerzej. Ustawa włącza przedsiębiorców telekomunikacyjnych do krajowego systemu cyberbezpieczeństwa, ale nie nakłada dodatkowych obowiązków.

160.	art. 4 pkt 5	Konfederacja Lewiatan	W art. 4. skreślić pkt. 5 - przedsiębiorców telekomunikacyjnych. Brak jest wymienienia przedsiębiorców telekomunikacyjnych w przywoływanej Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148. Przedsiębiorcy telekomunikacyjni nie powinni zatem być wymienieni też w Ustawie. W konsekwencji należy zatem także wykreślić art. 61;	Uwaga nieuwzględniona. W kwestii przedsiębiorców telekomunikacyjnych - ustawa ma szerszy zakres niż tylko implementację dyrektywy 2016/1148. Jest to implementacja minimalna, a projekt traktuje materię szerzej. Ustawa włącza przedsiębiorców telekomunikacyjnych do krajowego systemu cyberbezpieczeństwa, ale nie nakłada dodatkowych obowiązków.
161.	art. 4 pkt 5	Polska Izba Informatyki i Telekomunikacji	W art. 4. skreślić pkt 5 przedsiębiorców telekomunikacyjnych. Brak jest bowiem wymienienia przedsiębiorców telekomunikacyjnych w przywoływanej Dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148. Ujęcie przedsiębiorców telekomunikacyjnych w projektowanej Ustawie jest zatem działaniem nadmiarowym i nie znajdującym podstaw na gruncie zapisów Dyrektywy. Przedsiębiorcy telekomunikacyjni nie powinni zatem być wymienieni w projektowanej Ustawie. W konsekwencji należy zatem także wykreślić art. 28 ust. 7 pkt 12) art. 61. Alternatywnie do wykreślenia pkt 5) proponujemy dodać na końcu treść „posiadających infrastrukturę krytyczną w rozumieniu art. 3 pkt 2 ustawy o zarzadzaniu kryzysowym” – uzasadnienie: każdy inny przedsiębiorca telekomunikacyjny nie będący operatorem usług kluczowych lub dostawcą usług cyfrowych zgodnie z art. 175a ust. 1 Pt już obecnie przekazuje bezpośrednio i niezwłocznie do Prezesa UKE informacje o naruszeniu bezpieczeństwa lub integralności sieci telekomunikacyjnej lub usług telekomunikacyjnych. Prezes UKE zgodnie z art. 61 przedmiotowego projektu ustawy przekazuje te informacje do CSIRT właściwego dla danego zgłaszającego przedsiębiorcy telekomunikacyjnego, co w konsekwencji wskazuje na fakt, że takiego przedsiębiorcy nie obejmuje krajowy system cyberbezpieczeństwa.	Uwaga nieuwzględniona. Dyrektywa 2016/1148 nie pozwala na nakładanie żadnych nowych obowiązków na przedsiębiorców telekomunikacyjnych dotyczących cyberbezpieczeństwa i zgłaszania incydentów. Przedmiotowy projekt ma szerszy zakres niż tylko implementację ww. dyrektywy. Przedsiębiorcy telekomunikacyjni, nawet po wejściu w życie ustawy, zgłaszają incydenty w sposób określony w Prawie telekomunikacyjnym. Niniejszy projekt nie zmienia tego zakresu ani nie nakłada na przedsiębiorców telekomunikacyjnych nowych obowiązków w tym zakresie.

162.	art. 4 pkt 5	Fundacja Bezpieczna Cyberprzestrzeń	Czy punkt ten obejmuje zespoły reagowania na incydenty komputerowe funkcjonujące w ramach tych przedsiębiorstw? Może warto wyrazić to explicite.	Wyjaśnienie. Przepisy uwzględniają przedsiębiorców telekomunikacyjnych w krajowym systemie cyberbezpieczeństwa, ale z uwagi na ograniczenia określone w dyrektywie 2016/1148 ustawa nie nakłada żadnych nowych obowiązków na przedsiębiorców telekomunikacyjnych dotyczących cyberbezpieczeństwa i zgłaszania incydentów. Ustawa uwzględnia możliwość dobrowolnego zgłoszenia incydentów przez przedsiębiorców telekomunikacyjnych do CSIRT NASK, jak również umożliwia ministrowi właściwemu ds. informatyzacji zapewnienie przedsiębiorcom telekomunikacyjnym, na wniosek, dostępu do systemu teleinformatycznego służącemu wymianie informacji o podatnościach, zagrożeniach i incydentach, jak również zbierającemu informacje o poziomie ryzyka wystąpienia poważnego incydentu.
163.	art. 4 pkt 5	Krajowa Izba Komunikacji Ethernetowej	Zgodnie z art. 4 pkt 5 projektu ustawy w skład krajowego systemu cyberbezpieczeństwa wchodzą m.in. przedsiębiorcy telekomunikacyjni. Tymczasem, zgodnie z art. 1 ust. 3 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS), transponowanej przedmiotowym projektem do polskiego prawa „Wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w niniejszej dyrektywie nie mają zastosowania do przedsiębiorstw, które podlegają wymogom art. 13a i 13b dyrektywy 2002/21/WE, ani do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia (UE) nr	Uwaga nieuwzględniona. W kwestii przedsiębiorców telekomunikacyjnych - ustawa ma szerszy zakres niż tylko implementację dyrektywy 2016/1148. Jest to implementacja minimalna, a projekt traktuje materię szerzej. Ponadto przepisy uwzględniają przedsiębiorców telekomunikacyjnych w krajowym systemie cyberbezpieczeństwa, ale z uwagi na ograniczenia określone w dyrektywie 2016/1148 ustawa nie nakłada żadnych nowych obowiązków na przedsiębiorców telekomunikacyjnych dotyczących

			910/2014". Przepisy art. 13a i 13b dyrektywy 2002/21/WE (dyrektywy ramowej) określają wymogi dla „przedsiębiorstw udostępniających publiczne sieci łączności" lub „świadczących publicznie dostępne usługi łączności elektronicznej", czyli – zgodnie z terminologią ustawy – Prawo telekomunikacyjne – dla przedsiębiorców telekomunikacyjnych. W związku z powyższym ustawa transponująca dyrektywę NIS do polskiego porządku prawnego nie powinna nakładać żadnych nowych obowiązków na przedsiębiorców telekomunikacyjnych. Nałożenie nowych obowiązków na przedsiębiorców telekomunikacyjnych byłoby nie tylko niezgodne z dyrektywą NIS, lecz również byłoby niezasadne, jako że przedsiębiorcy telekomunikacyjni realizują już od dawna szereg obowiązków w zakresie bezpieczeństwa na podstawie ustawy – Prawo telekomunikacyjne. Należy zwrócić uwagę, że projekt nakłada obowiązki – w odniesieniu do przedsiębiorców – zasadniczo na operatorów usług kluczowych oraz na dostawców usług cyfrowych.	cyberbezpieczeństwa i zgłaszania incydentów. Ustawa uwzględnia możliwość dobrowolnego zgłoszenia incydentów przez przedsiębiorców telekomunikacyjnych do CSIRT NASK, jak również umożliwia ministrowi właściwemu ds. informatyzacji zapewnienie przedsiębiorcom telekomunikacyjnym, na wniosek, dostępu do systemu teleinformatycznego służącemu wymianie informacji o podatnościach, zagrożeniach i incydentach, jak również zbierającemu informacje o poziomie ryzyka wystąpienia poważnego incydentu.
164.	art. 4 pkt 5	Polska Izba Komunikacji Elektronicznej	PIKE wskazuje treść motywu 7 dyrektywy NIS, oznaczającego, iż spod regulacji ustawy o krajowym systemie cyberbezpieczeństwa wyłączeni powinni zostać przedsiębiorcy telekomunikacyjni. Pragniemy wskazać, iż przedmiotowe kwestie w stosunku do przedsiębiorców telekomunikacyjnych regulują przepisy działu VIIA „Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych" ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne. Jednak, pomimo wskazanej powyżej treści dyrektywy, projekt ustawy o krajowym systemie cyberbezpieczeństwa nie zawiera zgodnego z dyrektywą wyłączenia jej zastosowania w stosunku do przedsiębiorców telekomunikacyjnych. Zamiast tego, w art. 4 pkt 5 projektu ustawy przedsiębiorcy telekomunikacyjni zaliczeni zostali do Krajowego systemu cyberbezpieczeństwa.	Uwaga nieuwzględniona. W kwestii przedsiębiorców telekomunikacyjnych - ustawa ma szerszy zakres niż tylko implementację dyrektywy 2016/1148. Jest to implementacja minimalna, a projekt traktuje materię szerzej. Przepisy uwzględniają przedsiębiorców telekomunikacyjnych w krajowym systemie cyberbezpieczeństwa, ale z uwagi na ograniczenia określone w dyrektywie 2016/1148 ustawa nie nakłada żadnych nowych obowiązków na przedsiębiorców telekomunikacyjnych dotyczących cyberbezpieczeństwa i zgłaszania incydentów. Ustawa uwzględnia możliwość dobrowolnego zgłoszenia

			Wskazując na powyższą niezgodność pomiędzy treścią dyrektywy a projektem ustawy wnosimy o wprowadzenie zmian do projektu ustawy i zapisanie wprost, iż jej przepisów nie stosuje się do przedsiębiorców telekomunikacyjnych, w rozumieniu ustawy Prawo telekomunikacyjne. Wnioskowana zmiana doprowadzi do zgodności pomiędzy treścią dyrektywy a projektem ustawy, a także wyeliminuje dwukrotne uregulowanie tych samych zagadnień w stosunku do przedsiębiorców telekomunikacyjnych w dwóch odrębnych ustawach, co z pewnością nie jest zgodne ze strategią rządu wprowadzania ułatwień w funkcjonowanie biznesu w Polsce. Pozostawienie projektu ustawy w obecnym brzmieniu może doprowadzić do jego niezgodności z treścią dyrektywy, którą implementuje. W konsekwencji, w przypadku wystąpienia sporów na tle stosowania przepisów ustawy w stosunku do przedsiębiorców telekomunikacyjnych może dojść do sytuacji, iż przedsiębiorcy będą powoływać się w sporach sądowych bezpośrednio na treść dyrektywy, a nie nieprawidłowo zaimplementowanej ustawy. Będzie to powodować niepożądaną przez nikogo niepewność dotyczącą stosowanego w praktyce prawa. Wprowadzenie do projektu ustawy wnioskowanego przez PIKE zapisu skuteczne wyeliminuje to zagrożenie.	incydentów przez przedsiębiorców telekomunikacyjnych do CSIRT NASK, jak również umożliwia ministrowi właściwemu ds. informatyzacji zapewnienie przedsiębiorcom telekomunikacyjnym, na wniosek, dostępu do systemu teleinformatycznego służącemu wymianie informacji o podatnościach, zagrożeniach i incydentach, jak również zbierającemu informacje o poziomie ryzyka wystąpienia poważnego incydentu.
165.	art. 4 pkt 15	Fundacja Bezpieczna Cyberprzestrzeń	Punkt ten wymaga doprecyzowania. Czy w ramach niego mieszczą się CSIRT-y należące do prywatnego biznesu. Gdzie w tym układzie jest przewidziane miejsce dla CSIRT-ów sektorowych – np. PSE, Bankowe Centrum Cyberbezpieczeństwa. Czy będzie istnieć jakieś kryterium decyzyjne o możliwości przynależności podmiotu? Kto lub co będzie o tym decydować? Wskazanie podmiotów poziomu „pośredniego” tylko częściowo odpowiada na te wątpliwości.	Wyjaśnienie. Projekt zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa CSIRT jest zarezerwowana dla zespołów poziomu krajowego. Podmioty świadczące usługi z zakresu cyberbezpieczeństwa będą uczestnikami krajowego

				systemu cyberbezpieczeństwa. Nie będzie dodatkowych arbitralnych kryteriów kwalifikujących.
166.	art. 4 pkt 15	Polska Izba Informatyki i Telekomunikacji	Artykuł 4 p. 15 podmioty świadczące usługi z zakresu cyberbezpieczeństwa – bardzo szeroka definicja przy braku określenia usług z zakresu cyberbezpieczeństwa – w zasadzie opowiadając o bezpieczeństwie urządzeń jako doradczego klienta, możemy zostać jesteśmy uznani jako podmiot kluczowy i podlegamy wszystkim obowiązkom wynikającym z ustawy. Uwaga: moim zdaniem nie obejmuje tego definicja 12.	Wyjaśnienie. Przepis art. 15 ust. 2 zawiera katalog zadań, które mogą być realizowane przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa. Decyzja o uznaniu za operatora usług kluczowych dotyczy operatora i nie dotyczy podmiotu, który na podstawie zobowiązań umownych może realizować w imieniu operatora usług kluczowych obowiązki z zakresu cyberbezpieczeństwa. Decyzja jest wydawana w oparciu o szereg parametrów świadczenie przez dany podmiot usług kluczowych (określonych w rozporządzeniu), za pomocą systemów informacyjnych, gdzie incydent ma istotny skutek zakłócający (próg istotności określony przez Radę Ministrów w drodze uchwały).
167.	art. 5	Związek Pracodawców w Branży Internetowej IAB Polska	Przechodząc do zapisów Projektu dotyczących operatorów usług kluczowych, należy na początku wskazać, że zgodnie z Dyrektywą NIS ustawa ma być przyjęta do 9 maja a stosowana od 10 maja 2018 r. włącznie z tym, że operatorzy usług kluczowych mają być wskazani najpóźniej do 9 listopada 2018 r. W Projekcie przewidziano tylko 14-dniowe vacatio legis. W przypadku tak krótkiego terminu pozostaje bardzo mało czasu na wdrożenie jakichkolwiek obowiązków wynikających z ustawy. Oczywiście niektóre podmioty mają zapewne już wdrożone wewnątrz organizacji część z obowiązków, jednak, nawet sam czas rekrutowania stanowiska specjalistycznego w cyberbezpieczeństwie, to nawet nie licząc ograniczeń finansowych, w Polsce to około 6-9 miesięcy, a na świecie nawet rok. Przy vacatio legis przewidzianym w Projekcie dostosowanie się do zapisów ustawy w wymaganym terminie przez podmioty do tego	Uwaga uwzględniona. Termin w art. 64 zostanie zmieniony. Zostanie wskazany 9 listopada 2018 r., jako termin wynikający z dyrektywy 2016/1148. Wymogi z art. 11 i art. 68 zostaną określone w jednym przepisie, wskazującym na terminy realizacji obowiązków.

			zobowiązane wydaje się zadaniem niemal niemożliwym do zrealizowania.	
168.	art. 5	Związek Banków Polskich	Wydanie decyzji przez OW o uznaniu za OUK, to jest bardzo niebezpiecznym ograniczeniem, gdyż tak jak to miało miejsce w przypadku afery Amber Gold, podmiot świadczył usługi bankowe a de facto nie podlegał nadzorowi. Dlatego głównym kryterium uznania danego podmiotu za OUK powinno być określenie czy świadczone przez niego usługi stanowią usługę kluczową. Uznanie podmioty za świadczącego usługi kluczowe to już jest czynność "techniczna" a samo świadczenie usługi kluczowej "z urzędu" powinno powodować, że taki podmiot podlega przepisom projektowanej ustawy.	Wyjaśnienie. Ustawa wzorem dyrektywy 2016/1148 ustanawia obowiązki o charakterze podmiotowym, a nie obowiązki o charakterze przedmiotowym (usługowym) wzorem licznego ustawodawstwa krajowego i europejskiego dotyczącego usług finansowych. Podstawą wpisania na listę operatorów usług kluczowych jest decyzja administracyjna o uznaniu za operatora usługi kluczowej, a w więc przejrzysta forma regulowania obowiązków pomiędzy organem administracji a stroną, zobowiązaną do wypełniania tych obowiązków.
169.	art. 5	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	W Rozdziale 2 Projektodawca pominął podmioty, które jako spółki samorządowe lub podmioty – spółki prawa handlowego funkcjonują w obszarze samorządowym i są operatorami usług kluczowych – np. gminne spółki wodno-kanalizacyjne, elektrociepłownie. Należy uszczegółowić zakres operatorów usług kluczowych w zakresie struktur samorządowych. Wyjaśnienia wymaga przepis art. 5 Projektu dotyczący decyzji o uznaniu za operatora usługi kluczowej. Projektodawca powinien wskazać, czy od decyzji takiej będzie przysługiwało odwołanie do organu wyższego rzędu, bądź też innego wskazanego organu. Ponadto należy precyzyjnie wskazać, czy decyzje te będą jawne – w przypadku braku zastrzeżenia wyłączenia ich jawności istnieje niebezpieczeństwo, że lista operatorów usług kluczowych zostanie udostępniona w trybie wniosków o udostępnianie informacji	Uwaga częściowo uwzględniona. Katalog podmiotów (załącznik) został poszerzony o samorządowe osoby prawne utworzone na podstawie odrębnej ustawy (ustawy z dnia 27 kwietnia 2001 r. - Prawo ochrony środowiska [Dz. U. z 2017 r. poz. 519 z późn. zm.]) w celu wykonywania zadań publicznych w zakresie zaopatrzenia w wodę pitną i jej dystrybucję. Uwaga nieuwzględniona. Wykaz operatorów usług kluczowych będzie udostępniany w trybie i na zasadach określonych w art. 8 ust. 6. Nie ma konieczności utajniania tego

			publicznej. Wyjaśnienia także wymaga kwestia jawności wykazu operatorów usług kluczowych, wydaje się bowiem, że jawność powinna być w tym przypadku wyłączona. Niezależnie, decyzja o uznaniu danego podmiotu za operatora usługi kluczowej nie może mieć skutku natychmiastowego. W zależności od skali oczekiwanych zmian wydaje się, że podmiot takiej decyzji powinien mieć czas na przygotowanie się do realizacji zapisów ustawy lub mieć czas na wycofanie się ze świadczenia usługi kluczowej (wypowiedzenie umów, etc).	wykazu, gdyż dostęp do niego został ograniczony ustawowo. Wpisanie lub wykreślenie z rejestru będzie następować na wniosek ze względu na centralizację rejestru operatorów.
170.	art. 5 ust. 1	Krajowa Izba Komunikacji Ethernetowej	Operatorem usługi kluczowej na podstawie projektu ustawy, może zostać podmiot należący do jednego z sektorów, podsektorów oraz rodzajów podmiotów wymienionych w załączniku do projektu ustawy. W załączniku do projektu ustawy, w dziale infrastruktura cyfrowa, wskazano jedynie podmioty świadczące usługi DNS, podmioty prowadzące punkt wymiany ruchu internetowego (IXP) oraz podmioty zarządzające rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD). W tym kontekście należy wskazać, że w projekcie ustawy należy zawrzeć definicję usługi DNS. Zgodnie z art. 1 pkt 15 w zw. z at. 1 pkt 14 dyrektywy NIS, dostawca usług DNS świadczy usługę odpowiadania na zapytania o nazwy domen w hierarchicznym, rozproszonym systemie nazw sieciowych. Naszym zdaniem nie jest to usługa telekomunikacyjna, a zatem tym bardziej nie jest zrozumiała przyczyna, dla której projekt ustawy włącza przedsiębiorców telekomunikacyjnych do krajowego systemu cyberbezpieczeństwa. W opinii KIKE art. 4 pkt 5 projektu ustawy należy wykreślić.	Wyjaśnienie. W sektorze infrastruktury cyfrowej wyróżniono rodzaje podmiotów posiłkując się załącznikiem dyrektywy 2016/1148, której założenia są implementowane do polskiego prawa przez projektowaną ustawę o krajowym systemie cyberbezpieczeństwa. W kwestii przedsiębiorców telekomunikacyjnych - ustawa ma szerszy zakres niż tylko implementację dyrektywy 2016/1148. Jest to implementacja minimalna, a projekt traktuje materię szerzej.
171.	art., 5 ust. 1	Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa	Na gruncie opublikowanego projektu samej ustawy nie tylko nie można jednoznacznie stwierdzić, które podmioty zostaną uznane za operatorów usług kluczowych, ale także w pełni ocenić, jaki wpływ projektowana regulacja będzie miała na podmioty, które zostaną uznane za takich operatorów. Kwestie szczegółowe, mające istotne znaczenie zarówno dla tej oceny, jak i dla prawidłowego wdrożenia	Wyjaśnienie. Kwestia ta została szczegółowo wyjaśniona w rozdziale II projektu ustawy.

			projektowanych regulacji zostaną bowiem uregulowane w drodze aktów wykonawczych. Projekty tych aktów nie zostały jednak udostępnione wraz z projektem ustawy.	Wykaz usług kluczowych oraz progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w wykazie, zostaną określone w drodze rozporządzenia.
172.	art. 5 ust. 1	Instytut Logistyki i Magazynowania	Operator usługi kluczowej a dostawca usług cyfrowych W art.4 pkt.1 operatorów usług kluczowych i dostawców usług cyfrowych wymieniono wspólnie. Dlatego jeżeli intencją było ograniczenie dostawców usług cyfrowych wyłącznie do tych, którzy współpracują z operatorami usług kluczowych to z zapisów art.17 to nie wynika. Wg uzasadnienia do projektu, art. ten miał wskazywać jacy dostawcy będą uczestnikami krajowego systemu cyberbezpieczeństwa. Zgodnie z zakresem obowiązków operator (art.12 ust.1) zgłasza incydent do właściwego CSIRT a dostawca (art.20 ust.1) do CSIRT NASK. Jeżeli operator i dostawca współpracują przy świadczeniu tej samej usługi to najprawdopodobniej będą pojawiać się powielone zgłoszenia incydentów i dodatkowo jest prawdopodobne, że trafią do różnych CSIRT. W art.19 ust.1 zapisano, że dostawca poza zgłoszeniem do CSIRT NASK informuje operatora usługi kluczowej o incydencie. Dlatego aby uniknąć powielania zgłoszeń (również różnego opisu incydentu) zgłoszenie powinien wykonać tylko operator (i jednocześnie koordynować jego dalszą obsługę również na poziomie dostawcy usługi).	Uwaga uwzględniona. W katalogu w oddzielnych punktach pojawia się operatorzy usług kluczowych i dostawcy.
173.	art. 5 ust. 1 oraz art 5 ust. 2 pkt 1	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Sugerujemy iż zawartość decyzji o uznaniu za operatora usługi kluczowej powinna doprecyzować jakie usługi kluczowe realizuje operator usługi kluczowej, które są objęte tymi przepisami. W wykazie usług kluczowych powinny być sprecyzowane usługi kluczowe dla poszczególnych obszarów działalności w celu precyzyjnego określenia zakresu w jakim dostawcy usług mają wdrożyć wymagania ustawy.	Wyjaśnienie. Kwestia ta została szczegółowo wyjaśniona w rozdziale II projektu ustawy. Kodeks postępowania administracyjnego reguluje elementy decyzji administracyjnej. Kwestie określające czas na spełnienie wymagań ustawowych przez operatora usług kluczowych określono w art. 68.

174.	art. 5 ust. 1 oraz art 5 ust. 2 pkt 1	Konfederacja Lewiatan	Sugerujemy, iż zawartość decyzji o uznaniu za operatora usługi kluczowej powinna doprecyzować jakie usługi kluczowe realizuje operator usługi kluczowej, które są objęte tymi przepisami. W wykazie usług kluczowych powinny być sprecyzowane usługi kluczowe dla poszczególnych obszarów działalności w celu precyzyjnego określenia zakresu w jakim dostawcy usług mają wdrożyć wymagania ustawy.	Wyjaśnienie. Kwestia ta została szczegółowo wyjaśniona w rozdziale II projektu ustawy. Kodeks postępowania administracyjnego reguluje elementy decyzji administracyjnej. Kwestie określające czas na spełnienie wymagań ustawowych przez operatora usług kluczowych określono w art. 68.
175.	art. 5 ust. 2	Polska Izba Ubezpieczeń	Wątpliwość sektora budzi sposób wskazywania przez podmiot uprawniony operatora kluczowego. W przypadku gdyby w przyszłości do grona operatorów kluczowych zostaną zaliczone inne sektory w tym np. sektor ubezpieczeniowy to ustawa powinna precyzować w jaki sposób zostanie poinformowany i w jakim trybie operator kluczowy oraz ile będzie miał czasu na spełnienie obowiązków wynikających z przepisów ustawy od momentu otrzymania informacji.	Wyjaśnienie. Kwestia ta została szczegółowo wyjaśniona w rozdziale II projektu ustawy. Kodeks postępowania administracyjnego reguluje elementy decyzji administracyjnej, kwestie doręczenia. Kwestie określające czas na spełnienie wymagań ustawowych przez operatora usług kluczowych określono w art. 68.
176.	art. 5 ust. 2	Izba Gospodarcza Gazownictwa	Obecny zapis jest niejednoznaczny. Zgodnie z uzasadnieniem projektu wszystkie 3 wymagania muszą być łącznie spełnione aby zostać uznanym za operatora usługi kluczowej. Przykład: Organ właściwy wydaje decyzję o uznaniu za operatora usługi kluczowej, jeżeli łącznie spełnione są poniższe wymagania:	Wyjaśnienie. Rzeczywiście wszystkie wspomniane wymagania muszą być spełnione.
177.	art. 5 ust. 2 pkt 2	Fundacja Bezpieczna Cyberprzestrzeń	Potrzeba doprecyzowania - informacyjnych czy informatycznych? Projekt ustawa proponuje nowe pojęcie „system informacyjny” i definiuje go jako system teleinformatyczny wraz z danymi w formie cyfrowej (Ustawa Art. 1. 18). To będzie stwarzało niepotrzebne niejasności. Dyrektywa używa określenia „systemy i sieci informatyczne”. W Ustawie powinno pozostać taki określenie albo „systemy i sieci teleinformatyczne” stosowane w przeważającej części dokumentu Ustawy.	Wyjaśnienie. Użyty w projekcie termin „systemy informacyjne” zawiera w sobie zarówno część infrastrukturalną (elementem systemu teleinformatycznego jest również sieć) wraz z przetwarzanymi w nich danymi w postaci elektronicznej. Jest to podejście szersze (obejmujące również dane), zatem definicja z art. 2 pkt 5 nie dotyczy wyłącznie kwestii sieci teleinformatycznych.

				Konieczność zapewnienia cyberbezpieczeństwa dotyczy ww. systemów informacyjnych i ich atrybutów (triada CIA – Confidentiality, Integrity, Availability). Ustawa nie reguluje tylko kwestii bezpieczeństwa teleinformatycznego, ale też m.in. ciągłości działania.
178.	art. 5 ust. 2 pkt 5	Fundacja Bezpieczna Cyberprzestrzeń	Czy w związku z założeniem, że system cyberbezpieczeństwa dotyczy podmiotów krajowych (o zasięgu krajowym), wystąpienie incydentu związanego z ograniczonym obszarem geograficznym de facto nie wyklucza istotności skutku incydentu dla świadczenia usługi kluczowej? Jaki jest próg?	Wyjaśnienie. Ograniczony obszar geograficzny nie wyklucza istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w wykazie. Progi dla incydentu znajdą się w akcie wykonawczym, o którym mowa w art. 13 ust. 4 i 5, natomiast kryteria uznania za operatora usługi kluczowej będą wynikać z przepisów, o których mowa w art. 7 ust. 1.
179.	art. 5 ust. 3	Krajowa Izba Komunikacji Ethernetowej	Pragniemy poddać pod rozwagę Pani Minister wprowadzenie również w przypadku operatorów usług kluczowych progu, poniżej którego dany podmiot nie będzie mógł zostać uznany za operatora usługi kluczowej. Dyrektywa NIS, a za nią projekt ustawy, przy wyznaczaniu operatorów usług kluczowych każe brać pod uwagę – w pierwszej kolejności – czy podmiot świadczy usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, a następnie – czy świadczenie tej usługi zależy od sieci i systemów informatycznych oraz czy incydent miałby istotny skutek zakłócający dla świadczenia tej usługi. Z kolei przy określaniu istotności skutku zakłócającego należy brać pod uwagę m.in. liczbę użytkowników zależnych od usługi świadczonej przez dany podmiot oraz znaczenie podmiotu w utrzymywaniu wystarczającego poziomu usługi przy uwzględnieniu dostępności alternatywnych sposobów świadczenia tej usługi.	Wyjaśnienie. Kwestia progów zostanie określona w przepisach wydanych na podstawie art. 8. W kwestii przedsiębiorców telekomunikacyjnych - ustawa ma szerszy zakres niż tylko implementację dyrektywy 2016/1148. Jest to implementacja minimalna, a projekt traktuje materię szerzej. Przepisy uwzględniają przedsiębiorców telekomunikacyjnych w krajowym systemie cyberbezpieczeństwa, ale z uwagi na ograniczenia określone w dyrektywie 2016/1148 ustawa nie nakłada żadnych nowych obowiązków na przedsiębiorców telekomunikacyjnych dotyczących cyberbezpieczeństwa i zgłaszania incydentów. Ustawa

			Dyrektywa, zgodnie z jej art. 5 ust. 7 lid. d, umożliwia wprowadzenie progów w celu określenia „[…] odpowiedniego poziomu dostaw w powiązaniu z liczbą użytkowników zależnych od tej usługi […] lub znaczenia tego konkretnego operatora usług kluczowych […]". Innymi słowy istnieje możliwość ustanowienia progu, poniżej którego dany podmiot nie będzie mógł zostać uznany za operatora usług kluczowych. Niezależnie od tego, że stoimy na stanowisku, iż przedsiębiorcy telekomunikacyjni nie powinni być uznawani za operatorów usług kluczowych, przepisy mające zastosowanie w ich przypadku mogą stanowić dobry punkt odniesienia. W tym względzie warto przywołać obowiązujące wciąż rozporządzenie Rady Ministrów w sprawie wypełniania przez przedsiębiorców telekomunikacyjnych zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Rozporządzenie to nakłada na przedsiębiorców telekomunikacyjnych obowiązki na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Dotyczy ono zatem kwestii bezpieczeństwa, podobnie jak i projekt ustawy. Zgodne z § 3 ust. 4 rozporządzenia z obowiązku uzyskania świadectwa bezpieczeństwa przemysłowego zwolnieni są przedsiębiorcy telekomunikacyjni obsługujący do 500 zakończeń sieci. Z kolei projekt rozporządzenia Rady Ministrów w sprawie wymagań i sposobu zapewnienia warunków dostępu i utrwalania przekazów telekomunikacyjnych i danych oraz rodzajów działalności telekomunikacyjnej lub rodzajów przedsiębiorców telekomunikacyjnych niepodlegających temu obowiązkowi, który znajduje się na etapie uzgodnień międzyresortowych i konsultacji publicznych, zwalnia z takiego obowiązku przedsiębiorców telekomunikacyjnych obsługujących do 50 000 zakończeń sieci. W opinii KIKE ta druga liczba zakończeń sieci znacznie bardziej przystaje do aktualnych realiów polskiego rynku. Stoimy na stanowisku, że przy wyznaczaniu operatorów usług kluczowych, powinny znaleźć zastosowanie podobne „progi	uwzględnia możliwość dobrowolnego zgłoszenia incydentów przez przedsiębiorców telekomunikacyjnych do CSIRT NASK, jak również umożliwia ministrowi właściwemu ds. informatyzacji zapewnienie przedsiębiorcom telekomunikacyjnym, na wniosek, dostępu do systemu teleinformatycznego służącemu wymianie informacji o podatnościach, zagrożeniach i incydentach, jak również zbierającemu informacje o poziomie ryzyka wystąpienia poważnego incydentu. Uwagi w zakresie progów odcięcia zostaną wykorzystane w toku opracowywania aktów wykonawczych do ustawy.

			odcięcia”, czyli przedsiębiorca świadczący usługi dla mniej niż 50 000 użytkowników nie powinien być uznany za operatora usług kluczowych. Mamy tutaj na myśli „użytkowników”, rozumiejąc w ten sposób podmioty korzystające z usług kluczowych na końcu łańcucha dostaw, czyli np. konsumentów. Pojęcie „użytkownika” nie jest jednak w pełni jasne na gruncie projektu ustawy. Należy podkreślić, że skoro usługi cyfrowe, w rozumieniu projektu ustawy, są usługami świadczonymi drogą elektroniczną, projekt ustawy powinien posługiwać się pojęciem „usługobiorcy” zamiast „użytkownika”. Jednocześnie pojęcie „usługobiorcy” będzie również bardziej uniwersalne i odpowiednie w przypadku usług kluczowych, które nie będą kwalifikowane jako przynależne do „infrastruktury cyfrowej”, o której mowa w załączniku do projektu ustawy. W związku z niejasnym na gruncie projektu ustawy pojęciem „użytkownika” należy zwrócić uwagę na specyfikę usług określonych jako przynależne do „infrastruktury cyfrowej”. Są to bowiem usługi świadczone bezpośrednio przedsiębiorcom. Dopiero przedsiębiorcy ci mogą świadczyć usługi konsumentom. W razie, gdyby w projekcie ustawy pod pojęciem „użytkownika” rozumiano podmiot, z którym potencjalny operator usług kluczowych zawiera umowę bezpośrednio, wówczas należałoby wskazać inne „progi odcięcia”. W przypadku usługi IXP możemy powołać się na bardzo dobre opracowanie przygotowane przez ICT Professional: „Zestawienie polskich węzłów wymiany ruchu internetowego w kontekście usług dla MiŚOT” (http://ictprofessional.pl/zestawienie-polskich-wezlow-wymiany-ruchu-internetowego-w-kontekscie-uslug-dla-misot/). Artykuł ten zawiera odnośnik do zestawienia węzłów wymiany ruchu internetowego (czyli podmiotów świadczących usługi IXP), obrazujące ich wielkość. Z zestawienia tego wynika, że można przyjąć, iż węzły obsługujące poniżej 20 przedsiębiorców telekomunikacyjnych nie powinny być uznawane za operatorów usług kluczowych. Takie węzły obsługiwane są przez niewielkie	

			podmioty. Realizacja przez takie podmioty obowiązków określonych w projekcie ustawy mogłaby stanowić dla nich zbyt duże obciążenie i być równoznaczna z koniecznością zaprzestania działalności.	
180.	art. 5 ust. 3	Związek Banków Polskich	Proponuje się aby ust. 3 otrzymał brzmienie: „3. Istotność skutku incydentu mającego wpływ na świadczenie usługi kluczowej, o którym mowa w ust. 2 pkt 3, określana jest na podstawie progów istotności skutku z uwzględnieniem co najmniej następujących czynników:”	Uwaga nieuwzględniona. Nie jest to uzasadniona zmiana.
181.	art. 5 ust. 3	Polska Izba Informatyki i Telekomunikacji	W zakresie interpretacji, czy dany incydent był „istotny” będzie określana na podstawie progów istotności skutku zakłócającego z uwzględnieniem czynników przywołanych w projekcie. Chcielibyśmy zwrócić uwagę, iż pojedynczy parametr nie powinien wystarczyć, aby uczynić incydent "istotnym". Jedynie łączna interpretacja kryteriów określonych w art. 5 ust 3 (i art. 16 ust. 4 dyrektywy) może zapewnić, że spełnia ona funkcję "progową". Wykorzystanie konkretnej liczby użytkowników jako wyjątkowego lub głównego progu dla "istotnego wpływu" stawia wyzwania techniczne. Poza potencjalnymi trudnościami technicznymi, które mogą wyniknąć z potrzeby obliczenia określonej liczby użytkowników, duża liczba obsługiwanych przez takie podmioty konsumentów, może spowodować każdy rodzaj incydentu, będzie spełniał próg proponowany przez ustawę, niezależnie od rzeczywistego wpływu incydentu na poziom bezpieczeństwa sieci i systemów informatycznych (co jest celem dyrektywy NIS zgodnie z art. 1). Ponadto, jeśli incydent nie może wyrządzić szkód osobistych lub jeśli ryzyko zostało złagodzone przez dostawcę, to taki incydent nie powinien być uważany za "istotny".	Wyjaśnienie. Progi istotności zostaną określone odrębnym aktem wykonawczym, wynikającym z zapisu art. 7 projektu ustawy.
182.	art. 5 ust. 3	Izba Gospodarcza Gazownictwa	Zapis niezrozumiały „Istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej…”, przykład: Istotność skutku incydentu zakłócającego dla świadczenia usługi kluczowej…	Uwaga nieuwzględniona.

183.	art. 5 ust. 3 pkt 3	Polska Izba Informatyki i Telekomunikacji	Czyją działalność gospodarczą podmiotu zgłaszającego, czy też partnerów? Jak to zmierzyć?	Wyjaśnienie. Zapis art. 5 ust. 3 pkt 3 jasno odnosi się do operatorów usług kluczowych. Progi istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej, w tym przywoływany w ust. 3 pkt. 3 wpływ incydentu, zostaną określony odrębnym aktem wykonawczym, wynikającym z zapisu art. 7 projektu ustawy.
184.	art. 5 ust. 3 pkt 4	Krajowy Związek Banków Spółdzielczych	Doprecyzowania wymaga jaki udział w rynku podmiotu świadczącego usługę kluczową będzie brany pod uwagę przy określaniu istotności skutku zakłócającego incydentu dla świadczenia usługi kluczowej. W przypadku banków mogą to być przykładowo udziały rynkowe w zakresie wolumenu kredytów, depozytów, ilości klientów, ilości klientów korzystających z bankowości internetowej, aktywów, itp.	Wyjaśnienie. Będzie to wynikać z progów istotności opracowanych przez ministra właściwego ds. informatyzacji we współpracy z organami właściwymi oraz dyrektorem RCB, zgodnie z zapisem art. 7 projektu ustawy.
185.	art. 5 ust. 5	Business Centre Club	W zakresie natychmiastowej wykonalności decyzji, o której mowa w art. 5 ust. 5 Projektu podkreślamy, że podjęcie decyzji o tym, że jakiś podmiot jest operatorem usługi kluczowej, wydaje się być szybkie do przeprowadzenia, natomiast dla tego podmiotu oznaczać to może niezwykle wysokie wydatki i długi czas na dostosowanie do wszystkich wymagań ustawy. Taka decyzja nie może zatem mieć skutku natychmiastowego. W zależności od skali oczekiwanych zmian wydaje się, że adresat takiej decyzji powinien mieć czas na przygotowanie się do realizacji zapisów ustawy lub mieć czas na wycofanie się ze świadczenia usługi kluczowej (wypowiedzenie umów, etc.). Po podjęciu decyzji, że dany podmiot świadczy usługę kluczową, podmiot ten powinien mieć np. 3 miesiące na poinformowanie podmiotu wydającego decyzję, że z uwagi na koszty lub inne przyczyny podejmuje decyzję o zaprzestaniu świadczenia tej usługi i określa czas potrzebny na podjęcie koniecznych działań w tym zakresie, nie dłuższy niż 1 rok	Uwaga nieuwzględniona. Artykuł 5 precyzyjnie wskazuje, iż skutek natychmiastowy ma decyzja o uznaniu bądź wygaśnięciu decyzji o uznaniu za operatora usługi kluczowej. Natomiast obowiązki nałożone przepisami projektu ustawy na operatorów usług kluczowych, powinni oni zacząć realizować wedle zapisów art. 68 ust. 1 projektu ustawy.

			(może być zależny od branży) lub określa zakres prac, które musi przeprowadzić i określa czas (nie dłużej niż 1 rok) potrzebny mu na ich zrealizowanie.	
186.	art. 5 ust. 5	Związek Pracodawców Branży Internetowej IAB Polska	W zakresie natychmiastowej wykonalności decyzji, o której mowa w art. 5 ust. 5 Projektu podkreślamy, że podjęcie decyzji o tym, że jakiś podmiot jest operatorem usługi kluczowej, wydaje się być szybkie do przeprowadzenia, natomiast dla tego podmiotu oznaczać to może niezwykle wysokie wydatki i długi czas na dostosowanie do wszystkich wymagań ustawy. Taka decyzja nie może zatem mieć skutku natychmiastowego. W zależności od skali oczekiwanych zmian wydaje się, że adresat takiej decyzji powinien mieć czas na przygotowanie się do realizacji zapisów ustawy lub mieć czas na wycofanie się ze świadczenia usługi kluczowej (wypowiedzenie umów, etc.). Po podjęciu decyzji, że dany podmiot świadczy usługę kluczową, podmiot ten powinien mieć np. 3 miesiące na poinformowanie podmiotu wydającego decyzję, że z uwagi na koszty lub inne przyczyny podejmuje decyzję o zaprzestaniu świadczenia tej usługi i określa czas potrzebny na podjęcie koniecznych działań w tym zakresie, nie dłuższy niż 1 rok (może być zależny od branży) lub określa zakres prac, które musi przeprowadzić i określa czas (nie dłużej niż 1 rok) potrzebny mu na ich zrealizowanie.	Uwaga nieuwzględniona. Artykuł 5 precyzyjnie wskazuje, iż skutek natychmiastowy ma decyzja o uznaniu bądź wygaśnięciu decyzji o uznaniu za operatora usługi kluczowej. Natomiast obowiązki nałożone przepisami projektu ustawy na operatorów usług kluczowych, powinni oni zacząć realizować wedle zapisów art. 68 ust. 1 projektu ustawy.
187.	art. 5 ust. 5	Związek Banków Polskich	Wejście w w reżim ustawy wymaga "vacatio legis" na dostosowanie się. Jak szybko OUK musi dostosować się do wymogów niniejszej ustawy i wymogów nadzorczych z niej wynikających? W zaproponowanym brzmieniu przepis ten może okazać się niemożliwy do zastosowania. Głównym kryterium powinno być faktyczne świadczenie usługi i obowiązek dla takiego operatora stosowania niniejszej ustawy. Proponuje się wprowadzenie przepisu, który wprost będzie stanowił, że ten kto świadczy usługi kluczowe wchodzi w reżim ustawy o KSC.	Uwaga nieuwzględniona. Artykuł 5 precyzyjnie wskazuje, iż skutek natychmiastowy ma decyzja o uznaniu bądź wygaśnięciu decyzji o uznaniu za operatora usługi kluczowej. Natomiast obowiązki nałożone przepisami projektu ustawy na operatorów usług kluczowych, powinni oni zacząć realizować wedle zapisów art. 68 ust. 1 projektu ustawy.

188.	art. 5 ust. 5	Polska Izba Radiodyfuzji Cyfrowej	Postulujemy uzupełnienie art. 5 ust. 5. Podjęcie decyzji o tym, że jakiś podmiot jest operatorem usługi kluczowej, wydaje się być szybkie do przeprocedowania, natomiast dla tego podmiotu oznaczać to może niezwykle wysokie wydatki i długi czas na dostosowanie do wszystkich wymagań ustawy. Taka decyzja nie może zatem mieć skutku natychmiastowego. W zależności od skali oczekiwanych zmian wydaje się, że podmiot takiej decyzji powinien mieć czas na przygotowanie się do realizacji zapisów ustawy lub mieć czas na wycofanie się ze świadczenia usługi kluczowej (wypowiedzenie umów, etc). Po podjęciu decyzji, że dany podmiot świadczy usługę kluczową, podmiot ten powinien mieć np. 3 miesiące na poinformowanie podmiotu wydającego decyzję, że z uwagi na koszty lub inne przyczyny podejmuje decyzję o zaprzestaniu świadczenia tej usługi i określa czas potrzebny na to nie dłuższy niż 1 rok (może być zależny od branży) lub określa zakres prac, które musi przeprowadzić i określa czas (nie dłużej niż 1 rok) potrzebny mu na ich zrealizowanie.	Uwaga nieuwzględniona. Artykuł 5 precyzyjnie wskazuje, iż skutek natychmiastowy ma decyzja o uznaniu bądź wygaśnięciu decyzji o uznaniu za operatora usługi kluczowej. Natomiast obowiązki nałożone przepisami projektu ustawy na operatorów usług kluczowych, powinni oni zacząć realizować wedle zapisów art. 68 ust. 1 projektu ustawy.
189.	art. 5 ust. 5	Konfederacja Lewiatan	Podjęcie decyzji o tym, że jakiś podmiot jest operatorem usługi kluczowej, wydaje się być szybkie do przeprocedowania, natomiast dla tego podmiotu oznaczać to może niezwykle wysokie wydatki i długi czas na dostosowanie do wszystkich wymagań ustawy. Taka decyzja nie może zatem mieć skutku natychmiastowego. W zależności od skali oczekiwanych zmian wydaje się, że podmiot takiej decyzji powinien mieć czas na przygotowanie się do realizacji zapisów ustawy lub mieć czas na wycofanie się ze świadczenia usługi kluczowej (wypowiedzenie umów, etc). Po podjęciu decyzji, że dany podmiot świadczy usługę kluczową, podmiot ten powinien mieć np. 3 miesiące na poinformowanie podmiotu wydającego decyzję, że z uwagi na koszty lub inne przyczyny podejmuje decyzję o zaprzestaniu świadczenia tej usługi i określa czas potrzebny na to nie dłuższy niż 1 rok (może być zależny	Uwaga nieuwzględniona. Artykuł 5 precyzyjnie wskazuje, iż skutek natychmiastowy ma decyzja o uznaniu bądź wygaśnięciu decyzji o uznaniu za operatora usługi kluczowej. Natomiast obowiązki nałożone przepisami projektu ustawy na operatorów usług kluczowych, powinni oni zacząć realizować wedle zapisów art. 68 ust. 1 projektu ustawy.

			od branży) lub określa zakres prac, które musi przeprowadzić i określa czas (nie dłużej niż 1 rok) potrzebny mu na ich zrealizowanie. Proponujemy usunięcie Art. 5 ust. 5.	
190.	art. 5 ust. 5	Polska Izba Informatyki i Telekomunikacji	Podjęcie decyzji o tym, że jakiś podmiot jest operatorem usługi kluczowej, wydaje się być szybkie do przeprocedowania, natomiast dla tego podmiotu oznaczać to może niezwykle wysokie wydatki i długi czas na dostosowanie do wszystkich wymagań ustawy. Taka decyzja nie może zatem mieć skutku natychmiastowego. W zależności od skali oczekiwanych zmian wydaje się, że podmiot takiej decyzji powinien mieć czas na przygotowanie się do realizacji zapisów ustawy lub mieć czas na wycofanie się ze świadczenia usługi kluczowej (wypowiedzenie umów, etc). Po podjęciu decyzji, że dany podmiot świadczy usługę kluczową, podmiot ten powinien mieć np. 3 miesiące na poinformowanie podmiotu wydającego decyzję, że z uwagi na koszty lub inne przyczyny podejmuje decyzję o zaprzestaniu świadczenia tej usługi i określa czas potrzebny na to nie dłuższy niż 1 rok (może być zależny od branży) lub określa zakres prac, które musi przeprowadzi i określa czas (nie dłużej niż 1 rok) potrzebny mu na ich zrealizowanie.	Uwaga nieuwzględniona. Artykuł 5 precyzyjnie wskazuje, iż skutek natychmiastowy ma decyzja o uznaniu bądź wygaśnięciu decyzji o uznaniu za operatora usługi kluczowej. Natomiast obowiązki nałożone przepisami projektu ustawy na operatorów usług kluczowych, powinni oni zacząć realizować wedle zapisów art. 68 ust. 1 projektu ustawy.
191.	art. 5 ust. 5	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy usunięcie Art. 5 ust. 5. Z faktem uznania danego podmiotu za operatora usługi kluczowej związane są daleko idące obowiązki ciążące na takim podmiocie, w tym konieczność poniesienia istotnych kosztów w związku z dostosowaniem do wymagań przewidzianych w ustawie. Biorąc pod uwagę zakres powyższych obowiązków natychmiastowa wykonalność decyzji jest zbyt daleko idącym obciążeniem dla podmiotu mogącego być uznanym za operatora usługi kluczowej.	Uwaga nieuwzględniona. Artykuł 5 precyzyjnie wskazuje, iż skutek natychmiastowy ma decyzja o uznaniu bądź wygaśnięciu decyzji o uznaniu za operatora usługi kluczowej. Natomiast obowiązki nałożone przepisami projektu ustawy na operatorów usług kluczowych, powinni oni zacząć realizować wedle zapisów art. 68 ust. 1 projektu ustawy.
192.	art. 6	Związek Banków Polskich	A co z innymi kryteriami np. 2) świadczona jest przy użyciu cyberprzestrzeni (sieci i systemów informacyjnych); 3) cyberincydent miałby istotny skutek zakłócający dla świadczenia tej	Wyjaśnienie.

			usługi; 4) spełnia kryteria jakościowe i ilościowe – tzw. „progi odcięcia”.	Usługi kluczowe zgodnie z koncepcją przyjętą w dyrektywie 2016/1148 mogą, ale nie muszą być świadczone za pomocą systemów informacyjnych. Muszą za to być od nich zależne. Ustawa wzorem dyrektywy 2016/1148 ustanawia obowiązki o charakterze podmiotowym, a nie obowiązki o charakterze przedmiotowym (usługowym) wzorem licznego ustawodawstwa krajowego i europejskiego dotyczącego usług finansowych.
193.	art. 6	Polska Izba Informatyki i Telekomunikacji	W art. 6 na końcu dodać treść „z wyłączeniem publicznie dostępnych usług telekomunikacyjnych, w rozumieniu art. 2 pkt 31 Pt” Uzasadnienie: konieczność tego wyłączenia wynika z treści pkt 7 wdrażanej przedmiotową ustawą Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016r., bowiem obowiązki przedsiębiorców telekomunikacyjnych w zakresie zapewnienia bezpieczeństwa i integralności sieci i usług telekomunikacyjnych określone są w Dziale VIIA Pt, w tym nałożone są w przywołanym Dziale obowiązki informacyjne w omawianym zakresie, co stanowi szczegółowe wymogi w zakresie bezpieczeństwa i integralności ustanowione w Dyrektywie 2002/21/WE Parlamentu Europejskiego i Rady.	Uwaga nieuwzględniona. Z uwagi na ograniczenia określone w dyrektywie 2016/1148 ustawa nie nakłada żadnych nowych obowiązków na przedsiębiorców telekomunikacyjnych dotyczących cyberbezpieczeństwa i zgłaszania incydentów. Sektor telekomunikacyjny nie jest wskazany jako sektor/podsektor w załączniku do ustawy.
194.	art. 6 art. 7 ust. 1	Business Centre Club	Również rozporządzenia o których mowa w art. 6 i art. 7 ust. 1 Projektu będą miały ogromne znaczenie dla przedsiębiorców i mogą mieć znaczący wpływ na swobodę prowadzenia działalności. Wiele usług kluczowych realizowanych przez przedsiębiorców wymaga bowiem planowania na kilka lat naprzód. Nagła zmiana przepisów może radykalnie zaburzyć modele biznesowe tych podmiotów gdyż będzie wymagać od nich poczynienia nowych wydatków i znacznych nakładów pracy. Wiele z takich podmiotów realizuje swoje plany m.in. w oparciu o kredyty lub dotacje celowe z programów krajowych lub europejskich, co związane jest z określonymi	Uwaga nieuwzględniona. W przypadku decyzji o uznaniu za operatora usługi kluczowej, zgodnie z treścią art. 68 ust. 1 OUK, będą dysponowali odpowiednim okresem, w którym powinni rozpocząć realizację obowiązków określonych w art. 10 ust. 2, art. 12 ust. 1 oraz art. 15 ust. 1.

			zobowiązaniami realizowania tychże planów. Z uwagi na potencjalnie bardzo znaczące skutki takich zmian legislacyjnych, powinny być one zawarte w przepisach rangi ustawowej, a nie rozporządzeń. W przypadku jednak pozostawienia formy rozporządzenia dla uregulowania powyższego zakresu, należałoby zmienić treści art. 7 ust. 1 Projektu, poprzez uwzględnienie w jego treści operatorów usług kluczowych, nadając mu brzmienie: „Minister właściwy do spraw informatyzacji we współpracy z organami właściwymi, dyrektorem Rządowego Centrum Bezpieczeństwa oraz operatorami usługi kluczowej (…)". Opracowanie progów istotności może w przyszłości w zauważalny sposób wpłynąć na koszty funkcjonowania przedsiębiorców związane z obsługą usług kluczowych, stąd udział przedsiębiorców w procesie ich opracowania jest w pełni zasadny. Dodatkowo, w ramach art. 7 ust. 3 Projektu zapis: „Progi istotności skutku zakłócającego dla świadczenia usług kluczowych przyjmuje Rada Ministrów w drodze uchwały" należy zmienić na „(…) przyjmuje Rada Ministrów w drodze rozporządzenia". Jak już wskazano, progi istotności skutku zakłócającego dla świadczenia usług kluczowych będą mieć wpływ na koszty funkcjonowania przedsiębiorcy. W przypadku, gdy będą przyjmowane w formie uchwał Rady Ministrów, ich opracowywanie odbywać się będzie poza jakąkolwiek wiedzą bezpośrednio zainteresowanych przedsiębiorców, co jest niezasadne i wpłynie negatywnie na skuteczność systemu cyberbezpieczeństwa. Progi nie powinny mieć charakteru niejawnego, ponieważ podmioty realizujące obowiązki wynikające z ustawy lub planujące wejść w dany zakres usług muszą mieć możliwość zapoznania się z nimi w celu określenia własnego planu działania. Nie ma też wymogu, aby podmioty realizujące usługi kluczowe podlegały przepisom ustawy o ochronie informacji niejawnych. Nieznajomość progu zakłócającego dla świadczenia usług kluczowych uniemożliwia	Upublicznienie progów w drodze rozporządzenia mogłoby pośrednio wpłynąć na ujawnienie kryteriów identyfikujących operatorów infrastruktury krytycznej.

			bowiem podmiotowi świadczącemu taką usługę przeprowadzenie analizy ryzyka i zaplanowanie odpowiednich środków zaradczych.	
195.	art. 6 i art. 7 ust. 1	Związek Pracodawcó w Branży Internetowej IAB Polska	Również rozporządzenia o których mowa w art. 6 i art. 7 ust. 1 Projektu będą miały ogromne znaczenie dla przedsiębiorców i mogą mieć znaczący wpływ na swobodę prowadzenia działalności. Wiele usług kluczowych realizowanych przez przedsiębiorców wymaga bowiem planowania na kilka lat naprzód. Nagła zmiana przepisów może radykalnie zaburzyć modele biznesowe tych podmiotów gdyż będzie wymagać od nich poczynienia nowych wydatków i znacznych nakładów pracy. Wiele z takich podmiotów realizuje swoje plany m.in. w oparciu o kredyty lub dotacje celowe z programów krajowych lub europejskich, co związane jest z określonymi zobowiązaniami realizowania tychże planów. Z uwagi na potencjalnie bardzo znaczące skutki takich zmian legislacyjnych, powinny być one zawarte w przepisach rangi ustawowej, a nie rozporządzeń.	Uwaga nieuwzględniona. W przypadku decyzji o uznaniu za operatora usługi kluczowej, zgodnie z treścią art. 68 ust. 1 OUK, będą dysponowali odpowiednim okresem, w którym powinni rozpocząć realizację obowiązków określonych w ustawie. Natomiast zmiana rozporządzeń wynikających z art. 6 i 7 projektu będzie procedowana w drodze rządowego procesu legislacyjnego, zatem wszelkie zmiany będą musiały być upublicznione w odpowiednim czasie, konsultowane i będą musiały mieć odpowiednio długi termin dostosowania się do nowych przepisów.
196.	art. 6 i art. 7 ust. 1	Polska Izba Radiodyfuzji Cyfrowej	Zmiany tych rozporządzeń będą miały ogromne znaczenie dla przedsiębiorców i mogą mieć znaczący wpływ na swobodę prowadzenia działalności. Wiele usług kluczowych realizowanych przez przedsiębiorców wymaga bowiem planowania na wiele lat naprzód. Nagła zmiana przepisów może radykalnie zaburzyć modele biznesowe tych podmiotów gdyż będzie wymagać od nich nowych wydatków i znacznych nakładów pracy. Wiele z takich podmiotów realizuje swoje plany m.in. w oparciu o kredyty lub dotacje celowe z programów krajowych lub europejskich, co związane jest z określonymi zobowiązaniami realizowania tychże planów. Z uwagi na potencjalnie bardzo znaczące skutki takich zmian legislacyjnych, powinny być one oparte o ustawę, a nie o rozporządzanie.	Uwaga nieuwzględniona. W przypadku decyzji o uznaniu za operatora usługi kluczowej, zgodnie z treścią art. 68 ust. 1 OUK, będą dysponowali odpowiednim okresem, w którym powinni rozpocząć realizację obowiązków określonych w ustawie. Natomiast zmiana rozporządzeń wynikających z art. 6 i 7 projektu będzie procedowana w drodze rządowego procesu legislacyjnego, zatem wszelkie zmiany będą musiały być upublicznione w odpowiednim czasie, konsultowane i będą musiały mieć odpowiednio długi termin dostosowania się do nowych przepisów.

197.	art. 6 i art. 7 ust. 1	Konfederacja Lewiatan	Zmiany tych rozporządzeń będą miały ogromne znaczenie dla przedsiębiorców i mogą mieć znaczący wpływ na swobodę prowadzenia działalności. Wiele usług kluczowych realizowanych przez przedsiębiorców wymaga bowiem planowania na wiele lat naprzód. Nagła zmiana przepisów może radykalnie zaburzyć modele biznesowe tych podmiotów gdyż będzie wymagać od nich nowych wydatków i znacznych nakładów pracy. Wiele z takich podmiotów realizuje swoje plany m.in. w oparciu o kredyty lub dotacje celowe z programów krajowych lub europejskich, co związane jest z określonymi zobowiązaniami realizowania tychże planów. Z uwagi na potencjalnie bardzo znaczące skutki takich zmian legislacyjnych, powinny być one oparte o ustawę, a nie o rozporządzanie.	Uwaga nieuwzględniona. W przypadku decyzji o uznaniu za operatora usługi kluczowej, zgodnie z treścią art. 68 ust. 1 OUK, będą dysponowali odpowiednim okresem, w którym powinni rozpocząć realizację obowiązków określonych w ustawie. Natomiast zmiana rozporządzeń wynikających z art. 6 i 7 projektu będzie procedowana w drodze rządowego procesu legislacyjnego, zatem wszelkie zmiany będą musiały być upublicznione w odpowiednim czasie, konsultowane i będą musiały mieć odpowiednio długi termin dostosowania się do nowych przepisów.
198.	art. 6 i art. 7 ust. 1	Polska Izba Informatyki i Telekomunikacji	Zmiany tych rozporządzeń będą miały ogromne znaczenie dla przedsiębiorców i mogą mieć znaczący wpływ na swobodę prowadzenia działalności. Wiele usług kluczowych realizowanych przez przedsiębiorców wymaga bowiem planowania na wiele lat naprzód. Nagła zmiana przepisów może radykalnie zaburzyć modele biznesowe tych podmiotów, gdyż będzie wymagać od nich nowych wydatków i znacznych nakładów pracy. Wiele z takich podmiotów realizuje swoje plany m.in. w oparciu o kredyty lub dotacje celowe z programów krajowych lub europejskich, co związane jest z określonymi zobowiązaniami realizowania tychże planów. Z uwagi na potencjalnie bardzo znaczące skutki takich zmian legislacyjnych, powinny być one oparte o ustawę, a nie o rozporządzanie.	Uwaga nieuwzględniona. W przypadku decyzji o uznaniu za operatora usługi kluczowej, zgodnie z treścią art. 68 ust. 1 OUK, będą dysponowali odpowiednim okresem, w którym powinni rozpocząć realizację obowiązków określonych w ustawie. Natomiast zmiana rozporządzeń wynikających z art. 6 i 7 projektu będzie procedowana w drodze rządowego procesu legislacyjnego, zatem wszelkie zmiany będą musiały być upublicznione w odpowiednim czasie, konsultowane i będą musiały mieć odpowiednio długi termin dostosowania się do nowych przepisów.
199.	art. 6 i art. 7 ust. 1	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Art. 6 i art.7 ust.1 Zmiany tych rozporządzeń będą miały ogromne znaczenie dla przedsiębiorców i mogą mieć znaczący wpływ na swobodę prowadzenia działalności. Wiele usług kluczowych realizowanych przez przedsiębiorców wymaga bowiem planowania na wiele lat naprzód. Nagła zmiana przepisów może radykalnie zaburzyć modele biznesowe tych podmiotów gdyż będzie wymagać	Uwaga nieuwzględniona. W przypadku decyzji o uznaniu za operatora usługi kluczowej, zgodnie z treścią art. 68 ust. 1 OUK, będą dysponowali odpowiednim okresem, w którym powinni rozpocząć realizację obowiązków

			od nich nowych wydatków i znacznych nakładów pracy. Liczne podmioty objęte projektem ustawy realizuje swoje plany w oparciu o kredyty lub dotacje celowe z programów krajowych lub europejskich, co skutkuje określonymi zobowiązaniami co do realizacji tych planów. Biorąc pod uwagę znaczące skutki proponowanych zmian legislacyjnych, uważamy iż powinny być one uwzględnione w ustawie, a nie w rozporządzeniu. Ponadto, opracowanie progów istotności może w przyszłości w zauważalny sposób wpłynąć na koszty funkcjonowania przedsiębiorcy związane z obsługą usług kluczowych, stąd udział przedsiębiorców w procesie ich opracowania jest w pełni zasadny. Z tego względu wnosimy o uzupełnienie treści art.7 ust. 1 poprzez nadanie mu brzmienia: „Minister właściwy do spraw informatyzacji we współpracy z organami właściwymi, dyrektorem Rządowego Centrum Bezpieczeństwa oraz operatorami usługi kluczowej (…)”.	określonych w ustawie. Natomiast zmiana rozporządzeń wynikających z art. 6 i 7 projektu będzie procedowana w drodze rządowego procesu legislacyjnego, zatem wszelkie zmiany będą musiały być upublicznione w odpowiednim czasie, konsultowane i będą musiały mieć odpowiednio długi termin dostosowania się do nowych przepisów. Nie sposób dołączyć operatorów usług kluczowych do podmiotów, które będą opracowywać jeden z pierwszych elementów w procesie uznania podmiotu za OUK, jakim jest określenie progów. Na tym etapie podmioty wymienione w art. 7 ust. 1 nie będą jeszcze dysponować wiedzą, kto jest uznany za OUK.
200.	art. 7	Związek Banków Polskich	Proponujemy usunięcie z ust. 1 Rządowego Centrum Bezpieczeństwa, gdyż RCB zajmuje się infrastrukturą krytyczną i zarządzaniem kryzysowym a nie stricte cyberbezpieczeństwem. 2. Nasuwają się wątpliwości dotyczące trybu wprowadzania progów istotności (uchwały Rady Ministrów), które nie są prawem obowiązującym dla przedsiębiorców sektora prywatnego.	Uwaga nieuwzględniona. Konstrukcja ustawy reguluje prawa i obowiązki operatorów usług kluczowych i dostawców usług cyfrowych, jednak zawiera łączniki z ustawą o zarządzaniu kryzysowym i Dyrektorem Rządowego Centrum Bezpieczeństwa, ponieważ aby zapewnić wymianę informacji i zapobiec dublowaniu obowiązków operatorów usług kluczowych, którzy są równocześnie operatorami infrastruktury krytycznej. Upublicznienie progów w drodze rozporządzenia mogłoby pośrednio wpłynąć na ujawnienie kryteriów identyfikujących operatorów infrastruktury krytycznej.
201.	art. 7 ust. 1	Związek Pracodawców Branży	W przypadku jednak pozostawienia formy rozporządzenia dla uregulowania powyższego zakresu, należałoby zmienić treści art. 7 ust. 1 Projektu, poprzez uwzględnienie w jego treści operatorów	Uwaga nieuwzględniona.

		Internetowej IAB Polska	usług kluczowych, nadając mu brzmienie: „Minister właściwy do spraw informatyzacji we współpracy z organami właściwymi, dyrektorem Rządowego Centrum Bezpieczeństwa oraz operatorami usługi kluczowej (…)". Opracowanie progów istotności może w przyszłości w zauważalny sposób wpłynąć na koszty funkcjonowania przedsiębiorców związane z obsługą usług kluczowych, stąd udział przedsiębiorców w procesie ich opracowania jest w pełni zasadny. Dodatkowo, w ramach art. 7 ust. 3 Projektu zapis: „Progi istotności skutku zakłócającego dla świadczenia usług kluczowych przyjmuje Rada Ministrów w drodze uchwały" należy zmienić na „(…) przyjmuje Rada Ministrów w drodze rozporządzenia". Jak już wskazano, progi istotności skutku zakłócającego dla świadczenia usług kluczowych będą mieć wpływ na koszty funkcjonowania przedsiębiorcy. W przypadku, gdy będą przyjmowane w formie uchwał Rady Ministrów, ich opracowywanie odbywać się będzie poza jakąkolwiek wiedzą bezpośrednio zainteresowanych przedsiębiorców, co jest niezasadne i wpłynie negatywnie na skuteczność systemu cyberbezpieczeństwa. Progi nie powinny mieć charakteru niejawnego, ponieważ podmioty realizujące obowiązki wynikające z ustawy lub planujące wejść w dany zakres usług muszą mieć możliwość zapoznania się z nimi w celu określenia własnego planu działania. Nie ma też wymogu, aby podmioty realizujące usługi kluczowe podlegały przepisom ustawy o ochronie informacji niejawnych. Nieznajomość progu zakłócającego dla świadczenia usług kluczowych uniemożliwia bowiem podmiotowi świadczącemu taką usługę przeprowadzenie analizy ryzyka i zaplanowanie odpowiednich środków zaradczych.	Upublicznienie progów w drodze rozporządzenia mogłoby pośrednio wpłynąć na ujawnienie kryteriów identyfikujących operatorów infrastruktury krytycznej. Nie sposób dołączyć operatorów usług kluczowych do podmiotów, które będą opracowywać jeden z pierwszych elementów w procesie uznania podmiotu za OUK, jakim jest określenie progów. Na tym etapie podmioty wymienione w art. 7 ust. 1 nie będą jeszcze dysponować wiedzą, kto jest uznany za OUK.
202.	art. 7 ust. 1	Polska Izba Radiodyfuzji Cyfrowej	Należy zmienić treść tego ustępu nadając mu brzmienie: „ Minister właściwy do spraw informatyzacji we współpracy z organami właściwymi, dyrektorem Rządowego Centrum Bezpieczeństwa – dodać – oraz operatorami usługi kluczowej (…)".	Uwaga nieuwzględniona. Nie sposób dołączyć operatorów usług kluczowych do podmiotów, które będą opracowywać jeden z pierwszych elementów w procesie uznania podmiotu

			Opracowanie progów istotności może w przyszłości w zauważalny sposób wpłynąć na koszty funkcjonowania przedsiębiorcy związane z obsługą usług kluczowych, stąd udział przedsiębiorców w procesie ich opracowania jest w pełni zasadny.	za OUK, jakim jest określenie progów. Na tym etapie podmioty wymienione w art. 7 ust. 1 nie będą jeszcze dysponować wiedzą, kto jest uznany za OUK.
203.	art. 7 ust. 1	Konfederacja Lewiatan	Należy dodatkowo zmienić treść tego ustępu nadając mu brzmienie: „ Minister właściwy do spraw informatyzacji we współpracy z organami właściwymi, dyrektorem Rządowego Centrum Bezpieczeństwa – dodać – oraz operatorami usługi kluczowej (…)”. Opracowanie progów istotności może w przyszłości w zauważalny sposób wpłynąć na koszty funkcjonowania przedsiębiorcy związane z obsługą usług kluczowych, stąd udział przedsiębiorców w procesie ich opracowania jest w pełni zasadny.	Uwaga nieuwzględniona. Nie sposób dołączyć operatorów usług kluczowych do podmiotów, które będą opracowywać jeden z pierwszych elementów w procesie uznania podmiotu za OUK, jakim jest określenie progów. Na tym etapie podmioty wymienione w art. 7 ust. 1 nie będą jeszcze dysponować wiedzą, kto jest uznany za OUK.
204.	art. 7 ust. 1	Polska Izba Informatyki i Telekomunikacji	Należy dodatkowo zmienić treść tego ustępu nadając mu brzmienie: „Minister właściwy do spraw informatyzacji we współpracy z organami właściwymi, dyrektorem Rządowego Centrum Bezpieczeństwa dodać oraz operatorami usługi kluczowej (…)”. Opracowanie progów istotności może w przyszłości w sposób istotny wpłynąć na koszty funkcjonowania przedsiębiorcy związane z obsługą usług kluczowych, stąd udział przedsiębiorców w procesie ich opracowania jest w pełni zasadny.	Uwaga nieuwzględniona. Nie sposób dołączyć operatorów usług kluczowych do podmiotów, które będą opracowywać jeden z pierwszych elementów w procesie uznania podmiotu za OUK, jakim jest określenie progów. Na tym etapie podmioty wymienione w art. 7 ust. 1 nie będą jeszcze dysponować wiedzą, kto jest uznany za OUK.
205.	art. 7 ust. 2	Fundacja Bezpieczna Cyberprzestrzeń	Ten zapis wymaga doprecyzowania. Czym są czynniki sektorowe? W Dyrektywnie NIS omówione są tylko czynniki międzysektorowe.	Wyjaśnienie. Dyrektywa 2016/1148 dopuszcza stosowanie czynników sektorowych (art. 6 ust. 2 Dyrektywy). Są to czynniki dodatkowe, biorące pod uwagę specyfikę oraz właściwości danego sektora bądź podsektora wymienionego w załączniku do projektu ustawy.
206.	art. 7 ust. 3	Związek Banków Polskich	Podejście takie determinuje dostęp do danych o obsłudze incydentu (kwestia posiadania właściwych poświadczeń bezp. oraz stosownej infrastruktury ochrony informacji niejawnych), chyba, że dane te zostaną udostępnione na podstawie zapisu art. 3 ust. 2	Wyjaśnienie. Kwestie dostępu do informacji niejawnych reguluje ustawa o ochronie informacji niejawnych.

207.	art. 7 ust. 3	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Nie jest jasne wprowadzenie przez projektodawcę aktów wykonawczych regulujących tą sama lub zbliżona kwestię. Zgodnie z art. 7 ust. 3 Projektu Rada Ministrów, w drodze uchwały przyjmuje progi istotności skutku zakłócającego dla świadczenia usług kluczowych. Przy uwzględnianiu progów istotności należy wziąć pod uwagę czynniki wymienione w art. 5 ust. 3 projektu. Zgodnie z projektem, do uchwały tej stosuje się przepisy o ochronie informacji niejawnych – nie zostało jednak wskazane, które przepisy znajdują tutaj zastosowanie. Przy określaniu progów istotności mogą być uwzględnione czynniki sektorowe, nigdzie jednak nie wytłumaczono czym są te czynniki. Z kolei zgodnie z art. 12 ust. 4 projektu Rada Ministrów określi w drodze rozporządzenia progi uznania incydentu za poważny w poszczególnych sektorach. Przy wydawaniu rozporządzenia uwzględnione mają być czynniki bliźniaczo podobne do tych, które uwzględnia się przy wydawaniu uchwały. Uzasadnienie nie tłumaczy, dlaczego kwestia istotności skutków regulowana jest podwójnie i to raz jako akt niejawny i wewnętrznie obowiązujący i raz jako źródło powszechnie obowiązującego prawa. Projektodawca powinien uzasadnić wydawania w różnej formie dwóch tak zbliżonych do siebie treściowo aktów prawnych. Niezależnie od powyższych uwag, wnosimy o zmianę brzmienia zapisu w art.7 ust.3: „Progi istotności skutku zakłócającego dla świadczenia usług kluczowych przyjmuje Rada Ministrów w drodze uchwały rozporządzenia”. Progi istotności skutku zakłócającego dla świadczenia usług kluczowych będą mieć wpływ na koszty funkcjonowania przedsiębiorcy. W przypadku, gdy będą przyjmowane w formie uchwał Rady Ministrów, ich opracowywanie odbywać się będzie poza jakąkolwiek wiedzą bezpośrednio zainteresowanych przedsiębiorców, co jest niezasadne i wpłynie negatywnie na skuteczność systemu cyberbezpieczeństwa. Progi istotności powinny mieć charakter jawny, jako że nieznajomość progu zakłócającego dla świadczenia usług kluczowych uniemożliwia podmiotowi świadczącemu taką usługę	Wyjaśnienie. Minister właściwy ds. informatyzacji opracowując progi istotności skutku zakłócającego, weźmie pod uwagę specyfikę oraz właściwości danego sektora bądź podsektora wymienionego w załączniku do projektu ustawy, z uwagi na szeroką rozbieżność przedmiotową sektorów bądź podsektorów. Operatorzy usług kluczowych w istotnej mierze będą również operatorami infrastruktury krytycznej, gdzie to zgodnie z ustawą o zarządzaniu kryzysowym kryteria identyfikujące są określone w załączniku do NPOIK, będącym dokumentem zawierającym informacje niejawne o klauzuli „zastrzeżone”. Upublicznienie progów w drodze rozporządzenia mogłoby pośrednio wpłynąć na ujawnienie kryteriów identyfikujących operatorów infrastruktury krytycznej.

			przeprowadzenie analizy ryzyka i zaplanowanie odpowiednich środków zaradczych.	
208.	art. 7 ust. 3	Polska Izba Radiodyfuzji Cyfrowej	Zapis „Progi istotności skutku zakłócającego dla świadczenia usług kluczowych przyjmuje Rada Ministrów w drodze uchwały" należy zmienić na „(…) przyjmuje Rada Ministrów w drodze rozporządzenia". Progi istotności skutku zakłócającego dla świadczenia usług kluczowych będą mieć wpływ na koszty funkcjonowania przedsiębiorcy. W przypadku, gdy będą przyjmowane w formie uchwał Rady Ministrów, ich opracowywanie odbywać się będzie poza jakąkolwiek wiedzą bezpośrednio zainteresowanych przedsiębiorców, co jest niezasadne i wpłynie negatywnie na skuteczność systemu cyberbezpieczeństwa. Progi nie powinny mieć charakteru niejawnego, ponieważ podmioty realizujące obowiązki wynikające z ustawy lub planujące wejść w dany zakres usług muszą mieć możliwość zapoznania się z nimi w celu określenia własnego planu działania. Nie ma też wymogu, aby podmioty realizujące usługi kluczowe podlegały przepisom ustawy o ochronie informacji niejawnych. Nieznajomość progu zakłócającego dla świadczenia usług kluczowych uniemożliwia bowiem podmiotowi świadczącemu taką usługę przeprowadzenie analizy ryzyka i zaplanowanie odpowiednich środków zaradczych.	Uwaga nieuwzględniona. Operatorzy usług kluczowych w istotnej mierze będą również operatorami infrastruktury krytycznej, gdzie to zgodnie z ustawą o zarządzaniu kryzysowym kryteria identyfikujące są określone w załączniku do NPOIK, będącym dokumentem zawierającym informacje niejawne o klauzuli „zastrzeżone". Upublicznienie progów w drodze rozporządzenia mogłoby pośrednio wpłynąć na ujawnienie kryteriów identyfikujących operatorów infrastruktury krytycznej.
209.	art. 7 ust. 3	Konfederacja Lewiatan	Dodatkowo zapis „Progi istotności skutku zakłócającego dla świadczenia usług kluczowych przyjmuje Rada Ministrów w drodze uchwały" należy zmienić na „(…) przyjmuje Rada Ministrów w drodze rozporządzenia". Progi istotności skutku zakłócającego dla świadczenia usług kluczowych będą mieć wpływ na koszty funkcjonowania przedsiębiorcy. W przypadku, gdy będą przyjmowane w formie uchwał Rady Ministrów, ich opracowywanie odbywać się będzie poza jakąkolwiek wiedzą bezpośrednio zainteresowanych przedsiębiorców, co jest niezasadne i wpłynie negatywnie na skuteczność systemu cyberbezpieczeństwa.	Uwaga nieuwzględniona. Operatorzy usług kluczowych w istotnej mierze będą również operatorami infrastruktury krytycznej, gdzie to zgodnie z ustawą o zarządzaniu kryzysowym kryteria identyfikujące są określone w załączniku do NPOIK, będącym dokumentem zawierającym informacje niejawne o klauzuli „zastrzeżone". Upublicznienie progów w drodze rozporządzenia mogłoby pośrednio wpłynąć na ujawnienie kryteriów

			Progi nie powinny mieć charakteru niejawnego, ponieważ podmioty realizujące obowiązki wynikające z ustawy lub planujące wejść w dany zakres usług muszą mieć możliwość zapoznania się z nimi w celu określenia własnego planu działania. Nie ma też wymogu, aby podmioty realizujące usługi kluczowe podlegały przepisom ustawy o ochronie informacji niejawnych. Nieznajomość progu zakłócającego dla świadczenia usług kluczowych uniemożliwia bowiem podmiotowi świadczącemu taką usługę przeprowadzenie analizy ryzyka i zaplanowanie odpowiednich środków zaradczych.	identyfikujących operatorów infrastruktury krytycznej.
210.	art. 7 ust. 3	Polska Izba Informatyki i Telekomunikacji	Dodatkowo „Progi istotności skutku zakłócającego dla świadczenia usług kluczowych przyjmuje Rada Ministrów w drodze uchwały" należy zmienić na „(…) przyjmuje Rada Ministrów w drodze rozporządzenia". Progi istotności skutku zakłócającego dla świadczenia usług kluczowych będą mieć wpływ na koszty funkcjonowania przedsiębiorcy. W przypadku, gdy będą przyjmowane w formie uchwał Rady Ministrów, ich opracowywanie odbywać się będzie poza jakąkolwiek wiedzą bezpośrednio zainteresowanych przedsiębiorców, co jest niezasadne i wpłynie negatywnie na skuteczność systemu cyberbezpieczeństwa. Progi nie powinny mieć charakteru niejawnego, ponieważ podmioty realizujące obowiązki wynikające z ustawy lub planujące wejść w dany zakres usług muszą mieć możliwość zapoznania się z nimi w celu określenia własnego planu działania. Nie ma też wymogu, aby podmioty realizujące usługi kluczowe podlegały przepisom ustawy o ochronie informacji niejawnych. Nieznajomość progu zakłócającego dla świadczenia usług kluczowych uniemożliwia bowiem podmiotowi świadczącemu taką usługę przeprowadzenie analizy ryzyka i zaplanowanie odpowiednich środków zaradczych.	Uwaga nieuwzględniona. Operatorzy usług kluczowych w istotnej mierze będą również operatorami infrastruktury krytycznej, gdzie to zgodnie z ustawą o zarządzaniu kryzysowym kryteria identyfikujące są określone w załączniku do NPOIK, będącym dokumentem zawierającym informacje niejawne o klauzuli „zastrzeżone". Upublicznienie progów w drodze rozporządzenia mogłoby pośrednio wpłynąć na ujawnienie kryteriów identyfikujących operatorów infrastruktury krytycznej.
211.	art. 7 ust. 3	Izba Gospodarcza Gazownictwa	Czy proponowane brzmienie zapisu wskazuje na możliwość objęcia informacji związanych z incydentem przepisami o ochronie informacji niejawnych? Przepis jest niejednoznaczny.	Wyjaśnienie. Operatorzy usług kluczowych w istotnej mierze będą również operatorami infrastruktury krytycznej, gdzie

				to zgodnie z ustawą o zarządzaniu kryzysowym kryteria identyfikujące są określone w załączniku do NPOIK, będącym dokumentem zawierającym informacje niejawne o klauzuli „zastrzeżone”.
212.	art. 8	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Brak jest uzasadnienia dla udostępniania informacji z wykazu operatorów usług kluczowych w trybie wnioskowym. Powinien być stworzony mechanizm umożliwiający podmiotom uprawnionym prawie natychmiastowy dostęp do tych danych, a nie kierowanie wniosku do ministra właściwego i oczekiwanie na jego odpowiedź. Należy podkreślić, że w cyberbezpieczeństwie jednym z najistotniejszych czynników jest szybkość reakcji, a wprowadzanie regulacji zawierających szereg wymogów formalnych, jak dzieje się to w przedstawionym Projekcie, szybkość tę znacząco opóźnia. Uważamy, iż informacje z wykazu operatorów usług kluczowych powinny być też udostępniane wszystkim podmiotom wchodzącym w skład krajowego systemu cyberbezpieczeństwa, ponieważ może to być brane przez nich pod uwagę przy wyborze partnera biznesowego.	Wyjaśnienie. Udostępnianie informacji z wykazu operatorów usług kluczowych zawiera obostrzenia, włącznie z trybem wnioskowym określonej kategorii podmiotów.
213.	art. 8 ust. 2	Polska Izba Informatyki i Telekomunikacji	Istotna jest lokalizacja usługi i obszar, jaki obejmuje, skoro jest to wykorzystywany przy ocenie istotności usługi i wpływu incydentu	Wyjaśnienie. Te cechy mogą zostać wykorzystane przy ocenie istotności.
214.	art. 8 ust. 2	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 8 ust 2 – warto dodać do danych OUK wyszczególnionych w przepisie danych kontaktowych a nie tylko sam adres firmy (adres e-mail, numery telefonów ew. osobę do kontaktu)	Uwaga nieuwzględniona.
215.	art. 8 ust. 3	Związek Banków Polskich	Dlaczego tylko OW może wnioskować o wpisanie lub wykreślenie OUK do/z wykazu? Przecież taką możliwość powinni mieć np. sami przedsiębiorcy świadczący usługi kluczowe.	Uwaga nieuwzględniona.

				Kwestia została uregulowana w art. 5 ust. 2 i 4 projektu ustawy.
216.	art. 8 ust. 5	Związek Banków Polskich	A co z CSIRT sektorowymi, przecież ich byt jest faktem i odgrywają coraz istotniejszą rolę w koordynacji obsługi incydentów o skutkach oddziaływania sektorowych, międzysektorowych i międzynarodowych. Pozbawienie ich dostępu do tych informacji może doprowadzić do ograniczenia skutecznego działania w zakresie koordynacji obsługi cyberincydentu.	Wyjaśnienie. Zespoły świadczące usługi z zakresu cyberbezpieczeństwa będą miały dostęp jeśli będą obsługiwać operatorów usług kluczowych.
217.	art. 8 ust. 5	Związek Banków Polskich	Proponujemy aby przedmiotowy wykaz był wykazem jawnym publikowanym na stronie internetowej BIP.	Uwaga nieuwzględniona. Operatorzy usług kluczowych w istotnej mierze będą również operatorami infrastruktury krytycznej, gdzie to zgodnie z ustawą o zarządzaniu kryzysowym kryteria identyfikujące są określone w załączniku do NPOIK, będącym dokumentem zawierającym informacje niejawne o klauzuli „zastrzeżone”.
218.	art. 8 ust. 5	Krajowy Związek Banków Spółdzielczych	Proponujemy doprecyzowanie sformułowania, iż minister właściwy do spraw informatyzacji udostępnia informacje z wykazu operatorów usług kluczowych na wniosek „…i dyrektora Rządowego Centrum Bezpieczeństwa”.	Uwaga uwzględniona.
219.	art. 8 ust. 6	Business Centre Club	Wskazujemy również, że informacje z wykazu operatorów usług kluczowych powinny być udostępniane (art. 8 ust. 6 Projektu) wszystkim podmiotom wchodzącym w skład krajowego systemu cyberbezpieczeństwa, ponieważ może to być brane przez nich pod uwagę przy wyborze partnera biznesowego (jeśli jeden podmiot świadczy usługę kluczową to chciałby on korzystać z usług podmiotu, który też świadczy taką usługę, gdyż daje to większe bezpieczeństwo własnej usługi kluczowej – szczególnie jeśli jedna zależy od drugiej).	Uwaga nieuwzględniona. Informacje będą udostępniane w niezbędnym zakresie wyłącznie wybranym podmiotom określonym w art. 8 ust. 6 w związku z realizowanymi przez nie zadaniami, wynikającymi z odrębnych przepisów.

220.	art. 8 ust. 6	Związek Banków Polskich	W kontekście propozycji do Art.8. ust. 5 przepis ten staje się bezprzedmiotowy.	Wyjaśnienie. Informacje z wykazu operatorów usług kluczowych będą udostępniane z tytułu właściwości CSIRT określonych w projekcie ustawy oraz w niezbędnym zakresie z tytułu właściwości instytucji wymienionych w art. 8 ust. 6 w związku z realizowanymi przez nie zadaniami, wynikającymi z odrębnych przepisów. Z uwagi na odrębny charakter oraz cel przetwarzania tych danych, właściwym jest rozróżnienie w projekcie ustawy.
221.	art. 8 ust. 6	Związek Pracodawców w Branży Internetowej IAB Polska	Wskazujemy również, że informacje z wykazu operatorów usług kluczowych powinny być udostępniane (art. 8 ust. 6 Projektu) wszystkim podmiotom wchodzącym w skład krajowego systemu cyberbezpieczeństwa, ponieważ może to być brane przez nich pod uwagę przy wyborze partnera biznesowego (jeśli jeden podmiot świadczy usługę kluczową to chciałby on korzystać z usług podmiotu, który też świadczy taką usługę, gdyż daje to większe bezpieczeństwo własnej usługi kluczowej – szczególnie jeśli jedna zależy od drugiej).	Uwaga nieuwzględniona. Informacje będą udostępniane w niezbędnym zakresie wyłącznie wybranym podmiotom określonym w art. 8 ust. 6 w związku z realizowanymi przez nie zadaniami, wynikającymi z odrębnych przepisów.
222.	art. 8 ust. 6	Polska Izba Radiodyfuzji Cyfrowej	Informacje z wykazu operatorów usług kluczowych powinny być też udostępniane wszystkim podmiotom wchodzącym w skład krajowego systemu cyberbezpieczeństwa, ponieważ może to być brane przez nich pod uwagę przy wyborze partnera biznesowego (jeśli świadczę usługę kluczową to chciałbym korzystać z usług podmiotu, który też świadczy taką usługę, gdyż daje to większe bezpieczeństwo własnej usługi kluczowej – szczególnie jeśli jedna zależy od drugiej).	Uwaga nieuwzględniona. Informacje będą udostępniane w niezbędnym zakresie wyłącznie wybranym podmiotom określonym w art. 8 ust. 6 w związku z realizowanymi przez nie zadaniami, wynikającymi z odrębnych przepisów.
223.	art. 8 ust. 6	Konfederacja Lewiatan	Informacje z wykazu operatorów usług kluczowych powinny być też udostępniane wszystkim podmiotom wchodzącym w skład krajowego systemu cyberbezpieczeństwa, ponieważ może to być	Uwaga nieuwzględniona.

			brane przez nich pod uwagę przy wyborze partnera biznesowego (jeśli świadczę usługę kluczową to chciałbym korzystać z usług podmiotu, który też świadczy taką usługę, gdyż daje to większe bezpieczeństwo własnej usługi kluczowej – szczególnie jeśli jedna zależy od drugiej).	Informacje będą udostępniane w niezbędnym zakresie wyłącznie wybranym podmiotom określonym w art. 8 ust. 6 w związku z realizowanymi przez nie zadaniami, wynikającymi z odrębnych przepisów.
224.	art. 8 ust. 6	Polska Izba Informatyki i Telekomunikacji	Informacje z wykazu operatorów usług kluczowych powinny być też udostępniane wszystkim podmiotom wchodzącym w skład krajowego systemu cyberbezpieczeństwa, ponieważ może to być brane przez nich pod uwagę przy wyborze partnera biznesowego (jeśli świadczę usługę kluczową to chciałbym korzystać z usług podmiotu, który też świadczy taką usługę, gdyż daje to większe bezpieczeństwo własnej usługi kluczowej – szczególnie jeśli jedna zależy od drugiej). Artykuł 8 p.6.7) i 8) skąd taka dysproporcja pomiędzy służbami – tu tylko szefowie służb	Uwaga nieuwzględniona. Informacje będą udostępniane w niezbędnym zakresie wyłącznie wybranym podmiotom określonym w art. 8 ust. 6 w związku z realizowanymi przez nie zadaniami, wynikającymi z odrębnych przepisów.
225.	art. 9	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Zgodnie z art. 9 Projektu operator usługi kluczowej jest obowiązany informować organ właściwy o każdej zmianie jego danych w terminie 14 dni. Projektodawca powinien wyjaśnić, czemu rezygnuje z promowania idei interoperacyjności i porozumiewania się państwowych rejestrów – zmiana danych adresowych musi być zgłaszana do szeregu innych rejestrów i to stamtąd dane te mogłyby być automatycznie pobierane do rejestru prowadzonego przez ministra właściwego do spraw informatyzacji.	Uwaga uwzględniona. Obowiązek aktualizacji danych zostanie przeniesiony na organy właściwe. Termin zgłoszenia zmiany danych zostanie wydłużony do 6 miesięcy. Nastąpi też rezygnacja z nakładania kary za brak aktualizacji danych w wykazie
226.	art. 10	Pracodawcy RP	Należy doprecyzować, że wymaganie uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm.	Uwaga nieuwzględniona. Przedsiębiorcy posiadający certyfikat zgodności z SZBI w rozumieniu ISO 27000 będą spełniać większość wymagań określonych dla usług kluczowych lub usług cyfrowych, pod warunkiem, że certyfikacją były objęte te usługi.

227.	art. 10	Polska Izba Informatyki i Telekomunikacji	Art. 10 - obowiązek zapewnienia przez operatora usługi kluczowej bezpieczeństwa świadczonych usług kluczowych oraz ich ciągłości. Sygnalizujemy brak odwołania do Polskich Norm, zgodnie, z którymi ww. wymaganie uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm – proponujemy wprowadzenie odpowiedniego uzupełnienia. Ponadto art. 10 ust. 2 pkt. 11 projektu nakłada na operatorów usług kluczowych bardzo dużo zadań i związanych z tym kosztów, w związku z tym budowa systemu bezpiecznej łączności na potrzeby komunikacji w ramach krajowego systemu cyberbezpieczeństwa powinna zostać przejęta przez ministra właściwego ds. informatyzacji. Dlatego też należy zaproponować zmianę zapisu w art. 10 ust. 2 pkt. 11 oraz ust. 3 tego artykułu na następujący: „2. […] 11) stosowanie środków bezpiecznej łączności, dostarczonych przez ministra właściwego do spraw informatyzacji, umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa. 3. Minister właściwy do spraw informatyzacji opracuje i udostępni operatorom usług kluczowych środki bezpiecznej łączności, o których mowa w ust. 2 pkt 11, kierując się potrzebą zapewnienia bezpieczeństwa środków łączności na odpowiednim poziomie.”	Uwaga nieuwzględniona. Przedsiębiorcy posiadający certyfikat zgodności z SZBI w rozumieniu ISO 27000 będą spełniać większość wymagań określonych dla usług kluczowych lub usług cyfrowych, pod warunkiem, że certyfikacją były objęte te usługi.
228.	art. 10	Konfederacja Lewiatan	Sygnalizujemy brak odwołania do Polskich Norm, zgodnie, z którymi ww. wymaganie uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm – proponujemy wprowadzenie odpowiedniego uzupełnienia.	Uwaga nieuwzględniona. Przedsiębiorcy posiadający certyfikat zgodności z SZBI w rozumieniu ISO 27000 będą spełniać większość wymagań określonych dla usług kluczowych lub usług cyfrowych, pod warunkiem, że certyfikacją były objęte te usługi.

229.	art. 10	Izba Gospodarcza Gazownictwa	Konieczność stworzenia norm branżowych (dla sektorów i podsektorów) w celu doprecyzowania jaki sa rzeczywiste wymagania – normy powinien wydawać min właściwy ds. informatyzacji. Brak jest konkretnego odniesienia jak ma być zapewnione bezpieczeństwo – odpowiednie punkty nie maja przełożenia na normy techniczne lub standardy (nie ma takich) Proponowany dodatkowo zapis umożliwia tworzenie szczegółowych norm lub standardów obszarowych (branżowych) w drodze rozporządzenia odpowiedniego ministerstwa (organu właściwego wg par 38), przykład: Ust. 4. Organ właściwy dla danego sektora może dodatkowo określić w drodze rozporządzenia minimalne wymagania dla ust. 2 pkt 1-10, kierując się potrzebą zapewnienia cyberbezpieczeństwa na odpowiednim poziomie - wprowadzenie szczegółowych norm dla różnych rodzajów IK (uszczegółowienie) – np. jak w USA NERC CIP dla energetyki	Uwaga nieuwzględniona. Przedsiębiorcy posiadający certyfikat zgodności z SZBI w rozumieniu ISO 27000 będą spełniać większość wymagań określonych dla usług kluczowych lub usług cyfrowych, pod warunkiem, że certyfikacją były objęte te usługi.
230.	art. 10	A.K. (uwagi osoby prywatnej)	Obowiązek zapewnienia przez operatora usługi kluczowej bezpieczeństwa świadczonych usług kluczowych oraz ich ciągłości (art. 10) - Brak odwołania do Polskich Norm, zgodnie z którym ww. wymaganie uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy PN-ISO/IEC 27001, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm.	Uwaga nieuwzględniona. Przedsiębiorcy posiadający certyfikat zgodności z SZBI w rozumieniu ISO 27000 będą spełniać większość wymagań określonych dla usług kluczowych lub usług cyfrowych, pod warunkiem, że certyfikacją były objęte te usługi.
231.	art. 10	Krajowy Związek Banków Spółdzielczych	Wskazane byłoby doprecyzowanie jak wymienione tu wymagania dotyczące system zarządzania bezpieczeństwem mają się do innych przepisów regulujących tę sferę funkcjonowania poszczególnych podmiotów. Przykładowo, w sektorze bankowym, kwestie związane z zarządzaniem bezpieczeństwem świadczonych usług reguluje m. in. Rekomendacja D KNF dotycząca zarządzania obszarami	Wyjaśnienie. Wymagania bezpieczeństwa będą mogły być określone w rekomendacjach do działań mających na celu wzmocnienie cyberbezpieczeństwa, o których mowa w art. 39 ust. 1 pkt. 4). Wytyczne doprecyzują

			technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach.	w wymiarze sektorowym wymagania bezpieczeństwa, o których mowa w artykule 10. Rekomendacja D jest przykładem takich wytycznych, które spełniają wymogi z art. 39 ust. 1 pkt. 4). Wspomniana kwestia została opisana w uzasadnieniu do projektu ustawy.
232.	art. 10 ust. 1	Związek Banków Polskich	Zapewnienie ciągłości świadczenia usług wchodzi w skład działań podejmowanych w ramach zapewnienia bezpieczeństwa świadczonych usług. W związku z powyższym nie ma potrzeby akcentowania kwestii zapewnienia ciągłości działania.	Wyjaśnienie. Zapewnienie cyberbezpieczeństwa systemów informacyjnych służących do świadczenia usług kluczowych i zapewnienie ciągłości działania to dwie kwestie objęte odrębnym zakresem normatywnym, stąd odrębne uwzględnienie w art. 10 i art. 16.

233.	art. 10 ust. 1 pkt 1	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	W art. 10 ust. 1 pkt 1 Projektu konieczne jest jasne i konkretne podanie, że dotyczy to zarówno sieci IT jak i OT (technologicznych) - jeżeli takie istnieją, inaczej będzie to ustawa rozwiązująca problem częściowo – w tym zakresie, ze względu na istotę problemu, należy bardziej uszczegółowić zakres procesów i usług jakie będą objęte regulacją już na poziomie ustawy. W zakresie art. 10 ust. 1 pkt 2 Projektu powstaje wątpliwość, czy CSIRT będą mieć specjalistów od analizy wszystkich incydentów - trzeba pamiętać, że ile technologii produkcyjnych tyle protokołów na świecie, co oznacza, że nie ma standaryzacji protokołów transmisyjnych w sieciach technologicznych. W konsekwencji Izba postuluje utworzenie pojęcia CERT'ów sektorowych specjalizujących się w technologiach sieci produkcyjnych. W tym zakresie ponownie wskazujemy, że przewidziane w OSR założenia (obejmujące koszt 5-10 tys. na pracownika SOC, koszt SOC - 1 mln zł oraz audyt 50 tys. zł) są nierealne i nieproporcjonalne. Dlatego też Izba postuluje utworzenie CERT'ów sektorowych i sugerowanie operatorom usług kluczowych oraz CERT'om sektorowym wykorzystywanie specjalistycznych narzędzi audytowych do sieci technologicznych i do stałego monitorowania tych sieci.	Wyjaśnienie. Systemy OT zawierają się w definicji systemów informacyjnych.
234.	art. 10 ust. 2	Pracodawcy RP	Zasadne jest, aby art. 10 ust. 2, który zawiera opis wymagań wdrażanego systemu zarządzania bezpieczeństwem (informacji) zawierał także wymóg zapewnienia bezpieczeństwa informacji podczas zarządzania usługami świadczonymi przez dostawców i kontrahentów. Ponadto wskazane jest, żeby w ustępie tym umieścić również wymóg uwzględnienia bezpieczeństwa systemów informatycznych na etapie ich projektowania oraz podczas rozwoju i modernizacji. Wprowadzenie obowiązku określenia odpowiednich wymagań bezpieczeństwa w fazie projektowania oraz obowiązek przeprowadzenia analizy ryzyka na etapie projektowania systemu informacyjnego.	Uwaga nieuwzględniona. Operator ma obowiązek zapewnić bezpieczeństwo świadczonej usługi niezależnie, czy korzysta z outsourcingu.

235.	art. 10 ust. 2	Fundacja Bezpieczna Cyberprzestrzeń	Jaki czas przewidziany jest na wdrożenie?	Wyjaśnienie. Wynika to z przepisów przejściowych – art. 68 ust. 1.
236.	art. 10 ust. 2	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 10 ust 2 – brak terminu w jakim OUK mają wdrożyć system zarządzania bezpieczeństwem	Wyjaśnienie. Wynika to z przepisów przejściowych – art. 68 ust. 1.
237.	art. 10 ust. 2	Instytut Logistyki i Magazynowania	System zarządzania bezpieczeństwem ust.10 Procedury zgłaszania i obsługi incydentów przez uczestników powinny być tworzone z uwzględnieniem wytycznych właściwych CSIRT dla zapewnienia odpowiedniej jakości obsługi incydentu i ujednolicenia procedur. Ust.2 i ust 10 można połączyć. System powinien zapewnić dodatkowo analizę informacji o zagrożeniach (przekazywanych przez właściwy CSIRT) i podejmowanie odpowiednich działań prewencyjnych (w porozumieniu z dostawcą usług).	Uwaga nieuwzględniona.
238.	art. 10 ust. 2 pkt 2	Krajowy Związek Banków Spółdzielczych	W art. 10 ust. 2 pkt 2 oraz dalszych niezbędne jest doprecyzowanie, że CSIRT właściwy dla poszczególnych operatorów usług kluczowych został określony w art. 28.	Uwaga nieuwzględniona. Właściwy CSIRT wynika z dalszych przepisów projektu ustawy. Nie ma potrzeby wskazywania za każdym razem właściwej jednostki redakcyjnej w treści projektu.
239.	art. 10 ust. 2 pkt 3	Związek Przedsiębiorców Polskich	Zgodnie z art. 10 ust. 2 pkt 3 Projektu operatorzy usług kluczowych wdrażają system zarządzania bezpieczeństwem zapewniający w szczególności odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu analizowania i zarządzania ryzykami, na jakie narażone są systemy informacyjne wykorzystywane przez nich do świadczenia usług kluczowych uwzględniając najnowszy stan wiedzy	Uwaga nieuwzględniona. Projektodawca nie przewiduje umiejscowienia przykładowych technicznych sposobów zabezpieczeń w akcie prawnym o randze ustawy.

			oraz zapewniając poziom bezpieczeństwa systemów informacyjnych odpowiedni do istniejącego ryzyka. Analogiczne postanowienie dotyczy dostawców usług cyfrowych w zakresie świadczonych przez nich usług cyfrowych (vide art. 18 ust. 2 Projektu). Takie ujęcie sprawy podyktowanej jest prawdopodobnie słusznym przyjęciem przez ustawodawcę, że wprowadzenie konkretnych sposobów zabezpieczeń do porządku prawnego nie jest rozwiązaniem idealnym. Nie sposób bowiem nowelizować ustawę za każdym razem jak pojawią się nowe sposoby zabezpieczania systemów informacyjnych. Z drugiej strony zatrzymanie się na sformułowaniu „odpowiednie i proporcjonalne środki techniczne (…) uwzględniając najnowszy stan wiedzy" jest dalece niewystarczające. Jak wynika z doświadczeń, zebranych m. in. na kanwie ustawy o ochronie danych osobowych z 1997 roku, gdzie przyjęto podobne rozwiązanie (vide art. 36 tejże ustawy), tak ogólne sformułowanie wymagań stawianych podmiotom przetwarzającym dane jest rozwiązaniem błędnym. Po pierwsze podmioty zobowiązane nie mają informacji, a jedynie mogą się domyślać, jak należy zabezpieczać dane. W celu dookreślenia ich obowiązków muszą samodzielnie, albo poprzez zewnętrznych konsultantów, dokonywać interpretacji na pograniczu prawa i techniki, co i tak nie daje im pewności co do zgodności z ustawą. Po drugie ustawodawca, który wprowadza tak ogólne postanowienia, ma problem z egzekucją celu jakiemu one służą. To jest ochroną danych. Spektrum możliwych interpretacji takiego postanowienia jest bowiem zbyt rozległe. Przyjmując, że doprecyzowanie tej kwestii nie może odbywać się poprzez narzucenie obowiązanym konkretnego rozwiązania, wskazać należy na dwa sposoby rozwiązania tego problemu. Po pierwsze można do Projektu wprowadzić przykładowe techniczne sposoby zabezpieczeń, które ponad wszelką wątpliwość	

			zapewniają realizację celów ustawodawcy. Alternatywnie, można wprowadzić do Projektu delegację ustawową do wydania rozporządzenia w tym zakresie, co zapewniałoby większą elastyczność regulacji prawnych, przy jednoczesnej realizacji celu. Idąc dalej, wskazać należy, że odpowiednimi sposobami zabezpieczeń, jakie mogłyby znaleźć się w katalogu otwartym na poziomie Projektu lub rozporządzenia są szyfrowanie lub anonimizacja danych, przy czym szyfrowanie jest możliwe do zastosowania w szerszym zakresie. Pamiętając o celu, jakim jest ochrona danych przed nieuprawnionym dostępem lub usunięciem, nie ulega wątpliwości, że odpowiednim sposobem ochrony tych danych jest szyfrowanie. Utrata kontroli nad zaszyfrowanymi danymi nie powoduje bowiem ujawnienia ich treści. Do tego wymagany jest dodatkowo dostęp do klucza szyfrującego, który dla bezpieczeństwa powinien być przechowywany w innym miejscu niż systemy informacyjne, w których dane są przetwarzane. Dlatego też należy postulować dodanie katalogu otwartego środków technicznych zapewniających cyberbezpieczeństwo, w którym znajdzie się szyfrowanie. Cyberbezpieczeństwo dotyczy zarówno przesyłu jak i przechowywania danych, w tym w usługach przetwarzania w chmurze, zdefiniowanych w Projekcie jako część usług cyfrowych (vide art. 1 pkt 20 i 21 Projektu), co Projekt powinien uwzględniać.	
240.	art. 10 ust. 2 pkt 3	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu Zapis „odpowiednie i proporcjonalne” jest nieprecyzyjny	Uwaga nieuwzględniona. Przepis w formie przyjętej przez projektodawcę jest czytelny.

241.	art. 10 ust. 2 pkt 3	Federacja Przedsiębiorców Polskich	Doprecyzowanie przepisów dotyczących zabezpieczeń systemów informacyjnych. Zgodnie z art. 10 ust. 2 pkt 3 Projektu operatorzy usług kluczowych wdrażają system zarządzania bezpieczeństwem zapewniający w szczególności odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu analizowania i zarządzania ryzykami, na jakie narażone są systemy informacyjne wykorzystywane przez nich do świadczenia usług kluczowych uwzględniając najnowszy stan wiedzy oraz zapewniając poziom bezpieczeństwa systemów informacyjnych odpowiedni do istniejącego ryzyka. Analogiczne postanowienie dotyczy dostawców usług cyfrowych w zakresie świadczonych przez nich usług cyfrowych (vide art. 18 ust. 2 Projektu). Takie ujęcie sprawy podyktowanej jest prawdopodobnie słusznym przyjęciem przez ustawodawcę, że wprowadzenie konkretnych sposobów zabezpieczeń do porządku prawnego nie jest rozwiązaniem idealnym. Nie sposób bowiem nowelizować ustawę za każdym razem jak pojawią się nowe sposoby zabezpieczania systemów informacyjnych. Z drugiej strony zatrzymanie się na sformułowaniu „odpowiednie i proporcjonalne środki techniczne (…) uwzględniając najnowszy stan wiedzy” jest dalece niewystarczające. Jak wynika z doświadczeń, zebranych m. in. na kanwie ustawy o ochronie danych osobowych z 1997 roku, gdzie przyjęto podobne rozwiązanie (vide art. 36 tejże ustawy), tak ogólne sformułowanie wymagań stawianych podmiotom przetwarzającym dane jest rozwiązaniem błędnym. Po pierwsze podmioty zobowiązane nie mają informacji, a jedynie mogą się domyślać, jak należy zabezpieczać dane. W celu dookreślenia ich obowiązków muszą samodzielnie, albo poprzez zewnętrznych konsultantów, dokonywać interpretacji na pograniczu prawa i techniki, co i tak nie daje im pewności co do zgodności z ustawą. Po drugie ustawodawca, który wprowadza tak ogólne postanowienia, ma problem z egzekucją celu jakiemu one służą. To	Uwaga nieuwzględniona. Projektodawca nie przewiduje umiejscowienia przykładowych technicznych sposobów zabezpieczeń w akcie prawnym o randze ustawy.

			jest ochroną danych. Spektrum możliwych interpretacji takiego postanowienia jest bowiem zbyt rozległe. Przyjmując, że doprecyzowanie tej kwestii nie może odbywać się poprzez narzucenie obowiązanym konkretnego rozwiązania, wskazać należy na dwa sposoby rozwiązania tego problemu. Po pierwsze można do Projektu wprowadzić przykładowe techniczne sposoby zabezpieczeń, które ponad wszelką wątpliwość zapewniają realizację celów ustawodawcy. Alternatywnie, można wprowadzić do Projektu delegację ustawową do wydania rozporządzenia w tym zakresie, co zapewniałoby większą elastyczność regulacji prawnych, przy jednoczesnej realizacji celu. Idąc dalej, wskazać należy, że odpowiednimi sposobami zabezpieczeń, jakie mogłyby znaleźć się w katalogu otwartym na poziomie Projektu lub rozporządzenia są szyfrowanie lub anonimizacja danych, przy czym szyfrowanie jest możliwe do zastosowania w szerszym zakresie. Pamiętając o celu, jakim jest ochrona danych przed nieuprawnionym dostępem lub usunięciem, nie ulega wątpliwości, że odpowiednim sposobem ochrony tych danych jest szyfrowanie. Utrata kontroli nad zaszyfrowanymi danymi nie powoduje bowiem ujawnienia ich treści. Do tego wymagany jest dodatkowo dostęp do klucza szyfrującego, który dla bezpieczeństwa powinien być przechowywany w innym miejscu niż systemy informacyjne, w których dane są przetwarzane. Dlatego też należy postulować dodanie katalogu otwartego środków technicznych zapewniających cyberbezpieczeństwo, w którym znajdzie się szyfrowanie. Cyberbezpieczeństwo dotyczy zarówno przesyłu jak i przechowywania danych, w tym w usługach przetwarzania w chmurze, zdefiniowanych w Projekcie jako część usług cyfrowych (vide art. 1 pkt 20 i 21 Projektu), co Projekt powinien uwzględniać.	

242.	art. 10 ust. 2 pkt 5	Izba Gospodarcza Gazownictwa	Zapis za mało precyzyjny. Brak definicji co jest rozumiane jako system monitorowania. Należy również wskazać co ma być monitorowane, jakiego rodzaju zdarzenia, pod jakim kątem na wypadek jakiej ewentualności. (monitorowaniem można objąć to co monitoruje się w ramach funkcjonowania SOC – Security Operations Center). Duże zagrożenie niesie za sobą też zapis „w trybie ciągłym". Oznacza to konieczność zapewnienia w trybie 24x7 obsługi systemów monitorowania, a tym samym zmianę organizacji pracy w instytucjach/firmach.	Wyjaśnienie. Przyjęta przez projektodawcę koncepcja zakłada, że monitorowanie obejmuje system zarządzania bezpieczeństwem operatora usług kluczowych wskazany w ust. 2. Wymagania w zakresie monitorowania będą mogły być doprecyzowane w rekomendacjach do działań mających na celu wzmocnienie cyberbezpieczeństwa, o których mowa w art. 39 ust. 1 pkt. 4). Wytyczne mogą doprecyzować w wymiarze sektorowym wymagania dotyczące funkcjonowania SOC – Security Operations Center.
243.	art. 10 ust. 2 pkt 5	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Użyte w przepisie pojęcie trybu ciągłego jest niewystarczająco precyzyjne. Prosimy o doprecyzowanie jakie elementy infrastruktury teleinformatycznej powinny być objęte ciągłym monitorowaniem.	Wyjaśnienie. Intencją projektodawcy było zapewnienie monitoringu bezpieczeństwa w trybie ciągłym, a sposób realizacji tego zadania zależy już od operatora.
244.	art. 10 ust. 2 pkt 5	Konfederacja Lewiatan	Użyte w przepisie pojęcie trybu ciągłego jest niewystarczająco precyzyjne. Prosimy o doprecyzowanie jakie elementy infrastruktury teleinformatycznej powinny być objęte ciągłym monitorowaniem. Proponujemy doprecyzowanie zapisu.	Wyjaśnienie. Intencją projektodawcy było zapewnienie monitoringu bezpieczeństwa w trybie ciągłym, a sposób realizacji tego zadania zależy już od operatora.
245.	art. 10 ust. 2 pkt 6	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. „bezpieczeństwo fizyczne i środowiskowe, w tym kontrolę dostępu" - Zapis jest mało precyzyjny (bezpieczeństwo fizyczne i środowiskowe jakiego elementu systemu)	Uwaga nieuwzględniona. Przepis w formie przyjętej przez projektodawcę jest czytelny.

246.	art. 10 ust. 2 pkt 7	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. „utrzymanie i bezpieczną eksploatacją systemów informacyjnych” - Zapis jest mało precyzyjny (utrzymanie i bezpieczną eksploatację)	Uwaga nieuwzględniona. Przepis w formie przyjętej przez projektodawcę jest czytelny.
247.	art. 10 ust. 2 pkt 8 [błędnie oznaczne jako art. 10 pkt 8]	Fundacja Bezpieczna Cyberprzestrzeń	Jak ten zapis odnosi się do definicji cyberbezpieczeństwa, która nie wspomina to „niezaprzeczalności”, ale wymienia za to „autentyczność”?	Uwaga nieuwzględniona. W opinii projektodawcy, istotniejsze jest zapewnienie autentyczności (wymienionej zresztą też w dyrektywie 2016/1148) niż niezaprzeczalności systemów informacyjnych. Są to różne elementy bezpieczeństwa informacji i nie są równoważne (por. np. definicje bezpieczeństwa informacji z PN-ISO/IEC 27000).
248.	Art. 10 ust. 2 pkt 8	Pracodawcy RP	Wskazane jest, żeby przepis art. 10 ust. 2 pkt 8 rozszerzyć o wymóg testowania planów ciągłości działania.	Uwaga nieuwzględniona.
249.	art. 10 ust. 2 pkt 11	Izba Gospodarcza Gazownictwa	Brak spójności z art. 42 ust. 1.	Uwaga nieuwzględniona.
250.	art. 10 ust. 2 i 3	Polska Organizacja Przemysłu i Handlu Naftowego	Właściwości sytemu zarządzania bezpieczeństwem wskazane w art. 10 ust. 2 Projektu są sformułowane w sposób ogólny i niejednoznaczny. Jedynie obowiązek stosowania środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa (art. 10 ust. 2 pkt. 11 Projektu), zostanie doprecyzowany w rozporządzeniu wydanym przez Ministra właściwego ds. informatyzacji (art. 10 ust. 3 Projektu). W ocenie POPiHN zamiast wskazywania w kolejnych aktach prawnych kolejnych właściwości stosowanych systemów	Wyjaśnienie. Intencją projektodawcy było zapewnienie monitoringu bezpieczeństwa w trybie ciągłym, a sposób realizacji tego zadania zależy już od operatora.

			informatycznych oraz wymagań technicznych dla stosowanych środków technicznych i organizacyjnych Ustawodawca powinien rozważyć powołanie się na obowiązujące normy i specyfikacje w zakresie systemu zarządzania bezpieczeństwem informacji powszechnie stosowane i przestrzegane przez (potencjalnych) operatorów usług kluczowych, w szczególności norma ISO 27001. Wiele podmiotów (w szczególności podmiotów należących do międzynarodowych grup kapitałowych) przestrzega międzynarodowych norm w zakresie bezpieczeństwa informacji, zatem wyznaczanie własnych norm przez każdy kraj stworzyłoby dodatkowe obciążenie i rozbieżności. Zatem jednym z możliwych rozwiązań prowadzących do uproszczenia i ujednolicenia obowiązujących wymagać jest uznanie zgodności z pewnymi uznanymi międzynarodowo normami za spełniające wymogi ustawodawstwa polskiego. Zachęcamy również do współpracy z branżowymi ekspertami i usługodawcami w tworzeniu wytycznych sektorowych – np. w ramach grupy roboczej, mającej zapewnić zgodność wytycznych z dobrymi praktykami w danej branży.	
251.	art. 11	Pracodawcy RP	Przepis art. 11 w treści zawartej w udostępnionym projekcie nakłada tylko wymóg opracowania i przechowywania dokumentacji. *Art. 11.* *1. Operatorzy usług kluczowych opracowują dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, w ciągu sześciu miesięcy od otrzymania decyzji o uznaniu za operatora usługi kluczowej, oraz przechowują tę dokumentację przez okres 5 lat liczonych od początku roku następującego po roku jej wytworzenia.* Przepis ten nie spełnia roli polegającej na postawieniu wymogu wdrożenia i utrzymywania systemu zarządzania bezpieczeństwem informacji, czego potwierdzeniem będzie posiadanie	Uwaga uwzględniona. Przepis zostanie zmieniony.

			udokumentowanych procedur lub polityk, które będą odpowiadały potrzebom organizacji. Zasadne jest, aby przepis ten stawiał wymóg opracowania, wdrożenia i utrzymywania w aktualności dokumentacji systemu zarządzania bezpieczeństwem informacji, a nie tylko posiadania opracowanej dokumentacji przez określony okres czasu.	
252.	art. 11	Polska Izba Radiodyfuzji Cyfrowej	Należy zmienić treść „w ciągu sześciu miesięcy od otrzymania decyzji" na „w ciągu sześciu miesięcy od otrzymania prawomocnej decyzji". Brak zapisu o prawomocności decyzji może skutkować tym, iż mimo wszczętego przez przedsiębiorcę procesu odwoławczego w stosunku do otrzymanej decyzji, operator usługi kluczowej będzie zmuszony przystąpić niezwłocznie do opracowania dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych. Dodatkowo okres 6 miesięcy jest realny do dotrzymania, jeżeli podmiot już wcześniej dostosował się do zapisów ustawy. W innym przypadku powinien obowiązywać czas na dostosowanie, jaki podmiot zadeklaruje na potrzeby przygotowania swoich systemów i procedur do działania w zgodzie z przepisami ustawy.	Uwaga nieuwzględniona. W opinii projektodawcy, termin sześciu miesięcy od wyznaczenia, jako operatora jest wystarczający.
253.	art. 11	Polska Izba Informatyki i Telekomunikacji	Art. 11 Obowiązek opracowania dokumentacji dot. cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych Należy zmienić treść „w ciągu sześciu miesięcy od otrzymania decyzji" na „w ciągu sześciu miesięcy od otrzymania prawomocnej decyzji". Brak zapisu o prawomocności decyzji może skutkować tym, iż mimo wszczętego przez przedsiębiorcę procesu odwoławczego w stosunku do otrzymanej decyzji, operator usługi kluczowej będzie zmuszony przystąpić niezwłocznie do opracowania dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych; Dodatkowo okres 6 miesięcy jest realny do dotrzymania, jeżeli podmiot już wcześniej dostosował się do zapisów ustawy. W innym przypadku powinien obowiązywać czas na dostosowanie, jaki	Uwaga nieuwzględniona. Decyzja o uznaniu za OUK określona w art. 5 ust. 2 projektu ustawy, ma natychmiastową wykonalność. Projekt wspomnianego rozporządzenia zostanie przygotowany w ramach procesu legislacyjnego.

			podmiot zadeklaruje na potrzeby przygotowania swoich systemów i procedur do działania w zgodzie z przepisami ustawy. Ponadto z uwagi na fakt, iż istotne warunki spełnienia tego obowiązku mają zostać określone w rozporządzeniu Rady Ministrów, a sam projekt rozporządzenia nie został przedstawiony, sygnalizujemy, że brak jest możliwości oceny przedmiotowego przepisu. W szczególności, istnieje ryzyko niedotrzymania terminu przygotowania wymaganej dokumentacji dot. cyberbezpieczeństwa w sytuacji opóźnienia w wydaniu rozporządzenia RM, o którym mowa w art. 11 ust. 3 ustawy. Rekomendujemy przedstawienie do konsultacji projektu rozporządzenia, a także wprowadzenie w projekcie ustawy odpowiedniego przepisu uzależniającego aktualizację obowiązku, o którym mowa w projektowanych art. 11 ust. 1 od wydania rozporządzenia, o którym mowa w art. 11 ust. 3, wraz z odpowiednio długim okresem przejściowym na przygotowanie tej dokumentacji wg wymagań rozporządzenia. Jest to szczególnie istotne, gdyż niewykonanie obowiązku zagrożone jest karą pieniężną.	
254.	art. 11	A.K. (uwagi osoby prywatnej)	Obowiązek opracowania dokumentacji dot. cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych (art. 11) - ryzyko niedotrzymania terminu przygotowania wymaganej dokumentacji dot. cyberbezpieczeństwa w sytuacji opóźnienia w wydaniu rozporządzenia RM, o którym mowa w art. 11 ust. 3 ustawy.	Wyjaśnienie. Projekt stosownego rozporządzenia RM, o którym mowa w art. 11 ust. 3 ustawy zostanie przygotowany w ramach procesu legislacyjnego. Opracowane akty wykonawcze do projektu ustawy, wejdą w życie w tym samym czasie, co projektowana ustawa, stąd obawa o opóźnienie jest bezzasadna.
255.	art. 11 ust. 1	Fundacja Bezpieczna Cyberprzestrzeń	Dokumentacja jest zgodnie z Dyr. NIS Art. 15 („Wdrażanie i egzekwowanie”) wymagana ale być może wystarczyłby audyt, o którym mowa w Art. 16 Ustawy, który byłby przeprowadzany raz na rok (zamiast zaproponowanych dwóch lat).	Uwaga nieuwzględniona. W zamyśle projektodawcy ten element dyrektywy 2016/1148 powinien zostać uwzględniony w projekcie ustawy o krajowym systemie cyberbezpieczeństwa.

256.	art. 11 ust. 1	Związek Banków Polskich	Brak informacji o utrzymywaniu w aktualności dokumentacji Cyberbezpieczeństwa; zapis powinien określać czas utrzymywania dokumentacji w odniesieniu do czasu życia systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.	Uwaga uwzględniona. Projekt zostanie uzupełniony o przepis dotyczący wymogu dotyczącego przeglądania i aktualizacji wytworzonej dokumentacji bezpieczeństwa, w celu zapewnienia, że odnosi się ona do aktualnego stanu infrastruktury i możliwych zagrożeń.
257.	art. 11 ust. 1	Business Centre Club	Z kolei w art. 11 ust. 1 Projektu, należy zmienić fragment przepisu „w ciągu sześciu miesięcy od otrzymania decyzji" na „w ciągu sześciu miesięcy od otrzymania prawomocnej decyzji". Brak zapisu o prawomocności decyzji może skutkować tym, iż mimo wszczętego przez przedsiębiorcę procesu odwoławczego w stosunku do otrzymanej decyzji, operator usługi kluczowej będzie zmuszony przystąpić niezwłocznie do opracowania dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych. Dodatkowo, okres 6 miesięcy jest realny do dotrzymania, jeżeli podmiot już wcześniej dostosował się do zapisów ustawy. W innym przypadku powinien obowiązywać taki czas na dostosowanie, jaki podmiot zadeklaruje na potrzeby przygotowania swoich systemów i procedur do działania w zgodzie z przepisami ustawy.	Uwaga nieuwzględniona. Decyzja o uznaniu za OUK określona w art. 5 ust. 2 projektu ustawy, ma natychmiastową wykonalność.
258.	art. 11 ust. 1	Związek Pracodawców Branży Internetowej IAB Polska	Z kolei w art. 11 ust. 1 Projektu, należy zmienić fragment przepisu „w ciągu sześciu miesięcy od otrzymania decyzji" na „w ciągu sześciu miesięcy od otrzymania prawomocnej decyzji". Brak zapisu o prawomocności decyzji może skutkować tym, iż mimo wszczętego przez przedsiębiorcę procesu odwoławczego w stosunku do otrzymanej decyzji, operator usługi kluczowej będzie zmuszony przystąpić niezwłocznie do opracowania dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych. Dodatkowo, okres 6 miesięcy jest realny do dotrzymania, jeżeli podmiot już wcześniej dostosował się do zapisów ustawy. W innym przypadku powinien obowiązywać taki czas na dostosowanie, jaki podmiot zadeklaruje	Uwaga nieuwzględniona. Decyzja o uznaniu za OUK określona w art. 5 ust. 2 projektu ustawy, ma natychmiastową wykonalność.

			na potrzeby przygotowania swoich systemów i procedur do działania w zgodzie z przepisami ustawy.	
259.	art. 11 ust. 1	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy następujące brzmienie art. 11 ust. 1: Art. 11. 1 Operatorzy usług kluczowych opracowują dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, w ciągu 2 lat od otrzymania decyzji o uznaniu za operatora usługi kluczowej, oraz przechowują tę dokumentację przez okres 5 lat liczonych od początku roku następującego po roku jej wytworzenia. Prosimy określenie okresu, w którym operator usług kluczowych musi się dostosować do wymagań niniejszej ustawy licząc od daty otrzymania decyzji o uznaniu za operatora usługi kluczowej. Dokumentacja, o której mowa w Art. 11 ust. 1 powinna powstać po wdrożeniu wymaganego systemu bezpieczeństwa. Okres 6 miesięcy jest stanowczo za krótki na wdrożenie wszystkich wymagań niniejszej ustawy. Proponujemy wprowadzenie okresu dostosowania do przepisów 2 lat.	Uwaga nieuwzględniona. Decyzja o uznaniu za OUK określona w art. 5 ust. 2 projektu ustawy, ma natychmiastową wykonalność. W opinii projektodawcy, termin sześciu miesięcy od wyznaczenia, jako operatora jest wystarczający.
260.	art. 11 ust. 1 i 2	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Ust. 1 odnosi się do systemów informatycznych wykorzystywanych do świadczenia usług kluczowych. Z kolei ust. 2 odnosi się do obiektów infrastruktury krytycznej, co może być węższym zakresem niż wskazany w ustępie 1. Proponujemy doprecyzowanie zakresu obowiązywania przepisów w przypadku ust. 1 i ust. 2 poprzez jednoznaczne określenie w jakim zakresie do operatorów usług kluczowych, o których mowa w ust. 2 przywołanego przepisu nie stosuje się przepisów ust. 1.	Wyjaśnienie W uzgodnieniu z RCB planowana jest zmiana wymagań dla planów sporządzonych przez IK tak aby obejmowały one wymagania dla świadczenia usług kluczowych.
261.	art. 11 ust. 1 i 2	Konfederacja Lewiatan	Należy zmienić treść „w ciągu sześciu miesięcy od otrzymania decyzji" na „w ciągu sześciu miesięcy od otrzymania prawomocnej decyzji". Brak zapisu o prawomocności decyzji może skutkować tym,	Uwaga nieuwzględniona.

			iż mimo wszczętego przez przedsiębiorcę procesu odwoławczego w stosunku do otrzymanej decyzji, operator usługi kluczowej będzie zmuszony przystąpić niezwłocznie do opracowania dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych. Dodatkowo okres 6 miesięcy jest realny do dotrzymania, jeżeli podmiot już wcześniej dostosował się do zapisów ustawy. W innym przypadku powinien obowiązywać czas na dostosowanie, jaki podmiot zadeklaruje na potrzeby przygotowania swoich systemów i procedur do działania w zgodzie z przepisami ustawy. Istnieje ryzyko niedotrzymania terminu przygotowania wymaganej dokumentacji dot. cyberbezpieczeństwa w sytuacji opóźnienia w wydaniu rozporządzenia RM, o którym mowa w art. 11 ust. 3 ustawy. Rekomendujemy przedstawienie do konsultacji projektu rozporządzenia, a także wprowadzenie w projekcie ustawy odpowiedniego przepisu uzależniającego aktualizację obowiązku, o którym mowa w projektowanych art. 11 ust. 1 od wydania rozporządzenia, o którym mowa w art. 11 ust. 3, wraz z odpowiednio długim okresem przejściowym na przygotowanie tej dokumentacji wg wymagań rozporządzenia. Jest to szczególnie istotne, gdyż niewykonanie obowiązku zagrożone jest karą pieniężną. Proponujemy wprowadzenie rocznego okresu dostosowania do przepisów, i konsekwentnie zmianę brzmienia art. 11 ust. 1 w następujący sposób: Proponujemy następujące brzmienie art. 11 ust. 1: Art. 11. 1 Operatorzy usług kluczowych opracowują dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, w ciągu roku od otrzymania decyzji o uznaniu za operatora usługi kluczowej, oraz przechowują tę dokumentację przez okres 5 lat liczonych od początku roku następującego po roku jej wytworzenia. Dodatkowo zwracamy uwagę na to, że Ust. 1 odnosi się do systemów informatycznych wykorzystywanych do świadczenia	Decyzja o uznaniu za OUK określona w art. 5 ust. 2 projektu ustawy, ma natychmiastową wykonalność. W opinii projektodawcy, termin sześciu miesięcy od wyznaczenia, jako operatora jest wystarczający. Ponadto, w uzgodnieniu z RCB planowana jest zmiana wymagań dla planów sporządzonych przez IK tak aby obejmowały one wymagania dla świadczenia usług kluczowych.

			usług kluczowych. Z kolei ust. 2 odnosi się do obiektów infrastruktury krytycznej, co może być węższym zakresem niż wskazany w ustępie 1. Proponujemy doprecyzowanie zakresu obowiązywania przepisów w przypadku ust. 1 i ust. 2 poprzez jednoznaczne określenie w jakim zakresie do operatorów usług kluczowych, o których mowa w ust. 2 przywołanego przepisu nie stosuje się przepisów ust. 1.	
262.	art. 11 ust. 1 i 3	Polska Organizacja Przemysłu i Handlu Naftowego	Art. 11 ust. 1 projektu nakłada na operatora usług kluczowych obowiązek sporządzenia szczegółowej dokumentacji dotyczącej cyberbezpieczeństwa systemów informatycznych wykorzystywanych do świadczenia usług kluczowych w terminie 6 miesięcy od dnia uznania dany podmiot za operatora usług kluczowych, przy czym szczegółowe wymogi dotyczące dokumentacji zostaną określone przez Radę Ministrów w rozporządzeniu. W zależności od stopnia skomplikowania dokumentacji, który zostanie określony w rozporządzeniu, wskazany w Projekcie termin 6 miesięcy może okazać się niewystarczający na opracowania odpowiedniej dokumentacji. Terminem który pozwoli na przeanalizowanie aktualnych rozwiązań, wdrożenie nowych (w tym wynikających z wdrożenia Dyrektywy) i opracowanie stosownej dokumentacji to termin co najmniej 12 miesięcy od dnia uznania danego podmiotu za operatora usług kluczowych. Co więcej, sposób tworzenia, aktualizacji oraz zakres informacji zawartych w dokumentacji określony w rozporządzeniu nie powinien być skomplikowany ani nadmiernie szeroki – powinien sprowadzać się do wprowadzenia jasnych zasad tworzenia i aktualizacji dokumentacji oraz określać podstawową treść dokumentacji w precyzyjny i zrozumiały sposób. Dodatkowo, należy wskazać, że Dyrektywa nie przewiduje takiego obowiązku, stanowiąc jedynie w art. 15 ust. 2 lit. a), że Państwa	Uwaga nieuwzględniona. Decyzja o uznaniu za OUK określona w art. 5 ust. 2 projektu ustawy, ma natychmiastową wykonalność. W opinii projektodawcy, termin sześciu miesięcy od wyznaczenia, jako operatora jest wystarczający.

			członkowskie zapewniają, aby właściwe organy miały uprawnienia i środki, pozwalające wymagać od operatorów usług kluczowych przekazywania: informacji niezbędnych do oceny bezpieczeństwa ich sieci i systemów informatycznych, w tym dokumentów dotyczących polityki w zakresie bezpieczeństwa. Co więcej, propozycje rozwiązań implementujących Dyrektywę przyjęte w innych krajach implementujących Dyrektywę nie przewidują tak rygorystycznego i szczegółowego obowiązku tworzenia dokumentacji dotyczącej cyberbezpieczeństwa (w szczególności brak jest analogicznych obowiązków w propozycji Wielkiej Brytanii, Niemiec i Holandii).	
263.	art. 12	Pracodawcy RP	Brak jednoznacznego i nie budzącego wątpliwości określenia odpowiedzialności za obsługę incydentu poważnego – z jednej strony odpowiedzialność za obsługę incydentu spoczywa na operatorze, z drugiej strony projekt ustawy przewiduje wprost uprawnienia CSIRT w zakresie obsługi incydentów poważnych, nie wskazując przy tym zasad przejmowania przez CSIRT incydentów do obsługi oraz przyznając CSIRT pewne uprawnienia „władcze" wobec operatora (np. wezwanie za pośrednictwem organu właściwego operatora do usunięcia podatności, żądanie informacji itd.). Tym samym, CSIRT miałby możliwość ingerencji w działalność jednostkowego operatora z pominięciem jakiejkolwiek odpowiedzialności za podejmowane wobec operatora działania. Uszczegóławiając powyższe, zwracamy uwagę, że zgodnie z projektowanym art. 12 ust. 1 pkt 6 operator ma zapewnić obsługę incydentu poważnego i incydentu krytycznego we współpracy z właściwym CSIRT, w tym poinformować o usunięciu podatności, które doprowadziły lub mogły doprowadzić do poważnego incydentu. Na wniosek operatora CSIRT może zapewnić wsparcie w obsłudze lub obsługę poważnych incydentów (art. 28 ust.2), przy czym odpowiednio – zgodnie z projektowanym art. 28 ust. 2 - zadaniem	Wyjaśnienie. Założeniem projektodawcy było z jednej strony zapewnienie możliwości technicznej obsługi poważnych i krytycznych incydentów przez wyspecjalizowane do tego typu podmioty, czyli CSIRT poziomu krajowego. Z drugiej strony projektodawca chce zagwarantować, aby możliwe było zastosowanie władztwa o charakterze administracyjno-prawnym w przypadku działań na rzecz zapobiegania rozprzestrzeniania się incydentu. Zadania CSIRT w art. 28 zostaną doprecyzowane.

			CSIRT jest realizacja zadań na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewnienie koordynację obsługi poważnych incydentów. Natomiast zgodnie z projektowanym art. 28 ust. 5, 6 i 7 do zadań CSIRT należy obsługa lub koordynacja obsługi incydentów zgłaszanych przez wskazane w ustawie podmioty. Z tym uprawnieniem korelują uprawnienia CSIRT wskazane w art. 34, zgodnie z którym CSIRT może: „wykonywać niezbędne działania techniczne, związane z monitorowaniem zagrożeń, obsługa incydentów poważnych (…), a także dokonywać analiz (…)", „wystąpić do organu właściwego z wnioskiem o wezwanie operatora, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do poważnego incydentu" oraz „może wystąpić bezpośrednio do operatora o udostępnienie informacji technicznych związanych z incydentem, które będą niezbędne do przeprowadzenia analizy zdarzenia lub obsługi incydentu" W praktyce może to oznaczać, że dla jednego incydentu, właściwe będą dwa ośrodki, co w praktyce znacznie utrudni, o ile nie uniemożliwi jego właściwą obsługę. Po drugie, istnieje znaczące ryzyko, że CSIRT może definiować względem operatora nieadekwatne wymagania, które mogą generować nadmierne obciążenia kosztowe, jednocześnie nie stanowiąc najbardziej efektywnego rozwiązania zaistniałego problemu.	
264.	art. 12. ust. 1. pkt 1	Związek Banków Polskich	Ustawa nie określa klasyfikacji incydentów. Proponuje się stworzenie delegowanego aktu/rozporządzenia, w którym określona zostanie identyfikacja incydentu w oparciu o skutek oddziaływania oraz istotność z wykorzystaniem np. klasyfikacji ENISA. https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies	Wyjaśnienie. Ustawa przewiduje w art. 12 ust. 5 wydanie rozporządzenia, w którym zostaną określone progi uznania incydentu za poważny, co uwzględnia również skutek oddziaływania.

265.	art. 12. ust. 1. pkt 1 [w piśmie z uwagami jako art.12 pkt1]	Instytut Logistyki i Magazynowania	Projekt zakłada opcjonalność zgłaszania incydentów zwykłych, należy jednak rozważyć zgłaszanie wszystkich incydentów (wszystkich klas). W efekcie wszystkie incydenty będą rejestrowane a analizy zagrożeń na poziomie CSIRT będą bazować na pełnych danych. Wg projektu incydenty zakwalifikowane przez uczestników jako zwykłe nie będą weryfikowane przez CSIR a wstępna kwalifikacja zwykłego incydentu może okazać się błędna. Jeżeli będą zgłaszane incydenty wszystkich klas, ich rejestrowanie będzie niepotrzebne ponieważ na liście funkcjonalności systemu teleinformatycznego jest rejestrowanie incydentów (art.42 ust.1), po co to robić dodatkowo poza tym systemem? Dzięki temu, utrzymywanie odrębnych rejestrów po stronie uczestników systemu nie będzie konieczne. Do czasu uruchomienia systemu teleinformatycznego (2021) uczestnicy będą rejestrowali incydenty samodzielnie jednak w obowiązkach podmiotu publicznego nie zapisano obowiązku rejestracji incydentów (tylko jego zgłoszenie).	Wyjaśnienie. Definicje incydentów zostaną przeredagowane dla większej przejrzystości.
266.	art. 12 ust. 1 pkt 3	Fundacja Bezpieczna Cyberprzestrzeń	Ten zapis jest niejasny z uwagi na powtórzenie „identyfikować” w tym ustępie, jak i ustępie 1, art. 12. Sugerowana zmiana na „w tym rozpoznawać incydent poważny na podstawie…”	Uwaga uwzględniona. Przepisy zostaną przeredagowane..
267.	art. 12 ust. 1 pkt 3 [w piśmie z uwagami błędnie jako art.12 pkt3]	Instytut Logistyki i Magazynowania	Dlaczego obowiązek klasyfikacji incydentów dla operatora usług kluczowych jest opisany inaczej niż dla pozostałych dostawców usług i podmiotów publicznych? Na potrzeby klasyfikacji wszyscy uczestnicy powinni posługiwać się tymi samymi kryteriami. Powinni samodzielnie decydować o klasyfikacji incydentu również jako incydentu krytycznego. Wg projektu ustawy tylko CSIRT nadaje taką klasę (art.28 ust.3). Tu raczej powinien być zapis o weryfikacji przez CSIRT zgłoszeń (w kolejności klas nadanych przez operatorów, dostawców i podmioty publiczne) i ewentualnej zmianie klasy incydentu. Możliwość zgłoszenia incydentu od razu jako krytycznego może przyspieszyć jego obsługę.	Uwaga nieuwzględniona. Wynika to z określonych w projekcie ustawy właściwości i różnic występujących pomiędzy UOK, DUC oraz podmiotów publicznych.

			Przekazywanie obsługi incydentów pomiędzy CSIRT opisane w art. 28 ust.8 powinno zostać przeniesione do ust.3. W art.28 ust.11 jest błędne odwołanie do ust.8, powinno być ust.11. Ogólnie w art.28 pomieszane są ze sobą zdania związane z obsługą incydentów i finansowaniem zadań.	
268.	art.12. ust. 1 pkt 3-6	Związek Banków Polskich	Nie jest jasna różnica między incydentem krytycznym i poważnym oraz sposobem ich obsługi; podobnie jak brak odniesienia się do obsługi incydentu istotnego.	Wyjaśnienie. Definicje ww. incydentów znajdują się w art. 2 pkt 9 i 10. Różnice będące przedmiotem pytań zostały określone w rozdziałach dotyczących zadań OUK, DUC, podmiotów publicznych oraz CSIRT.
269.	art.12. ust. 1. pkt 4	Związek Banków Polskich	Rygor czasowy 24h od wykrycia incydentu może uniemożliwić przeprowadzenie tak skrupultanej i głębokiej analizy. W tym okresie większym priorytetem jest prowadzenie działań mitygujących ryzyko – obsługa incydentu, a nie przeprowadzenie takiej analizy. Proponujemy kierunek aby raportowanie i informowanie o incydencie było oparte o: 1. wstępne zgłoszenie - ograniczony zakresem informacji w ciągu 24h; 2. sukcesywne uzupełnianie informacji związanych z incydentem. Wszystko to powinno być jednoznacznie opisane w stosownym rozporządzeniu będącym aktem wykonawczym do ustawy.	Wyjaśnienie. Zgłoszenie to ma charakter inicjujący obsługę incydentu i może być ono uzupełnione oraz analizowane w trakcie obsługi incydentu.
270.	art.12. ust. 1. pkt 4	Polska Organizacja Przemysłu i Handlu Naftowego	Progi uznania incydent za incydent poważny, podlegający obowiązkowi zgłoszenia (które mają zostać określone w drodze rozporządzenia przez Radę Ministrów), powinny zostać określone po dodatkowej konsultacji z przedstawicielami operatorów usług kluczowych. Progi nie powinny być ustawione zbyt nisko, aby uniknąć wprowadzania niepotrzebnych obciążeń i powinny być zgodne z ewentualnymi istniejącymi dotychczas wymogami (np. określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr	Uwaga uwzględniona częściowo. Nie sposób dołączyć operatorów usług kluczowych do podmiotów, które będą opracowywać jeden z pierwszych elementów w procesie uznania podmiotu za OUK, jakim jest określenie progów. Na tym etapie podmioty wymienione w art. 7 ust. 1 nie będą jeszcze dysponować wiedzą, kto jest uznany za OUK. Zgłoszenie ma charakter inicjujący obsługę incydentu i może być uzupełniony w trakcie obsługi incydentu.

			1227/2011 z dnia 25 października 2011 r. w sprawie integralności i przejrzystości hurtowego rynku energii). Należy również określić czy i jakie przestoje produkcyjne lub sprzedażowe podlegają zgłaszaniu (np. czy uznaje się za incydent podlegający zgłaszaniu przypadek, kiedy wyciek wody spowodował awarię serwera, co z kolei wpłynęło na poziom produkcji). W związku z poufnym charakterem informacji objętych zgłoszeniem incydentu, rekomendujemy również zapewnienie poufności zgłoszeń. Sugerujemy również uwzględnienie możliwości dokonywanie jednego zgłoszenia, które będzie wypełniało: 1) zarówno obowiązek zgłoszenia incydentu wynikający z przepisów o ochronie danych osobowych (zgłoszenie na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE), jak i 2) obowiązek zgłoszenia incydentu poważnego lub istotnego na podstawie ustawy o krajowym systemie cyberbezpieczeństwa, jeżeli w określonym przypadku dany incydent podlega obowiązkowi zgłoszenia na podstawie obu powyższy regulacji. Projekt przewiduje obowiązek zgłoszenia incydentu poważnego i incydentu istotnego nie później niż w ciągu 24 godzien od momentu jego wykrycia. Wskazany termin jest rażąco krótki i jego zachowanie w praktyce będzie niemożliwe. W zgłoszeniu incydentu operator usług kluczowych (i odpowiednio dostawca usług cyfrowych) powinien zawrzeć m.in.: szczegółowy opis wpływu incydentu na usługi kluczowe, informacje umożliwiające właściwemu CSIRT określenie transgranicznego wpływu incydentu, informacje o przyczynie i źródle incydentu, informacje o podjętych działaniach zapobiegawczych i środkach	

			naprawczych oraz inne istotne informacje, dodatkowo w przypadku incydentu, który mógł mieć wpływ w na usługi kluczowe - opis przyczyn incydentu tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne (art. 13 ust. 1 Projektu i odpowiednio art. 21 ust 1 Projektu). Samo przeanalizowanie sytuacji związanej z wykryciem incydentu, weryfikacja czy incydent faktycznie miał miejsce i przeprowadzenie kwalifikacji czy jest to incydent istotny może zająć kilkadziesiąt godzin, a dodatkowo ustalenie i przenalizowanie dodatkowych informacji, które należy zawrzeć w zgłoszeniu (art. 13 ust. 1 Projektu i odpowiednio art. 21 ust 1 Projektu) może zajac kolejne kilkadziesiąt godzin. Ponadto należy mieć na uwadze, że incydent może zostać wykryty przez inny podmiot niż operatora usług kluczowych (np. przez podmiot, który na zlecenie operatora usług kluczowych wykonuje na rzecz operatora odpowiednie usługi związane z cyberbezpieczeństwem). W takiej sytuacji konieczność przekazania odpowiedniej informacji pomiędzy operatorem a podmiotem trzecim również może zająć kilkadziesiąt godzin i doprowadzić do naruszenia wskazanego w Projekcie terminu. Mając na uwadze powyższe w normalnych okolicznościach racjonalnym terminem, jaki jest wystarczający do dokonania zgłoszenia, jest termin 72 godzin od momentu wykrycia incydentu lub uzyskania wiedzy o incydencie przez operatora usług kluczowych. Należy jednak rozważyć przypadki szczególne, w szczególności w przypadku cyberataków badanie podejrzanego wydarzenia, stwierdzenie jego zakresu i pełna ocena potencjalnych efektów wydarzenia może trwać wiele dni lub tygodni. Dlatego ustawa o krajowym systemie cyberbezpieczeństwa powinna stanowić, że zgłoszenie zostanie dokonane niezwłocznie (podobnie jak stanowi art. 14 ust. 3 i 16 ust. 3 Dyrektywy oraz projekty ustaw implementujących Dyrektywę przygotowanych w Niemczech i Holandii), a jeśli zamiarem Ustawodawcy jest	

			wskazanie konkretnego terminu – termin ten nie powinien być krótszy niż 72 godziny od momentu wykrycia incydentu lub uzyskania wiedzy o incydencie przez operatora usług kluczowych, przy czym ustawa powinna dodatkowo precyzować, że w przypadku kiedy kompletne zgłoszenie nie jest możliwe w tym terminie – zgłoszenie będzie mogło być odpowiednio uzupełnione w późniejszym terminie (w miarę możliwości operatora usług kluczowych).	
271.	art.12. ust. 1. pkt 4	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy następujące brzmienie art. 12 ust. 1 pkt 4: Art. 12. 1. Operatorzy usług kluczowych są obowiązani: … 4) zgłaszać incydent poważny niezwłocznie, nie później niż w ciągu 72 godzin od momentu wykrycia, za pośrednictwem systemu teleinformatycznego, o którym mowa w art. 42 ust. 1, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV Dostawca usługi kluczowej może nie być w stanie zebrać i przekazać wartościowych informacji w tak krótkim czasie jak 24 godziny. Proponujemy wydłużenie tego czasu do 72 godzin.	Uwaga nieuwzględniona. Termin za zgłoszenie incydentu, określony w projekcie ustawy, jest zdaniem projektodawcy wystarczający. Zgłoszenie to ma charakter inicjujący obsługę incydentu i może być uzupełniony w trakcie obsługi incydentu.
272.	art.12. ust. 1. pkt 4	Konfederacja Lewiatan	Dostawca usługi kluczowej może nie być w stanie zebrać i przekazać wartościowych informacji w tak krótkim czasie jak 24 godziny. Proponujemy wydłużenie tego czasu do 48 godzin. Proponujemy następujące brzmienie art. 12 ust. 1 pkt 4: Art. 12. 1. Operatorzy usług kluczowych są obowiązani: … 4) zgłaszać incydent poważny niezwłocznie, nie później niż w ciągu 48 godzin od momentu wykrycia, za pośrednictwem systemu teleinformatycznego, o którym mowa w art. 42 ust. 1, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV Poprosimy o doprecyzowanie na czym miała by polegać zwiększona odpowiedzialność operatora usługi kluczowej od której będzie on zwolniony, przepis jest w tym zakresie niejasny. Proponujemy doprecyzowanie zapisu.	Uwaga nieuwzględniona. Termin za zgłoszenie incydentu, określony w projekcie ustawy, jest zdaniem projektodawcy wystarczający. Zgłoszenie to ma charakter inicjujący obsługę incydentu i może być uzupełniony w trakcie obsługi incydentu.

273.	art.12. ust. 1 pkt 6	Związek Banków Polskich	W celu uniknięcia wątpliwości interpretacyjnych proponuje się wprowadzenie definicji "podatności".	Uwaga uwzględniona.
274.	art.12. ust. 1 pkt 6	A.K. (uwagi osoby prywatnej)	Brak jest jednoznacznego i nie budzącego wątpliwości określenia odpowiedzialności za obsługę incydentu poważnego – z jednej strony odpowiedzialność za obsługę incydentu spoczywa na operatorze, z drugiej strony ustawa przewiduje wprost uprawnienia CSIRT w zakresie obsługi incydentów poważanych nie wskazując przy tym zasad przejmowania przez CSIRT incydentów do obsługi oraz przyznając CSIRT pewne uprawnienia "władcze" wobec operatora (np. wezwanie za pośrednictwem organu właściwego operatora do usunięcia podatności, żądanie informacji itd.), tym samym umożliwiając CSIRT ingerencję w działalność jednostkowego operatora z pominięciem jakiejkolwiek odpowiedzialności za podejmowane wobec operatora działania. Zgodnie z art. 12 ust. 1 pkt 6 operator ma zapewnić obsługę incydentu poważnego i incydentu krytycznego we współpracy z właściwym CSIRT, w tym poinformować o usunięciu podatności, które doprowadziły lub mogły doprowadzić do poważnego incydentu. Na wniosek operatora CSIRT może zapewnić wsparcie w obsłudze lub obsługę poważnych incydentów (art. 28 ust.2), przy czym odpowiednio – zgodnie z art. 28 ust. 2 - zadaniem CSIRT jest realizacja zadań na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewnienie koordynację obsługi poważnych incydentów. Natomiast zgodnie z art. 28 ust. 5, 6 i 7 do zadań CSIRT należy obsługa lub koordynacja obsługi incydentów zgłaszanych przez wskazane w ustawie podmioty. Z tym uprawnieniem korelują uprawnienia CSIRT wskazane w art. 34, zgodnie z którym CSIRT może: "wykonywać niezbędne działania techniczne, związane z monitorowaniem zagrożeń, obsługa incydentów poważnych (…), a także dokonywać analiz (…)", "wystąpić do organu właściwego z	Wyjaśnienie. Założeniem projektodawcy było z jednej strony zapewnienie możliwości technicznej obsługi poważnych i krytycznych incydentów przez wyspecjalizowane do tego typu podmioty, czyli CSIRT poziomu krajowego. Z drugiej strony projektodawca chce zagwarantować, aby możliwe było zastosowanie władztwa o charakterze administracyjno-prawnym w przypadku działań na rzecz zapobiegania rozprzestrzeniania się incydentu. Przepisy art. 28 dotyczące zadań CSIRT zostaną przeredagowane.

			wnioskiem o wezwanie operatora, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do poważnego incydentu" oraz " może wystąpić bezpośrednio do operatora o udostępnienie informacji technicznych związanych z incydentem, które będą niezbędne do przeprowadzenia analizy zdarzenia lub obsługi incydentu". W praktyce może to oznaczać dwa ośrodki decyzyjne co do obsługi incydentu, co utrudnić może o ile nie uniemożliwi właściwą jego obsługę. Po drugie natomiast CSIRT może definiować względem operatora nieadekwatne wymagania, ewentualnie będą generować nadmierne obciążenia kosztowe.	
275.	art.12. ust. 1 pkt 6	Instytut Audytorów Wewnętrznych IIA Polska	Art. 12 ust. 1 pkt 6) zapis „o usunięciu podatności, które doprowadziły lub mogłyby doprowadzić do poważnego incydentu" - ostatni zapis proponujemy wykreślić. Nie sformułowano szczegółowej definicji podatności, która mogłaby doprowadzić do poważnego incydentu, a jednocześnie nie określono terminu na jej zgłoszenie.	Uwaga nieuwzględniona. Termin „podatność" zostanie zdefiniowany.
276.	art.12. ust. 2	Związek Banków Polskich	Nieznane są powody, dla których Ministerstwo Cyfryzacji pomija istnienie i funkcjonowanie CSIRT sektorowych. Najczęściej incydenty mają skutek oddziaływania lokalny lub sektorowy i wówczas angażowanie CSIRT MON, CSIRT NASK lub CSIRT GOV może być nadmiarowe i związane z ponoszeniem nieuzasadnionych kosztów finansowych, obciążających budżety tych CSIRT, a więc Państwo.	Wyjaśnienie. Projekt ustawy zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa CSIRT jest natomiast zarezerwowana dla zespołów poziomu krajowego.
277.	art.12. ust. 2	Związek Banków Polskich	Proponujemy: zgłoszenie, o którym mowa w ust. 1 pkt 4, nie może narażać operatora usługi kluczowej na odpowiedzialność względem podmiotu przyjmującego zgłoszenie. [3. Progi istotności skutku zakłócającego dla świadczenia usług kluczowych przyjmuje Rada Ministrów w drodze uchwały. Do uchwały mają zastosowanie przepisy o ochronie informacji niejawnych.]	Uwaga nieuwzględniona.

			Wprowadzenie tego wymogu uchwałą Rady Ministrów spowoduje, że akt ten nie będzie stosowany przez OUK - przedsiębiorców prywatnych.	
278.	art.12. ust. 2	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Poprosimy o doprecyzowanie na czym miała by polegać zwiększona odpowiedzialność operatora usługi kluczowej od której będzie on zwolniony, przepis jest w tym zakresie niejasny.	Uwaga nieuwzględniona.
279.	art. 12. ust. 3	Związek Banków Polskich	Z zastosowaniem środków łączności określonych na podstawie art. 10 ust. 3?	Uwaga nieuwzględniona.
280.	art. 12. ust. 4	Związek Banków Polskich	Poszczególne sektory posiadają lub są w budowie systemowych rozwiązań sektorowych w zakresie raportowania incydentów np. dla organów nadzorczych. Zmuszanie ich do raportowania tych samych informacji do innego systemu wiąże się z nieuzasadnionymi kosztami finansowym. Ministerstwo Cyfryzacji przed wprowadzeniem przedmiotowej propozycji winno dokonać szczegółowej analizy stanu posiadania i inwentaryzacji systemów IT i podjąć próbę ich wykorzystania. Budowa własnego systemu IT angazuje środki publiczne na pozyskanie i dystrybuję informacji, które są lub będą gromadzone w systemach IT sektorowych.	Uwaga nieuwzględniona. Projektodawca uznaje powstanie centralnego systemu za konieczne. W ramach procesu analizy interesariuszy problematyki cyberbezpieczeństwa oraz w ramach prekonsultacji projektu ustawy o krajowym systemie cyberbezpieczeństwa przeprowadzono stosowne konsultacje z organami właściwymi.
281.	art. 12. ust. 4	Instytut Logistyki i Magazynowania	Projekt przewiduje zdefiniowanie w rozporządzeniu progów liczbowych (dla wymienionych czynników) dla klasy incydent poważny. Zapis ten znajduje się w sekcji opisującej obowiązki operatorów. Należy rozszerzyć zakres definicji dla wszystkich klas incydentów (definicja nie tylko progów ale ogólnie kryteriów) na drodze rozporządzenia. Ten artykuł powinien poprzedzać opisy obowiązków uczestników krajowego systemu cyberbezpieczeństwa.	Wyjaśnienie. Progi z art. 12 ust. 4 dotyczą tylko incydentów, które wystąpią u operatorów usług kluczowych.

282.	art.12. ust. 2 [błędnie jako art.12. ust. 6]	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy zmianę zapisu. Jest: „Zgłoszenie, o którym mowa w ust. 1 pkt 4, nie może narażać operatora usługi kluczowej na zwiększoną odpowiedzialność” Powinno być: „Zgłoszenie, o którym mowa w ust. 1 pkt 4, nie naraża operatora usługi kluczowej na zwiększoną odpowiedzialność”	Uwaga nieuwzględniona.
283.	art. 13	Pracodawcy RP	Obowiązek zgłoszenia „incydentu, który mógł mieć wpływ na usługi kluczowe” (ust. 1 pkt 6) jest określony zbyt szeroko. Potencjalnie może dotyczyć to każdego zdarzenia. Stanowi to zbytnie obciążenie podmiotów obowiązanych, a jednocześnie nie realizuje celu ustawy. Może też prowadzić do przeładowania CSIRT-ów niepotrzebnymi zgłoszeniami. Tym samym wnioskujemy o usunięcie tego obowiązku.	Uwaga nieuwzględniona.
284.	art. 13 ust. 1 pkt 4) lit. od b, c f)	Instytut Audytorów Wewnętrznych IIA Polska	Art. 13 ust. 1 pkt 4) lit. od b, c f) b) liczbę użytkowników, na których incydent poważny miał wpływ, - prosimy o doprecyzowanie zapisu liczby użytkowników, w szczególności dla organizacji świadczącej usługi B2B. c) czas trwania incydentu poważnego, - wskazany zapis nie ma odzwierciedlenia w praktyce zarządzania incydentami. Jeśli incydent się nie zakończył w ciągu 24 godzin - proponujemy dodać zapis „o ile proces zarządzania danym incydentem się nie zakończył"; f) przyczynę zaistnienia incydentu poważnego oraz sposób jego przebiegu i skutki jego oddziaływania na systemy informacyjne i usługi kluczowe; - wskazany zapis nie ma odzwierciedlenia w praktyce zarządzania incydentami, w szczególności, aby w ciągu 24 godzin wszystkie wymagane informacje przekazać. Należy podkreślić, iż często zdarza się, ze proces analizy incydentu trwa nawet wiele tygodni - proponujemy dodać zapis „o ile proces zarządzania danym incydentem się nie zakończył".	Uwaga nieuwzględniona.

285.	art. 13 ust. 1 pkt 4 lit. f oraz pkt 7	Polska Izba Informatyki i Telekomunikacji	Zgodnie z projektowanym art. 13 ust. 1 pkt 6 na operatorze spoczywa obowiązek zgłaszania „incydentu, który mógł mieć wpływ na usługi kluczowe", czyli potencjalnie każdego incydentu. W praktyce może to stanowić znaczące rozszerzenie spoczywającego na operatorze obowiązku notyfikacyjnego. W związku z tym rekomendujemy wykreślenie zapisu. Ponadto sygnalizujemy, że zakresy obowiązków informacyjnych zdają się nakładać. Zgodnie z projektowanym pkt 4 lit. f należy wskazać m.in. przyczynę zaistnienia incydentu, a zgodnie z ust. 7 mamy podać przyczynę i źródło incydentu, jeżeli są one znane w chwili zgłoszenia. W naszej ocenie należy pozostawić obowiązek określony w pkt. 7.	Uwaga nieuwzględniona.
286.	art. 13 ust. 1 pkt 4 lit. f oraz pkt 7	Konfederacja Lewiatan	Zgodnie z projektowanym art. 13 ust. 1 pkt 6 na operatorze spoczywa obowiązek zgłaszania „incydentu, który mógł mieć wpływ na usługi kluczowe", czyli potencjalnie każdego incydentu. W praktyce może to stanowić znaczące rozszerzenie spoczywającego na operatorze obowiązku notyfikacyjnego. W związku z tym rekomendujemy wykreślenie zapisu. Ponadto sygnalizujemy, że zakresy obowiązków informacyjnych zdają się nakładać. Zgodnie z projektowanym pkt 4 lit. f należy wskazać m.in. przyczynę zaistnienia incydentu, a zgodnie z ust. 7 mamy podać przyczynę i źródło incydentu, jeżeli są one znane w chwili zgłoszenia. W naszej ocenie należy pozostawić obowiązek określony w pkt. 7. Czas 24 godzin na opisanie przyczyny, przebiegu, i skutków incydentu jest niewytaczający. Prosimy o zmianę w art. 12 ust. 1 pkt 4 na 48 godzin. Nowe brzmienie ma związek z zaproponowaną powyżej zmiana brzmienia art. 12 ust. 1 pkt 4.	Uwaga nieuwzględniona.
287.	art. 13 ust. 1	A.K. (uwagi osoby prywatnej)	Obowiązek zgłaszania incydentów poważnych (art. 13 ust. 4 lit. f i ust. 7) - Art. 13 ust. 6 - w praktyce stanowić może rozszerzenie spoczywającego na operatorze obowiązku notyfikacyjnego; zgodnie	Uwaga nieuwzględniona.

	pkt 4f i pkt 6 i 7		z powołanym zapisem na operatorze spoczywa obowiązek zgłaszania “incydentu, który mógł mieć wpływ na usługi kluczowe”, czyli potencjalnie każdego incydentu - potrzebne wykreślenie tego zapisu. Brak konsekwencji: w ust. 4 lit. f mamy wskazać m.in. przyczynę zaistnienia incydentu, a zgodnie z ust. 7 mamy podać przyczynę i źródło incydentu, jeżeli są one znane w chwili zgłoszenia – zasadny jest zapis w ust. 7.	
288.	art. 13 ust. 1 pkt 4 lit. f	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Ma związek z zaproponowaną powyżej zmiana brzmienia art. 12 ust. 1 pkt 4. Czas 24 godzin na opisanie przyczyny, przebiegu, i skutków incydentu jest niewytaczający. Prosimy o zmianę w art. 12 ust. 1 pkt 4 na 72 godziny.	Uwaga nieuwzględniona. Zgłoszenie, o którym mowa w art. 13 będzie zawierało dane znane operatorowi w momencie zgłaszania. Może zawierać szacunkowe liczby, aktualne na moment zgłoszenia. Zgłoszenie to ma charakter inicjujący obsługę incydentu i może być uzupełniony w trakcie obsługi incydentu.
289.	art. 13. ust. 1 pkt. 6	Izba Gospodarcza Gazownictwa	W momencie zgłaszania incydentu istnieje duże prawdopodobieństwo, że nie będzie jeszcze możliwe określenie sposobu jego przebiegu oraz opisu przyczyn. Propozycja: w przypadku incydentu, który mógł mieć wpływ na usługi kluczowe – opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne, jeśli są znane w chwili zgłaszania;	Wyjaśnienie. Zgłoszenie, o którym mowa w art. 13 będzie zawierało dane znane operatorowi w momencie zgłaszania. Może zawierać szacunkowe liczby, aktualne na moment zgłoszenia. Zgłoszenie to ma charakter inicjujący obsługę incydentu i może być uzupełniony w trakcie obsługi incydentu.
290.	art. 13. ust. 1 pkt 6	Instytut Audytorów Wewnętrznych IIA Polska	Art. 13 ust. 1 pkt 6) - wskazany zapis nie ma odzwierciedlenia w praktyce zarządzania incydentami, w szczególności, aby w ciągu 24 godzin wszystkie wymagane informacje przekazać. Należy podkreślić, iż często zdarza się, że proces analizy incydentu trwa nawet wiele tygodni - proponujemy dodać zapis „o ile proces zarządzania danym incydentem się nie zakończył";	Wyjaśnienie. Zgłoszenie, o którym mowa w art. 13 będzie zawierało dane znane operatorowi w momencie zgłaszania. Może zawierać szacunkowe liczby, aktualne na moment zgłoszenia. Zgłoszenie to ma charakter

				inicjujący obsługę incydentu i może być uzupełniony w trakcie obsługi incydentu.
291.	art. 13. ust. 1 pkt 8 i 9	Instytut Audytorów Wewnętrznych IIA Polska	Art. 13 ust. 1 pkt 8) i 9) - wskazany zapis nie ma odzwierciedlenia w praktyce zarządzania incydentami, w szczególności, aby w ciągu 24 godzin wszystkie wymagane informacje przekazać. Należy podkreślić, iż często zdarza się, że proces analizy incydentu trwa nawet wiele tygodni - proponujemy dodać zapis „o ile proces zarządzania danym incydentem się nie zakończył";	Wyjaśnienie. Zgłoszenie, o którym mowa w art. 13 będzie zawierało dane znane operatorowi w momencie zgłaszania. Może zawierać szacunkowe liczby, aktualne na moment zgłoszenia. Zgłoszenie to ma charakter inicjujący obsługę incydentu i może być uzupełniony w trakcie obsługi incydentu.
292.	art. 13. ust. 2	Związek Banków Polskich	Dokonując zgłoszenia operatorzy usług kluczowych są uprawnieni do przekazywania informacji stanowiących tajemnice prawnie chronione. W zgłoszeniu operatorzy usług kluczowych oznaczają informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa. Niezależnie od powyższej zmiany – z punktu widzenia sektora bankowego koniecznym jest wprowadzenie zmian w ustawach: - ustawa prawo bankowe, - ustawa o obrocie instrumentami finansowymi, - ustawa o działalności ubezpieczeniowej i reasekuracyjnej, które stanowić będą podstawę ustawową do ujawnienia organom przyjmującym zgłoszenia oraz wykonującym audyty u operatorów usług kluczowych – danych objętych tajemnicą prawnie chronioną.	Wyjaśnienie. Przepisy zostaną przeredagowane tak, aby wyłączyć tajemnice prawnie chronione.
293.	art. 13. ust. 2	Krajowy Depozyt Papierów Wartościowych S.A.	W art. 13 ust. 2 mowa jest o oznaczaniu informacji stanowiących tajemnice prawnie chronione w zgłoszeniach incydentów dokonywanych przez operatorów usług kluczowych, a tym samym zakłada się, że w treści zgłoszeń incydentów informacje prawnie chronione mogą się znajdować. W kontekście operatorów usług kluczowych przetwarzających informacje objęte tajemnicą zawodową w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi należałoby zatem zweryfikować, czy	Wyjaśnienie. Przepisy zostaną przeredagowane tak, aby wyłączyć tajemnice prawnie chronione.

			nałożenie na nich obowiązku zgłaszania incydentów do właściwego CSIRT nie wymaga zmiany w przepisach wskazanej ustawy (art. 147-153). W naszym przekonaniu wymagałoby rozszerzenia katalogu przypadków dozwolonego przekazania informacji stanowiącej taką tajemnicę, zawartego w art. 150 ust. 1 ustawy o obrocie instrumentami finansowymi, o przypadki zgłaszania przez operatora usług kluczowych incydentu poważnego zgodnie z art. 12 ust. 1 pkt 4 projektowanej ustawy.	
294.	art. 13 ust. 2	Pracodawcy RP	W zgłoszeniu operatorzy usług kluczowych oznaczają informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa. 2.Dokonując zgłoszenia operatorzy usług kluczowych są uprawnieni do przekazywania informacji stanowiących tajemnice prawnie chronione. W zgłoszeniu operatorzy usług kluczowych oznaczają informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa. Niezależnie od powyższej zmiany – z punktu widzenia sektora bankowego koniecznym jest wprowadzenie zmian w ustawach: - ustawa prawo bankowe, - ustawa o obrocie instrumentami finansowymi, - ustawa o działalności ubezpieczeniowej i reasekuracyjnej, które stanowić będą podstawę ustawową do ujawnienia organom przyjmującym zgłoszenia oraz wykonującym audyty u operatorów usług kluczowych – danych objętych tajemnicą prawnie chronioną.	Wyjaśnienie. Przepisy zostaną przeredagowane tak, aby wyłączyć tajemnice prawnie chronione.
295.	art. 14	Pracodawcy RP	Art. 14 – Nie jest potrzebne wskazanie możliwości fakultatywnego przekazywania pewnych informacji do CSIRT, szczególnie, że pozostałe przepisy przywidują już szczegółową i obligatoryjną sprawozdawczość. Wymiana informacji bieżących i ogólnych może następować w ramach współpracy poszczególnych jednostek bez szczególnego przepisu. Wnosimy o usunięcie przepisu z projektu.	Uwaga nieuwzględniona. Zdaniem projektodawcy obecny zapis jest zasadny.

296.	art. 14	Polska Izba Informatyki i Telekomunikacji	Z uwagi na brak szczególnego uzasadnienia, brak określenia sposobu wykorzystywania danych przez CSIRT, a także fakultatywny charakter projektowanego art. 14 rekomendujemy usuniecie zapisu. Ponadto zasadne jest wprowadzenie obowiązku wymiany informacji pomiędzy poszczególnymi CSIRT poziomu krajowego, w sytuacji zgłoszenie incydentu przez operatora usługi kluczowej tak aby uniknąć sytuacji, w której należy raportować dany incydent do wielu CSIRT a informacja znajduje się już po stronie administracji.	Uwaga nieuwzględniona. Zdaniem projektodawcy obecny zapis jest zasadny.
297.	art. 14	Konfederacja Lewiatan	Z uwagi na brak szczególnego uzasadnienia, brak określenia sposobu wykorzystywania danych przez CSIRT, a także fakultatywny charakter projektowanego art. 14 rekomendujemy usuniecie zapisu.	Uwaga nieuwzględniona. Zdaniem projektodawcy obecny zapis jest zasadny.
298.	art. 14	A.K. (uwagi osoby prywatnej)	Przekazywanie przez operatorów usług kluczowych do właściwego CSIRT informacji o zagrożeniach, szacowaniach ryzyka, podatnościach, wykorzystywanych technologiach (art. 14) - nie wskazano ani celu przekazania tych informacji, ani sposobu ich wykorzystywania przez CSIRT - konieczne usunięcie zapisu.	Uwaga nieuwzględniona. Zdaniem projektodawcy obecny zapis jest zasadny. Ze względu na fakt, że przekazywanie informacji dot. szacowania ryzyka jest dobrowolne, zakres przekazywanych informacji zależy od typu podmiotu przekazującego.
299.	art. 14 ust. 1 pkt 5	Polska Izba Informatyki i Telekomunikacji	W art. 14 ust. 1 pkt 5 należy doprecyzować poprzez dodanie na końcu zdania zapisu: „związanych z cyberbezpieczeństwem”	Uwaga częściowo uwzględniona. Przepis zostanie przeformułowany poprzez wskazanie, że na podstawie przekazanych informacji o wykorzystywanych technologiach informatycznych CSIRT może przekazać do podmiotu informacje o podatnościach i sposobie ich usunięcia w technologiach wykorzystywanych przez dany podmiot.

300.	art. 14 ust. 1 pkt 5	Konfederacja Lewiatan	W art. 14 ust. 1 pkt 5 należy doprecyzować poprzez dodanie na końcu zdania zapisu: „związanych z cyberbezpieczeństwem”.	Uwaga częściowo uwzględniona. Przepis zostanie przeformułowany poprzez wskazanie, że na podstawie przekazanych informacji o wykorzystywanych technologiach informatycznych CSIRT może przekazać do podmiotu informacje o podatnościach i sposobie ich usunięcia w technologiach wykorzystywanych przez dany podmiot.
301.	art. 15 ust. 1	A.K. (uwagi osoby prywatnej)	Obowiązek powołania osoby odpowiedzialnej ds. cyberbezpieczeństwa świadczonych usług kluczowych (art. 15 ust. 1 Ustawy) – ustawa ogranicza się wyłącznie do wskazania obowiązku wyznaczenia ww. osoby nie precyzując wymagań, roli oraz odpowiedzialności	Wyjaśnienie. Przepis zostanie zmieniony. OUK będzie wyznaczał osobę odpowiedzialną za kontakty z CSIRT oraz innymi podmiotami krajowego systemu cyberbezpieczeństwa.
302.	art. 15 ust. 1 pkt 1	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu Należy zdefiniować zakres obowiązków i odpowiedzialności osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług kluczowych. Nie określono czasu na wyznaczenie osoby odpowiedzialnej za cyberbezpieczeństwo świadczonych usług kluczowych. Określono natomiast sankcję finansową za niewyznaczenie takiej osoby	Wyjaśnienie. Przepis zostanie zmieniony. OUK będzie wyznaczał osobę odpowiedzialną za kontakty z CSIRT oraz innymi podmiotami krajowego systemu cyberbezpieczeństwa.
303.	art. 15 ust. 1 pkt 1	Polska Organizacja Przemysłu i Handlu Naftowego	Projekt przewiduje obowiązek wyznaczenia przez operatora usług kluczowych osoby odpowiedzialnej za cyberbezpieczeństwo (art. 15 ust. 1 pkt. 1 Projektu). Przy czym Projekt nie precyzuje: 1) jakie będę obowiązki wyznaczonej przez operatora osoby, 2) czy ta osoba ma być wybrana spośród pracowników operatora czy ma to być podmiot zewnętrzny, 3) czy taki obowiązek istnieje nawet w przypadku zawarcia umowy z odpowiednim podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa.	Wyjaśnienie. Przepis zostanie zmieniony. OUK będzie wyznaczał osobę odpowiedzialną za kontakty z CSIRT oraz innymi podmiotami krajowego systemu cyberbezpieczeństwa.

			Projekt powinien dopuszczać możliwość wyznaczenia osoby zatrudnionej przez operatora jak i spoza grona pracowników, przy czym może to być osoba wyznaczona również przez innych operatorów lub osoba nie posiadająca miejsca zamieszkania w Polsce ani obywatelstwa polskiego. Takie rozwiązanie umożliwi spółkom należącym do międzynarodowej grupy kapitałowej, operującym na tych samych systemach informatycznych i posiadającym wspólny system zarządzania cyberbezpieczeństwem do wyznaczania wspólnego „przedstawiciela" tj. osoby odpowiedzialnej za cyberbezpieczeństwo we wszystkich spółkach. Dodatkowo Projekt powinien stanowić, że w przypadku zawarcia umowy z odpowiednim podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa (na podstawie art. 16 Projektu) i nałożeniem na ten podmiot odpowiedzialności za cyberbezpieczeństwo wyznaczenie osoby odpowiedzialnej za cyberbezpieczeństwo nie jest konieczne.	
304.	art. 15 ust. 1 pkt 1	Polska Izba Informatyki i Telekomunikacji	Zasadne jest doprecyzowanie zadań, roli i odpowiedzialności osoby wymienionej w Art. 15 ust. 1 pkt. 1).	Wyjaśnienie. Przepis zostanie zmieniony. OUK będzie wyznaczał osobę odpowiedzialną za kontakty z CSIRT oraz innymi podmiotami krajowego systemu cyberbezpieczeństwa.
305.	Art. 15 ust. 1 pkt 2	Pracodawcy RP	W naszej ocenie nie jest uzasadnione przeniesienie na operatorów usług kluczowych obowiązków informacyjnych i edukacyjnych w zakresie cyberbezpieczeństwa. Kompleksową wiedzę, w tym przekrojowe informacje pochodzące ze sprawozdawczości będą posiadały CSIRT-y oraz organy koordynujące kwestie cyberbezpieczeństwa na poziomie krajowym. To właśnie centralne, publiczne organy powinny być odpowiedzialne za zwiększenie świadomości zagrożeń w sieci oraz promowanie właściwych działań, np. w formie kampanii informacyjnych, przygotowania publikacji,	Wyjaśnienie. W ocenie projektodawcy zapis art. 15 ust. 1 pkt 2 wydaje się być właściwym. Obowiązki nałożone na OUK mają wymiar podstawowy w kwestii informowania i dostępu do wiedzy użytkowników usługi kluczowej. OUK nie wykonują zadań o szerszym charakterze, jakie nałożone zostały w projekcie

			materiałów czy kodeksów dobrych praktyk. Podmioty świadczące usługi kluczowe mogą jedynie wspierająco uzupełniać te działania w ramach szeroko rozumianej dbałości o interesy swoich klientów. Nie mogą być jednak w żaden sposób odpowiedzialne, ani rozliczane za prowadzone w tym zakresie dodatkowe działania.	ustawy na CSIRT, na podstawie przepisów określonych w art. 28 ust. 3 pkt 3 i 4.
306.	art. 15 ust. 1 pkt 2	Polska Organizacja Przemysłu i Handlu Naftowego	Projekt nakłada na operatora usługi kluczowej obowiązek zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczenia się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługa kluczową (art. 15 ust.1 pkt 2) Projektu). Przy czym Projekt nie precyzuje: 1) kim jest użytkownik usługi kluczowej i jakie są kryteria ustalenia, że dany podmiot jest użytkownikiem usługi kluczowej (czy np. chodzi o podmiot, który zawarł z operatorem usługi kluczowej umowę, której przedmiotem jest usługa kluczowa czy jakikolwiek podmiot, który jest odbiorcą usługi kluczowej, niezależnie od tego czy zawarł z operatorem umowę), 2) kiedy ten obowiązek ma być zrealizowany (czy np. przy zawieraniu umowy z użytkownikiem usługi kluczowej, czy po wejściu w życie ustawy operator usług kluczowych będzie zobowiązany zapewnić dostęp do wiedzy wszystkim dotychczasowym użytkownikom), 3) w jaki sposób realizacja tego obowiązku ma nastąpić, w szczególności w jaki sposób dostęp do wiedzy mam być zapewniony użytkownikowi usługi kluczowej, jakie informacje mają zostać mu przekazane (użyte w Projekcie sformułowanie „pozwalające na zrozumienie" jest subiektywne i trudno obiektywnie ocenić jakie informacje pozwolą na zrozumienie określonych faktów określonej osobie). POPiHN proponuje, aby ze względu na liczne wątpliwości dotyczące powyższego obowiązku i brak możliwości jego uniwersalnego	Wyjaśnienie. W ocenie projektodawcy zapis art. 15 ust. 1 pkt 2 wydaje się być właściwym. Obowiązki nałożone na OUK mają wymiar podstawowy w kwestii informowania i dostępu do wiedzy użytkowników usługi kluczowej. OUK nie wykonują zadań o szerszym charakterze, jakie nałożone zostały w projekcie ustawy na CSIRT, na podstawie przepisów określonych w art. 28 ust. 3. Ustawa tworzy wymagania w zakresie podmiotowym dotyczące sektorów wskazanych w załączniku. Jednocześnie ustawa wzorem dyrektywy zawiera przepisy dotyczące obowiązków informacyjnych względem użytkowników usług kluczowych i cyfrowych (usługobiorców).

			doprecyzowania (tj. na poziomie zrozumiałym i umożliwiającym realizację tego obowiązku przez operatorów usług kluczowych we wszystkich sektorach) Ustawodawca zrezygnował z powyższej regulacji. Warto przy tym podkreślić, że Dyrektywa nie wymaga nałożenia na operatorów usług kluczowych takiego obowiązku, co więcej, propozycje rozwiązań przyjęte w innych krajach implementujących Dyrektywę nie przewidują analogicznego obowiązku zapewnienie dostępu do wiedzy (w szczególności brak jest analogicznych obowiązków w propozycji Wielkiej Brytanii, Niemiec i Holandii).	
307.	art. 15. ust.1 pkt. 2	Instytut Kościuszki	Zgodnie z art. 15 ust. 1 pkt 2 operatorzy usług kluczowych zobowiązani są do zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową. Pominąwszy nieprecyzyjny charakter przepisu, warto wskazać, iż jest on również pozbawiony sankcji (art. 57), co w znacznym stopniu może przyczynić się do braku realizacji dyspozycji ustanowionej nim normy. Operatorzy usług kluczowych, jako podmioty realizujące zadania o podstawowym znaczeniu dla funkcjonowania współczesnego społeczeństwa i gospodarki, powinni być zobowiązani do uczestnictwa w budowaniu świadomości użytkowników w obszarze cyberbezpieczeństwa. Warto w tym kontekście rozważyć nałożenie obowiązku przesyłania okresowej informacji (nie tylko „zapewniania dostępu do wiedzy") dotyczącej aktualnych zagrożeń cybernetycznych mogących wiązać się z korzystaniem z danej usługi kluczowej (np. na zasadzie aktualizacji polityki prywatności udostępnianych użytkownikom przez platformy cyfrowe lub działań edukacyjnych). Będzie to też miało korzystny wpływ na cyberbezpieczeństwo operatorów usług kluczowych, którzy mogą dzięki temu uzyskiwać bieżącą informację od użytkowników na	Wyjaśnienie. W ocenie projektodawcy zapis art. 15 ust. 1 pkt 2 wydaje się być właściwym. Obowiązki nałożone na OUK mają wymiar podstawowy w kwestii informowania i dostępu do wiedzy użytkowników usługi kluczowej. OUK nie wykonują zadań o szerszym charakterze, jakie nałożone zostały w projekcie ustawy na CSIRT, na podstawie przepisów określonych w art. 28 ust. 3.

			temat wykrytych podatności i incydentów (zidentyfikowanych dzięki ostrzeżeniom operatorów). Warto również rozważyć, aby obowiązek ten dotyczył także innych podmiotów krajowego systemu cyberbezpieczeństwa, np. przedsiębiorstw telekomunikacyjnych (art. 4 pkt 5), organów administracji publicznej (art. 4 pkt 6), jednostek samorządu terytorialnego (art. 4 pkt 12).	
308.	art. 15. ust.1 pkt. 2	Izba Gospodarcza Gazownictwa	Dodatkowo zapis może wiązać się z koniecznością ujawnienia mechanizmów zabezpieczających usługę kluczową bądź wskazywać na zastosowane rozwiązania techniczno-technologiczne lub ich braki. Wątpliwości budzi tutaj użyte słowo „skutecznych". Nie istnieją skuteczne sposoby zabezpieczenia się przed zagrożeniami, dlatego sugeruje się wskazanie sposobów zabezpieczeń przez właściwe organy ds. cyberbezpieczeństwa. Propozycja zapisu: Art. 15. 1. Operatorzy usług kluczowych są obowiązani do: 2) zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów wskazanych przez właściwy organ zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.	Uwaga nieuwzględniona. Skuteczny ma być rozumiane jako najlepsze praktyki wskazywane przykładowo w obszarze normatywnym.
309.	art. 15. ust.1 pkt. 2	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy następujące brzmienie art. 15 ust. 1 pkt 2: Art. 15. 1. Operatorzy usług kluczowych są obowiązani do: … 2) zapewnienia użytkownikowi usługi kluczowej, o ile użytkownik ma wpływ na ciągłość świadczonej usługi kluczowej, dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową. Ustęp ten może wnieść korzyści np. w sektorze bankowości. Jednakże w sektorze energii elektrycznej koszty zapewnienie dostępu do wiedzy może być wysokie a korzyści niewielkie gdyż	Uwaga nieuwzględniona. Oczywiście w dużej mierze zależy to od oferowanej usługi kluczowej i architektury systemu informacyjnego służącego do jej świadczenia. Należy przypuszczać, że wraz z informatyzacją sektora usług, wzorem bankowości elektronicznej użytkownik będzie miał stale rosnący wpływ na usługę kluczową, szczególnie wówczas gdy będzie bezpośrednia interakcja z klientem masowym.

			użytkownicy nie są wstanie przeciwdziałać atakom na infrastrukturę elektroenergetyczną. Alternatywnie artykuł powinien być szeroko doprecyzowany lub całkowicie usunięty. Zakres informacji, sposób realizacji ani cel nie jest wystarczająco precyzyjny aby możliwe były konkretne kroki do podjęcia.	
310.	art. 15. ust.1 pkt. 2	Konfederacja Lewiatan	Ustęp ten może wnieść korzyści np. w sektorze bankowości. Jednakże w sektorze energii elektrycznej koszty zapewnienia dostępu do wiedzy mogą być wysokie, a korzyści niewielkie gdyż użytkownicy nie są wstanie przeciwdziałać atakom na infrastrukturę elektroenergetyczną. Proponujemy następujące brzmienie art. 15 ust. 1 pkt 2: Art. 15. 1. Operatorzy usług kluczowych są obowiązaniu do: … 2) zapewnienia użytkownikowi usługi kluczowej, o ile użytkownik ma wpływ na ciągłość świadczonej usługi kluczowej, dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową.	Uwaga nieuwzględniona. Oczywiście w dużej mierze zależy to od oferowanej usługi kluczowej i architektury systemu informacyjnego służącego do jej świadczenia. Należy przypuszczać, że wraz z informatyzacją sektora usług, wzorem bankowości elektronicznej użytkownik będzie miał stale rosnący wpływ na usługę kluczową, szczególnie wówczas gdy będzie bezpośrednia interakcja z klientem masowym.
311.	art. 15. ust.1 pkt. 2 [w uwagach błędnie oznaczone jako art. 15 ust. 2]	A.K. (uwagi osoby prywatnej)	Obowiązek zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowania skutecznych sposobów zabezpieczania (art. 15 ust. 2) - Obowiązek prowadzenia działalności edukacyjnej powinien spoczywać przede wszystkim przez CSIRT oraz przez organy właściwe czy koordynujące kwestie cyberbezpieczeństwa na poziomie krajowym. Działalność operatorów usług kluczowych w tym zakresie powinna mieć wyłącznie subsydiarny charakter. wiedza o zagrożeniach cyberbezpieczeństwa powinna obejmować pełne spektrum zagrożeń i zabezpieczeń oraz dawać użytkownikowi całościowy obraz, a nie traktować temat wyrywkowo ograniczając się do pojedynczych usług. Uważamy, że to zadanie powinno być to realizowane przez wskazane w Ustawie CSiRT'y lub MC, które	Wyjaśnienie. W ocenie projektodawcy zapis art. 15 ust. 1 pkt 2 wydaje się być właściwym. Obowiązki nałożone na OUK mają wymiar podstawowy w kwestii informowania i dostępu do wiedzy użytkowników usługi kluczowej. OUK nie wykonują zadań o szerszym charakterze, jakie nałożone zostały w projekcie ustawy na CSIRT, na podstawie przepisów określonych w art. 28 ust. 3 pkt 3 i 4, oraz na ministra właściwego do spraw cyfryzacji, który na podstawie zapisów art. 41 pkt .7 projektowanej ustawy, ma za zadanie prowadzenie działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii

			dysponują wiedzą kompleksową na temat zagrożeń w cyberprzestrzeni i posiadają dane statystyczne. Zauważyć można przy tym wyraźny brak proporcji między zakresem informacji pozyskiwanym przez CSIRT oraz organy właściwe (o incydentach, ale również o stosowanych zabezpieczeniach stosowanych przez operatorów, itd.) a ich praktycznym wykorzystaniem przez te organy (np. właśnie w działalności edukacyjnej).	i szkoleń na rzecz poszerzania wiedzy i podnoszenia świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników.
312.	art. 15 ust. 2	Instytut Kościuszki	Zgodnie z literalną wykładnią przepisów ustawy, jedynie operatorzy usług kluczowych mogą powierzać realizację poszczególnych zadań, podmiotom świadczącym usługi z zakresu cyberbezpieczeństwa. Takiej możliwości nie przewidują regulacje dotyczące dostawców usług cyfrowych, jak i podmiotów publicznych. Takie ograniczenie zdaje się nieuzasadnione. Przy okazji warto nadmienić, że Wskazane w art. 4 pkt 15 projektu ustawy podmioty świadczące usługi z zakresu cyberbezpieczeństwa powinny być poddane certyfikacji ABW lub SKW (co najmniej mechanizm analogiczny do nadania certyfikatu bezpieczeństwa teleinformatycznego - zgodnie z art. 50 ust. 3 ustawy o ochronie informacji niejawnych). Z uwagi na zakres zadań w obszarze, który może być przez nie realizowany (art. 15 ust 2 w związku z art. 10 ust. 2, art. 11 ust. 1, art. 12 ust. 1 oraz art. 14, art. 23), jak i zadania z zakresu współpracy z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań (art. 35 ust. 5) oraz dostęp do systemu teleinformatycznego, o którym mowa w art. 42 ust. 1 pkt 1), należy rozważyć, czy ustawa nie powinna w sposób literalny odnosić się do wymogu certyfikacji podmiotów świadczących usługi z zakresu cyberbezpieczeństwa. W tym aspekcie, nadzór ministra właściwego ds. informatyzacji przewidziany w art. 47 ust. 1 pkt. 1 projektu ustawy, należy uznać za model niewystarczający zarówno w kontekście ograniczonych kryteriów kontroli (zawężonych do czynników wskazanych w art. 15 ust. 2), następczego charakteru realizacji przedmiotowej	Uwaga nieuwzględniona. Różnica wynika z odrębnego charakteru OUK w porównaniu z DUC lub podmiotem publicznym wedle zapisów projektu ustawy.

			kompetencji, jak i ograniczonego zakresu czynności kontrolnych (zgodnie z procedurą kontroli działalności gospodarczej przedsiębiorcy opisaną w ustawie o swobodzie działalności gospodarczej - art. 48 ust. 1 w związku z art. 47 ust. 1 pkt 1 projektu ustawy). Potrzeba literalnego ustanowienia mechanizmu certyfikacji podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, które wchodzą w skład krajowego systemu cyberbezpieczeństwa wynika zarówno z okoliczności faktycznych, dokumentów programowych Ministerstwa Cyfryzacji oraz generalnego postulatu jasności prawa (kompleksowości tekstu prawnego). Po pierwsze, z uwagi na podstawowe interesy bezpieczeństwa państwa, certyfikacja ABW zminimalizuje ryzyko wykorzystywania w ramach ochrony teleinformatycznej operatorów usług kluczowych (oraz pozostałych wskazanych powyżej sferach) rozwiązań, które przyczyniałyby się do obniżenia poziomu cyberbezpieczeństwa poprzez m.in. użytkowanie oprogramowania zawierającego celowo umieszczone luki (m.in. backdoor). Postulat udziału ABW w procesie weryfikacji producentów i usługodawców rozwiązań w ramach sieci teleinformatycznych organów administracji państwowej, podnoszony był również w Założeniach strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej z 2016 roku. Literalne odniesienie czy to do wymogu certyfikacji bezpieczeństwa teleinformatycznego ABW, pozwoli także zniwelować ewentualną niejasność co do stosowania właściwych przepisów w kontekście czynności realizowanych przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa, które wchodzą w skład krajowego systemu cyberbezpieczeństwa. Umożliwi to zdjęcie z operatorów usług kluczowych obowiązku każdorazowej wykładni przepisów dotyczących informacji niejawnych w kontekście realizacji poszczególnych zadań i obowiązków przewidzianych w projekcie ustawy przy pomocy podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, co z kolei będzie miało pozytywny wpływ na	

			stopień faktycznej ich realizacji – a zatem odporności krajowego systemu cyberbezpieczeństwa.	
313.	art. 15 ust. 2	Krajowy Depozyt Papierów Wartościowych S.A.	W art. 15 ust. 2, dotyczącym tworzenia wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawierania umów z podmiotami świadczącym usługi z zakresu cyberbezpieczeństwa, dostrzegamy potrzebę uwzględnienia kwestii wynikających z organizacji procesów zarządzania infrastrukturą informatyczną oraz bezpieczeństwem teleinformatycznym w grupach kapitałowych, w których jeden z podmiotów świadczy usługi w tym zakresie dla innych podmiotów z grupy. W szczególności może też wystąpić sytuacja, w której więcej niż jeden podmiot z grupy będzie uznany za operatora usługi kluczowej lub w której jeden podmiot w grupie będzie operatorem usługi kluczowej, natomiast inny podmiot będzie operatorem infrastruktury krytycznej. Proponujemy, aby w takich sytuacjach dopuszczalne było tworzenie struktur odpowiedzialnych za cyberbezpieczeństwo dla całej grupy kapitałowej, co do zasady osadzonych w tym podmiocie, który zajmuje się zarządzaniem infrastrukturą informatyczną oraz bezpieczeństwem teleinformatycznym na rzecz pozostałych spółek grupy. W związku z powyższym proponujemy dodanie w art. 15 ust. 2a w brzmieniu: „2a. W przypadku operatora usług kluczowych wchodzącego w skład grupy kapitałowej w rozumieniu ustawy o rachunkowości, wewnętrzna struktura odpowiedzialna za cyberbiezpieczeństwo, o której mowa w ust.2, może zostać utworzona w innej jednostce powiązanej, jeżeli świadczy ona w tym zakresie usługi na rzecz pozostałych jednostek tworzących tę grupę kapitałową.”	Uwaga nieuwzględniona. W opinii projektodawcy obecne przepisy pozwalają grupom kapitałowym korzystać z jednego podmiotu świadczącego usługi z zakresu cyberbezpieczeństwa.
314.	art. 15 ust. 2	Polska Organizacja Przemysłu i	Art. 15 ust. 2 Projektu przewiduje obowiązek powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeńswto lub zawarcia umowy z podmiotami świadczącymi usługi z zakresu	Uwaga uwzględniona/nieuwzględniona.

		Handlu Naftowego	cyberbezpieczeństwa (w drugim przypadku należy poinformować odpowiedni CSIRT o podmiocie, z którym umowa zastała zawarta) w celu realizacji obowiązków wynikających z Projektu. Przy czym, zarówno w/w struktury jak i podmiot, z którym odpowiednia umowa ma być zawarta muszą spełniać określone wymagania wskazane w art. 15 ust. 2 Projektu, których sposób spełnienia zostanie doprecyzowany w rozporządzeniu Ministra właściwego ds. informatyzacji. Powyższy obowiązek wymaga doprecyzowania, w szczególności poprzez określenie: 1) jakich formalności należy dopełnić aby można było uznać, że struktury zostały prawidłowo powołane, 2) a w przypadku zawarcia umowy z podmiotami świadczącymi usługi z zakresu cybebezpieczeństwa – czy to na tych podmiotach spoczywa obowiązek realizowania obowiązków wynikających z Projektu i czy ponoszą konsekwencje jego naruszenia (w tym kary administracyjne) i czy pomimo zawarcia odpowiedniej umowy operator w dalszym ciągu jest odpowiedzialny do powołania osoby odpowiedzialnej za cyberbezpieczeństwo, Ponadto sposób realizacji wymagań wskazanych w art. 15 ust. 2 Projektu powinien być określony w racjonalny sposób, pozwalający na spełnienie wymagań wskazanych w art. 15 ust. 2 Projektu operatorom usług kluczowych, posiadającym złożoną strukturę organizacyjna i operacyjną. Co więcej, Projekt powinien przewidywać, że powołanie wewnętrznych struktur może odbyć się poprzez powołanie takich struktur w ramach spółek należących do jednej, międzynarodowej grupy kapitałowej, wspólnych dla każdej ze spółek, w szczególności w przypadku gdy spółki posiadają wspólny system zarządzania cyberbezpieczeństwem.	Do decyzji MKS. Zwłaszcza, że bardzo często takie obowiązki są powierzane przedsiębiorstwom telekomunikacyjnym z grupy kapitałowej. Co powodować może kolizję praw i obchodzenie przepisów z zakresu krajowego systemu cyberbezpieczeństwa. Uwaga nieuwzględniona. Nie ma potrzeby regulować formalności dotyczących prawidłowego powołania struktur, o których mowa w art. 15 ust. 2, ponieważ istotne jest zapewnienie bezpieczeństwa świadczonych usług kluczowych. Niezależnie od sposobu realizacji obowiązku (poprzez utworzenie odpowiednich struktur bądź outsourcing usługi), odpowiedzialność za realizację obowiązków spoczywa na operatorze. Projektowane przepisy pozwalają grupom kapitałowym korzystać z jednego podmiotu świadczącego usługi z zakresu cyberbezpieczeństwa.

315.	art. 15 ust. 2	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	(W Projekcie słusznie wskazano, że do krajowego systemu cyberbezpieczeństwa wchodzą podmioty świadczące usługi z zakresu reagowania na incydenty. Krok ten jest słuszny wydaje się jednak, że działalność takich podmiotów powinna być w jakiś sposób certyfikowana. W obecnej wersji przepisów wymogi o charakterze ogólnym wskazane zostały w art. 15 ust. 2 Projektu. Doprecyzowane one mają zostać w rozporządzeniu wydawanym przez ministra właściwego do spraw informatyzacji wskazującym sposób realizacji ustawowych wymagań i wewnętrzne struktury odpowiedzialne za bezpieczeństwo. Odnosząc się do tak sformułowanej treści rozporządzenia wskazać należy, że nie ma uzasadnienia dla wskazywania wewnętrznych struktur podmiotu prowadzącego określoną działalność. Bardziej uzasadnione byłoby wskazanie wymogów technicznych, wymogów wykształcenia dla zespołu ludzkiego lub fizycznych wymagań dla wydzielenia pomieszczeń i serwerowni. Wewnętrzna struktura działania jakiegoś podmiotu nie powinna być regulowana w aktach prawnych.	Uwaga nieuwzględniona. Nie jest przewidywane certyfikowanie podmiotów świadczących usługi z zakresu cyberbezpieczeństwa. Odpowiedzialność za wybór takiego podmiotu leży po stronie operatora.
316.	art. 15 ust. 2	Konfederacja Lewiatan	Obowiązek prowadzenia działalności edukacyjnej powinien spoczywać przede wszystkim na CSIRT oraz przez organach państwa koordynujących kwestie cyberbezpieczeństwa na poziomie krajowym. Działalność operatorów usług kluczowych, w tym zakresie powinna mieć wyłącznie subsydiarny charakter. Jest to uzasadnione faktem, że wiedza o zagrożeniach cyberbezpieczeństwa powinna obejmować pełne spektrum zagrożeń i zabezpieczeń oraz dawać użytkownikowi całościowy obraz, a nie ograniczać się do pojedynczych usług. Uważamy, że to zadanie powinno być to realizowane przez wskazane w ustawie CSiRT'y lub MC, które dysponują wiedzą kompleksową na temat zagrożeń w cyberprzestrzeni i posiadają dane statystyczne. Do prowadzenia takiej działalności predestynuje te podmioty również zakres informacji pozyskiwanych przez CSIRT-y oraz organy właściwe o incydentach, ale również o stosowanych	Wyjaśnienie. W ocenie projektodawcy zapis art. 15 ust. 1 pkt 2 wydaje się być właściwym. Obowiązki nałożone na OUK mają wymiar podstawowy w kwestii informowania i dostępu do wiedzy użytkowników usługi kluczowej. OUK nie wykonują zadań o szerszym charakterze, jakie nałożone zostały w projekcie ustawy na CSIRT, na podstawie przepisów określonych w art. 28 ust. 3 pkt 3 i 4, oraz na ministra właściwego do spraw cyfryzacji, który na podstawie zapisów art. 41 pkt .7 projektowanej ustawy, ma za zadanie prowadzenie działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i podnoszenia

			zabezpieczeniach stosowanych przez operatorów, itd.. Tego typu informacje, w formie dostosowanej do potrzeb edukacyjnych, zagregowanej i zanonimizowanej mogłyby być wykorzystywane właśnie w działalności edukacyjnej. Zwiększyłoby to istotnie proporcjonalność wykorzystania pozyskanych od podmiotów rynkowych danych.	świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników.
317.	art. 15 ust. 2	Polska Izba Informatyki i Telekomunikacji	Obowiązek prowadzenia działalności edukacyjnej powinien spoczywać przede wszystkim na CSIRT oraz przez organach państwa koordynujących kwestie cyberbezpieczeństwa na poziomie krajowym. Działalność operatorów usług kluczowych, w tym zakresie powinna mieć wyłącznie subsydiarny charakter. Jest to uzasadnione faktem, że wiedza o zagrożeniach cyberbezpieczeństwa powinna obejmować pełne spektrum zagrożeń i zabezpieczeń oraz dawać użytkownikowi całościowy obraz, a nie ograniczać się do pojedynczych usług. Uważamy, że to zadanie powinno być to realizowane przez wskazane w ustawie CSiRT'y lub MC, które dysponują wiedzą kompleksową na temat zagrożeń w cyberprzestrzeni i posiadają dane statystyczne. Do prowadzenia takiej działalności predestynuje te podmioty również zakres informacji pozyskiwanych przez CSIRT-y oraz organy właściwe o incydentach, ale również o stosowanych zabezpieczeniach stosowanych przez operatorów, itd. Tego typu informacje, w formie dostosowanej do potrzeb edukacyjnych, zagregowanej i zanonimizowanej mogłyby być wykorzystywane właśnie w działalności edukacyjnej. Zwiększyłoby to istotnie proporcjonalność wykorzystania pozyskanych od podmiotów rynkowych danych.	Wyjaśnienie. W ocenie projektodawcy zapis art. 15 ust. 1 pkt 2 wydaje się być właściwym. Obowiązki nałożone na OUK mają wymiar podstawowy w kwestii informowania i dostępu do wiedzy użytkowników usługi kluczowej. OUK nie wykonują zadań o szerszym charakterze, jakie nałożone zostały w projekcie ustawy na CSIRT, na podstawie przepisów określonych w art. 28 ust. 3 pkt 3 i 4, oraz na ministra właściwego do spraw cyfryzacji, który na podstawie zapisów art. 41 pkt .7 projektowanej ustawy, ma za zadanie prowadzenie działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i podnoszenia świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników.
318.	art. 15 ust. 2 pkt 2	Fundacja Bezpieczna Cyberprzestrzeń	O jakich zagrożeniach i zabezpieczeniach mowa? Czy takimi pokojami muszą również dysponować operatorzy usług kluczowych?	Uwaga uwzględniona. Treść przepisu zostanie doprecyzowana.

319.	art. 15 ust. 2 pkt 2	Instytut Audytorów Wewnętrznych IIA Polska	Art. 15 ust. 2 pkt 2) - sugerujemy zmienić pomieszczenia na infrastrukturę;	Uwaga nieuwzględniona. Termin „infrastruktura” obejmowałby pkt 1 i 2 z art. 15 ust. 2, co nie było intencją projektodawcy
320.	art. 15 ust. 2 pkt 3	Fundacja Bezpieczna Cyberprzestrzeń	Jak ten zapis odnosi się do definicji cyberbezpieczeństwa, która nie wspomina o „niezaprzeczalności”, ale wymienia za to „autentyczność”?	Uwaga nieuwzględniona.
321.	art. 15 ust. 3	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 15. „3. Operatorzy usług kluczowych informują organ właściwy i właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV o podmiocie, z którym została zawarta umowa na świadczenie usług z zakresu cyberbezpieczeństwa.” – usługi z zakresu cyberbezpieczeństwa to bardzo szerokie pojęcie, zależnie od kontekstu może dotyczyć nawet znakomitej większości umów dotyczących usług IT zawieranych przez firmy (np. budowy/dostawy niemal dowolnego oprogramowania wspierającego działalność operatora usług krytycznych, zakupu wybranych rodzajów oprogramowania gotowego, szczególnie służącego celom bezpieczeństwa IT, wsparcia/utrzymania oprogramowania i sprzętu). Czy faktycznie intencją ustawodawcy było zebranie tak szerokiej listy umów? Być może korzystne byłoby doprecyzowanie, o jakie typy umów chodzi lub zdelegowanie tego doprecyzowania na stosowny organ.	Wyjaśnienie. Jeśli usługa serwisowa dotyczy bezpieczeństwa i ciągłości świadczenia usługi kluczowej to spełnia wymogi z art. 15 ust 3.
322.	art. 15 ust. 4	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 15. „4. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia sposób realizacji wymagań, o których mowa w ust. 2, przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa oraz wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo, uwzględniając potrzebę zapewnienia cyberbezpieczeństwa świadczonych usług kluczowych na wysokim poziomie.” – Czy faktycznie intencją ustawodawcy jest obciążenie Ministerstwa	Wyjaśnienie. Intencją projektodawcy było określenie w drodze rozporządzenia wymagań techniczno-organizacyjnych dla świadczenia tego typu usług. Ze względu na znaczenie bezpieczeństwa w przypadku świadczenia usług na rzecz podmiotów tworzących krajowy system cyberbezpieczeństwa nie byłoby uzasadnione

			zbudowaniem wymagań dla świadczenia przedmiotowych usług oraz budowy wewnętrznych struktur regulowanych tą ustawą podmiotów? Może to być odbierane jako nadmierna regulacja, szczególnie w świetle KSH. Być może korzystne byłoby ograniczenie już na poziomie ustawy zakresu tego rozporządzenia do ogólnych wytycznych lub zadań/celów, które mają być realizowane.	ograniczania zakresu rozporządzania do wytycznych lub zadań/celów, które mają być realizowane.
323.	art. 15 ust. 4	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	W zakresie delegacji przewidzianej w art. 15 ust. 4 Projektu, w ocenie Izby, to nie Minister ds. Cyfryzacji powinien określać wymagania np. na CERT dla energetyki albo CERT dla branży zbrojeniowej. Kompetencje te powinny być delegowane do innych właściwych organów tj. powinien to robić CSIRT właściwy dla danego operatora kluczowego.	Uwaga nieuwzględniona.
324.	art. 15 ust. 4	A.K. (uwagi osoby prywatnej)	Powołanie wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo – struktury cyberbezpieczeństwa u dużych działają, ale z uwagi na fakt, że ustawa zawiera delegację dla ministra właściwego ds. cyfryzacji do szczegółowego uregulowania w drodze rozporządzenia wymagań dla ww. struktur (lokalnych CERT-ów), może się w praktyce okazać, że obecne struktury wymagają dostosowania. Jakiego? Nie wiadomo bo brak tego rozporządzenia - postulat: rozporządzenie powinno się ukazać wraz z ustawą.	Wyjaśnienie. Projekty rozporządzeń wspomnianych w projekcie ustawy zostaną przygotowane.
325.	Art. 16	Pracodawcy RP	Projekt wymaga licznych uzupełnień w zakresie planowanych audytów. W szczególności należy doprecyzować: określenie „akredytowanej jednostki”, sposób jej akredytowania, instytucję akredytującą, zasad prowadzenia działań audytowych, zasad i podmiotu dokonującego „analizy ryzyka”, o której mowa w ust. 3. Ponadto należy doprecyzować, że posiadanie przez operatora usług kluczowych aktualnego certyfikatu ISO/IEC 27001 (np. w zakresie cyberbezpieczeństwa) będącego wynikiem audytu systemu zarządzania bezpieczeństwem informacji zwalnia operatora usług kluczowych z obowiązku poddawania się ww. audytowi. Stanowi to	Wyjaśnienie. Audytu może dokonać jednostka, która będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PN-ISO/IEC 27006. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE.

			wystarczające potwierdzenie zdolności organizacyjnych i kompetencji.	
326.	art. 16	Business Centre Club	W zakresie audytu, o którym mowa w art. 16 Projektu, wskazujemy, że w Projekcie nie określono kto ma akredytować jednostkę audytującą (art. 16 ust. 2 Projektu). Kwestia ta powinna być bardzo szczegółowo uregulowana w ustawie. Należy w szczególności zmienić zapis: „Audyt jest przeprowadzany przez akredytowana jednostkę oceniającą zgodność systemu bezpieczeństwa i zarządzania ciągłością działania" na „Audyt jest przeprowadzany przez akredytowaną jednostkę oceniającą zgodność systemu bezpieczeństwa i zarządzania ciągłością działania, która otrzymała akredytacje od Polskiego Centrum Akredytacji". Ustawowy wymóg przeprowadzania co najmniej raz na dwa lata audytu bezpieczeństwa teleinformatycznego powinien być bowiem realizowany przez podmioty, których akredytacje nie budzą wątpliwości prawnych i merytorycznych.	Wyjaśnienie. Audytu może dokonać jednostka, która będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PN-ISO/IEC 27006. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE.
327.	art. 16	Związek Pracodawcó w Branży Internetowej IAB Polska	W zakresie audytu, o którym mowa w art. 16 Projektu, wskazujemy, że w Projekcie nie określono kto ma akredytować jednostkę audytującą (art. 16 ust. 2 Projektu). Kwestia ta powinna być bardzo szczegółowo uregulowana w ustawie. Należy w szczególności zmienić zapis: „Audyt jest przeprowadzany przez akredytowana jednostkę oceniającą zgodność systemu bezpieczeństwa i zarządzania ciągłością działania" na „Audyt jest przeprowadzany przez akredytowaną jednostkę oceniającą zgodność systemu bezpieczeństwa i zarządzania ciągłością działania, która otrzymała akredytacje od Polskiego Centrum Akredytacji". Ustawowy wymóg przeprowadzania co najmniej raz na dwa lata audytu bezpieczeństwa teleinformatycznego powinien być bowiem realizowany przez podmioty, których akredytacje nie budzą wątpliwości prawnych i merytorycznych.	Wyjaśnienie. Audytu może dokonać jednostka, która będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PN-ISO/IEC 27006. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE.

328.	art. 16	Polska Organizacja Przemysłu i Handlu Naftowego	Zgodnie z art. 16 ust. 1 i 2 Projektu operator usług kluczowych jest zobowiązany do przeprowadzenia raz na dwa lata audytu bezpieczeństwa teleinformatycznego, przy czym audyt ma być przeprowadzony przez zewnętrzny podmiot - akredytowaną jednostkę oceniającą zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania. Przyjęcie takiego rozwiązania będzie powodowało dodatkowe koszty i trudności organizacyjne po stronie operatorów usług kluczowych. Proponujemy, aby w Projekcie zmienić częstotliwość audytów poprzez wskazanie, że audyt ma być przeprowadzony raz na pięć lat. Projekt powinien również określać jakie czynności mają być podjęte w ramach audytu i jakie elementy ma zawierać sprawozdanie z audytu. Projekt powinien zawierać postanowienie dotyczące zasad udzielania akredytacji dla podmiotów, które mają przeprowadzać audyt. Ponadto, w celu wyeliminowania konieczności przeprowadzenia więcej niż jednego audytu dotyczącego tego samego systemu zarządzania cyberbezpieczeństwem (np. w przypadku gdy spółek należących do jeden, międzynarodowej grupy kapitałowej, które mają wspólny system zarządzania cyberbezpieczeństwem) Projekt powinien przewidywać, że audyt może być przeprowadzony przez jednostkę, która uzyskała właściwą akredytację w innym kraju, który dokonał implementacji Dyrektywy.	Wyjaśnienie. Audytu może dokonać jednostka, która będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PN-ISO/IEC 27006. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE. Szczegółowe metody przeprowadzania audytów nie są materią ustawową.
329.	art. 16	Związek Banków Polskich	Przepis rodzi niejasności i kontrowersje w kontekście: 1.kto/jak będzie akredytował jednostkę która będzie mogła oceniać „zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania”. 2. W ustawie nie odnajdujemy informacji, że tego typu audyt miałby być bezpłatny…. Jeżeli to nie przeoczenie to temat wymaga koniecznie doprecyzowania by rynek nie został zdominowany przez pojedyncze firmy. 3. Akredytowaną jednostkę	Wyjaśnienie. Audytu może dokonać jednostka, która będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PN-ISO/IEC 27006.

			należy rozumieć jako ‘audyt zewnętrzny, z poza instytucji”, czy takie jest rozumienie zapisu? 4. niejasny jest tryb uruchamiania audytu. To operator usług kluczowych będzie musiał poprosić Akredytowaną jednostkę o wykonanie audytu, i na nim spoczywa obowiązek ‘zorganizowania’ takiego audytu? 5. W oparciu o jakie standardy ma być realizowany audyt? 6. o jaką akredytację chodzi? Kto będzie jej udzielał i na jakich zasadach? 7. Jednostka przeprowadzająca audyt jest akredytowana przez kogo? Z czym ma być weryfikowana zgodność, z niniejszą ustawą? 8. Weryfikowana jest zgodność ale z czym? 9 Czy będzie możliwość połączenia tych audytów razem z innymi typami audytów np. audytem na ISO27001?	Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE. Szczegółowe metody przeprowadzania audytów nie są materią ustawową.
330.	art. 16	Polska Izba Ubezpieczeń	Zwracamy uwagę na treść art. 16, w którym znajdują się zapisy dot. audytu systemu bezpieczeństwa operatora usługi kluczowej przez akredytowaną jednostkę audytową. Ogólny zapis przywołany w ustawie nie wskazujący precyzyjnie o jakiego rodzaju akredytację chodzi. Zapis powinien precyzować przez kogo będą akredytowani audytorzy oraz zabezpieczać przed sytuacją, w których będą oni niezależni od podmiotów audytowanych.	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE.
331.	art. 16	Izba Gospodarcza Gazownictwa	Rekomendujemy zobowiązanie akredytowanych jednostek audytowych do oznaczania wyników przeprowadzonych audytów tajemnicą przedsiębiorstwa bądź postępowania zgodnie z ustawą o ochronie informacji niejawnych. Również warte rozważenia byłoby odpowiednie zastosowanie art. 13 ust. 2 w sytuacji wskazanej w art. 16 ust. 5.	Uwaga nieuwzględniona.
332.	art. 16	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Pytania dotyczące treści artykułu Czy lista akredytowanych jednostek zostanie udostępniona, i kiedy, dla operatorów usług kluczowych ?	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE.

333.	art. 16	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Prosimy o określenie czy i gdzie będzie dostępna lista akredytowanych jednostek oceniających zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania (audytorów).	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE.
334.	art. 16	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Prosimy określić względem jakiego standardu ma być realizowany audyt. Przepisy niniejszej ustawy nie są wystarczające precyzyjne w celu przeprowadzenia audytu.	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE.
335.	art. 16	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 16. „1. Operatorzy usług kluczowych przeprowadzają co najmniej raz na dwa lata audyt bezpieczeństwa teleinformatycznego” – Ustawa nie definiuje pojęcia bezpieczeństwa teleinformatycznego (i odnosi się do niego tylko 2 razy). Czy chodziło o cyberbezpieczeństwo?	Uwaga nieuwzględniona. Zdaniem autorów projektu ustawy aktualny zapis jest odpowiedni. Uwzględnia wymagania określone w dyrektywie 2016/1148.
336.	art. 16 ust. 1	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy następujące brzmienie art. 16 ust. 1: Art. 16. 1. Operatorzy usług kluczowych przeprowadzają co najmniej raz na cztery lata audyt bezpieczeństwa teleinformatycznego, zwany dalej „audytem”. Organizacja certyfikowanego audytu jest dodatkowym kosztem dla operatorów. Wzorem audytu energetycznego sugerujemy wyznaczyć częstotliwość audytu raz na 4 lata. Pozwoli to lepiej rozłożyć koszty oraz wysiłek jakie musi włożyć operator w przeprowadzenie audytu.	Uwaga nieuwzględniona. Zdaniem autorów projektu ustawy aktualny zapis jest odpowiedni.
337.	art. 16 ust. 1	Fundacja Bezpieczna Cyberprzestrzeń	Zważywszy na dynamiczny rozwój zagrożeń teleinformatycznych zasadne wydaje się przeprowadzenie takiego audytu raz do roku.	Uwaga nieuwzględniona. Zdaniem autorów projektu ustawy aktualny zapis jest odpowiedni.

338.	art. 16 ust. 1	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	W art. 16 ust. 1 Projektu wątpliwości rodzi zapis „akredytowana jednostka”. Nie jest jasne jaka to ma być akredytacja i jakie wymagania ma spełniać ta jednostka? Problem w tym, że nie ma standaryzacji tych jednostek a dodatkowo ograniczamy się do np. jednostek dużych bądź specjalizowanych typu PwC, EY, KPMG, wykluczając mniejsze polskie firmy realizujące takie audyty. Dlaczego CSIRT albo CERT sektorowe nie mogą przeprowadzać samodzielnie audytów przy użyciu powszechnie znanych i często dostępnych narzędzi dla tych operatorów?	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE.
339.	art. 16 ust. 1	Konfederacja Lewiatan	Organizacja certyfikowanego audytu jest dodatkowym kosztem dla operatorów. Wzorem audytu energetycznego sugerujemy wyznaczyć częstotliwość audytu raz na 4 lata. Pozwoli to lepiej rozłożyć koszty oraz wysiłek jakie musi włożyć operator w przeprowadzenie audytu. Proponujemy następujące brzmienie art. 16 ust. 1: Art. 16. 1. Operatorzy usług kluczowych przeprowadzają co najmniej raz na cztery lata audyt bezpieczeństwa teleinformatycznego, zwany dalej „audytem”.	Uwaga nieuwzględniona. Zdaniem autorów projektu ustawy aktualny zapis jest odpowiedni.
340.	art. 16 ust. 1	Instytut Kościuszki	Zgodnie z art. 16 ust. 1 projektu ustawy, operatorzy usług kluczowych są zobowiązani do przeprowadzenia co najmniej raz na dwa lata audytu bezpieczeństwa teleinformatycznego. Z uwagi na bezprecedensową dynamikę rozwoju liczby i zaawansowania zagrożeń w cyberprzestrzeni oraz fundamentalną rolę operatorów usług kluczowych dla funkcjonowania współczesnego społeczeństwa i gospodarki, audyty bezpieczeństwa teleinformatycznego powinny być realizowane co pół roku. Tym samym ustawa powinna doprecyzować procedurę wyboru (prawdopodobnej certyfikacji jak w przypadku podmiotów świadczących usługi z zakresu cyberbezpieczeństwa) oraz organ dokonujący akredytacji (art. 16 ust. 2) podmiotów uprawnionych do realizacji audytów.	Uwaga nieuwzględniona. Ustawa stawia wymóg przeprowadzenia audytu zewnętrznego raz na dwa lata. Nic nie stoi na przeszkodzie, aby przeprowadzać audyty częściej.

341.	art. 16 ust. 1	J.K. (uwagi osoby prywatnej)	W OSR-ze stwierdzono, że szacunkowy koszt jednostkowy wykonania audytu zewnętrznego będzie wynosił 50 tys. zł. Skoro audyt po raz pierwszy będzie przeprowadzony w roku 2019, ceny do tego czasu mogą znacznie wzrosnąć. 2. W 2016 roku Centralny Ośrodek Informatyki ogłosił przetarg na świadczenie usług audytu bezpieczeństwa informatycznego. Wybrana została firma, która wyceniła swoje usługi na 500 tys. złotych. Zatem koszty wymaganych audytów są faktycznie nieznane i trudne do oszacowania.	Uwaga nieuwzględniona.
342.	art. 16 ust. 1-5	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 16 ust 1-5 – uwagi ujęte w pkt 2 dotyczącym art. 5. Brak terminu na przeprowadzenie audytu. Odpowiedzialność za brak audytu w całości po stronie OUK choć audyt wykonywany jest przez stronę trzecią.	Uwaga nieuwzględniona.
343.	art. 16 ust. 6	Pracodawcy RP	Podstawową zasadą wszelkich rozstrzygnięć władczych organów państwa, jest prawo podmiotu obciążanego karą lub obowiązkami do odwołania się, a przynajmniej do przedstawienia swojego stanowiska w sprawie. Projektowany przepis natomiast miałby umożliwiać właściwemu organowi do nałożenia na inny podmiot (niebędący w strukturze tego organu) obowiązków, określonych wyłącznie na podstawie analizy wniosków z przeprowadzonego audytu. Na żadnym etapie procedury nie przewidziano możliwości jakiejkolwiek obrony przed formułowanymi tezami, wnioskami czy w końcu konkretnymi obowiązkami. Organ właściwy powinien być obowiązany do zapoznania się z opinią podmiotu audytowanego przed nałożeniem jakichkolwiek obowiązków.	Art. 16 ust. 6 zostanie usunięty.
344.	art. 16 ust. 2	Polskie Towarzystwa Przesyłu i Rozdziału	Proponujemy doprecyzowanie zapisu. Art. 16. „2. Audyt jest przeprowadzany przez akredytowaną jednostkę oceniającą zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania.” – o jakiego typu akredytację chodzi? Pożądane	Wyjaśnienie.

		Energii Elektrycznej	byłoby wskazanie zasad akredytacji lub zdelegowanie określenia zasad tej akredytacji na stosowny organ.	Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE.
345.	art. 16 ust. 2	J.K. (uwagi osoby prywatnej)	W wynikach kontroli "Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych" Najwyższa Izba Kontroli zwróciła uwagę na kwestię audytów przeprowadzanych przez akredytowaną jednostkę: "Kontrola zidentyfikowała w KRUS wprowadzenie praktycznie wszystkich procesów wymaganych przez przyjętą metodykę badań, czego nie stwierdzono w żadnej z pozostałych kontrolowanych jednostek. Było to związane z działaniami podjętymi w celu uzyskania przez KRUS certyfikatu ISO 27001. Porównując wyniki kontroli dla wszystkich skontrolowanych jednostek, zarówno posiadających jak i nieposiadających ww. certyfikat, należy wskazać na pozytywny wpływ wymagań procesu certyfikacji na uzyskaną ocenę warunków zapewnienia bezpieczeństwa IT. W konsekwencji ocena sformułowana dla KRUS była wyraźnie wyższa niż dla pozostałych jednostek. Jednakże również w systemie funkcjonującym w KRUS kontrola wykryła nieprawidłowości. Wskazywały one na występowanie błędów w implementacji wymagań norm stanowiących podstawę uzyskania certyfikatu. W ocenie NIK niektóre z nich były poważne i mogą mieć istotny, negatywny wpływ na szereg procesów zapewnienia bezpieczeństwa IT w KRUS. Stwierdzone nieprawidłowości dotyczyły rozbieżności pomiędzy deklarowanym a faktycznym poziomem zabezpieczenia informacji. Był to niepokojący stan, zwłaszcza że podmioty które zorganizowały swój system zarządzania bezpieczeństwem informacji, ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie na podstawie Polskich Norm zostały praktycznie zwolnione z przestrzegania szeregu wymagań rozporządzenia KRI. Wymagania wskazane w Normie są znacznie szersze i precyzyjniejsze niż w rozporządzeniu, jednak stwierdzona w KRUS	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE. Audytu może dokonać jednostka wewnętrzna, jeśli będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PNISO/IEC 27006. W zakresie bezpieczeństwa informacji może być to norma PN-ISO/IEC 27001, a dla zarządzania ciągłością działania – PN-ISO/IEC 22301.

			rozbieżność wskazywała na istnienie ryzyka niespełniania wymogów określonych w rozporządzeniu. Niezależnie od powyższego stwierdzić należy, że System Zarządzania Bezpieczeństwem Informacji w KRUS funkcjonował, chociaż występowały w nim istotne nieprawidłowości." Kontrolą objęto okres od 1 stycznia 2014 r. do 1 października 2015 r. Najniżej oceniono: - zarządzanie kluczami kryptograficznymi, - testowanie, nadzorowanie i monitorowanie bezpieczeństwa oraz - zarządzanie incydentami. Jednakże aktualny certyfikat ISO 27001 został wystawiony przez akredytowaną jednostkę w dniu 3.11.2015 - czyli miesiąc po zakończeniu kontroli NIK w KRUS - i jest ważny do 20.11.2017.3 2. W projekcie ustawy i pozostałych dokumentach nie wskazano, jak będą akredytowane jednostki upoważnione do przeprowadzania audytów. Audyt jest przeprowadzany przez akredytowaną jednostkę oceniającą zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania. 2a. Minister właściwy do spraw informatyzacji określi w drodze rozporządzenia sposób i tryb akredytacji jednostek upoważnionych do oceny zgodności systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania z wymogami określonymi w ustawie.	
346.	art. 16 ust. 2	A.K. (uwagi osoby prywatnej)	Obowiązek przeprowadzania co dwa lata audytu bezpieczeństwa teleinformatycznego (art. 15 ust. 2) przez akredytowaną jednostkę. Brak informacji w projekcie, co rozumie się przez akredytowaną jednostkę, która ma audyt przeprowadzać – kto ma takiej akredytacji udzielać? Nie jest znany sposób akredytacji jednostek, które mają prowadzić audyty u operatorów usług kluczowych. Brak informacji również o tym jaki audyt zdaniem projektodawcy będzie stanowić realizację tych wymagań, co jest istotne w kontekście ewentualnej sankcji pieniężnej przewidzianej w ustawie. Proponujemy wyraźnie wpisać do ustawy, że posiadanie przez operatora usług kluczowych aktualnego certyfikatu ISO/IEC 27001	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE. Audytu może dokonać jednostka wewnętrzna, jeśli będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PNISO/IEC 27006.

			(np. w zakresie cyberbezpieczeństwa) będącego wynikiem audytu systemu zarządzania bezpieczeństwem informacji zwalnia operatora usług kluczowych z obowiązku poddawania się ww. audytowi. Wątpliwości budzi ponadto zapis "Celem audytu jest potwierdzenie, na podstawie przeprowadzonej analizy ryzyka, że operatorzy usług kluczowych spełniają wymogi określone w ustawie" – kto ma przeprowadzać tę analizę ryzyka? Brakuje korelacji między obowiązkiem przeprowadzenia audytu (w praktyce na koszt operatora) wraz z obowiązkiem przekazania kopii sprawozdania z audytu organowi właściwemu a obowiązkiem poddania się kontroli, o której mowa w rozdziale VIII – skoro nakłada się na operatora obowiązek poddania się regularnemu audytowi to proponujemy w związku z tym ograniczenie uprawnień kontrolnych organu nadzorczego (audyt zastępuje kontrolę).	W zakresie bezpieczeństwa informacji może być to norma PN-ISO/IEC 27001, a dla zarządzania ciągłością działania – PN-ISO/IEC 22301.
347.	art. 16 ust. 2	Krajowy Depozyt Papierów Wartościowych S.A.	W związku z art. 16 ust. 2 projektu ustawy, dotyczącym obowiązku przeprowadzania audytu bezpieczeństwa teleinformatycznego, zwracamy uwagę na konieczność zmiany lub doprecyzowania sformułowania „akredytowana jednostka". Projekt jasno nie określa bowiem jaki rodzaj akredytacji musiałaby posiadać jednostka audytująca. Należy też zauważyć, że odpowiedni zapis w art. 15 ust. 2 lit b) dyrektywy (UE) 2016/1148 traktuje o wynikach audytu przeprowadzonego przez „wykwalifikowanego audytora", a zatem wydaje się, że intencją dyrektywy było podkreślenie konieczności posiadania odpowiednich kompetencji przez podmiot dokonujący audytu, przy zachowaniu jednak większej elastyczności, jeśli chodzi o uznanie określonego podmiotu jako odpowiedniego do przeprowadzenia audytu bezpieczeństwa teleinformatycznego. Na potrzebę zachowania takiej elastyczności wskazywać może również odmienna skala oraz specyfika działalności różnych operatorów usług kluczowych, z których wynikać mogą różnice, jeśli chodzi o złożoność i zakres wykorzystywania systemów informatycznych, a w	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE. Audytu może dokonać jednostka wewnętrzna, jeśli będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PNISO/IEC 27006.

			konsekwencji odmienne wymagania w zakresie doboru właściwej jednostki audytującej. W związku z powyższym proponujemy zastąpienie w art. 16 ust. 2 słowa „akredytowana" słowem „wykwalifikowana" bądź też doprecyzowanie zapisów dotyczących akredytacji podmiotu przeprowadzającego audyt bezpieczeństwa teleinformatycznego.	
348.	art. 16 ust. 2	Konfederacja Lewiatan	Nie jest określone kto ma akredytować jednostkę audytującą. Należy to bardzo precyzyjnie określić w zapisach ustawy. Należy w szczególności zmienić zapis „Audyt jest przeprowadzany przez akredytowana jednostkę oceniającą zgodność systemu bezpieczeństwa i zarządzania ciągłością działania" na „Audyt jest przeprowadzany przez akredytowaną jednostkę oceniającą zgodność systemu bezpieczeństwa i zarządzania ciągłością działania, która otrzymała akredytacje od Polskiego Centrum Akredytacji" –Ustawowy wymóg przeprowadzania co najmniej raz na dwa lata audytu bezpieczeństwa teleinformatycznego powinien być bowiem realizowany przez podmioty, których akredytacje nie budzą wątpliwości prawnych i merytorycznych. Nie został określony sposób akredytacji jednostek, które mają prowadzić audyty u operatorów usług kluczowych. Z uwagi na zagrożenie karą pieniężną, kluczowe jest również doprecyzowanie, zasady prowadzenia samego audytu, a także oczekiwanych jego efektów, które zostaną uznane za spełnienie ustawowych wymagań. Proponujemy doprecyzować, że posiadanie przez operatora usług kluczowych aktualnego certyfikatu ISO/IEC 27001 (np. w zakresie cyberbezpieczeństwa) będącego wynikiem audytu systemu zarządzania bezpieczeństwem informacji zwalnia operatora usług kluczowych z obowiązku poddawania się ww. audytowi. Wątpliwości budzi ponadto zapis w ust. 3, że „Celem audytu jest potwierdzenie, na podstawie przeprowadzonej analizy ryzyka, że operatorzy usług kluczowych spełniają wymogi określone w	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE. Audytu może dokonać jednostka wewnętrzna, jeśli będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PNISO/IEC 27006. W zakresie bezpieczeństwa informacji może być to norma PN-ISO/IEC 27001, a dla zarządzania ciągłością działania – PN-ISO/IEC 22301.

			ustawie.”. Wnosimy o doprecyzowanie podmiotu, który ma przeprowadzać tę analizę ryzyka oraz zasad jej wykonywania. Ponadto brakuje korelacji między obowiązkiem przeprowadzenia audytu (w praktyce na koszt operatora) z obowiązkiem przekazania kopii sprawozdania z audytu organowi właściwemu, a obowiązkiem poddania się kontroli, o której mowa w rozdziale VIII. Skoro bowiem nakłada się na operatora obowiązek poddania się regularnemu audytowi to proponujemy w związku z tym ograniczenie uprawnień kontrolnych organu nadzorczego (audyt zastępuje kontrolę).	
349.	art. 16 ust. 2	Fundacja Bezpieczna Cyberprzestrzeń	Jaka i przez kogo akredytowana jednostka. Skąd należy zaczerpnąć informacji o jednostkach, które mogą dokonać takiego audytu?	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE. Audytu może dokonać jednostka wewnętrzna, jeśli będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PNISO/IEC 27006.
350.	art. 16 ust. 2	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	W art. 16 ust. 2 Projektu wskazano, że audyt bezpieczeństwa teleinformatycznego przeprowadzany jest przez akredytowaną jednostkę oceniającą zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania. Wyjaśnienia wymaga o jaką akredytację tutaj chodzi, jeżeli Projektodawca miał na myśli akredytację ISO, to powinno to zostać wskazane wprost w przepisach. Wydaje się jednak, że bardziej uzasadnione byłoby przeprowadzanie takiej akredytacji przez jednostki wyspecjalizowane bądź podlegające państwu polskiemu (jak SKW, ABW, AW, Policja), bądź też posiadające certyfikat potwierdzający możliwość przeprowadzania procesu akredytacji wydany przez	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE. Audytu może dokonać jednostka wewnętrzna, jeśli będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PNISO/IEC 27006.

			odpowiednią jednostkę (trzeba by stworzyć w tym zakresie odpowiednią procedurę w ustawie).	
351.	art. 16 ust. 2	Polska Izba Radiodyfuzji Cyfrowej	Nie jest określone kto ma akredytować jednostkę audytującą. Należy to bardzo precyzyjnie określić w zapisach ustawy. Należy w szczególności zmienić zapis „Audyt jest przeprowadzany przez akredytowana jednostkę oceniającą zgodność systemu bezpieczeństwa i zarządzania ciągłością działania" na „Audyt jest przeprowadzany przez akredytowaną jednostkę oceniającą zgodność systemu bezpieczeństwa i zarządzania ciągłością działania, która otrzymała akredytacje od Polskiego Centrum Akredytacji" –Ustawowy wymóg przeprowadzania co najmniej raz na dwa lata audytu bezpieczeństwa teleinformatycznego powinien być bowiem realizowany przez podmioty, których akredytacje nie budzą wątpliwości prawnych i merytorycznych.	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE. Audytu może dokonać jednostka wewnętrzna, jeśli będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PNISO/IEC 27006.
352.	art. 16 ust. 2	Instytut Audytorów Wewnętrznych IIA Polska	Art. 16 ust. 2 - brak wyjaśnienia, kto to jest „Akredytowana jednostka oceniająca", jakie wymagania w stosunku do takiej jednostki oraz dlaczego audyt wskazany w Art. 16 nie może zostać przeprowadzony przez wewnętrzną niezależną funkcję audytu, której pracownicy posiadają odpowiednie kwalifikacje zarówno w zakresie audytu, jak i kompetencji dotyczących cyberbezpieczeństwa;	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE. Audytu może dokonać jednostka wewnętrzna, jeśli będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PNISO/IEC 27006.
353.	art. 16 ust. 2 i 3	Polska Izba Informatyki i Telekomunikacji	Z uwagi na zagrożenie karą pieniężną, kluczowe jest doprecyzowanie, zasady prowadzenia samego audytu, a także oczekiwanych jego efektów, które zostaną uznane za spełnienie ustawowych wymagań. Audyt, to jest sprawdzenie spełniania wymogów określonych precyzyjnie we wzorcu odniesienia. Co w przypadku tego wymagania ma być takim wzorcem? Brak takiego	Audyt ma dotyczyć zgodności z ustawą. Te normy mogą być podstawą, natomiast dla poszczególnych sektorów mogą być dodatkowe normy. W zakresie bezpieczeństwa informacji może być to norma PN-ISO/IEC 27001, a dla zarządzania ciągłością działania – PN-ISO/IEC 22301.

			wzorca uniemożliwia wykonanie audytu. Co ma potwierdzać taki audyt? Zgodność z czym z jakimi wymaganiami, gdzie opublikowanymi? Proponujemy doprecyzować, że posiadanie przez operatora usług kluczowych aktualnego certyfikatu ISO/IEC 27001 (np. w zakresie cyberbezpieczeństwa) będącego wynikiem audytu systemu zarządzania bezpieczeństwem informacji zwalnia operatora usług kluczowych z obowiązku poddawania się ww. audytowi. Ponadto brakuje korelacji między obowiązkiem przeprowadzenia audytu (w praktyce na koszt operatora) z obowiązkiem przekazania kopii sprawozdania z audytu organowi właściwemu, a obowiązkiem poddania się kontroli, o której mowa w rozdziale VIII. Skoro bowiem nakłada się na operatora obowiązek poddania się regularnemu audytowi to proponujemy w związku z tym ograniczenie uprawnień kontrolnych organu nadzorczego (audyt zastępuje kontrolę). Brakuje także informacji nt wymagań dla tej akredytacji.	
354.	art. 16 ust. 2 i 3	Izba Gospodarcza Gazownictwa	Postanowienia te budzą wątpliwość na czym miałaby polegać ocena „zgodności" systemu bezpieczeństwa i w ramach jakich kryteriów miałaby być ona oceniana. W związku z tym rekomendujemy połączenie obu wskazanych jednostek redakcyjnych.	Wyjaśnienie. Audyt będzie dotyczył obowiązków określonych w art. 10-13. Dodatkowo na postawie art. 39 organy właściwe będą wydawały wytyczne sektorowe precyzujące wymagania bezpieczeństwa, określone w art. 10. W oparciu o te wytyczne będą mogły być realizowane audyty przez podmioty oceniające zgodność, przy założeniu rozszerzenia możliwości prowadzenia tego audytu na inne podmioty zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) NR 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93.

355.	art. 16 ust. 2 i 3	Instytut Logistyki i Magazynowania	Audyt bezpieczeństwa teleinformatycznego. Opis audytu dotyczy weryfikacji zgodności wdrożonego u operatora organizacyjnego systemu zarządzania bezpieczeństwem z wymaganiami ustawy (art.10 ust.2). Dlatego należy tak należy go tytułować aby odróżnić od audytu bezpieczeństwa systemu informacyjnego. Zapis art.16 ust.2 powinien być ograniczony o określenia upoważnionych do przeprowadzenia audytu jednostek (i może zostać przeniesiony poniżej opisu celu audytu). W art.16 ust.3 należy pominąć tekst „na podstawie przeprowadzonej analizy ryzyka”.	Uwaga częściowo uwzględniona. Art. 16 ust. 2 zostanie uzupełniony o wskazanie upoważnionych jednostek.
356.	art. 16 ust. 2-4	Izba Gospodarcza Gazownictwa	Nie ma normy / zaleceń szczegółowych dla Art. 10 a więc następnie do procedur audytowych (warto porównać z NIST/ NERC CIP USA). Dla norm (branżowych - konieczność stworzenia norm branżowych powinny być akredytowane odpowiednio jednostki – np. dla energetyki może to być UDT (akredytacja minister Energii). Akredytowana jednostka – nie wiadomo jaka akredytacja ? do czego ? wg jakich jakich norm ma być prowadzony audyt? Rozwiązaniem może być akredytacja poprzez organ właściwy [(zgodnie z par 38) dla danego sektora (lista akredytowanych podmiotów)] ministra ds. informatyzacji, międzynarodową jednostkę akredytującą. Należy wskazać właściwą jednostkę akredytującą. Propozycja zapisu: doprecyzowanie sformułowania np. 2. Audyt jest przeprowadzany przez akredytowaną przez organ właściwy jednostkę oceniającą zgodność systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania.	Wyjaśnienie. Akredytować jednostki będzie Polskie Centrum Akredytacji lub równoważna mu jednostka akredytująca z obszaru UE. Audytu może dokonać jednostka wewnętrzna, jeśli będzie posiadać właściwą akredytację np. spełniająca wymagania dla jednostek prowadzących audyt i certyfikację systemów zarządzania bezpieczeństwem informacji PNISO/IEC 27006. Audyt ma dotyczyć zgodności z ustawą. Te normy mogą być podstawą, natomiast dla poszczególnych sektorów mogą być dodatkowe normy.
357.	art. 16 ust. 3	J.K. (uwagi osoby prywatnej)	Pozostaje pytanie, czy istotna jest tylko zgodność (ang. compliance) z ustawą czy też faktyczne cyberbezpieczeństwo. W Uzasadnieniu stwierdzono, że " Celem audytu jest potwierdzenie, na podstawie przeprowadzonej analizy ryzyka, że operatorzy usług kluczowych spełniają wymogi określone w ustawie." Audyt nie	Wyjaśnienie. Zgodnie z art. 15 ust. 2, audyt ma na celu potwierdzić zgodność z wymogami z ustawy.

			polega na potwierdzeniu na podstawie analizy ryzyka, czy operatorzy spełniają wymogi ustawy. Oto kilka definicji audytu: - NIST: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. - ENISA: The method by which procedures and/or documentation are measured against pre-agreed standards. - ISACA: Formal inspection and verification to check whether a standard or set of guidelines is being followed, records are accurate, or efficiency and effectiveness targets are being met. May be carried out by internal or external groups. - NIK/KPRM: badanie lub przegląd polegający na ustaleniu stanu faktycznego, porównaniu go ze stanem wymaganym/pożądanym oraz dokonanie jego oceny. Zgodnie ze standardem audytu SI 1202 Risk Assessment in Planning [Szacowanie ryzyka w planowaniu] opracowanym przez ISACA: The IS audit and assurance function shall use an appropriate risk assessment approach and supporting methodology to develop the overall IS audit plan and determine priorities for the effective allocation of IS audit resources. Zgodnie ze standardem 2010 Planowanie opracowanym przez IIA: Zarządzający audytem wewnętrznym musi opracować plan oparty na analizie ryzyka, określający priorytety działań audytu wewnętrznego zgodne z celami organizacji oraz standardem 2120 Zarządzanie ryzykiem: Audyt wewnętrzny musi oceniać skuteczność i przyczyniać się do usprawnienia procesów zarządzania ryzykiem. Analiza ryzyka pomaga audytorowi opracować plan i program audytu. Nie zastępuje czynności audytowych wyznaczonych w standardach wykonania audytu, obejmujących m.in. ocenę procesu zarządzania ryzykiem w badanym podmiocie.	

			Celem audytu jest potwierdzenie, że operatorzy usług kluczowych spełniają wymogi określone w ustawie.	
358.	art. 16 ust. 4	J.K. (uwagi osoby prywatnej)	Dowody, które musi zebrać audytor, są opisane w standardzie audytu SI 1205 Dowody. Są to: - wykonane procedury, - wyniki wykonanych procedur, - dokumenty źródłowe (w formacie papierowym lub elektronicznym), zapisy i informacje potwierdzające wykorzystane dla wsparcia realizacji zlecenia, - ustalenia i wyniki realizacji zlecenia, - dokumentacja potwierdzającą, że prace zostały wykonane zgodnie z odnośnym prawem, przepisami i politykami. Zatem zebrane dokumenty są dowodami audytowymi - nie muszą być wymieniane w ustawie. Dodatkowe wskazówki dotyczące sporządzania sprawozdania z audytu są zawarte w dokumencie ISACA "Information Systems Auditing: Tools and Techniques - IS Audit Reporting". Skoro - zgodnie z zapisem ust. 2 - audyt jest przeprowadzany przez akredytowaną jednostkę, to konsekwentnie zapis ust. 4 musi wskazywać na akredytowaną jednostkę jako podmiot, który będzie przekazywać sprawozdanie, nawet jeżeli w praktyce uczynią to audytorzy będący pracownikami lub podwykonawcami tej jednostki. Akredytowana jednostka przekazuje operatorowi usługi kluczowej sprawozdanie z przeprowadzonego audytu.	Wyjaśnienie. Ustawa musi precyzować obowiązki o charakterze ustawowym, a nie odnosić się do dokumentacji wskazywanej w dokumentach normalizacyjnych.
359.	art. 16 ust. 6	J.K. (uwagi osoby prywatnej)	Wszystkie znane standardy audytu wymagają od audytora wydania zaleceń / rekomendacji. Z zapisów ust. 6 ustawy wynika, że audytorom nie będzie wolno tego robić. Ich rola sprowadzi się do przedstawienia ustaleń i wniosków, natomiast wiążące polecenia będzie wydawać organ właściwy. Lepiej będzie przyjąć, że audytor, działając zgodnie ze standardami audytu, wyda zalecenia a organ będzie mógł je uzupełnić o swoje polecenia.	Uwaga częściowo uwzględniona. Projektodawca nie wskazuje standardów audytowych realizowanych wobec audytowanych podmiotów, ale określa obowiązki realizowane wobec organów właściwych i dyrektora Rządowego Centrum Bezpieczeństwa.

			Organ właściwy na podstawie analizy wyników audytu może wydawać dodatkowe wiążące polecenia wprowadzenia środków zaradczych w odniesieniu do stwierdzonych w trakcie audytu braków, niedociągnięć i słabości systemu zarządzania bezpieczeństwem i zarządzania ciągłością działania. W przypadku, o którym mowa w ust. 5 pkt 2, polecenia wydawane są po zasięgnięciu opinii dyrektora Rządowego Centrum Bezpieczeństwa.	Przepis zostanie częściowo zmieniony. Wyniki audytu mogą być podstawą przeprowadzenia kontroli przez organ właściwy.
360.	art. 16 ust. 6	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 16 ust 6 – brak terminu wykonania poleceń usunięcia uchybień wydanych przez organ właściwy, wynikających z analizy wyników audytu. Zapisano fakultatywne wydanie poleceń usunięcia uchybień – wydaje się że powinno być obligatoryjne. Przy istniejących zapisach jeśli audyt wykazał uchybienia a organ właściwy nie wydał poleceń ich usunięcia OUK nie ma obowiązku tego wykonać. Przepis wymaga doprecyzowania.	Uwaga częściowo uwzględniona. Usunięty zostanie ust. 6. Przepis zostanie częściowo zmieniony. Wyniki audytu mogą być podstawą przeprowadzenia kontroli przez organ właściwy.
361.	art. 16 ust. 6	Konfederacja Lewiatan	Z uwagi na konieczność zapewnienia możliwości obiektywnej oceny sytuacji, w szczególności z zachowaniem prawa podmiotu audytowanego do wypowiedzenia się oraz bycia wysłuchanym, w sprawach, które dotyczą jego istotnych interesów, wnosimy o wprowadzenie zapisów wskazujących na obowiązek „organu właściwego” do zapoznania się z odniesieniem podmiotu audytowanego do wyników audytu. Niedopuszczalna jest w naszej ocenie sytuacja, w której wyniki audytu (biorąc pod uwagę fakt braku precyzji przepisów w tym zakresie) miałyby bezpośrednio i bez jakiegokolwiek trybu odwoławczego, a nawet wysłuchania, skutkować nałożeniem, w trybie władczego rozstrzygnięcia, obowiązków na podmiot audytowany, które dodatkowo zagrożone są możliwością nałożenia kary pieniężnej do 50.000 zł w sytuacji niezastosowania się do ww. poleceń.	Wyjaśnienie. Usunięty zostanie ust. 6. Przepis zostanie częściowo zmieniony. Wiążące polecenia będą miały formę decyzji administracyjnej.

362.	art. 16 ust. 6	Polska Izba Informatyki i Telekomunikacji	Z uwagi na konieczność zapewnienia możliwości obiektywnej oceny sytuacji, w szczególności z zachowaniem prawa podmiotu audytowanego do wypowiedzenia się oraz bycia wysłuchanym, w sprawach, które dotyczą jego istotnych interesów, wnosimy o wprowadzenie zapisów wskazujących na obowiązek „organu właściwego” do zapoznania się z odniesieniem podmiotu audytowanego do wyników audytu. Niedopuszczalna jest w naszej ocenie sytuacja, w której wyniki audytu (biorąc pod uwagę fakt braku precyzji przepisów w tym zakresie) miałyby bezpośrednio i bez jakiegokolwiek trybu odwoławczego, a nawet wysłuchania, skutkować nałożeniem, w trybie władczego rozstrzygnięcia, obowiązków na podmiot audytowany, które dodatkowo zagrożone są możliwością nałożenia kary pieniężnej do 50.000 zł w sytuacji niezastosowania się do ww. poleceń	Wyjaśnienie. Usunięty zostanie ust. 6. Przepis zostanie częściowo zmieniony. Wiążące polecenia będą miały formę decyzji administracyjnej.
363.	art. 17	Związek Banków Polskich	Ust. 1 - Proponuje się dodanie po zwrocie: "główną siedzibę" dodanie zwrotu: "lub przedstawiciel". Wówczas ust. 3 jest niepotrzebny i można go usunąć.	Uwaga nieuwzględniona.
364.	art. 17	Polska Izba Informatyki i Telekomunikacji	Artykuł 17 - Zapisy nie odnoszą się do przypadku świadczenia usługi cyfrowych na terenie RP, ale z infrastruktury umiejscowionej poza UE i obszarem EFTA.	Uwaga nieuwzględniona. Przepisy mają na celu harmonizację świadczenie usług cyfrowych przez dostawców usług cyfrowych na terytorium UE. Wskazują warunki kiedy taki usługodawca realizuje obowiązki wobec organu właściwego w RP.
365.	art. 17 ust. 1	Instytut Logistyki i Magazynowania	Operator usługi kluczowej a dostawca usług cyfrowych W art. 4 pkt.1 operatorów usług kluczowych i dostawców usług cyfrowych wymieniono wspólnie. Dlatego jeżeli intencją było ograniczenie dostawców usług cyfrowych wyłącznie do tych, którzy współpracują z operatorami usług kluczowych to z zapisów art.17 to nie wynika. Wg uzasadnienia do projektu, art. ten miał wskazywać jacy dostawcy będą uczestnikami krajowego systemu cyberbezpieczeństwa.	Uwaga częściowo uwzględniona. Nie było intencją projektodawcy ograniczenie dostawców usług cyfrowych wyłącznie do tych, którzy współpracują z operatorami usług kluczowych, dlatego dostawcy zostaną odrębnie wymienieni w art. 4 ust. 1.

			Zgodnie z zakresem obowiązków operator (art.12 ust.1) zgłasza incydent do właściwego CSIRT a dostawca (art.20 ust.1) do CSIRT NASK. Jeżeli operator i dostawca współpracują przy świadczeniu tej samej usługi to najprawdopodobniej będą pojawiać się powielone zgłoszenia incydentów i dodatkowo jest prawdopodobne, że trafią do różnych CSIRT. W art.19 ust.1 zapisano, że dostawca poza zgłoszeniem do CSIRT NASK informuje operatora usługi kluczowej o incydencie. Dlatego aby uniknąć powielania zgłoszeń (również różnego opisu incydentu) zgłoszenie powinien wykonać tylko operator (i jednocześnie koordynować jego dalszą obsługę również na poziomie dostawcy usługi).	
366.	art. 18. ust. 3	Związek Banków Polskich	Proponuje się usunięcie wyrazów: "….. w celu zapewnienia ciągłości tych usług", gdyż zapewnieni ciągłości działania jest jednym z elementów sieci i systemów informatycznych.	Uwaga nieuwzględniona. Zdaniem autorów projektu ustawy, zapis jest odpowiedni.
367.	art. 19	Związek Banków Polskich	Błędne jest założenie, że incydent związany ze świadczeniem usługi cyfrowej winien być zgłaszany wyłącznie do CSIRT NASK, gdyż usługa ta może mieć wpływ na funkcjonowanie operatorów usług kluczowych, których funkcjonowanie i ich incydenty będą zarządzane np. przez CSIRT MON lub CSIRT GOV. Poza tym budzi wątpliwość możliwość uzyskania przez CSIRT NASK uprawnień przysługujących CSIRT resortów siłowych. Inną kwestią jest założenie, że dostawcy usług cyfrowych mają raportować do CSIRT NASK wszystkie incydenty, włączając te, które zdarzyły się poza terytorium RP i nie mają wpływu na funkcjonowanie OUK świadczących swoje usługi na terytorium RP. To oznacza, że pozostałe przepisy art. 20-23 są wysoce ograniczone w stosowaniu.	Uwaga nieuwzględniona. Obecny podział właściwości wynika z ustaleń CSIRT poziomu krajowego.
368.	art.19. ust. 1	Polska Izba Informatyki i Telekomunikacji	Wymóg zgłaszania przez dostawców usług cyfrowych incydentów w 2 różnych państwach członkowskich UE doprowadziłby do wielu absurdów. Na przykład, zgodnie z tym obowiązkiem dostawca musiałby zgłaszać incydent, który miał wpływ na jednego	Uwaga nieuwzględniona. Z przepisu nie wynika obowiązek zgłaszania incydentu istotnego w dwóch państwach.

			użytkownika we Francji i jednego użytkownika w Polsce. Dodatkowo, obecne brzmienia nie rozróżnia różnego charakteru takich klientów, którzy mogą nie płacić, wykorzystywać usługi na próbę, oraz tego czy incydent miał wpływ na dane produkcyjne lub usługi. Uważamy, że ten przepis powinien koncentrować się na szkodach, a nie na liczbie państw członkowskich. Incydent może dotyczyć kilku państw członkowskich i nie mieć znaczącego wpływu na użytkowników, których to dotyczy.	Progi zgłaszanego incydentu istotnego będą wynikały z decyzji wykonawczej KE.
369.	art.19. ust. 4	Związek Banków Polskich	Proponuje się przepis w brzmieniu: "Zgłoszenie, o którym mowa, nie może narażać operatora usługi kluczowej na odpowiedzialność względem podmiotu przyjmującego zgłoszenie."	Uwaga nieuwzględniona. Zdaniem autorów projektu ustawy, zapis jest odpowiedni.
370.	art. 20 ust. 1 pkt 4	Związek Pracodawców Branży Internetowej IAB Polska	Zasadnicze wątpliwości budzi także czas, w jakim dostawcy usług cyfrowych są zobowiązani do zgłaszania incydentów. Zgodnie z art. 20 ust. 1 pkt 4 Projektu, dostawcy usług cyfrowych są obowiązani zgłaszać incydenty istotne niezwłocznie, nie później niż 24 godziny od wykrycia incydentu (analogiczny obowiązek dotyczy operatorów usług kluczowych). Ten przepis jest jednak niespójny z art. 33 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. (ogólne rozporządzenie o ochronie danych), który przewiduje 72 godziny na dokonanie zgłoszenia. Jednym z kluczowych argumentów za wydłużeniem tego terminu w stosunku do 24-godzinnego terminu przedstawionego w projekcie Komisji było umożliwienie podmiotom, u których wystąpiło naruszenie ochrony danych osobowych skupienia się na rozwiązaniu/obsłudze incydentu i zebraniu niezbędnych informacji. W kontekście relacji treści Projektu i przepisów dotyczących ochrony danych osobowych podkreślenia wymaga również, że przy obecnym brzmieniu Projektu, podmioty zobowiązane do zgłaszania incydentów będą zmuszone do przesyłania zgłoszeń do dwóch odrębnych organów – GIODO i NASK.	Uwaga nieuwzględniona. Niniejszy przepis jest zgodny z przepisami UE. Dyrektywa 2016/1148 daje możliwość regulacji tych przepisów w ustawodawstwie krajowym.

			Bardziej odpowiednim rozwiązaniem wydaje się zapewnienie możliwości dokonywania zgłoszeń w jednym miejscu, a organy mogłyby następnie dystrybuować otrzymane informacje między sobą.	
371.	art. 20	Polska Izba Informatyki i Telekomunikacji	Niespójność z RODO Zgodnie z Art. 20 ust 1. Pkt 4 dostawcy usług cyfrowych są obowiązani zgłaszać incydenty istotne niezwłocznie, nie później niż 24 godziny od wykrycia incydentu (analogiczny obowiązek dotyczy operatorów usługi kluczowej). Ten przepis jest niespójny w art. 33 RODO, który przewiduje 72 godziny na dokonanie zgłoszenia. Jednym z kluczowych argumentów za wydłużeniem tego terminu w stosunku do 24 godzinnego terminu przedstawionego w projekcie Komisji było umożliwienie podmiotom, u których wystąpiło naruszenie ochrony danych osobowych skupienia się na rozwiązaniu/obsłudze incydentu i zebraniu niezbędnych informacji.	Uwaga nieuwzględniona. Niniejszy przepis jest zgodny z przepisami UE. Dyrektywa 2016/1148 daje możliwość regulacji tych przepisów w ustawodawstwie krajowym.
372.	art. 20 ust. 1	Fundacja Bezpieczna Cyberprzestrzeń	Czy obowiązki te dotyczą operatorów dowolnie małych platform handlowych?	Wyjaśnienie. Dostawcy usług cyfrowych oraz internetowe platformy handlowe zostali zdefiniowani w ustawie. Incydenty istotne, które podlegają zgłaszaniu, zostaną określone w decyzji wykonawczej Komisji Europejskiej i to one będą de facto decydowały o wielkości zgłaszanego incydentu.
373.	art. 20 ust. 1	Instytut Logistyki i Magazynowania	Rejestrowanie incydentów Projekt zakłada opcjonalność zgłaszania incydentów zwykłych, należy jednak rozważyć zgłaszanie wszystkich incydentów (wszystkich klas). W efekcie wszystkie incydenty będą rejestrowane a analizy zagrożeń na poziomie CSIRT będą bazować na pełnych danych. Wg projektu incydenty zakwalifikowane przez uczestników	Wyjaśnienie. Projekt zakłada obsługę wszystkich incydentów. W ramach obsługi zawiera się rejestracja incydentów.

			jako zwykłe nie będą weryfikowane przez CSIR a wstępna kwalifikacja zwykłego incydentu może okazać się błędna. Jeżeli będą zgłaszane incydenty wszystkich klas, ich rejestrowanie będzie niepotrzebne ponieważ na liście funkcjonalności systemu teleinformatycznego jest rejestrowanie incydentów (art.42 ust.1), po co to robić dodatkowo poza tym systemem? Dzięki temu, utrzymywanie odrębnych rejestrów po stronie uczestników systemu nie będzie konieczne. Do czasu uruchomienia systemu teleinformatycznego (2021) uczestnicy będą rejestrowali incydenty samodzielnie jednak w obowiązkach podmiotu publicznego nie zapisano obowiązku rejestracji incydentów (tylko jego zgłoszenie).	
374.	art. 20 ust. 1 pkt 4	Izba Gospodarki Elektronicznej	Zgodnie z art. 20 ust. 1 pkt 4 dostawcy usług cyfrowych są obowiązani zgłaszać incydenty poważne niezwłocznie, nie później niż 24 godziny od wykrycia incydentu (analogiczny obowiązek dotyczy operatorów usługi kluczowej). Podkreślenia wymaga, że jest to czas zbyt krótki. Powoduje on, że podmiot zobowiązany zamiast skupić się na rozwiązaniu incydentu i usunięciu zagrożenia, musi skierować swoje zasoby do opracowania zgłoszenia incydentu. Trzeba zwrócić uwagę, że zagadnienie to było przedmiotem analizy również w trakcie prac nad rozporządzeniem Parlamentu Europejskiego i Rady 2016/679 tzw. RODO, którego art. 33 zobowiązuje administratorów do zgłaszania naruszeń w terminie 72 godzin. Termin ten został przedłużony w trakcie prac legislacyjnych, gdyż pierwotny projekt zakładał 24 godziny na dokonanie zgłoszenia. Argumentem, który o tym zadecydował było właśnie umożliwienie administratorowi skoncentrowania swoich zasobów na usuwaniu zagrożenia, a nie opracowywaniu zgłoszenia.	Uwaga nieuwzględniona. Niniejszy przepis jest zgodny z przepisami UE.
375.	art. 20 ust. 1 pkt 5	Fundacja Bezpieczna	Czy ten zapis informuje o konieczność obsługi incydentu istotnego oraz incydentu krytycznego we współpracy z CSIRT NASK?	Wyjaśnienie.

		Cyberprzestrzeń		Przepis zostanie zmieniony – będzie dotyczył tylko incydentu krytycznego.
376.	art. 21. ust. 2	Związek Banków Polskich	Brak delegacji ustawowej do przekazywania informacji prawnie chronionych (w ustawie o KSC oraz w ustawach sektorowych).	Wyjaśnienie. Zasady dostępu do tajemnic prawnie chronionych określone są w przepisach regulujących te tajemnice.
377.	art. 24	Polska Izba Informatyki i Telekomunikacji	Każda jednostka niezależnie od wielkości?	Wyjaśnienie. Przepis dotyczy wszystkich podmiotów określonych w art. 4 pkt 6-14 projektu ustawy.
378.	art. 24 ust. 1 i 2	Związek Banków Polskich	Przepis, który stanie się martwym przepisem lub wypełnianym tylko formalnie. Już teraz są TJS przymuszane do wyznaczania pełnomocników ds. cyberbezpieczeństwa, którymi są osoby nie mające kwalifikacji i doświadczenia w tym zakresie np. główni księgowi. W zamian powinno się rozważyć możliwość powoływania Lokalnych Zespołów Reagowania na Incydenty Komputerowe ad-hoc na poziomie powiatu lub wojewódzkim przy wsparciu odpowiedniego systemu teleinformatycznego. To zapewni efektywność oraz redukcję niczym nieuzasadnionych kosztów ponoszonych z budżetu JTS.	Wyjaśnienie. Przepisy zostały zmienione. JST będą zobowiązane do wyznaczenia osoby do kontaktu z podmiotami krajowego systemu cyberbezpieczeństwa. Ustawa nie nakłada obowiązku powoływania zespołów reagowania o zasięgu regionalnym lub lokalnym, ale nie uniemożliwia ich powoływania.
379.	art. 24 ust. 2	Fundacja Bezpieczna Cyberprzestrzeń	Czy słowo „mogą” w zapisie oznacza, że wyznaczenie osoby jest nieobowiązkowe?	Wyjaśnienie. Nie. Słowo „mogą” oznacza, że mogą powołać jedną osobę dla więcej niż jednej jednostki.
380.	art. 25	Instytut Kościuszki	Zakres obowiązków podmiotów publicznych zgodnie z projektem ustawy jest znacznie ograniczony w porównaniu do operatorów usług kluczowych. Z uwagi na wymogi konsolidacji krajowego systemu cyberbezpieczeństwa, trudno zrozumieć ratio legis takiego zabiegu. Co najmniej organy centralnej administracji rządowej powinny być zobowiązane do realizacji obowiązków przewidzianych w art. 10, art. 11 ust. 1 i ust. 3, art. 12 ust. 1 pkt 6 zd. 2, art. 13 oraz	Wyjaśnienie. Większość obowiązków dotyczących administracji zostało określonych w ustawie o informatyzacji i wydanych do nich przepisach wykonawczych (przywoływanym rozporządzeniu o Krajowych Ramami Interoperacyjności, minimalnych

			art. 14 projektu ustawy. W tym też kontekście należy jasno określić relacje pomiędzy ustawą o krajowym systemie cyberbezpieczeństwa a obowiązkami wynikającymi z ustawy o ochronie danych osobowych (np. art. 3 ust. 1, art. 39a), rozporządzeniem MSWiA w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych, jak i Krajowymi Ramami Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.	wymaganiach dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych), stąd nie ma uzasadnienia do regulowania tych kwestii na poziomie ustawy o krajowym systemie cyberbezpieczeństwa.
381.	art. 25	Fundacja Bezpieczna Cyberprzestrzeń	Art. 25. Podmioty publiczne, o których mowa w art. 4 pkt 6-14, są obowiązane: Czy podmioty publiczne nie mają obowiązku rejestrowania incydentów? Tak jak ma to miejsce w przypadku operatorów usług kluczowych (Art. 12 ust. 1 pkt. 2) i dostawców usług cyfrowych (Art. 20 ust. 1 pkt. 2).	Uwaga uwzględniona. Obowiązek dokumentowania obsługi incydentu przez podmioty publiczne zgodnie z art. 25 pkt. 3, zostanie ujednolicony z obowiązkami OUK i DUC.
382.	art. 25 pkt 8	Izba Gospodarcza Gazownictwa	Wątpliwości budzi tutaj użyte słowo „skutecznych”. Nie istnieją skuteczne sposoby zabezpieczenia się przed zagrożeniami, dlatego sugeruje się wskazanie sposobów zabezpieczeń przez właściwe organy ds. cyberbezpieczeństwa. Propozycja zapisu: Art. 25. Podmioty publiczne, o których mowa w art. 4 pkt 6-14, są obowiązane: 8)…i stosowanie skutecznych sposobów wskazanych przez właściwy organ zabezpieczania się przed tymi zagrożeniami.	Uwaga nieuwzględniona. Wskazane jest, aby działania tego typu były prowadzone zgodnie z zasadą należytej staranności. Wystarczające będzie, zgodnie z literalnym brzmieniem przepisu, podawanie adekwatnych i zrozumiałych informacji, dostosowanych do przeciętnego użytkownika i dotyczących danej usługi. Przykładowo, może to być przystępnie przedstawiona polityka bezpiecznych haseł, ogólne zasady bezpiecznego korzystania z serwisu przedsiębiorcy czy też wysyłanie ostrzeżeń antyphishingowych.
383.	art. 26	Związek Banków Polskich	Podmioty publiczne nie będą świadczyć usług kluczowych, a jedynie będą ich instytucjonalnymi użytkownikami końcowymi. W projekcie ustawy zawarte są przepisy oparte na błędnych przesłankach	Wyjaśnienie.

			związanych z klasyfikacją usług kluczowych świadczonych w sektorze publicznym na rzecz ich beneficjentów. Usługą kluczową w sektorze publicznym będzie udostępnienie np. rejestru PESEL, OUK będzie w tym przypadku COI w imieniu MC, a urzędy korzystające z tego rejestru będą tylko tzw. użytkownikami końcowymi.	Zgodnie z definicjami ustawowymi, większość usług publicznych o których mowa w uwadze nie będzie usługami kluczowymi. Stąd konieczność osobnej regulacji podmiotów publicznych, które nie będą operatorami usług kluczowych.
384.	art. 28.	A.K. (uwagi osoby prywatnej)	Słabo została opisana wzajemna interakcja pomiędzy NASK, ABW i MON. Tymczasem istotą systemu cyberbezpieczeństwa powinno być sprawne zdefiniowanie mechanizmów współpracy pomiędzy nimi. Istotą cyberbezpieczeństwa państwa jest właśnie globalne spojrzenie na całość sytuacji w zakresie cyber tak z wojskowego, wywiadowczego czy cywilnego punktu widzenia. Zagrożenia będą się przenikać.	Wyjaśnienie. Ustawa zostanie uzupełniona o przepisy dot. tzw. Kolegium do spraw Cyberbezpieczeństwa, celem ułatwienia współpracy pomiędzy NASK, ABW i MON. Dokładne opisanie mechanizmu współpracy nie jest materią, która powinna być regulowana w ustawie.
385.	art. 28.	A.K. (uwagi osoby prywatnej)	W rozumieniu Ustawy CSIRT NASK staje się w zasadzie służbą specjalną. Posiada szerokie uprawnienia kontrolne, i uprawnienia do wydawania wiążących poleceń technicznych. W tej sytuacji konieczne jest nazwanie CSIRT NASK adekwatnie do roli, jaką nadaje tej jednostce Ustawa, i traktowanie CSIRT NASK jak służby specjalnej ze wszystkimi tego konsekwencjami - w szczególności zakazem prowadzenia działalności komercyjnej w tym obszarze.	Wyjaśnienie. CSIRT NASK nie jest służbą specjalną, gdyż nie posiada typowych cech charakterystycznych dla takich podmiotów. Kompetencje są ograniczone do wąskiego kręgu odbiorców (operatorzy usług kluczowych i dostawcy usług cyfrowych) i dotyczą wąskiego zakresu spraw (cyberbezpieczeństwo wybranych usług). Brak też aparatu siłowego czy umocowań prawnych do prowadzenia czynności operacyjno-rozpoznawczych. Jest to wyspecjalizowany zespół do wsparcia obsługi incydentów u wybranych podmiotów, który ustawa wyposaża w narzędzia do sprawnego wykonywania zadań.
386.	art. 28. ust. 1	Związek Banków Polskich	Brak CSIRT sektorowych, które już istnieją i sprawnie koordynują obsługę cyberincydentów. Poza tym brak integratora – CSIRT	Uwaga częściowo uwzględniona.

			Narodowego, który zapewniałby spójny i kompleksowy system zarządzania ryzykiem w zakresie cyberbezpieczeństwa RP. 51	Projekt zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa CSIRT jest zarezerwowana dla zespołów poziomu krajowego.
387.	art. 28. ust. 2	Związek Banków Polskich	CSIRT MON, CSIRT NASK i CSIRT GOV realizują zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniają koordynację obsługi poważnych incydentów. W uzasadnionych przypadkach na wniosek operatorów usług kluczowych, dostawców usług cyfrowych lub właścicieli, posiadaczy samoistnych i zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, zapewniają im wsparcie w obsłudze lub obsługę poważnych incydentów. W jakim trybie jest realizowany przedmiotowy wniosek?	Uwaga nieuwzględniona. Przepisy są wystarczające.
388.	art. 28. ust. 3	Związek Banków Polskich	CSIRT MON, CSIRT NASK i CSIRT GOV powinny być zintegrowane w płaszczyźnie technologicznej, procesowej i ludzkiej. Taka integracja jest możliwa poprzez utworzenie tzw. CSIRT Narodowego, w którym powinni uczestniczyć przedstawiciele ww. CSIRT, CSIRT Policji, Prokuratury CSIRT sektorowych. Taki model integracji został już wdrożony - Centrum CAT - Centrum Antyterrorystyczne. Rolą CSIRT Narodowego winno być: 1) zapewnianie dynamicznej analizy dostępności usług kluczowych i usług cyfrowych oraz ich bezpieczeństwa; 2) monitorowanie, analizowanie i wykrywanie podatności, cyberzagrożeń i cyberincydentów oraz przyjmowanie zgłoszeń w tym zakresie; 3) udostępnianie informacji: a) CSIRT sektorowym oraz za ich pośrednictwem operatorom usług kluczowych i dostawcom usług cyfrowych – ostrzeżeń, alarmów oraz ogłoszeń dotyczących cyberzagrożeń oraz cyberincydentów, b)	Wyjaśnienie. Ustawa nie przewiduje powołania CSIRT Narodowego. Projekt zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa CSIRT jest natomiast zarezerwowana dla zespołów poziomu krajowego (CSIRT GOV, CSIRT MON, CSIRT NASK). Porównanie do CAT ABW i sugestia przełożenia modelu integracji wydaje się być nie do końca

			pojedynczemu punktowi kontaktowemu, organom właściwym oraz i CSIRT sektorowym wynikających z realizacji zadań, o których mowa w pkt. 1 i 2; c) Prokuraturze, Agencji Bezpieczeństwa Wewnętrznego oraz Policji, oraz w zakresie cyberzagrożeń i cyberincydentów noszących znamiona przestępstw, o których mowa w odrębnych przepisach; 4) współpraca z CSIRT sektorowymi i za ich pośrednictwem z operatorami usług kluczowych oraz dostawcami usług cyfrowych, a także z organami właściwymi, pojedynczym punktem kontaktowym w zakresie działań edukacyjnych użytkownika końcowego; 5) współpraca z CSIRT sektorowymi i za ich pośrednictwem z operatorami usług kluczowych oraz dostawcami usług cyfrowych, a także z organami właściwymi, pojedynczym punktem kontaktowym w zakresie działań szkoleniowych dla pracowników odpowiedzialnych za cyberbezpieczeństwo; 6) wspieranie w zakresie budowy i rozwoju potencjału CSIRT sektorowych; 7) realizacja prac badawczo-rozwojowych w obszarze cyberbezpieczeństwa; 8) udział w Sieci CSIRT.	właściwa z uwagi na właściwość CAT ABW. Rozwiązania przyjęte w projekcie ustawy dokładnie regulują zakres wzajemnego udostępniania informacji oraz ogólnej współpracy pomiędzy trzema CSIRT poziomu krajowego, a także tworzą Zespół ds. Incydentów Krytycznych jako organ pomocniczy w sprawach obsługi incydentów krytycznych.
389.	art. 28. pkt 2 i 3	Związek Banków Polskich	Przypisane zadania CSIRT NASK w przeważającej mierze powinny być powierzone CSIRT Narodowemu. Takie rozwiązanie zapewni efektywność podejmowanych działań przy jednoczesnej optymalizacji kosztów.	Uwaga nieuwzględniona. Projekt ustawy nie przewiduje tworzenie „CSIRT Narodowego”.
390.	art. 28. ust. 3	Związek Banków Polskich	Brakuje uprawnień ustawowych do wydawania przedsiębiorcom telekomunikacyjnym poleceń blokowania dostępu dla użytkowników internetu do serwerów, zidentyfikowanych jako niebezpieczne lub wręcz przestępcze. Jest to kluczowe działanie mające na celu zapewnienie ochrony zarówno operatorom usług kluczowych, pozostałym przedsiębiorcom jak i uzytkownikom końcowym - obywatelom RP;	Wyjaśnienie. Ustawa nie ustanawia nowych obowiązków dla przedsiębiorców telekomunikacyjnych.

391.	art. 28. ust. 3 pkt 7	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. należy określić organizację SPOC, np. w kwestii dostępności czy 24/24/7 czy 8/24/5	Wyjaśnienie. W opinii projektodawcy obecne przepisy są wystarczające.
392.	art. 28. ust. 3 pkt 7	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu: Jest: „przyjmowanie zgłoszeń o incydentach z innych państw, w tym państw członkowskich Unii Europejskiej, i dokonywanie dystrybucji tych informacji do pozostałych CSIRT i do Pojedynczego Punktu Kontaktowego;” Powinno być: „przyjmowanie zgłoszeń o incydentach z innych państw i dokonywanie dystrybucji tych informacji do pozostałych CSIRT i do Pojedynczego Punktu Kontaktowego;”	Uwaga nieuwzględniona. Zdaniem autorów projektu, obecny zapis jest właściwy.
393.	art. 28. ust. 3. pkt 14	Związek Banków Polskich	Proponuje się dodanie: 14) Wsparcie merytoryczne i techniczne w obsłudze incydentów	Uwaga nieuwzględniona. Postulowane zmiany będą dublować się z zapisami art. 28 ust. 3 pkt 6 i 10.
394.	art. 28. ust. 4	Instytut Logistyki i Magazynowania	Procedury postępowania Zapis o wspólnym opracowywaniu przez krajowe CSIRT procedur postępowania „w przypadku incydentu i wystąpienia ryzyka” należałoby uogólnić np. na procedury zgłaszania i obsługi incydentów. Wydaje się istotne aby zgłaszanie i obsługa incydentów po stronie pozostałych uczestników systemu (szczególnie operatorów, dostawców i podmiotów publicznych) również odbywała się w ujednolicony sposób. Dlatego krajowe CSIRT poza własnymi procedurami mogłyby opracować wytyczne do stworzenia odpowiednich procedur u innych (a przynajmniej wymienionych wyżej) uczestników.	Wyjaśnienie. Przepis zostanie doprecyzowany i będzie dotyczył głównych elementów procedur postepowania w przypadku incydentu, którego koordynacja obsługi będzie wymagała współpracy CSIRT.

395.	art. 28 ust. 5	Fundacja Bezpieczna Cyberprzestrzeń	Podpunkty 1) i 2) są niepotrzebnie rozdzielone, ponieważ 2) zawiera się w 1)	Uwaga nieuwzględniona. Art. 28 ust. 5 pkt 2 ma na celu stworzenie przepisu wyodrębniającego infrastrukturę krytyczną będącą w zarządzie MON (por. art. 28 ust. 7 pkt 12).
396.	art. 28 ust. 5 pkt 3	Polska Izba Informatyki i Telekomunikacji	W art. 28 ust 5 pkt. 3 należy doprecyzować zapis umieszczony w nawiasie poprzez dodanie roku 2001 – po zmianie zapis powinien brzmieć: Dz. U. 2001 poz. 1320.	Uwaga nieuwzględniona. Zapis jest poprawny.
397.	art. 28 ust. 5 pkt 3	Konfederacja Lewiatan	W art. 28 ust 5 pkt. 3 (str. 17) należy doprecyzować zapis umieszczony w nawiasie poprzez dodanie roku 2001 – po zmianie zapis powinien brzmieć: Dz. U. 2001 poz. 1320.	Uwaga nieuwzględniona. Zapis jest poprawny.
398.	art. 28. ust. 6	A.K. (uwagi osoby prywatnej)	Z projektu słabo wynika, jakiego typu wsparcie otrzymają podmioty zobowiązane do współpracy z NASK w przypadku masowego zdarzenia. Zwłaszcza, jeśli będą to zdarzenia przekraczające swoim zasięgiem infrastrukturę pojedynczego podmiotu. Powinno być powoływanie sztabów kryzysowych, wspólne analizy, koordynacja działań na szczeblu centralnym, realne wsparcie w rozwiązywaniu problemów.	Wyjaśnienie. Opis procedur postępowania w przypadku zaistnienia incydentu nie jest informacją właściwą do zawarcia w dokumencie o randze ustawy. Współpraca pomiędzy CSIRT poziomu krajowego jest regulowana chociażby w art. 28 ust. 1. Natomiast w przypadku incydentu, który może spowodować wystąpienie sytuacji kryzysowej w rozumieniu stosownej ustawy, zastosowanie mają zapisy art. 36 projektowanej ustawy. W związku z wystąpieniem wyżej opisanej sytuacji, zapisy ustawy umożliwiają powołanie ciała koordynacyjno-analitycznego na szczeblu centralnym, w postaci Zespołu ds. Incydentów Krytycznych.
399.	art. 28. ust. 6 [jednostka red.	Związek Banków Polskich	Proponowany zapis nie sankcjonuje istnienia i działania CSIRT sektorowych.	Wyjaśnienie. Projekt zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe

	błędnie określona jako art. 28. pkt 6]			podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa CSIRT jest natomiast zarezerwowana dla zespołów poziomu krajowego (CSIRT GOV, CSIRT MON, CSIRT NASK).
400.	art. 28. ust. 6. pkt 1	Związek Banków Polskich	Przypisane zadania CSIRT NASK w przeważającej mierze powinny być powierzone CSIRT Narodowemu. CSIRT NASK nie będzie mógł zarządzać incydentami, gdyż nie będzie miał dostępu do najważniejszych systemów IT OUK i DUK, może jedynie podjąć próbę obsługi incydentu ale takie uprawnienia powinny przysługiwać i tak naprawdę już przysługują ABW i Policji i to ich CSIRT'y powinny realizować te zadania. Ponadto NASK nie ma prerogatyw do przetwarzania informacji prawnie chronionych.	Uwaga nieuwzględniona. Projekt ustawy nie przewiduje tworzenie „CSIRT Narodowego”.
401.	art. 28 ust. 6 pkt 3a	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Wnosimy o zmianę art. 28 ust. 6 pkt 3a oraz dodanie nowego pkt 3d: „3a. Prowadzi analizy złośliwego oprogramowania, funkcji ukrytych w systemach mikroelektronicznych oraz analizy podatności technicznych” „3d) zapewnia krajowe rozwiązania systemowe mające na celu podnoszenie bezpieczeństwa sprzętowych mikroelektronicznych komponentów systemów teleinformatycznych”. Naszym zdaniem Projekt obok zagadnień związanych z organizacją i oprogramowaniem winien odnieść się do kluczowego znaczenia sprzętu i podzespołów mikroelektronicznych dla bezpieczeństwa wszelkich systemów działających w cyberprzestrzeni. Stąd propozycja rozszerzenia definicji „cyberbezpieczeństwa” oraz zmiany postanowień w art. 28 Projektu. Zaniechanie takich działań spowoduje, że w obszarach kluczowych, w tym obronności, energetyki itp., rzeczywiste zabezpieczenie będzie niekompletne.	Uwaga nieuwzględniona. Nie ma potrzeby zawężania zakresu działalności tylko do systemów mikroelektronicznych oraz analizy podatności technicznych. Obecna treść art. 28 ust. 6 pkt 3 lit a pozwala prowadzić analizy także we wskazanym w uwadze zakresie.
402.	art. 28 ust. 7 pkt 12	Polska Izba Informatyki i	W art. 28 ust. 7 pkt 12 po wyrazie „podmioty”, dodać „z wyłączeniem przedsiębiorców telekomunikacyjnych” –	Uwaga nieuwzględniona. W art. 4 nie zostanie wykreślony pkt 5.

		Telekomunikacji	uzasadnienie: wprowadzić tę zmianę, gdy w art. 4 wykreślony zostanie pkt 5.	
403.	art. 28. ust. 8	Związek Banków Polskich	Brak określenia nadrzędnej roli któregoś z CSIRT będzie skutkował sporami kompetencyjnymi i w skrajnym przypadku nie będzie porozumienia kto ma koordynować dany incydent (jeżeli nie będzie jasno przypisany do któregoś z CSIRT). Dlatego tak ważne jest powołanie CSIRT Narodowego jako integratora.	Wyjaśnienie. Projekt ustawy nie przewiduje tworzenie „CSIRT Narodowego”.
404.	art. 28. ust. 8	Fundacja Bezpieczna Cyberprzestrzeń	Być może warto w tym zapisie podkreślić, iż zgłoszenie do właściwe CSIRT powinno być niezwłoczne.	Uwaga uwzględniona.
405.	art. 28. ust. 10	Związek Banków Polskich	Realizacja przedmiotowego przepisu wydaje się być niemożliwa, gdyż nie ma prawnej możliwości delegowania uprawnień wynikających np. z ustawy o AW i ABW w zakresie zadań określonych w art. 5 ust. 1 oraz ustawy o Policji w zakresie zadań określonych w art. 1 ust. 2.	Wyjaśnienie. Powierzenie realizacji zadań, o którym mowa w art. 28 ust. 10 nie dotyczy zadań ustawowych tych służb.
406.	art. 28 ust. 10 i 11	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Wątpliwości natury konstytucyjnej budzą art. 28 ust. 10 i 11 Projektu, które dopuszczają drogą aktów wewnętrznych publikowanych w Dziennikach Urzędowych poszczególnych organów modyfikacje przepisów rangi ustawowej. Przepisy te stanowią naruszenie hierarchii źródeł prawa w Polsce i stwarzają niepewność wśród podmiotów zobowiązanych ustawą co do tego, pod które CSIRT właściwie podlegają.	Wyjaśnienie. Porozumienia pozwalają na przekazywanie wykonywania zadań w stosunku do niektórych podmiotów innemu CSIRT, gdyby zaszła taka potrzeba.
407.	art. 28. ust. 11	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy następujące brzmienie: „Porozumienia, o których mowa w ust. 10, są ogłaszane w przypadku przejęcia zadań realizowanych dotychczasowo przez (…).” Art. 28 ust. 11 – oczywista pomyłka pisarska – jest: Porozumienia, o których mowa w ust. 8, są ogłaszane w przypadku przejęcia zadań realizowanych dotychczasowo przez (…) a powinno	Uwaga uwzględniona.

			być Porozumienia, o których mowa w ust. 10, są ogłaszane w przypadku przejęcia zadań realizowanych dotychczasowo przez (…).	
408.	art. 29	A.K. (uwagi osoby prywatnej)	Zaproponowana ustawa słabo koresponduje ze stanami w jakich może znajdować się państwo. Próba przeanalizowania działania tego projektu np. w sytuacji wojny, albo cyberataku paraliżującego normalne funkcjonowanie państwa byłaby świetnym ćwiczeniem. W pierwszym przypadku rolę wiodącą i sprawczą powinien przejmować MON, w drugim jednostką wiodącą powinno być ABW, w stanie normalnym jednostką wiodącą powinna być jednostka tu tymczasowo nazwana CSIRT NASK (o NASK w dalszej części). Tymczasem z projektu to nie wynika.	Wyjaśnienie. Ustawa nie ingeruje w obowiązujące przepisy dotyczące stanów nadzwyczajnych (w tym wojny) czy podstawowych kompetencji wynikających z ustawy o działach administracji rządowej. Ministrowie zachowują swoje zadania wynikające z poszczególnych ustaw.
409.	art. 29 ust. 3	Polska Izba Informatyki i Telekomunikacji	W art. 29 ust 3 wskazano błędna datę ustawy o stanie wojennym – zamiast 22 sierpnia 2002 r. należy wpisać datę 29 sierpnie 2002 r.	Uwaga uwzględniona.
410.	art. 29 ust. 3	Konfederacja Lewiatan	W art. 29 ust 3 (str. 19) wskazano błędna datę ustawy o stanie wojennym – zamiast 22 sierpnia 2002 r. należy wpisać datę 29 sierpnie 2002 r.	Uwaga uwzględniona.
411.	art. 30.	Związek Banków Polskich	To powinny być kompetencje CSIRT Narodowego.	Wyjaśnienie. Projekt ustawy nie przewiduje tworzenie „CSIRT Narodowego”.
412.	art. 30. ust. 1.	Fundacja Bezpieczna Cyberprzestrzeń	Powinno być: „jeśli może mieć on istotny”	Uwaga nieuwzględniona. Przepis wynika z treści art. 14 dyrektywy 2016/1148. Rozszerzenie jego zakresu nie jest konieczne.
413.	art. 30. ust. 2.	Związek Banków Polskich	Proponuje się przepis ust. 2 w brzmieniu: "2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV przekazuje, jeśli pozwalają na to okoliczności, zgłaszającemu operatorowi usługi kluczowej	Wyjaśnienie. Przepis zostanie przeredagowany.

			informacje dotyczące działań następczych jego zgłoszenia, które mogłyby pomóc w obsłudze danego incydentu.".	
414.	art. 31 ust. 2	Business Centre Club	Z kolei art. 31 ust 2 Projektu przewiduje możliwość przekazania do publicznej wiadomości, informacji o poszczególnych incydentach lub zobowiązać do tego dostawcę usług cyfrowych, w przypadku gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę trwającego incydentu albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym. Możliwość podania tej informacji do publicznej wiadomości powinna ograniczać się do informacji przydatnych innym firmom lub instytucjom do obrony. Podawanie nazwy podmiotu, którego dotyczy incydent nie jest potrzebne do tego celu. Relacja pomiędzy członkami krajowego systemu cyberbezpieczeństwa powinna opierać się na zaufaniu. Ryzyko upublicznienia takiej informacji może zniechęcać firmy do zgłaszania incydentów.	Wyjaśnienie. CSIRT NASK może przekazać informacje do publicznej wiadomości zgodnie z zapisami projektowanego przepisu – w przypadku gdy jest to niezbędne i po uprzedniej konsultacji z dostawcą usług cyfrowych, który zgłosił dany incydent.
415.	art. 31 ust. 2	Izba Gospodarki Elektronicznej	Artykuł przewiduje możliwość przekazania do informacji publicznej informacji o poszczególnych incydentach lub zobowiązać do tego dostawcę usług cyfrowych, w przypadku gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę trwającego incydentu albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym. Możliwość podania tej informacji do wiadomości publicznej powinna ograniczać się do informacji przydatnych innym podmiotom lub instytucjom do obrony. Podawanie nazwy podmiotu, którego dotyczy incydent nie jest potrzebne do realizacji tego celu. Relacja pomiędzy członkami Krajowego Systemu Cyberbezpieczeństwa powinna opierać się na zaufaniu. Ryzyko upublicznienia takiej informacji może zniechęcać spółki do zgłaszania incydentów.	Wyjaśnienie. CSIRT NASK może przekazać informacje do publicznej wiadomości zgodnie z zapisami projektowanego przepisu – w przypadku gdy jest to niezbędne i po uprzedniej konsultacji z dostawcą usług cyfrowych, który zgłosił dany incydent.

416.	art. 31 ust. 2	Polska Izba Informatyki i Telekomunikacji	Art. 31. ust 2 przewiduje możliwość przekazania do informacji publicznej informacji o poszczególnych incydentach lub zobowiązać do tego dostawcę usług cyfrowych, w przypadku, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę trwającego incydentu albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym. Możliwość podania tej informacji do wiadomości publicznej powinna ograniczać się do informacji przydatnych innym firmom lub instytucjom do obrony. Podawanie nazwy podmiotu, którego dotyczy incydent nie jest potrzebne do tego celu. Relacja pomiędzy członkami Krajowego Systemu Cyberbezpieczeństwa powinna opierać się na zaufaniu. Ryzyko upublicznienia takiej informacji może zniechęcać firmy do zgłaszania incydentów.	Wyjaśnienie. CSIRT NASK może przekazać informacje do publicznej wiadomości zgodnie z zapisami projektowanego przepisu – w przypadku gdy jest to niezbędne i po uprzedniej konsultacji z dostawcą usług cyfrowych, który zgłosił dany incydent.
417.	art. 31 ust. 2	Związek Pracodawców w Branży Internetowej IAB Polska	Z kolei art. 31 ust 2 Projektu przewiduje możliwość przekazania do publicznej wiadomości, informacji o poszczególnych incydentach lub zobowiązać do tego dostawcę usług cyfrowych, w przypadku gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę trwającego incydentu albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym. Możliwość podania tej informacji do publicznej wiadomości powinna ograniczać się do informacji przydatnych innym firmom lub instytucjom do obrony. Podawanie nazwy podmiotu, którego dotyczy incydent nie jest potrzebne do tego celu. Relacja pomiędzy członkami krajowego systemu cyberbezpieczeństwa powinna opierać się na zaufaniu. Ryzyko upublicznienia takiej informacji może zniechęcać firmy do zgłaszania incydentów.	Wyjaśnienie. CSIRT NASK może przekazać informacje do publicznej wiadomości zgodnie z zapisami projektowanego przepisu – w przypadku gdy jest to niezbędne i po uprzedniej konsultacji z dostawcą usług cyfrowych, który zgłosił dany incydent.
418.	art. 31. ust. 2.	Związek Banków Polskich	Propozycja ta budzi następujące wątpliwości: a) Czy Operator usługi kluczowej będzie informowany o przekazaniu przed przekazaniem informacji do publicznej wiadomości? b) Czy Operator usługi kluczowej będzie miał wpływ na treść komunikatu?	Wyjaśnienie. Zgodnie z projektowanym przepisem, przekazanie informacji nastąpi po konsultacji z danym dostawcą usługi kluczowej.

419.	art. 31 ust. 3 [w piśmie z uwagami błędnie oznaczone jako art. 32 ust. 3]	Fundacja Bezpieczna Cyberprzestrzeń	Powinno być: „organy właściwe”.	Wyjaśnienie. Przepis został usunięty.
420.	art. 32. ust. 1	Związek Banków Polskich	Błędne odwołanie do art. 24 ust. 2-7 - brak ustępów 3-7. Przez to brak możliwości odniesienia się do tej propozycji przepisu.	Uwaga uwzględniona. Odesłanie otrzyma brzmienie: w obszarze zadań realizowanych przez CSIRT zgodnie z art. 28 ust. 2-7.
421.	art. 33. ust. 3	Związek Banków Polskich	W zaproponowanym przepisie wskazano możliwość zgłoszenia incydentu przez osoby fizyczne do CSIRT NASK. Wskazano również kolejność obsługi zgłoszonych incydentów, pierwszeństwo mają incydenty zgłoszone przez OUK i to nie budzi wątpliwości. Jednak niewłaściwym rozwiązaniem jest wprowadzenie warunkowego rozpatrzenia zgłoszenia o ile "nie stanowi to nieproporcjonalnego czy nadmiernego obciążenia dla CSIRT NASK".Taka możliiwość budzi wątpliwości skąd na wstępnym etapie zgłoszenia incydenu CSIRT NASK będzie miał wiedzę o jego skali i istotności. Przepis ten jest zgody z Dyrektywą NIS, w której w art. 9 ust. 2 - Państwa członkowskie zapewniają, aby CSIRT miały odpowiednie zasoby w celu skutecznej realizacji swoich zadań określonych w załączniku I pkt 2, a więc m. in. (iii) reagowanie na incydenty. Ponadto klasyfikacja i prioretyzacja powinny odbywać się na początku, w równym stopniu dla każdego zgłoszonego incydentu, niezależnie z jakiego źródła pochodzi. Może się bowiem okazać że incydent	Uwaga nieuwzględniona. Zapis jest zgodny z dyrektywą 2016/1148.

			sektorowy może być poważniejszy niż zgłoszone w tym czasie incydenty dotyczące usług kluczowych.	
422.	art. 33. ust. 3	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy zmianę zapisu - jest: „Zgłoszenia, o których mowa w ust. 1, mogą zostać rozpatrzone, gdy nie stanowi to nieproporcjonalnego czy nadmiernego obciążenia dla CSIRT NASK. Zgłoszenia takie nie mogą skutkować nałożeniem na zgłaszającego dodatkowych obowiązków.” Powinno być „Zgłoszenia, o których mowa w ust. 1, mogą zostać rozpatrzone, gdy nie stanowi to nieproporcjonalnego czy nadmiernego obciążenia dla CSIRT NASK. Zgłoszenia takie nie skutkują nałożeniem na zgłaszającego dodatkowych obowiązków.”	Uwaga uwzględniona.
423.	art. 34	Pracodawcy RP	- Uprawnienia CSIRT określone w projektowanym art. 34 mogą skutkować naruszeniem regulacji związanych z ochroną tajemnicy telekomunikacyjnej oraz rozporządzenia RODO. - Projektowany art. 34 ust. 2 został określony w sposób zbyt ogólny i wymaga doprecyzowania poprzez wskazanie zamkniętego katalogu uprawnień, tak aby wskazać jasne ramy działania CSIRT-ów. - Należy wprowadzić mechanizm niezależnej, np. sądowej kontroli nad możliwością żądania od przedsiębiorców dokonania określonych, potencjalnie kosztownych czynności (ust. 3 - usuwanie podatności). Należy również wprowadzić mechanizm odwoławczy od takich władczych rozstrzygnięć. - Postulujemy doprecyzowanie, że obowiązek przekazania informacji CSIRT nie dotyczy informacji prawnie chronionych.	Uwaga częściowo uwzględniona. Projekt uzupełniono, wskazując iż w przypadkach przekazywanie informacji, działania te nie mogą naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych, a także przepisów o ochronie danych osobowych. Nie jest planowane wdrożenie mechanizmu niezależnej kontroli i odwoławczego. Tego typu mechanizmy opóźnią działanie, które ma mieć charakter nagły i doraźny.
424.	art. 34	Polska Izba Informatyki i Telekomunikacji	Postulujemy doprecyzowanie, że obowiązek przekazania informacji CSIRT nie dotyczy informacji prawnie chronionych. Projektowany art. 34 ust. 2 został określony w sposób zbyt ogólny i wymaga doprecyzowania poprzez wskazanie zamkniętego katalogu uprawnień. W swoim aktualnym brzmieniu umożliwiałby CSIRT	Wyjaśnienie. Projekt uzupełniono, wskazując iż w przypadkach przekazywanie informacji, działania te nie mogą naruszać przepisów o ochronie informacji niejawnych

			wręcz nieograniczony zakres działań, w tym np. możliwość instalowania w sieci służącej świadczeniu publicznych usług telekomunikacyjnych i będącej własnością komercyjnego podmiotu, własnych urządzeń telekomunikacyjnych CSIRT, które pozostawałyby poza kontrolą właściciela tej sieci. Takie potencjalne działania skutkowałyby brakiem możliwości spełnienia przez operatora jego podstawowych obowiązków, np. w zakresie ochrony tajemnicy telekomunikacyjnej. Projektowany art. 34 ust. 3 w zakresie obowiązku usunięcia podatności w wyznaczonym przez właściwy organ terminie może oznaczać konieczność poniesienia wysokich kosztów oraz istotnej przerwy w świadczeniu podstawowej usługi. Dodatkowo może naruszać zasadę adekwatności zabezpieczeń w stosunku do ryzyk i w ten sposób ingerować w model biznesowy operatorów telekomunikacyjnych. Podsumowując uprawnienia CSIRT określone w projektowanym art. 34 mogą skutkować naruszeniem regulacji związanych z ochroną tajemnicy telekomunikacyjnej oraz rozporządzenia RODO, a także duplikują istniejący mechanizm, który funkcjonuje dla służb ochrony państwa. Co więcej nie przewidziano żadnej niezależnej kontroli państwa nad tymi żądaniami, a w szczególności nie ma możliwości odwołania się od decyzji CSIRT, podczas gdy nawet dla działań ABW niezbędna jest zgoda sądu, a więc zapewnione są mechanizmy kontrolne przed nadużyciami uprawnień.	oraz innych tajemnic prawnie chronionych, a także przepisów o ochronie danych osobowych.
425.	art. 34	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Odnosząc się do przepisu art. 34 Projektu, dotyczącego uprawnień CSIRT wskazać należy na szczątkowość tej regulacji. Wydaje się, że powinna zostać ona stworzona na wzór przepisów art. 11 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych oraz art. 32a-32d ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Obecne brzmienie projektowanego przepisu będzie budziło wątpliwości co do tego, które działania podejmowane przez CSIRT są legalne, a które	Wyjaśnienie. Projekt uzupełniono, wskazując iż w przypadkach przekazywanie informacji, działania te nie mogą naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych, a także przepisów o ochronie danych osobowych.

			zabronione. W szczególności niejasna jest procedura opisana w art. 27 ust. 2 oraz 3 Projektu – nie jest jasne co będzie się działo w przypadku odmowy usunięcia wskazanych podatności lub przekazania odpowiednich informacji oraz kto będzie odpowiedzialny za ewentualną szkodę powstałą na skutek realizacji zaleceń CSIRT. Te same zarzuty braku precyzji podnieść należy w stosunku do brzmienia art. 42 ust. 6 - 9 Projektu, dotyczącego przetwarzania danych osobowych.	Przepisy dotyczące ochrony danych osobowych zostaną przebudowane.
426.	art. 34	Konfederacja Lewiatan	Postulujemy doprecyzowanie, że obowiązek przekazania informacji CSIRT nie dotyczy informacji prawnie chronionych. Projektowany art. 34 ust. 2 został określony w sposób zbyt ogólny i wymaga doprecyzowania poprzez wskazanie zamkniętego katalogu uprawnień. W swoim aktualnym brzmieniu umożliwiałby CSIRT wręcz nieograniczony zakres działań, w tym np. możliwość instalowania w sieci służącej świadczeniu publicznych usług telekomunikacyjnych i będącej własnością komercyjnego podmiotu, własnych urządzeń telekomunikacyjnych CSIRT, które pozostawałyby poza kontrolą właściciela tej sieci. Takie potencjalne działania skutkowałyby brakiem możliwości spełnienia przez operatora jego podstawowych obowiązków, np. w zakresie ochrony tajemnicy telekomunikacyjnej Projektowany art. 34 ust. 3 w zakresie obowiązku usunięcia podatności w wyznaczonym przez właściwy organ terminie może oznaczać konieczność poniesienia wysokich kosztów oraz istotnej przerwy w świadczeniu podstawowej usługi. Dodatkowo może naruszać zasadę adekwatności zabezpieczeń w stosunku do ryzyk i w ten sposób ingerować w model biznesowy operatorów telekomunikacyjnych. Podsumowując uprawnienia CSIRT określone w projektowanym art. 34 mogą skutkować naruszeniem regulacji związanych z ochroną tajemnicy telekomunikacyjnej oraz rozporządzenia RODO, a także duplikują istniejący mechanizm, który funkcjonuje dla służb ochrony	Wyjaśnienie. Projekt uzupełniono, wskazując iż w przypadkach przekazywanie informacji, działania te nie mogą naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych, a także przepisów o ochronie danych osobowych.

			państwa. Co więcej nie przewidziano żadnej niezależnej kontroli państwa nad tymi żądaniami, a w szczególności nie ma możliwości odwołania się od decyzji CSIRT, podczas gdy nawet dla działań ABW niezbędna jest zgoda sądu, a więc zapewnione są mechanizmy kontrolne przed nadużyciami uprawnień.	
427.	art. 34	A.K. (uwagi osoby prywatnej)	Uprawnienia CSIRT w zakresie pozyskiwania od operatora informacji (art. 34) - Należy zaznaczyć wyraźnie w ustawie, że obowiązek przekazania informacji CSIRT nie dotyczy informacji prawnie chronionych. Art. 34 ust. 2 ze względu na swoje niedodefiniowanie może oznaczać, że CSIRT NASK jest uprawniony do wstawiania własnych urządzeń do naszej sieci i podsłuchiwania naszych klientów lub ingerowania w nasze usługi np. wyłączenie routera. Art. 34 ust. 3 w zakresie usunięcia podatności w wyznaczonym przez organ właściwy terminie może bardzo często oznaczać wysokie koszty oraz istotną przerwę w świadczeniu usługi; dodatkowo może naruszać zasadę adekwatności zabezpieczeń w stosunku do ryzyk i w ten sposób ingerować w model biznesowy operatorów telekomunikacyjnych. Uprawnienie CSIRT z art. 34 może skutkować naruszeniem regulacji związanych z ochroną tajemnicy telekomunikacyjnej oraz rozporządzenia RODO; duplikuje istniejący mechanizm, który już działa dla służb ochrony państwa; nie przewidziano żadnej niezależnej kontroli państwa nad tymi żądaniami, nie ma możliwości odwołania się od decyzji CSIRT (dla działań ABW musi być zgoda sądu czyli są mechanizmy kontrolne przed nadużyciami uprawnień).	Wyjaśnienie. Projekt uzupełniono, wskazując iż w przypadkach przekazywanie informacji, działania te nie mogą naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych, a także przepisów o ochronie danych osobowych.
428.	art. 34. ust. 1	Związek Banków Polskich	Jakie działania techniczne mogą realizować CSIRTy, tj.. co się wiąże z tymi działaniami? Monitoring ruchu w sieci? Pozyskiwanie danych z korespondencji? Nie sa jasne jakie działania techniczne mogę podejmować CSIRTy - przepis nie jest ostry, może rodzić wątpliwości interpetacje.	Wyjaśnienie. Przepis zostanie przeredagowany.

429.	art. 34. ust. 2	Fundacja Bezpieczna Cyberprzestrzeń	O jakich czynnościach specjalistycznych jest tu mowa?	Wyjaśnienie. Przepis zostanie przeredagowany.
430.	art. 34. ust. 3	Fundacja Bezpieczna Cyberprzestrzeń	Czy nie powinno to dotyczyć również operatorów telekomunikacyjnych?	Wyjaśnienie. Ustawa nie wprowadza obowiązków dla przedsiębiorców telekomunikacyjnych.
431.	art. 34. ust. 3	Związek Banków Polskich	Termin oraz działania powinny być wypracowane w drodze uzgodnień Stron.	Wyjaśnienie. Zgodnie z treścią projektowanego przepisu, usuwanie podatności powinno nastąpić w czasie obsługi incydentu. Przepis zostanie przeredagowany.
432.	art. 34. ust. 3	Instytut Logistyki i Magazynowania	Jeżeli wezwanie do usunięcia podatności ma dotyczyć incydentów poważnych to tym bardziej powinno również dotyczyć incydentów krytycznych.	Uwaga uwzględniona.
433.	art. 34. ust. 4	Związek Banków Polskich	Proponuje się po wyrazach "obsługi incydentu" dodanie zwrotu: "przy zachowaniu udostępnionych informacji technicznych w poufności". Należy wskazać, co dzieje się w przypadku, kiedy zakres informacji, o które występuje podmiot CSIRT nie może być udostępniony (z przyczyn technicznych lub braku posiadania takich danych) przez operatora usługi kluczowej lub dostawcę usługi cyfrowej. Jak ustawodawca zabezpieczy dane objęte tajemnicą, np. bankową?	Wyjaśnienie. Projekt uzupełniono, wskazując iż w przypadkach przekazywanie informacji, działania te nie mogą naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych, a także przepisów o ochronie danych osobowych.
434.	art. 34. ust. 4	Związek Banków Polskich	Takie zapytania powinny być skoordynowane w ramach CSIRT Narodowego. Przepis jest nieprecyzyjny - wynika z niego, że każdy z wymienionych CSIRT może wystąpić do każdego OUK (a chyba nie taka była intencja). W skrajnej sytuacji może doprowadzić do zmultiplikowania działań informacyjnych na rzecz wielu CSIRT'ów.	Wyjaśnienie. Projekt ustawy nie przewiduje tworzenie „CSIRT Narodowego”.

435.	art. 34. ust. 5	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 34 ust. 5 – dotyczy współpracy z organami ścigania. Przy braku definicji „podmiotu świadczącego usługi z zakresu cyberbezpieczeństwa" (z ustawy nie wynika że jest to pojęcie równoznaczne z OUK) współpracę z organami ścigania podejmują jedynie CSIRT MON, CSIRT NASK i CSIRT GOV oraz podmioty zewnętrze świadczące usługi o których jest wzmianka w art. 15.ust 2. W razie istnienia w OUK własnych struktur odpowiedzialnych za cyberbezpieczeństwo, OUK nie współpracuje z organami ścigania.	Uwaga nieuwzględniona. Zapis art. 34 ust. 5 odnosi się do zadań CSIRT, których dotyczy rozdział V projektowanej ustawy. Nie dotyczy on podmiotów świadczących usługi z zakresu cyberbezpieczeństwa, operatorzy usług kluczowych, dostawcy usług cyfrowych i inne podmioty, współpracują z organami ścigania na zasadach ogólnych i na podstawie odrębnych przepisów, np. art. 15 § 2 i 3 KPK. Nie ma potrzeby dodatkowej regulacji tej problematyki.
436.	art. 35	Związek Banków Polskich	Brakuje przepisu pozwalającego na przekazywanie do wskazanych w ustawie jednostek (głównie CSIRT) informacji stanowiącej tajemnicę bankową – analogicznie do danych osobowych, opisanych w art. 35.	Uwaga nieuwzględniona. Zasady dostępu do informacji zawierających tajemnice prawnie chronione określone są w przepisach regulujących te tajemnice.
437.	art. 35	Związek Banków Polskich	1. Brak przesłanek do nadania takich uprawnień dyrektorowi RCB, które zajmuje się zarządzaniem kryzysowym i infrastrukturą krytyczną. 2. Biorąc pod uwagę, że CSIRT MON, CSIRT NASK i CSIRT GOV de facto będą obsługiwać incydenty, informacje takie powinny przekazywać do OUK w celu przeprowadzenia stosownych analiz. Analizy takie w chwili obecnej przeprowadzają również CSIRT sektorowe. 3. Cel przepisu - w przypadkach przestępstwa lub uzasadnionego podejrzenia popełnienia przestępstwa dokonywanego na szkodę operatora usług kluczowych lub dostawcy usług cyfrowych i ich klientów, w celu i zakresie niezbędnym do zapobiegania temu przestępstwu lub jego ścigania, a także w celu obsługi cyberincydentów.	Uwaga częściowo uwzględniona. Co do zasady nie przewiduje się przetwarzania danych wrażliwych, jednak może dojść do sytuacji, że w czasie obsługi incydentu dojdzie do takiej sytuacji. Dla przykładu - w przypadku sektora ochrony zdrowia może dojść do przetwarzania danych pacjentów, które wyciekły w czasie incydentu. CSIRT nie będą obsługiwać incydentów, a wspierać i koordynować ich obsługę. Przepisy zostaną doprecyzowane w tym zakresie. Przepisy niniejszego projektu nie regulują kwestii karnych.

			4. Katalog podmiotów uprawnionych do gromadzenia, przetwarzania, przechowywania i udostępniania ww. informacji powinien być rozszerzony m. in. o: OUK, DUC, CSIRT Narodowego, CSIRT sektorowe. 5. Zakres informacji to informacje prawnie chronione, czyli informacje niejawne w rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, inne tajemnice ustawowo chronione, dane osobowe w rozumieniu ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz rozporządzenia Parlamentu i Rady Europejskiej w sprawie ochrony danych osobowych. 6. Należy zaznaczyć, że ze względu na cel pozyskiwania ww. informacji przepisów art. 24, 25 i 33 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych nie stosuje się.	Operatorzy usług kluczowych i dostawcy usług kluczowych będą upoważnieni do przetwarzania takich informacji na zasadach ogólnych. Informacje, o których mowa w art. 9 rozporządzenia 2016/679 (tzw. RODO) to dane wrażliwe, a nie informacje prawnie chronione czy też informacje niejawne. Projekt zostanie uzupełniony o przepis dopuszczający możliwość powoływania przez organy właściwe podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla danego sektora. Nazwa CSIRT jest zarezerwowana dla zespołów poziomu krajowego.
438.	art. 35. ust. 2.	Związek Banków Polskich	Proponuje się dodanie słowa "wyłącznie": "2. CSIRT MON, CSIRT NASK i CSIRT GOV mogą wymieniać się danymi, o których mowa w ust. 1, wyłącznie w zakresie niezbędnym do realizacji zadań określonych w ustawie."	Uwaga nieuwzględniona. Zapis zaproponowany przez autorów projektu ustawy nie pozostawia CSIRT innej alternatywy dla wymiany danych poza wymianą w zakresie niezbędnym do realizacji zadań określonych w ustawie.
439.	art. 36. ust. 5	Fundacja Bezpieczna Cyberprzestrzeń	Zamiast „przekazywanie informacji przyczyni się” (czego nie wiemy), powinno być ewentualnie: „istnieje przekonanie, że przekazanie informacji przyczyni się do (…)”	Uwaga nieuwzględniona.
440.	art. 36. ust. 5	Związek Banków Polskich	Proponuje się ust 5 w brzmieniu: 5. CSIRT MON, CSIRT NASK i CSIRT GOV mogą przekazywać, po konsultacji z OUK lub DUC zaangażowanymi w obsługę incydentu, do publicznej wiadomości informacje o incydentach, oraz o zagrożeniach, w niezbędnym zakresie, o ile przekazywanie informacji przyczyni się do zwiększenia cyberbezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i	Uwaga nieuwzględniona.

			przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów.	
441.	art. 37	A.K. (uwagi osoby prywatnej)	Brak jest jednostki nadrzędnej, odwoławczej i decyzyjnej w przypadku sporów, konfliktów, lub konieczności skoordynowania działań MON, ABW i NASK na szczeblu centralnym. Powinien być wskazany Prezes Rady Ministrów, lub osoba przez niego uprawomocniona (chociażby ostatnio powołany pełnomocnik).	Uwaga częściowo uwzględniona. Sposób realizacji zadań i współpracy oraz właściwości CSIRT poziomu krajowego został określony w ustawie. Obecny model został zaproponowany przez CSIRT poziomu krajowego w ramach uzgodnień roboczych. Zasady koordynacji operacyjnej wskazują przepisy dot. CSIRT oraz Zespołu ds. Incydentów Krytycznych (m.in. art. 28 i art. 37). Projekt zostanie rozszerzony o przepisy przewidujące powołanie przy Radzie Ministrów Kolegium do spraw Cyberbezpieczeństwa w skład którego wchodzić będzie Minister Kooordynator Służb Specjalnych, MON, MSWiA, MC i RCB. W opinii projektodawcy przepisy dotyczące zarządzania ryzykiem na poziomie krajowym są wystarczające.
442.	art. 37	Związek Banków Polskich	Podstawowym determinantem decydującym o skuteczności obsługi incydentu jest czas. Proponowany przepis tworzą kolejną machinę biurokratyczną, która poprzez wydłużony proces decyzyjny faktycznie będzie obniżała efektywność podejmowanych działań. Taką rolę powinien pełnić CSIRT Narodowy działający w trybie ciągłym zdolny do podejmowania szybkich działań w oparciu o wypracowane i przećwiczone procedury. Zaproponowane rozwiązanie tworzy podatność krajowego systemu cyberbezpieczeństwa i obniża jego skuteczność.	Wyjaśnienie. Autorzy projektu ustawy nie przepisują stworzenia „CSIRT Narodowego”.
443.	art. 37 ust. 1	Fundacja Bezpieczna Cyberprzestrzeń	Powinno być: „W przypadku wystąpienia incydentu krytycznego dla krajowego systemu cyberbezpieczeństwa, zostaje powołany Zespół do spraw Incydentów Krytycznych (…)”	Uwaga nieuwzględniona.

444.	art. 37 ust. 2	Fundacja Bezpieczna Cyberprzestrzeń	Czy w określonych sytuacjach dopuszczalna jest współpraca z przedstawicielami operatorów telekomunikacyjnych? Art. 37 wydaje się nie dopuszczać takiej możliwości. Tymczasem w przypadku niektórych incydentów krytycznych współpraca z operatorami telekom. może mieć istotne znaczenie dla sprawnej i szybkiej obsługi incydentu.	Wyjaśnienie. Skład zespołu, o którym mowa w art. 37, który ma funkcję pomocniczą nie wklucza współpracy przy obsłudze incydentów krytycznych z innymi podmiotami.
445.	art. 37. ust. 4	Polska Izba Ubezpieczeń	W art. 37. ust. 4 proponujemy stworzyć możliwość włączania do prac Zespołu ekspertów zewnętrznych (tak, jak jest to umożliwione w przypadku kontroli; art. 53. ust. 2). Zatem końcówka ustępu mogłaby nabrać brzmienia: „(…) przedstawicieli organów ścigania, wymiaru sprawiedliwości, służb specjalnych lub niezależnych specjalistów.”	Uwaga nieuwzględniona. W opinii projektodawcy obecna wersja przepisów reguluje w wystarczający sposób poruszane kwestie. Jednakże nie wklucza to możliwości współpracy przy obsłudze incydentów krytycznych z innymi podmiotami, które nie muszą być w składzie zespołu koordynującego.
446.	art. 37 ust 4	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 37 ust 4 – w skład Zespołu do spraw Incydentów Krytycznych nie mogą wejść specjaliści OUK (lub podmiotu świadczącego usługi), nawet w przypadku posiadania szerszej wiedzy na temat danego incydentu. Zamknięty katalog uczestników.	Uwaga nieuwzględniona. W opinii projektodawcy obecna wersja przepisów reguluje w wystarczający sposób poruszane kwestie. Jednakże nie wklucza to możliwości współpracy przy obsłudze incydentów krytycznych z innymi podmiotami, które nie muszą być w składzie zespołu koordynującego.
447.	art. 38	Związek Banków Polskich	Organami właściwymi ds. bezpieczeństwa sieci i systemów informatycznych, zwanymi dalej „organami właściwymi” powinny być instytucje, które w chwili obecnej sprawują faktyczny nadzór nad działalnością OUK w poszczególnych sektorach i tak organami właściwymi powinni być: 1) dla sektora bankowego i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego; 2) dla sektora telekomunikacyjnego oraz infrastruktury cyfrowej – Prezes Urzędu Komunikacji Elektronicznej;	Wyjaśnienie. Przepis ulegnie przekształceniom w zakresie wskazania ministra właściwego do spraw gospodarki wodnej jako organu właściwego dla sektora zaopatrzenia w wodę i jej dystrybucji, zamiast ministra właściwego do spraw środowiska, na podstawie wprowadzonych zmian ustawowych (zmiana ustawy o działach administracji rządowej) wynikających z

			3) dla podsektora transportu lotniczego – Prezes Urzędu Lotnictwa Cywilnego; 4) dla podsektora transportu kolejowego – Prezes Urzędu Transportu Kolejowego; 5) dla podsektora transportu wodnego – minister właściwy do spraw gospodarki morskiej i żeglugi śródlądowej; 6) dla podsektora transportu drogowego – minister właściwy do spraw transportu; 7) dla sektora energetycznego – Prezes Urzędu Regulacji Energetyki; 8) dla sektora służby zdrowia – minister właściwy do spraw zdrowia; 9) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji oraz odprowadzania i uzdatniania ścieków – minister właściwy do spraw środowiska; 10) dla działu obrony narodowej – minister właściwy do spraw obrony narodowej; 11) dla działu sprawiedliwości – minister właściwy do spraw sprawiedliwości; 12) dla działu finansów publicznych – minister właściwy do spraw finansów publicznych; 13) dla działu informatyzacja – minister właściwy do spraw informatyzacji; 14) dla działu spraw wewnętrznych – minister właściwy do spraw wewnętrznych; 15) dla działu administracji publicznej – minister właściwy do spraw administracji publicznej; 16) dla działu ubezpieczeń społecznych – minister właściwy do spraw zabezpieczenia społecznego. 2. Organem właściwym dla dostawców usług cyfrowych jest Prezes Urzędu Komunikacji Elektronicznej. 3. Wykaz organów właściwych jest publikowany na stronie internetowej ministra właściwego do spraw informatyzacji oraz udostępniany w Biuletynie Informacji Publicznej. Zaproponowane przez MC rozwiązanie spowoduje potrzebę wydatkowania	ustawy z dnia 20 lipca 2017 r. – Prawo wodne (Dz. U. poz. 1566) oraz uchwalonej przez Sejm RP w dniu 27 października 2017 r. ustawy o zmianie ustawy o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków oraz niektórych innych ustaw. Pozostałe zapisy art. 38 zdaniem projektodawcy są odpowiednie dla ukształtowania zbioru organów właściwych dla poszczególnych sektorów i podsektorów wymienionych w załączniku do projektu ustawy oraz w załączniku do dyrektywy 2016/1148.

			dodatkowych środków finansowych na uzupełnienie kadr, sprzętu i opracowanie procesów związanych ze sprawowaniem nadzoru przez poszczególne ministerstwa w obszarze cyberbezpieczeństwa. Ponadto doprowadzi do dublowania działań z instytucjami obecnie faktycznie sprawującymi nadzór nad działaniem podmiotów z poszczególnych sektorów. To oznacza przede wszystkim brak zasadności wydawanych środków oraz ewentualne spory kompetencyjne. W dokumencie "Ocena Skutków Regulacji", cz. 6 - Wpływ na sektor finansów publicznych, część "Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń", w pierwszym akapicie Ministerstwo Cyfryzacji stwierdziło: "W związku z realizacją przez Ministerstwo Cyfryzacji funkcji organu właściwego dla sektora infrastruktury cyfrowej i dostawców usług cyfrowych niezbędne będzie stworzenie po 4 stanowiska pracy dedykowane do ww. zadań. Szacowany koszt jednostkowy uwzględniający zróżnicowanie stanowiskowe wynosi ok. 7 tys. brutto miesięcznie. Przewidziany koszt w 2018 r. to 462 tys. zł, a od 2019 r. 501 tys. zł rocznie. Uwzględniono także koszt stworzenia po cztery stanowiska pracy dedykowanych do ww. zadań w każdym z pozostałych organów właściwych (minister właściwy do spraw instytucji finansowych, minister właściwy do spraw transportu, minister właściwy do spraw gospodarki morskiej i żeglugi śródlądowej, minister właściwy do spraw energii, minister właściwy do spraw zdrowia, minister właściwy do spraw środowiska). Przewidziany koszt w 2018 r. to 2,235 mln zł, a od 2019 r. 2,425 mln zł rocznie.".	
448.	art. 38	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 38. „1. Organami właściwymi są, pkt 1: 1) dla sektora energetycznego – minister właściwy do spraw energii” – Nadzór nad bezpieczeństwem zaopatrzenia w energię elektryczną oraz nadzór nad bezpieczeństwem krajowych systemów energetycznych zgodnie z ustawą Prawo energetyczne i ustawą o działach administracji	Uwaga nieuwzględniona. Zdaniem projektodawcy przedstawiona w projekcie ustawy propozycja zapisu jest odpowiednia. Katalog organów właściwych jest zbieżny z wykazem sektorów

			rządowej sprawuje minister właściwy do spraw gospodarki / Pełnomocnik Rządu do spraw Strategicznej Infrastruktury Energetycznej. Sugerujemy uzupełnienie artykułu o wydzielony punkt dla operatorów sieci przesyłowych podobnie jak w pkt 2-3.	i podsektorów określonym w załączniku do projektu ustawy oraz w załączniku do dyrektywy 2016/1148..
449.	art. 38	Izba Gospodarcza Gazownictwa	Doprecyzowanie roli organu właściwego dla danego obszaru dla wyboru firm akredytowanych do prowadzenia audytów w danym obszarze oraz umożliwienie (w przyszłości) wydawania rozporządzeń ze szczegółowymi normami branżowymi. Dodanie: 9) dokonują akredytacji jednostek prowadzących audyty cyberbezpieczęnstwa dla danego obszaru 10) mogą wydawać dodatkowe rozporządzenia określające szczegółowe warunki ochrony cyberbezpieczeństwa infrastruktury krytycznej w danym obszarze	Uwaga nieuwzględniona. Zdaniem projektodawcy przedstawiona w projekcie ustawy propozycja zapisu jest odpowiednia. Katalog organów właściwych jest zbieżny z wykazem sektorów i podsektorów określonym w załączniku do projektu ustawy oraz w załączniku do dyrektywy 2016/1148.
450.	art. 38 ust. 1	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	W art. 38. ust.1 Projektu proponujemy dodać pkt. 8-10: „8) dla sektora administracji państwowej – minister właściwy do spraw wewnętrznych i administracji 9) dla sektora obrony narodowej – minister właściwy do spraw obrony narodowej 10) – dla rozwoju technologii i konstrukcji warunkujących cyberbezpieczeństwo państwa – minister właściwy do spraw gospodarki”	Uwaga nieuwzględniona. Zdaniem projektodawcy przedstawiona w projekcie ustawy propozycja zapisu jest odpowiednia. Katalog organów właściwych jest zbieżny z wykazem sektorów i podsektorów określonym w załączniku do projektu ustawy oraz w załączniku do dyrektywy 2016/1148.
451.	art. 38 ust. 1 pkt 7	Polska Izba Informatyki i Telekomunikacji	Sygnalizujemy, że w obszarze rynku telekomunikacyjnego może występować nakładanie się kompetencji ministra właściwego ds. informatyzacji oraz Prezesa UKE. Może to generować ryzyko nakładania się na siebie różnych, wykluczających się lub niespójnych obowiązków, a tym samym znacząco zwiększać ryzyko prowadzenia działalności gospodarczej.	Uwaga nieuwzględniona. W projekcie nie ma możliwości nałożenia się kompetencji ministra właściwego ds. informatyzacji oraz Prezesa UKE.
452.	art. 38 ust. 1 pkt 7	Konfederacja Lewiatan	Sygnalizujemy, że w obszarze rynku telekomunikacyjnego może występować nakładanie się kompetencji ministra właściwego ds. informatyzacji oraz Prezesa UKE. Może to generować ryzyko nakładania się na siebie różnych, wykluczających się lub niespójnych	Uwaga nieuwzględniona.

			obowiązków, a tym samym znacząco zwiększać ryzyko prowadzenia działalności gospodarczej.	W projekcie nie ma możliwości nałożenia się kompetencji ministra właściwego ds. informatyzacji oraz Prezesa UKE.
453.	art. 38 ust. 1 pkt 7	A.K. (uwagi osoby prywatnej)	Organy właściwe (art. 38 ust. 1 pkt 7) - W odniesieniu do rynku telekomunikacyjnego występuje nakładanie się kompetencji Ministerstwa Cyfryzacji z UKE i stawia operatorów telekomunikacyjnych wobec konieczności realizacji niespójnych ze sobą wymagań regulacyjnych.	Uwaga nieuwzględniona. W projekcie nie ma możliwości nałożenia się kompetencji ministra właściwego ds. informatyzacji oraz Prezesa UKE.
454.	art. 39. ust. 1 i 2	Związek Banków Polskich	Proponuje się aby zgodnie ze swoją właściwością aby organy właściwe sprawowały nadzór nad operatorami usług kluczowych w zakresie stosowania przepisów ustawy o krajowym systemie cyberbezpieczeństwa. W ramach sprawowanego nadzoru organy właściwe powinny: 1) realizować czynności związane z aktualizacją listy usług kluczowych; 2) realizować czynności związane z aktualizacją wykazu operatorów usług kluczowych; 3) posiadać uprawnienia do żądania niezwłocznego udostępnienia wszystkich niezbędnych informacji oraz dowodów w zakresie: a) oceny bezpieczeństwa sieci i systemów informatycznych operatorów usług kluczowych, w tym dokumentów dotyczących polityki w zakresie bezpieczeństwa; b) dowodów skutecznej realizacji polityk w zakresie bezpieczeństwa, takich jak wyniki audytu bezpieczeństwa, łącznie ze wspierającymi je dowodami, przeprowadzonego przez audytora posiadającego kompetencje. 4) prowadzić kontrole w zakresie stosowania przez operatorów usług kluczowych środków w zakresie bezpieczeństwa sieci i systemów informatycznych; 5) posiadać uprawnienia do wydawania zaleceń nadzorczych w przypadkach stwierdzenia nieprawidłowości;	Uwaga częściowo uwzględniona. Przepis w ust. 1 zostanie uzupełniony o zadania o których mowa w rozdziale VIII, szczególnie w zakresie kontroli. Przepis w ust. 2 zostanie przeniesiony do rozdziału VIII dotyczącego nadzoru i kontroli.

			6) nakładać sankcje i kary przewidziane w ustawie o krajowym systemie cyberbezpieczeństwa; 7) wykonywać inne zadania określone w odrębnych przepisach. Powyższe propozycje znajdują potwierdzenie w art. 47 projektowanej ustawy. Proponuje się następujące brzmienie ust. 2: "2. Organ właściwy żądając informacji lub dowodów powinien być zobowiązany do podania we wniosku o udostępnienie informacji celu, zakresu informacji i dowodów wraz z uzasadnieniem;"	
455.	art. 39. ust. 2	A.K. (uwagi osoby prywatnej)	Uprawnienia organu do żądania od operatora informacji (art. 39 ust. 2) - Zapis nadmiarowy – te informacje organ może pozyskać ze sprawozdania z audytu przeprowadzonego u operatora oraz z wykonanych przez organ w odniesieniu do danego operatora czynności kontrolnych. Poza tym zapis zbyt szeroko stanowi o uprawnieniach organu, ponieważ nie zawęża tego uprawnienia do informacji związanych z usługą kluczową – zapis tej treści jest nieakceptowalny i powinien bezwzględnie zostać usunięty z projektu.	Wyjaśnienie. Przepis ten wynika z art. 15 dyrektywy 2016/1148. Dokonywana przez organy właściwe ocena ma charakter formalny, a nie technologiczny i nie będzie polegała na ocenie bezpieczeństwa technicznego systemów teleinformatycznych dlatego nie ma potrzeby uzupełniania przedmiotowych przepisów. Przepis ten zostanie przeniesiony do rozdziału VIII dotyczącego nadzoru i kontroli.
456.	art. 39. ust. 2	Polska Izba Informatyki i Telekomunikacji	W naszej ocenie projektowany zapis w sposób zbyt szeroki określa uprawnienia organu właściwego, w szczególności nie zawężając tego uprawnienia do informacji związanych z usługą kluczową, jednocześnie w żaden sposób nie określając szczegółowych przesłanek, zakresu czy możliwości odwołania od arbitralnego rozstrzygnięcia. Dodatkowo, obowiązek odnosi się do informacji, które organ może pozyskać ze sprawozdania z audytu przeprowadzonego u operatora oraz z wykonanych przez organ w odniesieniu do danego operatora czynności kontrolnych. Tym samym wnosimy o wykreślenie art. 39 ust. 2 z projektu.	Wyjaśnienie. Przepis ten wynika z art. 15 dyrektywy 2016/1148. Dokonywana przez organy właściwe ocena ma charakter formalny, a nie technologiczny i nie będzie polegała na ocenie bezpieczeństwa technicznego systemów teleinformatycznych dlatego nie ma potrzeby uzupełniania przedmiotowych przepisów. Przepis ten zostanie przeniesiony do rozdziału VIII dotyczącego nadzoru i kontroli.

457.	art. 39. ust. 2	Konfederacja Lewiatan	W naszej ocenie projektowany zapis w sposób zbyt szeroki określa uprawnienia organu właściwego, w szczególności nie zawężając tego uprawnienia do informacji związanych z usługą kluczową, jednocześnie w żaden sposób nie określając szczegółowych przesłanek, zakresu, czy możliwości odwołania od arbitralnego rozstrzygnięcia. Dodatkowo, obowiązek odnosi się do informacji, które organ może pozyskać ze sprawozdania z audytu przeprowadzonego u operatora oraz z wykonanych przez organ w odniesieniu do danego operatora czynności kontrolnych. Tym samym wnosimy o wykreślenie art. 39 ust. 2 z projektu.	Wyjaśnienie. Przepis ten wynika z art. 15 dyrektywy 2016/1148. Dokonywana przez organy właściwe ocena ma charakter formalny, a nie technologiczny i nie będzie polegała na ocenie bezpieczeństwa technicznego systemów teleinformatycznych dlatego nie ma potrzeby uzupełniania przedmiotowych przepisów. Przepis ten zostanie przeniesiony do rozdziału VIII dotyczącego nadzoru i kontroli.
458.	Art. 39 ust. 2	Pracodawcy RP	W naszej ocenie projektowany zapis w sposób zbyt szeroki określa uprawnienia organu właściwego, w szczególności nie zawężając tego uprawnienia do informacji związanych z usługą kluczową, jednocześnie w żaden sposób nie określając szczegółowych przesłanek, zakresu, czy możliwości odwołania od arbitralnego rozstrzygnięcia. Dodatkowo, obowiązek odnosi się do informacji, które organ może pozyskać ze sprawozdania z audytu przeprowadzonego u operatora oraz z wykonanych przez organ w odniesieniu do danego operatora czynności kontrolnych. Tym samym wnosimy o wykreślenie art. 39 ust. 2 z projektu.	Wyjaśnienie. Przepis ten wynika z art. 15 dyrektywy 2016/1148. Dokonywana przez organy właściwe ocena ma charakter formalny, a nie technologiczny i nie będzie polegała na ocenie bezpieczeństwa technicznego systemów teleinformatycznych dlatego nie ma potrzeby uzupełniania przedmiotowych przepisów. Przepis ten zostanie przeniesiony do rozdziału dotyczącego nadzoru i kontroli.
459.	art. 39. ust. 3 [w uwagach błędnie oznaczona jako art. 39. ust. 35]	Związek Banków Polskich	Outsourcing sprawowania nadzoru nie może mieć miejsca, a tym bardziej przekazywanie uprawnień nadzorczych na podstawie porozumienia.	Uwaga nieuwzględniona.

460.	art. 41	Związek Banków Polskich	Wskazane w przepisie perogatywy winny być przypisane podmiotowi/instytucji będącego ponad resortami MON, MSWiA, Ministra Koordynatora ds. Służb Specjalnych, bezpośrednio nadzorowanemu przez Premiera. W skład tego ciała powinni wchodzić przedstawiciele ww. resortów, sektorów prywatnych, wymienionych w załączniku II do dyrektywy NIS. Powyższa propozycja wynika z braku możliwości faktycznego oddziaływania na cyberbezpieczeństwo, które pozostaje w chwili obecnej w gestii MON, MSWiA, czy Ministra Koordynatora ds. Służb Specjalnych.	Wyjaśnienie. Projekt zostanie rozszerzony o przepisy przewidujące powołanie przy Radzie Ministrów Kolegium do spraw Cyberbezpieczeństwa w skład którego wchodzić będzie Minister Koordynator Służb Specjalnych, MON, MSWiA, MC i RCB.
461.	art. 41 ust. 6	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Należy wskazać tryb udostępniania informacji i dobrych praktyk np. czy informacja ma być udostępniana na wniosek OUK DUC czy w jakimś innym trybie.	Uwaga uwzględniona. Chodzi o publicznie dostępne udostępnianie informacji, np. na stronie internetowej.
462.	art. 42	Izba Gospodarcza Gazownictwa	Czy ma to być system ogólny dla wszystkich rodzajów IK ? System taki należałoby zbudować przed wejściem w życie ustawy (co mało realne) albo zapewnić jak ma działać komunikacja przed powstaniem systemu. Doprecyzowanie ? artykuł wprowadza wymaganie raportowania poprzez system informatyczny który może nie istnieć Czy taki system istnieje ? ma zostać wdrożony ? kiedy ?	Wyjaśnienie. Właściwość wspomnianego systemu została określona w art. 42 projektowanej ustawy. Do czasu uruchomienia ww. sytemu teleinformatycznego, co zostało określone w przepisach przejściowych projektowanej ustawy (art. 69 ust. 1), OUK, DUC, CSIRT MON, CSIRT NASK oraz CSIRT GOV zgłaszają incydenty oraz wymieniają się informacjami zgodnie z zapisami przepisów przejściowych projektowanej ustawy (art. 69 ust. 2).
463.	art. 42	Business Centre Club	Wskazujemy również, że system teleinformatyczny, o którym mowa w art. 42 Projektu, który ma służyć m.in. do zgłaszana i obsługi incydentów powinien zapewniać automatyczny (machine-2-machine) interfejs umożliwiający przekazanie informacji o	Wyjaśnienie. Wytyczne techniczne systemu, o którym mowa w art. 42 ust. 1 projektu ustawy nie są materią, którą

			incydentach z uwagi na to, że w trakcie trwania poważnego incydentu może nie być czasu na ręczne wypełnianie formularzy. U podmiotów posiadających systemy zarządzania incydentami powinno wystarczyć odpowiednie oznakowanie incydentu, aby automatycznie został on przekazany do systemu, a także wszelkie aktualizacje danych dotyczących tego incydentu (ponieważ wiedza o incydencie będzie się zmieniać wraz z upływem czasu).	powinno się regulować w akcie prawnym o randze ustawy.
464.	art. 42	Związek Pracodawców Branży Internetowej IAB Polska	Wskazujemy również, że system teleinformatyczny, o którym mowa w art. 42 Projektu, który ma służyć m.in. do zgłaszana i obsługi incydentów powinien zapewniać automatyczny (machine-2-machine) interfejs umożliwiający przekazanie informacji o incydentach z uwagi na to, że w trakcie trwania poważnego incydentu może nie być czasu na ręczne wypełnianie formularzy. U podmiotów posiadających systemy zarządzania incydentami powinno wystarczyć odpowiednie oznakowanie incydentu, aby automatycznie został on przekazany do systemu, a także wszelkie aktualizacje danych dotyczących tego incydentu (ponieważ wiedza o incydencie będzie się zmieniać wraz z upływem czasu).	Wyjaśnienie. Wytyczne techniczne systemu, o którym mowa w art. 42 ust. 1 projektu ustawy nie są materią, którą powinno się regulować w akcie prawnym o randze ustawy.
465.	art. 42	Instytut Logistyki i Magazynowania	Ust.1 pkt1 Jakim kanałem mają trafiać do CSIR zgłoszenia incydentów od firm, instytucji i osób prywatnych, które nie będą miały dostępu do systemu teleinformatycznego? Czy temu ma służyć zapis w ust.14?	Wyjaśnienie. Instytucje oraz osoby fizyczne będą w myśl art. 69 ust. 2 zobowiązane zgłaszać incydenty do właściwego CSIRT jakim jest CSIRT NASK, przy pomocy dostępnych środków komunikacji elektronicznej. Ponadto art. 42 ust. 14 daje możliwość, umożliwienia podmiotowi niezobowiązanemu do zgłaszania incydentów, dostępu do sytemu, o którym mowa w ustawie, jeśli zdaniem ministra właściwego do spraw informatyzacji, umożliwienie ww. dostępu będzie niezbędne dla zapewnienia wysokiego poziomu cyberbezpieczeństwa.

466.	art. 42. ust. 1	Związek Banków Polskich	Jeśli wystąpi incydent, który uniemożliwi działanie systemu, musi istnieć alternatywny sposób raportowania i koordynowania incydentu. System nie może być kluczowym elementem do obsługi incydentu, bo sam może być jego przedmiotem.	Wyjaśnienie. Wówczas, podobnie jak do czasu uruchomienia systemu, o którym mowa w art. 42 ust. 1 projektu ustawy, incydenty będą zgłaszane przy pomocy dostępnych środków komunikacji elektronicznej.
467.	art. 42. ust. 2	Związek Banków Polskich	W projekcie nie przewidziano, że system będzie przetwarzał informacje prawnie chronione, w szczególności informacje niejawne i informacje objęte tajemnicami ustawowo chronionymi, czyli tzw. tajemnicami sektorowymi. Bez tego system będzie mógł przetwarzać informacje czysto techniczne, lecz nie będzie wspierał zwalczania cyberprzestępczości, co de facto wiąże się nierozerwalnie z większością incydentów.	Wyjaśnienie. Zagadnienia te były przedmiotem rozmów pomiędzy resortami w ramach prac nad ustawą o krajowym systemie cyberbezpieczeństwa. Niezbędne są analizy dotyczące przepisów karnych i przepisów z zakresu ścigania przestępczości będące w kompetencji innych resortów. Ewentualne zmiany przepisów w tym zakresie powinny być przedmiotem odrębnych ustaw przygotowanych przez właściwe resorty.
468.	art. 42. ust. 3	Związek Banków Polskich	Brak ogólnego lub obligatoryjnego obowiązku udostępniania informacji z systemu m. in takich podmiotów jak: 1) CSIRT sektorowych; 2) organów właściwych - narzędzie do sprawowania nadzoru (analitycznego i inspekcyjnego); 3) Policji oraz innych służb specjalnych; 4) Prokuratury 5) CSIRT Narodowy 6) Pojedynczy Punkt Kontaktowy 7) GIODO Główną rolą systemu powinno być raportowanie w czasie rzeczywistym zaistniałych incydentów i komunikacja przy ich obsłudze. Dlatego beneficjentami systemu powinni być wszyscy interesariusze, którzy będą zarządzać lub wspierać obsługę incydentu np. w przypadku incydentu w wyniku którego dojdzie do wycieku danych osobowych informacja ta winna automatycznie być przekazana do GIODO, jest to wymóg RODO. Dodatkowo, należy zapewnić aby OUK i DUC jeden incydent raportowali tylko raz do systemu i nie musieli duplikować informacji dla każdego z podmiotów osobno. Należy przy tym wykorzystać	Uwaga nieuwzględniona. Ust. 3 nie dotyczy udostępniania informacji z systemu, tylko użytkowników systemu. Treść uwagi jest niewłaściwa do wskazanej przez nadawcę jednostki redakcyjnej projektowanej ustawy. Drogą wyjaśnienia, udostępnianie informacji z systemu jest określone w art. 42 ust. 9-13; sektorowe zespoły reagowania na incydenty, będą mogły otrzymać dostęp do systemu na podstawie zapisu art. 42 ust. 14; organy właściwe mogą otrzymywać informacje z systemu na podstawie art. 42 ust. 12; Policja, prokuratura oraz „inne służby" będą miały dostęp do informacji na podstawie zapisu art. 42 ust. 10; projektodawca nie przewiduje konieczności tworzenia „CSIRT Narodowego"; GIODO jako organ

			utworzenie lub tworzone systemy informacji przez poszczególne sektory.	właściwy do spraw ochrony danych osobowych będzie miał dostęp do systemu na podstawie art. 42 ust. 12.
469.	art. 42 ust. 3	Fundacja Bezpieczna Cyberprzestrzeń	W spisie nie są wymienione firmy świadczące usługi cyberbezpieczeństwa, które zgodnie z Art. 4 należą do krajowego systemu cyberbezpieczeństwa i mogłyby być dostarczycielami istotnych informacji o zagrożeniach. Ponadto uczestnictwo operatorów telekomunikacyjnych w systemie odbywa się za pośrednictwem prezesa UKE co może utrudniać i spowalniać wymianę istotnych informacji z operatorami telekom.	Wyjaśnienie. Projektodawca daje wymienionym podmiotom możliwość pozyskania dostępu do systemu, o którym mowa w art. 42 ust. 1, na podstawie ust. 14 i 15.
470.	art. 42 ust. 3	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Pytania dotyczące treści artykułu: Dlaczego wśród użytkowników systemu teleinformatycznego wymienionego w art. 42. ust.1, nie ma dyrektora Rządowego Centrum Bezpieczeństwa?	Uwaga niejasna. W art. 42 ust. 3 pkt 5 projektodawca wyraźnie wskazał, że Rządowe Centrum Bezpieczeństwa jest użytkownikiem systemu, o którym mowa w art. 42 ust. 1.
471.	art. 42 ust. 5	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Art.42 ust.5 - uważamy iż system informatyczny powinien zapewniać automatyczny (Machine-2-Machine) interfejs umożliwiający przekazanie informacji o incydentach z uwagi na to, że w trakcie trwania poważnego incydentu może nie być czasu na ręczne wypełnianie formularzy. U podmiotów posiadających systemy zarządzania incydentami powinno wystarczyć odpowiednie oznakowanie incydentu, aby automatycznie został przekazany do systemu, a także wszelkie aktualizacje danych dotyczących tego incydentu (ponieważ wiedza o incydencie będzie się zmieniać wraz z upływem czasu).	Wyjaśnienie. Wytyczne techniczne systemu, o którym mowa w art. 42 ust. 1 projektu ustawy nie są materią, którą powinno się regulować w akcie prawnym o randze ustawy.
472.	art. 42 ust. 5	Polska Izba Radiodyfuzji Cyfrowej	System informatyczny powinien zapewniać automatyczny (machine-2-machine) interfejs, umożliwiający przekazanie informacji o incydentach z uwagi na to, że w trakcie trwania poważnego incydentu może nie być czasu na ręczne wypełnianie formularzy. U podmiotów posiadających systemy zarządzania incydentami powinno wystarczyć odpowiednie oznakowanie	Wyjaśnienie. Wytyczne techniczne systemu, o którym mowa w art. 42 ust. 1 projektu ustawy nie są materią, którą powinno się regulować w akcie prawnym o randze ustawy.

			incydentu, aby automatycznie został przekazany do systemu, a także wszelkie aktualizacje danych dotyczących tego incydentu (ponieważ wiedza o incydencie będzie się zmieniać wraz z upływem czasu).	
473.	art. 42 ust. 5	Konfederacja Lewiatan	System informatyczny powinien zapewniać automatyczny (machine-2-machine) interfejs umożliwiający przekazanie informacji o incydentach z uwagi na to, że w trakcie trwania poważnego incydentu może nie być czasu na ręczne wypełnianie formularzy. U podmiotów posiadających systemy zarządzania incydentami powinno wystarczyć odpowiednie oznakowanie incydentu, aby automatycznie został przekazany do systemu, a także wszelkie aktualizacje danych dotyczących tego incydentu (ponieważ wiedza o incydencie będzie się zmieniać wraz z upływem czasu).	Wyjaśnienie. Wytyczne techniczne systemu, o którym mowa w art. 42 ust. 1 projektu ustawy nie są materią, którą powinno się regulować w akcie prawnym o randze ustawy.
474.	art. 42 ust. 5	Polska Izba Informatyki i Telekomunikacji	System informatyczny powinien zapewniać automatyczny (machine-2-machine) interfejs umożliwiający przekazanie informacji o incydentach z uwagi na to, że w trakcie trwania poważnego incydentu może nie być czasu na ręczne wypełnianie formularzy. U podmiotów posiadających systemy zarządzania incydentami powinno wystarczyć odpowiednie oznakowanie incydentu, aby automatycznie został przekazany do systemu, a także wszelkie aktualizacje danych dotyczących tego incydentu (ponieważ wiedza o incydencie będzie się zmieniać wraz z upływem czasu). Artykuł 42 p.10. Zakres jest inny niż w artykule 8 p. 6	Wyjaśnienie. Wytyczne techniczne systemu, o którym mowa w art. 42 ust. 1 projektu ustawy nie są materią, którą powinno się regulować w akcie prawnym o randze ustawy.
475.	art. 42. ust. 10	Związek Banków Polskich	Niejasna jest rola np.. CBA czy Krajowej Administracji Skarbowej w Krajowym Systemie Cyberbepieczeństwa. W związku z tym powstają wątpliwości w jakim celu i zakresie mają być im udostępnianie informacje z przedmiotowego systemu. W chwili obecnej zarówno CBA jak i KASA posiada już dostęp do informacji objętych tajemnicą bankową, zgodnie z ustawą Prawo Bankowe.	Wyjaśnienie. Wymienione w art. 42 ust 10 podmioty będą miały dostęp do informacji, niezbędny do realizacji ich ustawowych zadań.

476.	art. 42. ust. 10	Instytut Logistyki i Magazynowania	Ust.10 Zamienić „o ile są one niezbędne” na „w zakresie niezbędnym”.	Uwaga nieuwzględniona. Sformułowanie użyte w projekcie jest właściwe.
477.	art. 42. ust. 11	Fundacja Bezpieczna Cyberprzestrzeń	Ten zapis jest bardzo szeroki i nieprecyzyjny. Potrzeba informacji o tym jakie dane z systemu informują o stanie bezpieczeństwa Państwa.	Uwaga nieuwzględniona. Zdaniem projektodawcy zapis jest właściwy. Doprecyzowanie mogłoby zawęzić katalog udostępnianych informacji. Zapis wyraźnie wyłącza udostępnianie danych obejmujących dane osobowe oraz wskazuje na charakter informacji będących w zainteresowaniu Szefa BBN, zgodnie z właściwością podległej mu instytucji.
478.	art. 42 ust. 13	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Zgodnie z art. 42 ust. 13 Projektu informacje z systemu teleinformatycznego mogą być udostępniane operatorom usług kluczowych oraz podmiotom świadczącym usługi z zakresu cyberbezpieczeństwa je obsługującym. Wydaje się, że doprecyzować należy zakres udostępnianych informacji oraz dodać uprawnienie do przetwarzania tych informacji dla operatorów usług kluczowych oraz podmiotów je obsługujących.	Uwaga nieuwzględniona.
479.	art. 42. ust. 13	Związek Banków Polskich	Kto o tym będzie decydował? Brak definicji ośrodka decyzyjnego.	Wyjaśnienie. Decyzyjny jest organ nadzorujący system wymieniony w art. 42 ust. 1.
480.	art. 44	Instytut Logistyki i Magazynowania	W zakresie odpowiedzialności Departamentu Cyberbezpieczeństwa MC jest prowadzenie Krajowego Punktu Kontaktowego PoC (wg inf. na stronie MC) Czy to to samo co Pojedynczy Punkt Kontaktowy wymieniany w projekcie?	Wyjaśnienie. Pojedynczy punkt kontaktowy to instytucja, która pojawi się wraz z przyjęciem projektu ustawy. Nie jest to zadanie opisane w regulaminie Departamentu.

481.	art. 46 pkt 2a	Fundacja Bezpieczna Cyberprzestrzeń	Z uwagi na złożoność zapisu, wymaga on przeformułowania, np. „o liczbie operatorów usług kluczowych, które były uczestnikiem rozmów z pojedynczymi punktami kontaktowymi państw członkowskich Unii Europejskiej na temat (…)”.	Uwaga nieuwzględniona. Przepis dotyczy rozmów prowadzonych z pojedynczymi punktami kontaktowymi z innych państw, a nie z operatorami.
482.	art. 47 [uwaga do rozdz. VIII]	Instytut Audytorów Wewnętrznych IIA Polska	Rozdział 8 Nadzór i kontrola - brak minimalnych kwalifikacji dla osób prowadzących kontrole. Prezes Rady Ministrów, w drodze stosownego rozporządzenia, powinien takie kompetencje określić, tak jak jest to obecnie: http://prawo.seim.gov.pi/isap.nsf/download.xsp/WDU20101771195/O/D20101195.pdf Mamy nadzieję, że przedstawione uwagi okażą się pomocne przy nadawaniu ostatecznego kształtu przedmiotowej ustawie.	Uwaga nieuwzględniona. W ocenie projektodawcy nie jest konieczne szczegółowe precyzowanie wymagań. Wskazanie odpowiednich osób pozostaje w gestii organów właściwych.
483.	art. 47. ust. 1. pkt 1	Związek Banków Polskich	Zadanie to winno być powierzone organom właściwym, gdyż Ministerstwo Cyfryzacji w praktyce nie będzie w stanie go realizować, chociażby ze względu na ilość OUK. To powinny być kompetencje organu właściwego, jakim jest w przypadku sektora bankowego i infrastruktury rynków finansowych - Komisja Nadzoru Finansowego na podstawie ustawy Prawo Bankowe oraz ustawy o nadzorze nad rynkiem finansowym.	Uwaga nieuwzględniona. Zdaniem projektodawcy zapis jest odpowiedni. Nadzór nad przestrzeganiem ustawy przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa będzie prowadzony wyłącznie przez ministra właściwego do spraw informatyzacji.
484.	art. 47. ust. 2	Związek Banków Polskich	To powinny być obowiązki organów właściwych. Ponadto błędnie przywołano zakres prowadzonych inspekcji, należy przywołać art. 39 projektu ustawy zgodnie z przedstawionymi propozycjami sektora bankowego.	Uwaga nieuwzględniona. Zdaniem projektodawcy zapis jest odpowiedni.
485.	art. 47. ust. 2 pkt 2	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 47 ust 2 pkt 2 – dot. przeprowadzanych kontroli – nie określono terminu usunięcia nieprawidłowości ustalonych w wyniku kontroli i w art. 52 ust 2 mówiącym co powinien zawierać protokół kontroli nie ma pozycji określającej ten termin. Ponadto jest sankcja finansowa za nieusunięcie uchybień więc tym bardziej termin powinien być doprecyzowany.	Uwaga nieuwzględniona. Termin usunięcia nieprawidłowości będzie ustalany podczas kontroli, gdyż może dotyczyć różnego zakresu uchybień do usunięcia. Ustawowy termin mógłby być niedopasowany.

486.	art. 48. ust. 1	Związek Banków Polskich	W związku z uwagą do art. 47 ust. 1 pkt. 1 przepis bezprzedmiotowy i winien być usunięty.	Uwaga nieuwzględniona. Zapis art. 42 ust. 1 nie zostanie zmieniony, a w związku z tym zapis art. 48 ust. 1 nie zostanie usunięty.
487.	art. 48. ust. 1	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy następujące brzmienie art. 48 ust. 1: Art. 48. 1. Do kontroli, której zakres określony jest w art. 47 ust. 1 pkt 1, stosuje się przepisy rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej. Proponujemy usunięcie wyłączenia art. 79 odnoszącego się do rozdziału 5 z ustawy o swobodzie działalności gospodarczej. Uważamy że przedsiębiorcy powinny mieć prawo do bycia powiadomionym o wszczęciu kontroli. Wcześniejsze zawiadomienie pozwala na prawidłową organizację, zapewnienie dostępności niezbędnego personelu i sprawny przebieg kontroli	Uwaga nieuwzględniona. Z uwagi na specyfikę i przedmiot kontroli, wcześniejsze poinformowanie mogłoby zniweczyć jej sens.
488.	art. 48. ust. 1	Konfederacja Lewiatan	Proponujemy usunięcie wyłączenia art. 79 odnoszącego się do rozdziału 5 z ustawy o swobodzie działalności gospodarczej. Uważamy że przedsiębiorcy powinny mieć prawo do bycia powiadomionym o wszczęciu kontroli. Wcześniejsze zawiadomienie pozwala na prawidłową organizację, zapewnienie dostępności niezbędnego personelu i sprawny przebieg kontroli. Proponujemy następujące brzmienie art. 48 ust. 1: Art. 48. 1. Do kontroli, której zakres określony jest w art. 47 ust. 1 pkt 1, stosuje się przepisy rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej.	Uwaga nieuwzględniona. Z uwagi na specyfikę i przedmiot kontroli, wcześniejsze poinformowanie mogłoby zniweczyć jej sens.
489.	art. 48 ust. 2	Izba Gospodarcza Gazownictwa	Nieprawidłowe odniesienie. W art. 48 ust. 2 znajduje się odniesienie do art. 47 ust. 1 pkt 2 i 3, podczas gdy art. 47 ust. 1 składa się jedynie z pkt 1 i 2.	Uwaga uwzględniona.
490.	art. 48. ust. 2. pkt 1	Związek Banków Polskich	Zasady kontroli w sektorze bankowym zostały określone w ustawie - Prawo bankowe oraz ustawie o nadzorze nad rynkiem finansowym. W związku z tym proponuje się usunięcie tego	Uwaga częściowo uwzględniona.

			przepisu. Poza tym kolejne przepisy art. 49-54 odnoszą się do kwestii zawartych w 5 rozdziale ustawy o swobodzie działalności gospodarczej.	Nadzór nad bankami określony w ustawie – Prawo bankowe oraz ustawie o nadzorze nad rynkiem finansowym ma inny zakres niż określony w projekcie ustawy. Zastosowanie zatem ma ustawa o swobodzie działalności gospodarczej.
491.	art. 48. ust. 2. pkt 1	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy następujące brzmienie art. 48 ust. 2 pkt 1: Art. 48 … 2. Do kontroli, której zakres określony jest w art. 47 ust. 1 pkt 2 i 3, realizowanej wobec podmiotów: 1) będących przedsiębiorcami, stosuje się przepisy rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej, Proponujemy usunięcie wyłączenia art. 79 odnoszącego się do rozdziału 5 z ustawy o swobodzie działalności gospodarczej. Uważamy że przedsiębiorcy powinny mieć prawo do bycia powiadomionym o wszczęciu kontroli. Wcześniejsze zawiadomienie pozwala na prawidłową organizację, zapewnienie dostępności niezbędnego personelu i sprawny przebieg kontroli	Uwaga nieuwzględniona. Takie wyłączenie narusza cele ustawy. Z uwagi na specyfikę i przedmiot kontroli, wcześniejsze poinformowanie mogłoby zniweczyć jej sens.
492.	art. 48. ust. 2. pkt 1	Konfederacja Lewiatan	Proponujemy usunięcie wyłączenia art. 79 odnoszącego się do rozdziału 5 z ustawy o swobodzie działalności gospodarczej. Uważamy że przedsiębiorcy powinny mieć prawo do bycia powiadomionym o wszczęciu kontroli. Wcześniejsze zawiadomienie pozwala na prawidłową organizację, zapewnienie dostępności niezbędnego personelu i sprawny przebieg kontroli. Proponujemy następujące brzmienie art. 48 ust. 2 pkt 1: Art. 48 … 2. Do kontroli, której zakres określony jest w art. 47 ust. 1 pkt 2 i 3, realizowanej wobec podmiotów: 1) będących przedsiębiorcami, stosuje się przepisy rozdziału 5 ustawy z dnia 2 lipca 2004 r. o swobodzie działalności gospodarczej,	Uwaga nieuwzględniona. Z uwagi na specyfikę i przedmiot kontroli, wcześniejsze poinformowanie mogłoby zniweczyć jej sens.

493.	art. 49	Pracodawcy RP	- Nie jest zasadne wprowadzenie rozwiązań dopuszczających możliwość dokonywania kontroli bez posiadania odpowiedniej przepustki. Nawet na poziomie praktycznym, istniejące systemy kontroli dostępu w siedzibach firm spowodują, że dokonywanie tych czynności bez przepustki będzie fizycznie niemożliwe. Należy wykreślić zapis dot. braku konieczności posiadania przepustki. W przypadkach, w których podmiot nie poddaje się dobrowolnie czynnościom kontrolnym, możliwe będzie korzystanie z asysty Policji. Ponadto w projekcie należy wyraźnie zaznaczyć, że kontrola może dotyczyć wyłącznie pomieszczeń, dokumentów i systemów wykorzystywanych do świadczenia usługi kluczowej. - W pkt 6 należy doprecyzować zakres działań związanych z „oględzinami urządzeń, nośników i systemów teleinformatycznych", w szczególności poprzez wskazanie, że takie „oględziny" nie mogą prowadzić do jakiejkolwiek ingerencji w działanie urządzeń, nośników i systemów (art. 49 pkt 6).	Wyjaśnienie. Kontroler będzie posiadał odpowiednie dokumenty upoważniające do kontroli, co wynika z art. 79a ustawy o swobodzie działalności gospodarczej. Tym samym wątpliwości wydają się nieuzasadnione. Ponadto, zgodnie z art. 80 ustawy o swobodzie działalności gospodarczej czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Przepis nie wyklucza stosowania wewnętrznych procedur obowiązujących w firmach. Ma on jedynie zapewnić kontrolerowi swobodny wstęp i zapobiec sytuacji, w której zostanie odmówiony wstęp osobie kontrolującej ze względu na brak posiadania przepustki. W tym zakresie zostanie uzupełnione uzasadnienie.
494.	art. 49-53	J.K. (uwagi osoby prywatnej)	W Uzasadnieniu projektodawca stwierdził: *W 2015 r. Minister Cyfryzacji zatwierdził również Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych. Celem Wytycznych jest zapewnienie wsparcia przeprowadzania kontroli działania systemów teleinformatycznych, używanych do realizacji zadań publicznych, w tym ww. wymagań w obszarze bezpieczeństwa informacji.* Niestety Wytyczne wymagają poważnego uzupełnienia. Swoje zastrzeżenia dotyczące Wytycznych przedstawiłam w moim piśmie do pani Minister Anny Streżyńskiej z dnia 13.01.2016 r. (w załączeniu do uwag).	Wyjaśnienie. Uwaga nie dotyczy materii regulowanej ustawą.
495.	art. 49	A.K. (uwagi osoby prywatnej)	Uprawnienia kontrole organu (rozdział VIIII) - Art. 49 – uprawnienie osoby prowadzącej czynności kontrolne do swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki - rozwiązanie niedopuszczalne; przede wszystkim osoba prowadząca czynności kontrolne powinna mieć	Wyjaśnienie. Kontroler będzie posiadał odpowiednie dokumenty upoważniające do kontroli, co wynika z art. 79a

			prawo wstępu i poruszania się po terenie podmiotu kontrolowanego wyłącznie w miejscach związanych ze świadczeniem usługi kluczowej. Nie wyobrażamy sobie sytuacji, w której osoba prowadząca czynności kontrolne pojawi się pod dowolną serwerownią i zażąda wstępu do wybranych przez siebie pomieszczeń. Skoro są pojedyncze przypadki, które zgodnie z uzasadnieniem uniemożliwiają prowadzenie czynności kontrolnych z uwagi na brak przepustki, to należy znaleźć skuteczny sposób na zmuszenie tych organów do poddania się kontroli – jest np. uprawnienie organu do korzystania z pomocy funkcjonariuszy Policji (art. 53). Czynność kontrolna musi podlegać rozliczalności. Oględziny do mogą prowadzić do ingerencji w działanie urządzeń (art. 49 pkt 6). Należy wyraźnie zaznaczyć, że kontrola może dotyczyć wyłącznie pomieszczeń, dokumentów i systemów wykorzystywanych do świadczenia usługi kluczowej. Nie jest ponadto akceptowalna zasada, zgodnie z którą organ "może włączyć do kontroli specjalistów" (art. 53 ust. 2) bez podania jakichkolwiek wymagań, jakie specjaliści muszą spełniać (jaka odpowiedzialność tego specjalisty; nie może świadczyć usług dla podmiotów konkurencyjnych; skąd wiadomo, że jest to specjalista – kim ma być ta osoba?). W związku z kontrolą operator będzie musiał zazwyczaj udostępnić informacje stanowiące tajemnicę przedsiębiorstwa i dlatego nieograniczone uprawnienie w zakresie dopraszania do zespołu kontrolnego bliżej nieokreślonych specjalistów - niedopuszczalne.	ustawy o swobodzie działalności gospodarczej. Tym samym wątpliwości wydają się nieuzasadnione. Ponadto, zgodnie z art. 80 ustawy o swobodzie działalności gospodarczej czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Przepis nie wyklucza stosowania wewnętrznych procedur obowiązujących w firmach. Ma on jedynie zapewnić kontrolerowi swobodny wstęp i zapobiec sytuacji, w której zostanie odmówiony wstęp osobie kontrolującej ze względu na brak posiadania przepustki. W tym zakresie zostanie uzupełnione uzasadnienie. Przepis dotyczący włączenia do kontroli specjalistów zostanie usunięty.
496.	art. 49 pkt 1	Business Centre Club	Należy również odnieść się do zapisów Projektu dotyczących kontroli i nadzoru. W kontekście art. 49 pkt 1 podkreślenia wymaga, że nie jest realnym, aby osoba prowadząca czynności kontrolne nie miała przepustki do poruszania się po obiekcie jednostki kontrolowanej. Bez takowej, w większości przypadków nie będzie miała fizycznie możliwości przemieszczania się z uwagi na systemy kontroli dostępu, które są zresztą wymagane przez tę ustawę i wiele	Wyjaśnienie. Kontroler będzie posiadał odpowiednie dokumenty upoważniające do kontroli, co wynika z art. 79a ustawy o swobodzie działalności gospodarczej. Tym samym wątpliwości wydają się nieuzasadnione.

			innych. Nie można też od początku określić pełnego zakresu dostępu fizycznego lub logicznego dla takiej osoby ponieważ może się to zmieniać w trakcie trwania czynności kontrolnych. Stosowny zapis powinien umożliwiać osobie kontrolującej dostęp tam, gdzie jest konieczny, ale sposób jego realizacji (przepustka, przewodnik, karta dostępu, czy inna metoda) powinien być wybrany przez kontrolowany podmiot, ponieważ silnie zależy od przyjętych w tym podmiocie zasad i technologii – np. podmiot może stosować dostęp na podstawie danych biometrycznych, a nie ma powodu, aby przetwarzał dane biometryczne osoby kontrolującej. Z kolei w zakresie przetwarzania danych o którym mowa w art. 49 pkt 4 podkreślenia wymaga, że dane osobowe dla poszczególnych podmiotów mogą być również danymi chronionymi innymi tajemnicami – np. tajemnicą bankową, informacją niejawną, tajemnicą handlową (dla spółek giełdowych, etc.), a więc takie dane nie mogą być ujawnione na podstawie tego zapisu osobie prowadzącej kontrolę. Należy zatem nałożyć na podmiot kontrolujący i osobę kontrolującą obowiązek zapewnienia takiego samego poziomu ochrony przekazanych informacji, jaki wynika z przepisów dotyczących ochrony danych w danym sektorze.	Ponadto, zgodnie z art. 80 ustawy o swobodzie działalności gospodarczej czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Przepis nie wyklucza stosowania wewnętrznych procedur obowiązujących w firmach. Ma on jedynie zapewnić kontrolerowi swobodny wstęp i zapobiec sytuacji, w której zostanie odmówiony wstęp osobie kontrolującej ze względu na brak posiadania przepustki. W tym zakresie zostanie uzupełnione uzasadnienie.
497.	art. 49 pkt 1	Związek Pracodawców w Branży Internetowej IAB Polska	Należy również odnieść się do zapisów Projektu dotyczących kontroli i nadzoru. W kontekście art. 49 pkt 1 podkreślenia wymaga, że nie jest realnym, aby osoba prowadząca czynności kontrolne nie miała przepustki do poruszania się po obiekcie jednostki kontrolowanej. Bez takowej, w większości przypadków nie będzie miała fizycznie możliwości przemieszczania się z uwagi na systemy kontroli dostępu, które są zresztą wymagane przez tę ustawę i wiele innych. Nie można też od początku określić pełnego zakresu dostępu fizycznego lub logicznego dla takiej osoby ponieważ może się to zmieniać w trakcie trwania czynności kontrolnych. Stosowny zapis powinien umożliwiać osobie kontrolującej dostęp tam, gdzie jest konieczny, ale sposób jego realizacji (przepustka, przewodnik, karta	Wyjaśnienie. Kontroler będzie posiadał odpowiednie dokumenty upoważniające do kontroli, co wynika z art. 79a ustawy o swobodzie działalności gospodarczej. Tym samym wątpliwości wydają się nieuzasadnione. Ponadto, zgodnie z art. 80 ustawy o swobodzie działalności gospodarczej czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej.

			dostępu, czy inna metoda) powinien być wybrany przez kontrolowany podmiot, ponieważ silnie zależy od przyjętych w tym podmiocie zasad i technologii – np. podmiot może stosować dostęp na podstawie danych biometrycznych, a nie ma powodu, aby przetwarzał dane biometryczne osoby kontrolującej. Z kolei w zakresie przetwarzania danych o którym mowa w art. 49 pkt 4 podkreślenia wymaga, że dane osobowe dla poszczególnych podmiotów mogą być również danymi chronionymi innymi tajemnicami – np. tajemnicą bankową, informacją niejawną, tajemnicą handlową (dla spółek giełdowych, etc.), a więc takie dane nie mogą być ujawnione na podstawie tego zapisu osobie prowadzącej kontrolę. Należy zatem nałożyć na podmiot kontrolujący i osobę kontrolującą obowiązek zapewnienia takiego samego poziomu ochrony przekazanych informacji, jaki wynika z przepisów dotyczących ochrony danych w danym sektorze.	Przepis nie wyklucza stosowania wewnętrznych procedur obowiązujących w firmach. Ma on jedynie zapewnić kontrolerowi swobodny wstęp i zapobiec sytuacji, w której zostanie odmówiony wstęp osobie kontrolującej ze względu na brak posiadania przepustki. W tym zakresie zostanie uzupełnione uzasadnienie.
498.	art. 49 pkt 1 [w piśmie z uwagami i błędnie oznaczony jako art. 49 ust. 1]	Polska Izba Radiodyfuzji Cyfrowej	Nie jest realnym, aby osoba prowadząca czynności kontrolne nie miała przepustki do przemieszczania się po obiekcie jednostki kontrolowanej. Bez takowej, w większości przypadków nie będzie miała fizycznie możliwości przemieszczania się z uwagi na systemy kontroli dostępu, które są zresztą wymagane przez tę ustawę i wiele innych. Nie można też od początku określić pełnego zakresu dostępu fizycznego lub logicznego dla takiej osoby ponieważ może się to zmieniać w trakcie trwania czynności kontrolnych. Stosowny zapis powinien umożliwiać osobie kontrolującej dostęp tam, gdzie jest konieczny, ale sposób jego realizacji (przepustka, przewodnik, karta dostępu czy inna metoda) powinien być wybrany przez kontrolowany podmiot ponieważ silnie zależy od przyjętych w tym podmiocie zasad i technologii – np. podmiot może stosować dostęp na podstawie danych biometrycznych, a nie ma powodu, aby przetwarzał dane biometryczne osoby kontrolującej. Podmioty świadczące usługi kluczowe, to np. energetyka. Kto weźmie odpowiedzialność za nieprzeszkoloną stanowiskowo osobę	Wyjaśnienie. Kontroler będzie posiadał odpowiednie dokumenty upoważniające do kontroli, co wynika z art. 79a ustawy o swobodzie działalności gospodarczej. Tym samym wątpliwości wydają się nieuzasadnione. Ponadto, zgodnie z art. 80 ustawy o swobodzie działalności gospodarczej czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Przepis nie wyklucza stosowania wewnętrznych procedur obowiązujących w firmach. Ma on jedynie zapewnić kontrolerowi swobodny wstęp i zapobiec sytuacji, w której zostanie odmówiony wstęp osobie kontrolującej ze względu na brak posiadania przepustki.

			poruszającą się po elektrowni czy petrochemii? Nieznajomość sygnałów czy zasad obowiązujących na obiekcie produkcyjnym może prowadzić nawet do śmierci osoby kontrolującej (wysokie napięcie, para wodna, chemikalia, wyziewy, etc).	W tym zakresie zostanie uzupełnione uzasadnienie.
499.	art. 49. pkt 1	Polska Izba Ubezpieczeń	W art. 49. pkt 1) proponujemy by przyjęcie treść: „1) swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego w okresie prowadzenia kontroli z uwzględnieniem zasad identyfikacji wynikających z regulacji podmiotu kontrolowanego;" W większości podmiotów funkcjonują zasady identyfikacji osób i trybu dostępu do pomieszczeń. Projekt ustawy powinien być w tym zakresie zbieżny z praktyką.	Uwaga nieuwzględniona. Kontroler będzie posiadał odpowiednie dokumenty upoważniające do kontroli, co wynika z art. 79a ustawy o swobodzie działalności gospodarczej. Tym samym uwaga wydaje się nieuzasadniona. Ponadto, zgodnie z art. 80 ustawy o swobodzie działalności gospodarczej czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej.
500.	art. 49 pkt 1 [w piśmie z uwagami i błędnie oznaczony jako art. 49 ust. 1]	Polska Izba Informatyki i Telekomunikacji	Uprawnienie osoby prowadzącej czynności kontrolne do swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki, można oceniać jako zdecydowanie zbyt daleko idące. Przede wszystkim osoba prowadząca czynności kontrolne powinna mieć prawo wstępu i poruszania się po terenie podmiotu kontrolowanego wyłącznie w miejscach związanych ze świadczeniem usługi kluczowej. W praktyce nie jest także realnym, aby osoba prowadząca czynności kontrolne nie miała przepustki do przemieszczania się po obiekcie jednostki kontrolowanej. Bez takowej, w większości przypadków nie będzie miała fizycznie możliwości przemieszczania się z uwagi na systemy kontroli dostępu, które są zresztą wymagane przez tą ustawę i wiele innych. Nie można też od początku określić pełnego zakresu dostępu fizycznego lub logicznego dla takiej osoby, ponieważ może się to zmieniać w trakcie trwania czynności kontrolnych. Stosowny zapis powinien umożliwiać osobie kontrolującej dostęp tam, gdzie jest	Wyjaśnienie. Kontroler będzie posiadał odpowiednie dokumenty upoważniające do kontroli, co wynika z art. 79a ustawy o swobodzie działalności gospodarczej. Tym samym wątpliwości wydają się nieuzasadnione. Ponadto, zgodnie z art. 80 ustawy o swobodzie działalności gospodarczej czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Przepis nie wyklucza stosowania wewnętrznych procedur obowiązujących w firmach. Ma on jedynie zapewnić kontrolerowi swobodny wstęp i zapobiec sytuacji, w której zostanie odmówiony wstęp osobie kontrolującej ze względu na brak posiadania przepustki.

			konieczny, ale sposób jego realizacji (przepustka, przewodnik, karta dostępu czy inna metoda) powinien być wybrany przez kontrolowany podmiot, ponieważ silnie zależy od przyjętych w tym podmiocie zasad i technologii – np. podmiot może stosować dostęp na podstawie danych biometrycznych, a nie ma powodu, aby przetwarzał dane biometryczne osoby kontrolującej. Podmioty świadczące usługi kluczowe, to np. energetyka. Kto weźmie odpowiedzialność za nieprzeszkoloną stanowiskowo osobę poruszającą się po elektrowni czy petrochemii? Nieznajomość sygnałów czy zasad obowiązujących na obiekcie produkcyjnym może prowadzić nawet do śmierci osoby kontrolującej (wysokie napięcie, para wodna, chemikalia, wyziewy, etc). Z uwagi na ochronę podstawowych interesów podmiotów kontrolowanych, w tym świadczonych przez nie usług, rozwiązanie taki budzi szczególne wątpliwości. Jednostkowe sytuacje, w których celowo utrudniane jest wykonywanie czynności kontrolnych, tudzież egzekucyjnych, są regulowane w innych przepisach prawa poprzez możliwość korzystania, np. z asysty Policji, co zresztą przewidziano już w projektowanym art. 53. Ponadto w projekcie należy wyraźnie zaznaczyć, że kontrola może dotyczyć wyłącznie pomieszczeń, dokumentów i systemów wykorzystywanych do świadczenia usługi kluczowej.	W tym zakresie zostanie uzupełnione uzasadnienie.
501.	art. 49 pkt 1	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Zasady wstępu i poruszania się po terenie podmiotu kontrolowanego należy doprecyzować w Art 50.	Uwaga nieuwzględniona. Kontroler będzie posiadał odpowiednie dokumenty upoważniające do kontroli, co wynika z art. 79a ustawy o swobodzie działalności gospodarczej. Tym samym uwaga wydaje się nieuzasadniona. Ponadto, zgodnie z art. 80 ustawy o swobodzie działalności gospodarczej czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej.

502.	art. 49 pkt 1 i 6	Konfederacja Lewiatan	Nie jest realnym, aby osoba prowadząca czynności kontrolne nie miała przepustki do przemieszczania się po obiekcie jednostki kontrolowanej. Bez takowej, w większości przypadków nie będzie miała fizycznie możliwości przemieszczania się z uwagi na systemy kontroli dostępu, które są zresztą wymagane przez tę ustawę i wiele innych. Nie można też od początku określić pełnego zakresu dostępu fizycznego lub logicznego dla takiej osoby ponieważ może się to zmieniać w trakcie trwania czynności kontrolnych. Stosowny zapis powinien umożliwiać osobie kontrolującej dostęp tam, gdzie jest konieczny, ale sposób jego realizacji (przepustka, przewodnik, karta dostępu czy inna metoda) powinien być wybrany przez kontrolowany podmiot ponieważ silnie zależy od przyjętych w tym podmiocie zasad i technologii – np. podmiot może stosować dostęp na podstawie danych biometrycznych, a nie ma powodu, aby przetwarzał dane biometryczne osoby kontrolującej. Podmioty świadczące usługi kluczowe, to np. energetyka. Kto weźmie odpowiedzialność za nieprzeszkoloną stanowiskowo osobę poruszającą się po elektrowni czy petrochemii? Nieznajomość sygnałów czy zasad obowiązujących na obiekcie produkcyjnym może prowadzić nawet do śmierci osoby kontrolującej (wysokie napięcie, para wodna, chemikalia, wyziewy, etc). Wnosimy o wykreślenie zapisu wskazującego na brak konieczności uzyskania przepustki. W projekcie należy wyraźnie zaznaczyć, że kontrola może dotyczyć wyłącznie pomieszczeń, dokumentów i systemów wykorzystywanych do świadczenia usługi kluczowej. Dodatkowo w pkt 6 należy doprecyzować zakres działań związanych z „oględzinami urządzeń, nośników i systemów teleinformatycznych”, w szczególności poprzez wskazanie, że takie „oględziny” nie mogą prowadzić do jakiejkolwiek ingerencji w działanie urządzeń, nośników i systemów (art. 49 pkt 6).	Wyjaśnienie. Kontroler będzie posiadał odpowiednie dokumenty upoważniające do kontroli, co wynika z art. 79a ustawy o swobodzie działalności gospodarczej. Tym samym wątpliwości wydają się nieuzasadnione. Ponadto, zgodnie z art. 80 ustawy o swobodzie działalności gospodarczej czynności kontrolnych dokonuje się w obecności kontrolowanego lub osoby przez niego upoważnionej. Przepis nie wyklucza stosowania wewnętrznych procedur obowiązujących w firmach. Ma on jedynie zapewnić kontrolerowi swobodny wstęp i zapobiec sytuacji, w której zostanie odmówiony wstęp osobie kontrolującej ze względu na brak posiadania przepustki. W tym zakresie zostanie uzupełnione uzasadnienie.

503.	art. 49 pkt 2	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 49 pkt 2 – należy doprecyzować zakres dokumentów mogących podlegać kontroli – w takim stanie kontrolujący może zażądać wglądu we wszystkie dokumenty podmiotu – nawet te nie związane z przedmiotem kontroli. Nie ujęto sposobu postępowania z dokumentami zawierającymi informacje niejawne w rozumieniu przepisów ustawy o ochronie informacji niejawnych;	Uwaga nieuwzględniona. Do zasad dostępu do dokumentów niejawnych zawsze będą stosowane przepisy ustawy o ochronie informacji niejawnych.
504.	art. 49. pkt 2 i 3	Polska Izba Ubezpieczeń	W art. 49. pkt 2) i pkt 3) proponujemy dodać zapis ograniczający do dokumentów dotyczących zakresu i obszaru kontroli. Proponujemy następujące brzmienie: „2) wglądu do związanych z zakresem kontroli dokumentów dotyczących działalności podmiotu kontrolowanego, pobierania za pokwitowaniem oraz zabezpieczenia dokumentów związanych z zakresem kontroli, z zachowaniem przepisów o tajemnicy prawnie chronionej;” „3) sporządzania, a w razie potrzeby żądania sporządzenia niezbędnych do kontroli kopii, odpisów lub wyciągów ze związanych z zakresem kontroli dokumentów oraz zestawień i obliczeń, z zachowaniem przepisów o tajemnicy prawnie chronionej;”	Uwaga nieuwzględniona. W czasie kontroli prowadzący kontrolę ma prawo żądać tylko tych dokumentów, które są związane z zakresem kontroli.
505.	art. 49 pkt 3	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 49 pkt 3 – brak zastrzeżenia dot. kopiowania dokumentów zawierających kluczowe informacje i dokumentów niejawnych w rozumieniu przepisów ustawy o ochronie informacji niejawnych;	Uwaga nieuwzględniona. Zasady kopiowania dokumentów niejawnych i dostępu do nich regulują przepisy dotyczące ochrony informacji niejawnych.
506.	art. 49 pkt 4	Związek Banków Polskich	Proponuje się aby pkt.4 otrzymał brzmienie: "4) dostępu do tajemnicy prawnie chronionej wyłącznie w zakresie niezbędnym do realizacji celu kontroli.".	Uwaga nieuwzględniona. Zasady dostępu do tajemnic prawnie chronionych określają przepisy szczegółowe dotyczące tych tajemnic.

				Ponadto, w czasie kontroli prowadzący kontrolę ma prawo żądać tylko tych dokumentów, które są związane z zakresem kontroli.
507.	art. 49 pkt 4 [w uwagach błędnie oznaczony jako art. 49 ust. 4]	Polska Izba Radiodyfuzji Cyfrowej	Dane osobowe dla poszczególnych podmiotów mogą być również danymi chronionymi innymi tajemnicami – np. tajemnicą bankową, informacją niejawną, tajemnicą handlową (dla spółek giełdowych, etc.) a więc takie dane nie mogą być ujawnione, na podstawie tego zapisu osobie prowadzącej kontrolę. Należy zatem nałożyć na podmiot kontrolujący i osobę kontrolującą obowiązek zapewnienia takiego samego poziomu ochrony przekazanych informacji jaki wynika z przepisów dotyczących ochrony danych w danym sektorze.	Uwaga nieuwzględniona. Zasady dostępu do tajemnic prawnie chronionych określają przepisy szczegółowe dotyczące tych tajemnic. Ponadto, w czasie kontroli prowadzący kontrolę ma prawo żądać tylko tych dokumentów, które są związane z zakresem kontroli.
508.	art. 49 pkt 4 [w uwagach błędnie oznaczony jako art. 49 ust. 4]	Konfederacja Lewiatan	Dane osobowe dla poszczególnych podmiotów mogą być również danymi chronionymi innymi tajemnicami – np. tajemnicą bankową, informacją niejawną, tajemnicą handlową (dla spółek giełdowych, etc.) a więc takie dane nie mogą być ujawnione, na podstawie tego zapisu osobie prowadzącej kontrolę. Należy zatem nałożyć na podmiot kontrolujący i osobę kontrolującą obowiązek zapewnienia takiego samego poziomu ochrony przekazanych informacji jaki wynika z przepisów dotyczących ochrony danych w danym sektorze.	Uwaga nieuwzględniona. Zasady dostępu do tajemnic prawnie chronionych określają przepisy szczegółowe dotyczące tych tajemnic. Ponadto, w czasie kontroli prowadzący kontrolę ma prawo żądać tylko tych dokumentów, które są związane z zakresem kontroli.
509.	art. 49 pkt 4 [w uwagach błędnie oznaczony jako art. 49 ust. 4]	Polska Izba Informatyki i Telekomunikacji	Dane osobowe dla poszczególnych podmiotów mogą być również danymi chronionymi innymi tajemnicami – np. tajemnicą bankową, informacją niejawną, tajemnicą handlową (dla spółek giełdowych, etc.) a więc takie dane nie mogą być ujawnione, na podstawie tego zapisu osobie prowadzącej kontrolę. Należy zatem nałożyć na podmiot kontrolujący i osobę kontrolującą obowiązek zapewnienia takiego samego poziomu ochrony przekazanych informacji jaki wynika z przepisów dotyczących ochrony danych w danym sektorze.	Uwaga nieuwzględniona. Zasady dostępu do tajemnic prawnie chronionych określają przepisy szczegółowe dotyczące tych tajemnic. Ponadto, w czasie kontroli prowadzący kontrolę ma prawo żądać tylko tych dokumentów, które są związane z zakresem kontroli.

510.	art. 49 pkt 4	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Przepisy rozdziału 8 „Nadzór i kontrola” Projektu wydają się nie przystawać do materii, którą reguluje przedmiotowy Projekt. Są one wzorowane na dotychczas obowiązujących przepisach dotyczących kontroli i nadzoru w innych dziedzinach prawa. Projektodawca zdaje się nie dostrzegać faktu, że kontrola z zakresu cyberbezpieczeństwa tylko w ograniczonym zakresie jest kontrolą „fizyczną”. Projekt powinien zostać uzupełniony o szereg postanowień dotyczących możliwości przeprowadzenia kontroli zdalnej, polegającej na wglądzie pracowników organów właściwych do systemów teleinformatycznych. W tym samym zakresie powinny być tez uzupełnione przepisy dotyczące CSIRT, które w celu mitygacji incydentu powinny mieć możliwość interwencji i przejęcie kontroli nad niektórymi systemami teleinformatycznymi. Przepisy powinny także umożliwiać osobie kontrolującej dostęp tam, gdzie jest on konieczny, ale sposób realizacji dostępu (przepustka, przewodnik, karta dostępu czy inna metoda) powinien być wybrany przez kontrolowany podmiot ponieważ silnie zależy od przyjętych w tym podmiocie zasad i technologii. Odnosząc się do art.49 ust. 4 pragniemy wskazać, iż dane osobowe dla poszczególnych podmiotów mogą być również danymi chronionymi innymi tajemnicami – np. tajemnicą bankową, informacją niejawną, tajemnicą handlową (dla spółek giełdowych, etc.) a więc takie dane nie mogą być ujawnione, na podstawie tego zapisu osobie prowadzącej kontrolę. Należy zatem nałożyć na podmiot kontrolujący i osobę kontrolującą obowiązek zapewnienia takiego samego poziomu ochrony przekazanych informacji jaki wynika z przepisów dotyczących ochrony danych w danym sektorze.	Uwaga nieuwzględniona.
511.	art. 49 pkt 6	Polskie Towarzystwa Przesyłu i Rozdziału	Proponujemy doprecyzowanie zapisu. Art. 49 pkt 6 – bardzo szeroki zakres urządzeń, nośników oraz systemów informacyjnych, które mogą być poddane oględzinom przez osobę kontrolującą. Wydaje się zasadnym zawężenie tego zakresu do urządzeń, nośników oraz systemów informacyjnych odpowiedzialnych za	Uwaga nieuwzględniona. Zdaniem projektodawcy zapis jest właściwy.

		Energii Elektrycznej	zabezpieczenie infrastruktury krytycznej a nie elementów tej infrastruktury. Przepis wymaga doprecyzowania	
512.	art. 52	J.K. (uwagi osoby prywatnej)	Zapis o doręczeniu protokołu w postaci elektronicznej jest dość enigmatyczny. Czy kontrolujący jest zobowiązany opatrzyć go kwalifikowanym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP, czy też wysyła skan wydruku ze swoim odręcznym podpisem ? W jaki sposób protokół w wersji elektronicznej zostanie doręczony podmiotowi kontrolowanemu - pocztą elektroniczną czy na nośniku elektronicznym wysłanym zwykłą pocztą ? Zgodnie z art. 39 KPA, strona postępowania musi wyrazić zgodę na doręczanie pism w postępowaniu za pomocą tych środków i wskazać organowi administracji publicznej adres elektroniczny. Protokół w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się kontrolowanemu, a w przypadku protokołu sporządzonego w postaci elektronicznej doręcza się go podmiotowi kontrolowanemu na wskazany przez niego adres elektroniczny za pomocą środków komunikacji elektronicznej w rozumieniu art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2016 r. poz. 1030 i 1579).	Wyjaśnienie. Tak szczegółowa regulacja nie wydaje się konieczna.
513.	art. 52 ust. 4	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy doprecyzowanie zapisu. Art. 52 ust.4 – jest możliwość wniesienia zastrzeżenia do protokołu a nie do wykonywanych przez osobę kontrolującą czynności. Możliwość taka również nie jest przewidziana w art. 52 ust 2 określającym co ma zawierać protokół kontroli.	Uwaga nieuwzględniona. Zdaniem projektodawcy zapis jest właściwy.
514.	art. 52 ust. 5	Polskie Towarzystwa Przesyłu i Rozdziału	Proponujemy doprecyzowanie zapisu. Art. 52 ust. 5 – przepis mówi, że w razie zgłoszenia zastrzeżeń, osoba prowadząca czynności kontrolne dokonuje ich analizy i, w razie potrzeby, podejmuje dodatkowe czynności kontrolne, a w przypadku	Uwaga nieuwzględniona. Zdaniem projektodawcy zapis jest właściwy.

		Energii Elektrycznej	stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu do protokołu. Wydaje się właściwym aby czynności analityczne i ewentualnie dodatkowe czynności kontrolne wykonywane na podstawie zgłoszonych zastrzeżeń, wykonywała inna osoba niż ta która wykonywała pierwszą kontrolę. W razie nieuwzględnienia zgłoszonych zastrzeżeń również powinien być sporządzony aneks do protokołu.	
515.	Art. 53	Pracodawcy RP	Należy wykreślić możliwość włączania do kontroli „specjalistów" bez określenia jakichkolwiek szczegółów w tym zakresie. W szczególności takie osoby powinny posiadać upoważnienie do prowadzenia kontroli, a także muszą legitymować się brakiem wykonywania jakiejkolwiek działalności konkurencyjnej wobec podmiotu kontrolowanego.	Uwaga uwzględniona.
516.	art. 53	J.K. (uwagi osoby prywatnej)	Zgodnie z art. 47 ust. 2 to organ właściwy lub minister właściwy do spraw informatyzacji prowadzi kontrole. Jeżeli dokonanie określonych czynności kontrolnych wymaga wiedzy specjalistycznej organ przeprowadzający kontrolę może włączyć do kontroli specjalistów.	Uwaga uwzględniona.
517.	art. 53 ust. 1	Związek Banków Polskich	Proponuje się aby ust.1 otrzymał brzmienie: "1. W toku kontroli, o której mowa w ust. 47 ust. 2 pkt 1, jeżeli istnieją do tego uzasadnione podstawy, osoba prowadząca czynności kontrolne może korzystać z pomocy funkcjonariuszy innych organów kontroli państwowej lub Policji." Jednocześnie wskazane jest opracowanie wytycznych w zakresie stosowania powyższego przepisu.	Uwaga nieuwzględniona. Jednakże, brzmienie przepisów w tym zakresie zostanie zmienione.
518.	art. 53 ust. 2	Polska Izba Informatyki i Telekomunikacji	Projektowany Art. 53 ust. 2 wprowadza uprawnienie do włączenia do kontroli „specjalistów". Sygnalizujemy, że tego typu uprawnienie nie znajduje uzasadnienia oraz rodzi istotne ryzyka dla podmiotu kontrolowanego. Przede wszystkim pojęcie „specjalisty" nie zostało w żaden sposób zdefiniowane, podobnie jak sposób jego	Uwaga uwzględniona.

			powoływania tudzież jego obowiązki i odpowiedzialność w zakresie wykonywanych czynności, w tym np. kwestii działalności konkurencyjnej. W praktyce umożliwia to organowi włączenie do czynności kontrolnych jakiejkolwiek osoby, niekoniecznie nawet posiadającej upoważnienie do prowadzenia czynności kontrolnych. Należy wziąć pod uwagę, że w związku z kontrolą operator będzie musiał zazwyczaj udostępnić informacje stanowiące tajemnicę przedsiębiorstwa i dlatego nieograniczone uprawnienie w zakresie dopraszania do zespołu kontrolnego bliżej nieokreślonej kategorii „specjalistów" jest w naszej ocenie naruszeniem podstawowych praw podmiotu kontrolowanego. Wnosimy o wykreślenie Art. 53 ust. 2.	
519.	art. 53 ust. 2	Konfederacja Lewiatan	Art. 53 ust. 2 wprowadza uprawnienie do włączenia do kontroli „specjalistów". Sygnalizujemy, że tego typu uprawnienie nie znajduje uzasadnienia oraz rodzi istotne ryzyka dla podmiotu kontrolowanego. Przede wszystkim pojęcie „specjalisty" nie zostało w żaden sposób zdefiniowane, podobnie jak sposób jego powoływania, tudzież jego obowiązki i odpowiedzialność w zakresie wykonywanych czynności, w tym np. kwestii działalności konkurencyjnej. W praktyce umożliwia to organowi włączenie do czynności kontrolnych jakiejkolwiek osoby, niekoniecznie nawet posiadającej upoważnienie do prowadzenia czynności kontrolnych. Należy wziąć pod uwagę, że w związku z kontrolą operator będzie musiał zazwyczaj udostępnić informacje stanowiące tajemnicę przedsiębiorstwa i dlatego nieograniczone uprawnienie w zakresie dopraszania do zespołu kontrolnego bliżej nieokreślonej kategorii „specjalistów" jest w naszej ocenie naruszeniem podstawowych praw podmiotu kontrolowanego. Wnosimy o wykreślenie art. 53 ust. 2.	Uwaga uwzględniona.
520.	art. 53 ust. 2	Fundacja Bezpieczna	Sformułowanie jest niejasne. Czy wiedzę specjalistyczną należy traktować jako wykraczającą poza kompetencje podmiotu kontrolnego? Być może warto napisać to wprost.	Uwaga uwzględniona.

		Cyberprzestrzeń		
521.	art. 56 ust. 2-3	Instytut Kościuszki	Zakres materii koniecznych do uwzględnienia w strategii cyberbezpieczeństwa wskazany w art. 56 ust. 3 pkt 1-7 projektu ustawy pomija wskazany w art. 7 ust. 1 lit. b Dyrektywy NIS a także podrozdziale 2.2. pkt II Załącznika do Komunikatu Komisji do Parlamentu Europejskiego i Rady Pełne Wykorzystanie Potencjału Bezpieczeństwa Sieci i Informacji – Zapewnienie Skutecznego Wdrożenia Dyrektywy NIS, wymóg ustalenia ram zarządzania służących realizacji celów i priorytetów krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, w tym ról i zakresów obowiązków organów rządowych i innych właściwych podmiotów. Projekt ustawy w przedmiotowej kwestii zdaje się odnosić wyłącznie do wymogu wskazania podmiotów zaangażowanych we wdrażanie strategii, co zgodnie z literalną wykładnią art. 7 ust.1 lit. g Dyrektywy NIS, stanowi odrębną materię. Zarówno z uwagi na konieczność prawidłowej implementacji prawa UE, a przede wszystkim podnoszone w m.in. Krajowych Ramach, Założeniach Strategii Cyberbezpieczeństwa dla RP opracowanych przez Zespół Zadaniowy Ministerstwa Cyfryzacji, Raporcie NIK dot. Realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP czy ekspertyzie NASK System bezpieczeństwa cyberprzestrzeni RP, postulaty konsolidacji krajowego systemu cyberbezpieczeństwa oraz określenia zadań i wzajemnych relacji podmiotów w nim uczestniczących, należy odpowiednio uzupełnić art. 56 ust. 3 ustawy. Podobnie należy odnieść się do art. 56 ust. 2 projektu ustawy, zgodnie z którym, strategia obejmuje sektory wskazane w załączniku do ustawy (a więc sektory, podsektory i podmioty z zakresu usług kluczowych) oraz usługi kluczowe. W związku z powyższym oraz w świetle art. 7 ust. 1 zdanie 1 Dyrektyw NIS, pojawia się wątpliwość, na ile intencją projektodawcy było	Uwaga uwzględniona.

			zawężenie zakresu strategii i wyłączenie z niej m.in. operatorów infrastruktury krytycznej czy administracji publicznej. Interpretując przedmiotowy przepis w kontekście całości ustawy – w szczególności podmiotów objętych krajowych systemem cyberbezpieczeństwa (art. 4), jak i obecnym zakresem Krajowych Ram, takie zawężenie zakresu strategii należy uznać za bezzasadne. Również w cytowanym już wyżej Załączniku dotyczącym skutecznego wdrożenia Dyrektywy NIS, podkreślono, iż w odniesieniu do zasady harmonizacji minimalnej, przywołanej w art. 3 Dyrektywy NIS, państwa członkowskie mogą obejmować zakresem strategii, sektory spoza usług kluczowych i cyfrowych, wskazanych w załącznikach do przedmiotowego aktu. W tym kontekście zalecane jest uwzględnienie wszystkich istotnych wymiarów społeczeństwa i gospodarki – w szczególności administracji publicznej oraz innych sektorów omawianych w wytycznych OECD i ITU.	
522.	art. 56 ust. 3 pkt 4	Fundacja Bezpieczna Cyberprzestrzeń	Zamiast „normalnego” powinno być: „stanu sprzed incydentu” albo „normalnego zakłóconego incydentem” albo „normalnego w zakresie cyberbezpieczeństwa”	Uwaga uwzględniona.
523.	art. 56. ust. 5 i 6	Związek Banków Polskich	Proponuje się aby Strategia podlegała obowiązkowemu przeglądowi, raz do roku. Jednocześnie proponuje się aby ust. 5 otrzymał brzmienie: "5. Strategia ustalana jest na okres pięcioletni i raz w roku w terminie do dnia 31 grudnia podlega przeglądowi pod kątem potrzeby jej aktualizacji. Przegląd dokonywany jest przez ministra właściwego ds. cyberbezpieczeństwa a wyniki przeglądu wraz z wnioskami przedstawiane Krajowej Radzie Cyberbezpieczeństwa."	Uwaga nieuwzględniona. Zdaniem projektodawcy zapis jest właściwy.
524.	art. 56. ust. 6	Krajowy Związek Banków	W art. 56 ust. 6 pod rozwagę poddajemy, czy dwuletni okres przeglądu Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej,	Uwaga nieuwzględniona. Zdaniem projektodawcy okres dwuletni jest właściwy.

		Spółdzielczych	biorąc pod uwagę dynamikę zmian zachodzących w tym zakresie, nie jest zbyt długi.	
525.	art. 57 [uwaga do rozdziału X]	Federacja Przedsiębiorców Polskich	Rozszerzenie przepisów penalizujących. Mając na uwadze powagę zagadnienia, postanowienia zawarte w Rodziale 10 Projektu „Przepisy o karach pieniężnych" są zdecydowanie niewystarczające. Maksymalną karą pieniężną przewidzianą Projektem jest 200.000,00 (dwieście tysięcy) złotych. Maksymalna wysokość kar pieniężnych jest rażąco niska. Porównać je można chociażby z karami finansowymi przewidzianymi w projekcie ustawy o ochronie danych osobowych z 12 września 2017 roku, który odsyła do Rozporządzenia ogólnego o ochronie danych osobowych z 27 kwietnia 2016 roku, które przewiduje kary pieniężne aż do 20 mln EURO lub do 4 % światowego obrotu podmiotu dokonującego naruszenia. Zważywszy na istotę regulacji wprowadzanych Projektem, w tym dla bezpieczeństwa obywateli i Państwa, w pełni uzasadnione jest twierdzenie, że naruszenia obowiązków nakładanych Projektem, w tym przez operatorów usług kluczowych, powinny penalizowane przepisami karnymi. Szeroko rozumiane bezpieczeństwo obywateli i Państwa jest ponad wszelką wątpliwość przedmiotem ochrony Projektu. Zauważyć należy, że przewidziane w Projekcie kary pieniężne są niewielkie. Przekładać się to będzie na marginalne traktowanie omawianych regulacji przez podmioty, które powinny stać na straży cyberbezpieczeństwa. Po drugie, kary finansowe mają być nakładane na instytucje, nie zaś osoby, które sprawują w nich funkcje kierownicze. Tym samym, brutalnie rzecz ujmując, osoby pełniące te funkcje, co do zasady, będą miały mniejszą motywację rzetelnego stosowania się do postanowień Projektu niż, gdyby przewidywał on sankcje karne, które z natury swojej dotykałyby te właśnie osoby.	Uwaga uwzględniona. Przepisy dotyczące wysokości kar zostaną zmienione.

			Wprowadzenie penalizacji działań i zaniechań, których skutkiem będzie lub może być uniemożliwienie wzrostu albo zamach na cyberbezpierzeństwo Rzeczpospolitej Polski wydaje się konieczne, zważywszy na doniosłość tego zagadnienia dla przyszłości kraju. Przepisy Kodeksu karnego, w tym dotyczące przestępstw przeciwko bezpieczeństwu powszechnemu (art. 163 i n. Kodeksu karnego) w żadnym stopniu nie przystają do istniejących zagrożeń płynących z cyberprzestrzeni. Przykładowymi przestępstwami, jakie mogłyby zostać ujęte w Projekcie są: (i) nieprawidłowe zabezpieczenie danych, zwłaszcza przez operatorów usług kluczowych lub sprowadzenie zagrożenia ujawnienia lub utraty danych przetwarzanych w systemach informacyjnych; (ii) umyślne (celowe lub poprzez rażące zaniechania) ujawnienie danych przetwarzanych w systemach informacyjnych. Rolę prewencyjną w tym zakresie ustawodawca prawdopodobnie zamierza zrealizować poprzez art. 57 ust. 3 Projektu, lecz kara w nim przewidziana wydaje się zbyt niska, biorąc pod uwagę przedmiot ochrony.	
526.	art. 57	Związek Przedsiębiorców Polskich	Mając na uwadze powagę zagadnienia, postanowienia zawarte w Rodziale 10 Projektu „Przepisy o karach pieniężnych" są zdecydowanie niewystarczające. Maksymalną karą pieniężną przewidzianą Projektem jest 200.000,00 (dwieście tysięcy) złotych. Maksymalna wysokość kar pieniężnych jest rażąco niska. Porównać je można chociażby z karami finansowymi przewidzianymi w projekcie ustawy o ochronie danych osobowych z 12 września 2017 roku, który odsyła do Rozporządzenia ogólnego o ochronie danych osobowych z 27 kwietnia 2016 roku, które przewiduje kary pieniężne aż do 20 mln EURO lub do 4 % światowego obrotu podmiotu dokonującego naruszenia. Zważywszy na istotę regulacji wprowadzanych Projektem, w tym dla bezpieczeństwa obywateli i Państwa, w pełni uzasadnione jest twierdzenie, że naruszenia obowiązków nakładanych Projektem, w	Uwaga uwzględniona. Przepisy dotyczące wysokości kar zostaną zmienione.

			tym przez operatorów usług kluczowych, powinny penalizowane przepisami karnymi. Szeroko rozumiane bezpieczeństwo obywateli i Państwa jest ponad wszelką wątpliwość przedmiotem ochrony Projektu. Zauważyć należy, że przewidziane w Projekcie kary pieniężne są niewielkie. Przekładać się to będzie na marginalne traktowanie omawianych regulacji przez podmioty, które powinny stać na straży cyberbezpieczeństwa. Po drugie, kary finansowe mają być nakładane na instytucje, nie zaś osoby, które sprawują w nich funkcje kierownicze. Tym samym, brutalnie rzecz ujmując, osoby pełniące te funkcje, co do zasady, będą miały mniejszą motywację rzetelnego stosowania się do postanowień Projektu niż, gdyby przewidywał on sankcje karne, które z natury swojej dotykałyby te właśnie osoby. Wprowadzenie penalizacji działań i zaniechań, których skutkiem będzie lub może być uniemożliwienie wzrostu albo zamach na cyberbezpierzeństwo Rzeczpospolitej Polski wydaje się konieczne, zważywszy na doniosłość tego zagadnienia dla przyszłości kraju. Przepisy Kodeksu karnego, w tym dotyczące przestępstw przeciwko bezpieczeństwu powszechnemu (art. 163 i n. Kodeksu karnego) w żadnym stopniu nie przystają do istniejących zagrożeń płynących z cyberprzestrzeni. Przykładowymi przestępstwami, jakie mogłyby zostać ujęte w Projekcie są: (i) nieprawidłowe zabezpieczenie danych, zwłaszcza przez operatorów usług kluczowych lub sprowadzenie zagrożenia ujawnienia lub utraty danych przetwarzanych w systemach informacyjnych; (ii) umyślne (celowe lub poprzez rażące zaniechania) ujawnienie danych przetwarzanych w systemach informacyjnych. Rolę prewencyjną w tym zakresie ustawodawca prawdopodobnie zamierza zrealizować poprzez art. 57 ust. 3 Projektu, lecz kara w nim przewidziana wydaje się zbyt niska, biorąc pod uwagę przedmiot ochrony.	

527.	art. 57	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Wskazać należy, że wysokość kar administracyjnych w art. 57 ust. 2 Projektu powinna być adekwatna do naruszenia, które jest sankcjonowane.	Uwaga uwzględniona. Przepisy dotyczące wysokości kar zostaną zmienione.
528.	art. 57	Polska Izba Ubezpieczeń	Wątpliwości budzi wskazana wysokość kar pieniężnych. Jest nieadekwatna do wydatków, jakie operatorzy kluczowi będą musieli ponieść na wdrożenie mechanizmów wynikających z ustawy (kara 100 000 zł wydaje się zbyt niska w porównaniu do szacowanych kosztów, które należy ponieść na budowę systemu zarządzania bezpieczeństwem przewidzianym dla operatorów kluczowych).	Uwaga uwzględniona. Przepisy dotyczące wysokości kar zostaną zmienione.
529.	art. 57	Instytut Kościuszki	Zgodnie z art. 57 ust. 1 projektu ustawy, karom pieniężnym podlegają wyłącznie operatorzy usług kluczowych. Biorąc pod uwagę postulat tworzenia skonsolidowanego krajowego systemy cyberbezpieczeństwa, zasadne byłoby, aby rozszerzyć ten zakres co najmniej o podmioty publiczne (w rozumieniu rozdziału 4 projektu ustawy) oraz we odpowiednim, niekolidującym z postanowieniami sektorowych aktów Komisji Europejskiej (art. 47 ust. 1 pkt 2 lit. b projektu ustawy, motyw 57 dyretywy NIS) – również dostawców usług cyfrowych (szczególnie w przypadku ich wykorzystania przez podmioty publiczne lub operatorów usług kluczowych – art. 19 ust. 2 projektu ustawy). Wysokość kar pieniężnych wskazana w art. 57 ust. 2-3 projektu ustawy w niedostatecznym stopniu odpowiada wymogowi skuteczności, proporcjonalności i odstraszającego charakteru sankcji, zgodnie z art. 21 Dyrektywy NIS. Biorąc pod uwagę wagę wyzwania budowy efektywnego systemy cyberbezpieczeństwa, jak i rolę oraz charakter przedsiębiorstw, które zostaną uznane za operatorów usług kluczowych, kary pieniężne powinny realnie spełniać funkcje prewencyjną (także w kontekście ograniczeń stopnia odpowiedzialności – np. art. 12 ust. 2 projektu ustawy). Zaproponowana w projekcie ustawy wysokość kar pieniężnych tego wymogu nie spełnia. Warto również	Uwaga częściowo uwzględniona. Przepisy dotyczące wysokości kar zostaną zmienione. Przewidziane zostaną kary pieniężne dla dostawców usług cyfrowych.

			rekomendować projektodawcy, aby uwzględnić w tym zakresie wytyczne z Załącznika, aby określić wysokość kary w postaci wartości procentowej światowego obrotu z poprzedniego roku obrotowego – podobnie jak w przypadku nowelizacji ustawy o ochronie danych osobowych.	
530.	art. 57	A.K. (uwagi osoby prywatnej)	Prawo organu do wydawania wiążących poleceń wprowadzenia środków zaradczych w odniesieniu do stwierdzonych w audycie uchybień (na podstawie kopii sprawozdania z przeprowadzonego audytu). Nieakceptowalnym jest rozwiązanie, w którym organ właściwy wyłącznie na postawie sprawozdania z audytu – z pominięciem elementarnego prawa jakim jest "wysłuchanie" zainteresowanego operatora odnośnie jego stanowiska co do sprawozdania z audytu - miał prawo wydawać operatorowi wiążące polecenia, zwłaszcza w kontekście kary pieniężnej do 50.000 zł w sytuacji niezastosowania się do ww. poleceń. Brak jest ścieżki odwoławczej.	Uwaga uwzględniona. Projekt ustawy zostanie zmieniony poprzez wykreślenie ust. 6 z art. 16 i pkt 7 z art. 57 ust. 1.
531.	art. 57. ust. 1 [nadawca podał błędny ustęp: Art.57-ust. 59]	Związek Banków Polskich	Ministerstwo Cyfryzacji nie przewidziało w projekcie możliwości wprowadzenia innych sankcji nadzorczych niż kary pieniężne. Może to wynikać z faktu, że MC planuje poprzez nakładanie kar pieniężnych zapewnienie wpływów do budżetu państwa. W dokumencie "Ocena Skutków Regulacji", cz. 6 - Wpływ na sektor finansów publicznych, część "Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń", w pierwszym akapicie Ministerstwo Cyfryzacji stwierdziło: "Na potrzeby krajowego systemu cyberbezpieczeństwa przewiduje się wpływy do budżetu państwa z tytułu kar płaconych przez operatorów usług kluczowych (art. 57 ust. 2). Z tytułu art. 57 ust. 2 pkt 1-3 przyjęto liczbę kar na poziomie dwudziestu rocznie w każdej z kategorii, zaś z tytułu art. 57 ust. 2 pkt 4 i 5 oraz ust. 3 przyjęto liczbę kar na poziomie dwóch rocznie w każdej kategorii." oraz w ostatnim akapicie: "Dodatkowo, w części dotyczącej dochodów, uwzględniono wpływy z tytułu podatku dochodowego oraz składek,	Uwaga nieuwzględniona. Projektując akty prawne konieczne jest oszacowanie przewidywanych dochodów wynikających z nakładanych kar. Są to szacunki, a nie cele. Należy podkreślić, że kary będą nakładane w drodze decyzji administracyjnej w następstwie naruszenia prawa, zgodnie z KPA, tym samym wyklucza to możliwość dowolności w zakresie ich nakładania. Składki, o których mowa w OSR, to obowiązkowe składki na ubezpieczenia zdrowotne i społeczne będące składnikiem wynagrodzeń pracowników;

			jak również wpływy z tytułu kar pieniężnych.". To może oznaczać, że w celu wygenerowania zamierzonych przychodów z kar, organy właściwe będą szukały uchybień tam gdzie ich nie ma, tylko po to aby mieć podstawę do nałożenia kary finansowej. Jednocześnie pojawiła się kwestia składek, które będą płacone przez OUC nie wiadomo na czyją rzecz i w jakiej wysokości?	stanowią one dochód Skarbu Państwa i przez to muszą być odnotowane w części dochodowej. OSR zostanie dokładniej opisany w tym zakresie.
532.	art. 57 ust. 1 i 2	Związek Banków Polskich	Uchwała Rady Ministrów nie ma charakteru prawa powszechnie obowiązującego i nie może wprost nakładać obowiązków na OUK, którzy są przedsiębiorcami prywatnymi.	Wyjaśnienie Obowiązki na operatorów usług kluczowych nałożone będą ustawą, a jedynie progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych będą przyjęte w drodze uchwały.
533.	art. 57 ust. 1-3	Polska Organizacja Przemysłu i Handlu Naftowego	Zaproponowane w Projekcie wysokości kar pieniężnych (do 200.000,00 zł – w zależności od naruszenia) w ocenie POPiHN są znacznie wygórowane. Istnieje również ryzyko nakładania „podwójnych kar" w wyniku zbiegu przepisów umożliwiających nałożenie kary (np. przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE) oraz dodatkowych kar od organów regulacyjnych z innych krajów w przypadku incydentu, którego efekty obejmują kilka krajów. Należy również rozważyć wprowadzenie instytucji odstąpienia od wymierzenia kary w przypadku dobrowolnego zgłaszania zagrożeń związanych z cyberbezpieczeństwem lub zgłaszaniem faktów naruszenia przez operatora przepisów Projektu. Skuteczniej zachęciłoby to do wymiany informacji dotyczących nowych zagrożeń oraz sposobu działania w celu zwiększenia świadomości w zakresie lepszej ochrony danego sektora usług kluczowych oraz minimalizacji zagrożeń i efektów cyberprzestępczości.	Uwaga nieuwzględniona. Zdaniem projektodawcy zapis jest właściwy. Ponadto, przesłanki odstąpienia od nałożenia administracyjnej kary pieniężnej zawarte są w art. 189f KPA.

534.	art. 58 ust. 1 w związku z art. 47 ust. 2 pkt 3	Instytut Kościuszki	Zgodnie z art. 58 ust. 1 projektu ustawy, organem właściwym z zakresie nakładania kar pieniężnych na operatorów usług kluczowych, jest organ właściwy dla danego sektora wyznaczony zgodnie z art. 38 ust. 1 projektu ustawy. Biorąc pod uwagę charakter (np. strukturę własnościową) większości podmiotów, które zostaną uznane za operatorów usług kluczowych (m.in. wskazani w OSR), należy rozważyć, na ile nie wpłynie to niekorzystnie na stopień faktycznej realizacji przedmiotowej kompetencji a w konsekwencji utrzymanie (uzyskiwanie, podnoszenie) odpowiedniego poziomu cyberbezpieczeństwa przez te podmioty. Potencjalnym rozwiązaniem w tej kwestii byłaby centralizacja – przekazanie kompetencji organowi nadrzędnemu lub innemu, który nie pozostaje w bezpośredniej relacji z operatorem usług kluczowych potencjalnie podlegającemu karze (przy zachowaniu przez organ właściwy uprawnień nadzorczych, kontrolnych oraz możliwości wezwania do usunięcia naruszenia – art. 58 ust. 2 projektu ustawy).	Uwaga nieuwzględniona. Zdaniem projektodawcy zapis jest właściwy. Kwestie te były konsultowane z potencjalnymi organami właściwymi.
535.	art. 64	Krajowy Związek Banków Spółdzielczych	Proponujemy by organy właściwe, po przeprowadzonej analizie podmiotów w danym sektorze pod kątem ich uznania za operatorów usług kluczowych, poinformowały zainteresowane podmioty o uznaniu ich za operatorów usług kluczowych.	Wyjaśnienie. Reguluje to art. 5 ust. 2 projektowanej ustawy. Podmiot otrzyma decyzję administracyjną o uznaniu za operatora usługi kluczowej.
536.	art. 68. ust.1 pkt 1	Izba Gospodarcza Gazownictwa	Zbyt krótki okres czasu na ewentualne zaprojektowanie, wdrożenie oraz stabilizację całego procesu monitorowania w trybie ciągłym działania usług oraz procesu BCP/DRP. Możliwość realizacja zapisów wymienionego artykułu uzależniona jest od tego, kiedy zostaną opublikowane akty wykonawcze definiujące np. odpowiednie środki techniczne i organizacyjne (patrz. Art. 15, ust. 4) Propozycja zmiany terminu z 6 m-cy na 9 m-cy.	Uwaga nieuwzględniona. Terminy zawarte w art. 68 są wystarczające, jednakże termin w art. 64 zostanie zmieniony. Zostanie wskazany 9 listopada 2018 r., jako termin wynikający z dyrektywy 2016/1148. Wymogi z art. 11 i art. 68 zostaną określone w jednym przepisie, wskazującym na terminy realizacji obowiązków.

537.	art. 68. ust.1 pkt 1	Konfederacja Lewiatan	Okres 6 miesięcy jest niewystarczający na wdrożenie wymagań ustawy. Proponujemy wyznaczenie okresu roku. Proponujemy następujące brzmienie art. 68 ust. 1 pkt 1: Art. 68. 1. Operatorzy usług kluczowych realizują obowiązki określone w: 1) art. 10 ust. 2 pkt 5 i 8 oraz art. 12 ust. 1 – w terminie roku od dnia otrzymania decyzji o uznaniu za operatora usługi kluczowej	Uwaga nieuwzględniona. Terminy zawarte w art. 68 są wystarczające, jednakże termin w art. 64 zostanie zmieniony. Zostanie wskazany 9 listopada 2018 r., jako termin wynikający z dyrektywy 2016/1148. Wymogi z art. 11 i art. 68 zostaną określone w jednym przepisie, wskazującym na terminy realizacji obowiązków.
538.	art. 68. ust.1 pkt 1	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy następujące brzmienie art. 68 ust. 1 pkt 1: Art. 68. 1. Operatorzy usług kluczowych realizują obowiązki określone w: 1) art. 10 ust. 2 pkt 5 i 8 oraz art. 12 ust. 1 – w terminie 2 lat od dnia otrzymania decyzji o uznaniu za operatora usługi kluczowej Okres 6 miesięcy jest niewystarczający na wdrożenie wymagań ustawy. Proponujemy wyznaczenie okresu 2 lat.	Uwaga nieuwzględniona. Terminy zawarte w art. 68 są wystarczające, jednakże termin w art. 64 zostanie zmieniony. Zostanie wskazany 9 listopada 2018 r., jako termin wynikający z dyrektywy 2016/1148. Wymogi z art. 11 i art. 68 zostaną określone w jednym przepisie, wskazującym na terminy realizacji obowiązków.
539.	art. 68. ust.1 pkt 2	Izba Gospodarcza Gazownictwa	Zbyt krótki okres czasu na ewentualne dostosowanie się do wymagań stawianych w ustawie. Propozycja zmiany terminu z 3 m-cy na 9 m-cy.	Uwaga nieuwzględniona. Terminy zawarte w art. 68 są wystarczające, jednakże termin w art. 64 zostanie zmieniony. Zostanie wskazany 9 listopada 2018 r., jako termin wynikający z dyrektywy 2016/1148. Wymogi z art. 11 i art. 68 zostaną określone w jednym przepisie, wskazującym na terminy realizacji obowiązków.
540.	art. 68. ust.1 pkt 2	Konfederacja Lewiatan	Okres 3 miesięcy jest niewystarczający na wdrożenie wymagań ustawy. Proponujemy wyznaczenie okresu 6 miesięcy . Proponujemy następujące brzmienie art. 68 ust. 1 pkt 2:	Uwaga nieuwzględniona. Terminy zawarte w art. 68 są wystarczające, jednakże termin w art. 64 zostanie zmieniony. Zostanie

			Art. 68. 1. Operatorzy usług kluczowych realizują obowiązki określone w: 2) art. 10 ust. 2 pkt 1-4, pkt 6-7 i pkt 9-11 oraz art. 15 ust. 1 – w terminie 6 miesięcy od dnia otrzymania decyzji o uznaniu za operatora usług kluczowych;	wskazany 9 listopada 2018 r., jako termin wynikający z dyrektywy 2016/1148. Wymogi z art. 11 i art. 68 zostaną określone w jednym przepisie, wskazującym na terminy realizacji obowiązków.
541.	art. 68. ust.1 pkt 2	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Proponujemy następujące brzmienie art. 68 ust. 1 pkt 2: Art. 68. 1. Operatorzy usług kluczowych realizują obowiązki określone w: 2) art. 10 ust. 2 pkt 1-4, pkt 6-7 i pkt 9-11 oraz art. 15 ust. 1 – w terminie 2 lat od dnia otrzymania decyzji o uznaniu za operatora usług kluczowych; Okres 3 miesięcy jest niewystarczający na wdrożenie wymagań ustawy. Proponujemy wyznaczenie okresu 2 lat.	Uwaga nieuwzględniona. Terminy zawarte w art. 68 są wystarczające, jednakże termin w art. 64 zostanie zmieniony. Zostanie wskazany 9 listopada 2018 r., jako termin wynikający z dyrektywy 2016/1148. Wymogi z art. 11 i art. 68 zostaną określone w jednym przepisie, wskazującym na terminy realizacji obowiązków.
542.	art. 69	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Izba nie zgadza się z podejściem do wymiany informacji przyjętym w art. 69 Projektu. Wynika z niego, że system teleinformatyczny dedykowany do wymiany informacji oraz komunikacji z CSIRT powstanie do 1 stycznia 2021 r., a do tego czasu wymiana informacji ma się odbywać środkami komunikacji elektronicznej. W związku z poufnym charakterem wymienianych informacji konieczne jest zapewnienie w okresie przejściowym środków zapewniających chociażby minimum bezpieczeństwa prowadzonej korespondencji.	Wyjaśnienie. Art. 69 ust. 2 jasno wskazuje na dostępne środki komunikacji elektronicznej oraz dostępne systemy teleinformatyczne służące do przetwarzania informacji. Należy zachować właściwy poziom bezpieczeństwa, proporcjonalny do poufności przekazywanych wiadomości.
543.	art. 69	Związek Banków Polskich	Wskazany termin uruchomienia systemu na dzień 1 stycznia 2021 r. i wydaje się bardzo odległym w stosunku do czasu przewidzianego na realizację pozostałych wymagań opisanych w ustawie.	Wyjaśnienie. System teleinformatyczny jest w fazie budowy.
544.	art. 69	Polskie Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej	Pytania dotyczące treści artykułu Czy do czasu wdrożenia systemu teleinformatycznego o którym mowa w art. 42, ust.1, zostanie opracowany przez właściwe Ministerstwo wydzielony bezpieczny kanał komunikacji elektronicznej, który posłuży do zgłaszania incydentów oraz wymiany informacjami pomiędzy	Wyjaśnienie. Nie. Art. 69 ust. 2 jasno i wyraźnie wskazuje na dostępne środki komunikacji elektronicznej oraz dostępne systemy teleinformatyczne służące do przetwarzania informacji.

			operatorami usług kluczowych, dostawcami usług cyfrowych, CSIRT MON, CSIRT NASK oraz CSIRT GOV?	
545.	art.69. ust. 2	Związek Banków Polskich	W związku z tym, że data graniczna udostepnienia przez Ministerstwo systemu to dzień 1 stycznia 2021 r, należy doprecyzować ust. 2, w tym Ministerstwo Cyfryzacji powinno stworzyć interfejs niezbędny do przekazywania takich danych – tak aby następowało to w wystandaryzowanym zakresie i formacie.	Uwaga nieuwzględniona. Art. 69 ust. 2 jasno wskazuje na dostępne środki komunikacji elektronicznej oraz dostępne systemy teleinformatyczne służące do przetwarzania informacji.
546.	Art. 72	Business Centre Club	Przechodząc do zapisów Projektu dotyczących operatorów usług kluczowych, należy na początku wskazać, że zgodnie z Dyrektywą NIS ustawa ma być przyjęta do 9 maja, a stosowana od 10 maja 2018 r. włącznie z tym, że operatorzy usług kluczowych mają być wskazani najpóźniej do 9 listopada 2018 r. W Projekcie przewidziano tylko 14-dniowe vacatio legis. W przypadku tak krótkiego terminu pozostaje bardzo mało czasu na wdrożenie jakichkolwiek obowiązków wynikających z ustawy. Oczywiście niektóre podmioty mają zapewne już wdrożone wewnątrz organizacji część z obowiązków, jednak, nawet sam czas rekrutowania stanowiska specjalistycznego w cyberbezpieczeństwie, to nawet nie licząc ograniczeń finansowych, w Polsce to około 6-9 miesięcy, a na świecie nawet rok. Przy vacatio legis przewidzianym w Projekcie dostosowanie się do zapisów ustawy w wymaganym terminie przez podmioty do tego zobowiązane wydaje się zadaniem niemal niemożliwym do zrealizowania.	Uwaga uwzględniona. Termin w art. 64 zostanie zmieniony. Zostanie wskazany 9 listopada 2018 r., jako termin wynikający z dyrektywy 2016/1148. Wymogi z art. 11 i art. 68 zostaną określone w jednym przepisie, wskazującym na terminy realizacji obowiązków.
547.	art. 72	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Przewidziany w projekcie ustawy czternastodniowy okres vacatio legis jest zdecydowanie zbyt krótki, aby umożliwić efektywne wdrożenie wynikających z ustawy wymogów i funkcjonalności technicznych.	Uwaga uwzględniona. Termin w art. 64 zostanie zmieniony. Zostanie wskazany 9 listopada 2018 r., jako termin wynikający z dyrektywy 2016/1148.

				Wymogi z art. 11 i art. 68 zostaną określone w jednym przepisie, wskazującym na terminy realizacji obowiązków.
548.	art. 72	Konfederacja Lewiatan	Zgodnie z Dyrektywą ustawa ma być przyjęta do 9 maja a stosowana od 10 maja włącznie z tym, że operatorzy usług kluczowych mają być wskazani najpóźniej do 9 listopada. Ustawa ma vacatio legis tylko 14 dni. Pozostaje bardzo mało czasu na wdrożenie jakichkolwiek obowiązków wynikających z ustawy. Oczywiście niektóre podmioty mają zapewne już wdrożone wewnątrz organizacji część z obowiązków, jednak, nawet sam czas rekrutowania stanowiska specjalistycznego w cyberbezpieczeństwie, to nawet nie licząc ograniczeń finansowych, w Polsce około 6-9 miesięcy, a na świecie nawet bliżej roku. Przy obecnym vacatio legis dostosowanie się do zapisów ustawy w wymaganym terminie przez podmioty do tego zobowiązane wydaje się wątpliwym.	Uwaga uwzględniona. Termin w art. 64 zostanie zmieniony. Zostanie wskazany 9 listopada 2018 r., jako termin wynikający z dyrektywy 2016/1148. Wymogi z art. 11 i art. 68 zostaną określone w jednym przepisie, wskazującym na terminy realizacji obowiązków.
549.	art. 72	Krajowa Spółdzielcza Kasa Oszczędnościowo-Kredytowa	Należy zauważyć, że przyszła ustawa ma wejść w życie po upływie 14 dni od dnia ogłoszenia, przy czym projekt nie przewiduje co do zasady okresów na dostosowanie się przez operatorów usług kluczowych do nowych wymogów. Wyjątkiem jest art. 11 projektu, nakładający na nich obowiązek opracowania dokumentacji dotyczącej systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, zgodnie z którym spełnienie tego obowiązku musi nastąpić w ciągu 6 miesięcy od dnia otrzymania decyzji o uznaniu za operatora usługi kluczowej. Aby jednak i ten obowiązek mógł zostać wykonany prawidłowo, niezbędna jest pełna znajomość wszystkich nakładanych nową ustawą wymogów, a zatem również tych, które wynikać będą z aktów wykonawczych do ustawy (w tym z rozporządzenia, o którym mowa w art. 11 ust. 3 projektu). Ponieważ na obecnym etapie prac wymogi te nie są jeszcze znane, a ponadto nie jest znany termin, w którym nastąpi wydanie przedmiotowych aktów wykonawczych, trudno	Uwaga uwzględniona. Termin w art. 64 zostanie zmieniony. Zostanie wskazany 9 listopada 2018 r., jako termin wynikający z dyrektywy 2016/1148. Wymogi z art. 11 i art. 68 zostaną określone w jednym przepisie, wskazującym na terminy realizacji obowiązków.

			oszacować, czy faktyczny termin, w jakim operatorzy usług kluczowych będą musieli wywiązać się z nowych obowiązków, będzie terminem realnym. Mając powyższe na względzie Kasa Krajowa prosi o rozważenie możliwości zapewnienia w przyszłych regulacjach ustawowych odpowiedniego terminu wejścia w życie wszystkich w/w, aktów wykonawczych do ustawy, jak również uwzględnienia przepisu, zapewniającego operatorom usług kluczowych (niezależnie od terminu określonego w art. 11 ust. 1) odpowiedni termin na dostosowanie się do nowych wymogów, liczony od dnia wydania ostatniego z aktów wykonawczych, mających wpływ na treść tych obowiązków.	
550.	załącznik	Związek Pracodawców Mediów Elektronicznych i Telekomunikacji MEDIAKOM	W ocenie MEDIAKOM prawidłowe jest przyjęte w projekcie rozwiązanie, że nie każdy z przedsiębiorców prowadzących działalność w ramach sektorów i podsektorów wymienionych w załączniku do ustawy będzie zobowiązany wykonywać obowiązki przewidziane dla operatorów usług kluczowych. Zasadnie uzależnia się to od decyzji właściwego organu, opartej na kryteriach liczby użytkowników, udziału w rynku czy zasięgu geograficznego usług przedsiębiorcy. MEDIAKOM zgłasza jednak obiekcje do nieprecyzyjnych zapisów ustawy, których uchwalenie może spowodować, że niepotrzebnie jej regulacjami objęci zostaną mali i średni operatorzy telekomunikacyjni. Przykładem braku precyzji jest proponowana treść załącznika do projektu ustawy, w części, w której jako podmioty, spośród których można wskazać operatora usług kluczowych wymienia się podmioty świadczące usługi DNS. Wskazać trzeba, że ustawa nie zawiera definicji pojęcia świadczenia usługi DNS i pojawia się w związku z tym pytanie, czy za usługodawcę takich usług nie będzie uznany także przedsiębiorca telekomunikacyjny, który wykorzystuje serwer DNS do celów świadczenia usług telekomunikacyjnych. Brak doprecyzowania	Wyjaśnienie. Decyzja o uznaniu za operatora usługi kluczowej będzie wydawana zgodnie z zapisem art. 5 projektowanej ustawy w oparciu o opracowane progi istotności, o których mowa w art. 7.Wskazane w załączniku do ustawy podmioty świadczące usługi DNS zostały określone zgodnie z załącznikiem do dyrektywy 2016/1148, która jest implementowana przez niniejszy projekt ustawy.

			pojęcia „świadczenia usług DNS” powoduje, że interpretacja tego pojęcia może być różna i skutkować tym, że także lokalni przedsiębiorcy telekomunikacyjni korzystający z serwera DNS dla potrzeb świadczenia usług innego typu będą kwalifikowane do tej grupy. W tej sytuacji MEDIAKOM podnosi konieczność doprecyzowania pojęcia „świadczenia usług DNS”, by nie wpadały pod to pojęcie podmioty, które realnie usług DNS nie świadczą, a jedynie korzystają z serwerów DNS dla celów świadczenia usług innego rodzaju.	
551.	OSR	Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji	Ponadto przedstawione w Ocenie Skutków Regulacji wyliczenia są nierealne i nie uwzględniają tego, że wraz z wejściem w życie ustawy gwałtownie wzrośnie popyt na usługi z zakresu IT, co w pierwszym okresie doprowadzi do wzrostu cen. Założenie, że koszt nałożony na operatorów usług kluczowych to 2 mln zł w skali roku jest nierealne – w samym OSR liczby potencjalnych operatorów usług kluczowych oszacowano na 360, zakup przez nich usług bezpieczeństwa lub stworzenie własnych kompetencji w tym zakresie to wydatek rzędu kilkuset milionów złotych rocznie. Projektodawca wydaje się tego w ogóle nie dostrzegać. Również przyjęte obciążenia dla sektora publicznego wydają się być niedoszacowane – pomimo tego że Projekt nakłada na ministra właściwego do spraw cyfryzacji szereg nowych zadań, planowane jest utworzenie w ministerstwie tylko 9 nowych etatów Wskazana ilość etatów jest zbyt mała na przeprowadzanie setek kontroli rocznie. W tym zakresie Projekt wymaga zatem dopracowania i urealnienia jego oceny społeczno-gospodarczej.	Uwaga nieuwzględniona. Należy zwrócić uwagę, że podmioty świadczące usługi zależne od systemów teleinformatycznych już teraz zapewniają bezpieczeństwo swoich systemów w celu ciągłego świadczenia usług. Odnośnie podmiotów publicznych, wskazać należy, że podmioty publiczne są obecnie zobowiązane na mocy obowiązujących przepisów do zapewnienia bezpieczeństwa swoich usług. Niniejsza ustawa doprecyzowuje tylko środki, jakie mają być przez nich stosowane.

TABELA ZGODNOŚCI
dla projektu ustawy o krajowym systemie cyberbezpieczeństwa

Tytuł projektu	Projekt ustawy o krajowym systemie cyberbezpieczeństwa
Tytuł wdrażanego aktu prawnego	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

Jednostka redakcyjna dyrektywy	**Treść przepisu dyrektywy 2016/1148**	**Jednostka redakcyjna projektu ustawy**	**Treść projektu ustawy o krajowym systemie cyberbezpieczeństwa**
Przedmiot i zakres stosowania Art. 1	1. Niniejsza dyrektywa ustanawia środki mające na celu osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, aby poprawić funkcjonowanie rynku wewnętrznego. 2. W tym celu niniejsza dyrektywa: a) ustanawia obowiązki dla wszystkich państw członkowskich dotyczące przyjęcia krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych; b) tworzy grupę współpracy, aby wspierać i ułatwiać strategiczną współpracę i wymianę informacji między państwami członkowskimi oraz rozwijać wśród nich zaufanie i pewność; c) tworzy sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwaną dalej „siecią CSIRT"), aby przyczyniać się do rozwijania zaufania i pewności między państwami członkowskimi oraz promować szybką i skuteczną współpracę operacyjną; d) ustanawia wymogi dotyczące bezpieczeństwa i zgłaszania incydentów dla operatorów usług kluczowych i dostawców usług cyfrowych; e) ustanawia obowiązki dla państw członkowskich dotyczące wyznaczania właściwych organów krajowych, pojedynczych punktów kontaktowych oraz CSIRT mających zadania związane z bezpieczeństwem sieci i systemów informatycznych. 3. Wymogi dotyczące bezpieczeństwa i zgłaszania incydentów przewidziane w niniejszej dyrektywie nie mają zastosowania do przedsiębiorstw, które podlegają wymogom art. 13a i 13b dyrektywy 2002/21/WE, ani do dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia (UE) nr 910/2014.	Art. 1	**Art. 1.** 1. Ustawa określa: 1) organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu; 2) sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy; 3) zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. 2. Ustawy nie stosuje się do: 1) przedsiębiorców telekomunikacyjnych, o których mowa w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138 i 650) w zakresie wymogów dotyczących bezpieczeństwa i zgłaszania incydentów; 2) dostawców usług zaufania, którzy podlegają wymogom art. 19 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr

	4. Niniejszą dyrektywę stosuje się bez uszczerbku dla dyrektywy Rady 2008/114/WE (14) i dyrektyw Parlamentu Europejskiego i Rady 2011/93/UE (15) oraz 2013/40/UE (16). 5. Bez uszczerbku dla art. 346 TFUE informacje, które są poufne zgodnie z przepisami unijnymi i krajowymi, takimi jak przepisy dotyczące tajemnicy przedsiębiorstwa, podlegają wymianie z Komisją i innymi odpowiednimi organami tylko wtedy, gdy wymiana taka jest niezbędna do stosowania niniejszej dyrektywy. Informacje podlegające wymianie ogranicza się do tego, co jest istotne dla celów takiej wymiany i proporcjonalne do jej celów. Taka wymiana informacji musi zachować poufność tych informacji oraz chronić bezpieczeństwo i interesy handlowe operatorów usług kluczowych i dostawców usług cyfrowych. 6. Niniejsza dyrektywa pozostaje bez uszczerbku dla działań podejmowanych przez państwa członkowskie w celu zagwarantowania ich podstawowych funkcji państwowych, w szczególności w celu ochrony bezpieczeństwa narodowego – w tym działań na rzecz ochrony informacji, których ujawnienie państwa członkowskie uważają za sprzeczne z podstawowymi interesami swojego bezpieczeństwa – oraz w celu utrzymania porządku publicznego, w szczególności w celu umożliwienia prowadzenia postępowań przygotowawczych w sprawie przestępstw, ich wykrywania i ścigania. 7. W przypadku gdy sektorowy akt prawny Unii wymaga od operatorów usług kluczowych lub dostawców usług cyfrowych, aby zapewniali bezpieczeństwo swoich sieci i systemów informatycznych albo zgłaszali incydenty, stosuje się przepisy tego sektorowego aktu prawnego Unii, pod warunkiem że takie wymogi są przynajmniej równoważne pod względem skutku z obowiązkami określonymi w niniejszej dyrektywie.		910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73);
Przetwarzanie danych osobowych Art. 2	1. Przetwarzanie danych osobowych na mocy niniejszej dyrektywy odbywa się zgodnie z dyrektywą 95/46/WE. 2. Przetwarzanie danych osobowych przez instytucje i organy Unii na mocy niniejszej dyrektywy odbywa się zgodnie z rozporządzeniem (WE) nr 45/2001.	Art. 39	**Art. 39.** 1. W celu realizacji zadań, o których mowa w 26 ust. 3 pkt 1-11 i 14-15 i ust. 5-8 oraz art. 44 ust. 1-3, CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa przetwarzają dane pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa, w tym dane osobowe, obejmujące także dane określone w art. 9 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE L 119 z

			4.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679”, w zakresie i celu niezbędnym do realizacji tych zadań. 2. CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa przetwarzając dane osobowe określone w art. 9 ust. 1 rozporządzeniem 2016/679, prowadzą analizę ryzyka, stosują środki ochrony przed złośliwym oprogramowaniem, stosują mechanizmy kontroli dostępu oraz opracowują procedury bezpiecznej wymiany informacji. 3. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa przetwarzają dane pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa: 1) dotyczące użytkowników systemów informacyjnych oraz użytkowników telekomunikacyjnych urządzeń końcowych; 2) dotyczące telekomunikacyjnych urządzeń końcowych w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne; 3) gromadzone przez operatorów usług kluczowych i dostawców usług cyfrowych w związku ze świadczeniem usług; 4) gromadzone przez podmioty publiczne w związku z realizacją zadań publicznych dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1. 4. W celu realizacji zadań określonych w ustawie minister właściwy do spraw informatyzacji, Dyrektor Rządowego Centrum Bezpieczeństwa, Pełnomocnik oraz organy właściwe przetwarzają dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa: 1) gromadzone przez operatorów usług kluczowych i dostawców usług cyfrowych w związku ze świadczeniem usług; 2) gromadzone przez podmioty publiczne w związku z realizacją zadań publicznych; 3) dotyczące podmiotów zgłaszających incydent zgodnie z art. 30 ust. 1. 5. Dane, o których mowa w ust. 3 i 4, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK i sektorowy zespół cyberbezpieczeństwa niezwłocznie po stwierdzeniu, że nie są niezbędne dla realizacji zadań, o których mowa w art. 26 pkt 1-11, 14-15 i ust. 5-8 oraz art. 44 ust. 1-3.

			6. Dane, o których mowa w ust. 3 i 4, niezbędne dla realizacji zadań, o których mowa w art. 26 pkt 1-11 i 14-15 i ust. 5-8 oraz art. 44 ust. 1-3, są usuwane lub anonimizowane przez CSIRT MON, CSIRT NASK i sektorowy zespół cyberbezpieczeństwa w terminie 5 lat od zakończenia obsługi incydentu, którego dotyczą. 7. W celu realizacji zadań określonych w ustawie CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa mogą wzajemnie przekazywać dane osobowe, o których mowa w ust. 3, w zakresie niezbędnym do realizacji tych zadań i współpracować z organem właściwym do spraw ochrony danych osobowych. 8. Przetwarzanie przez CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa danych osobowych, o których mowa w ust. 3, nie wymaga realizacji obowiązków, o których mowa w art. 15, art. 16 i art. 18 ust. 1 lit. a i d i art. 19 zdanie drugie rozporządzenia 2016/679, jeżeli uniemożliwiłoby to realizację zadań CSIRT NASK, CSIRT MON i sektorowych zespoły cyberbezpieczeństwa, o których mowa w art. 26 pkt 1-11 i 14-15 i ust. 5-8 oraz art. 44 ust. 1-3, i jest możliwe, gdy CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa prowadzą analizę ryzyka, stosują środki ochrony przed złośliwym oprogramowaniem, stosują mechanizmy kontroli dostępu oraz opracowują procedury bezpiecznej wymiany informacji. 9. CSIRT MON, CSIRT NASK i sektorowe zespoły cyberbezpieczeństwa publikują na swojej stronie internetowej: 1) dane kontaktowe administratora danych oraz gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych; 2) cele przetwarzania i podstawę prawną przetwarzania; 3) kategorie przetwarzanych danych osobowych; 4) informacje o odbiorcach danych osobowych; 5) okres, przez który dane osobowe będą przechowywane; 6) informacje, o ograniczeniach obowiązków i praw osób, których dane dotyczą; 7) informacje o prawie wniesienia skargi do organu właściwego do spraw ochrony danych osobowych; 8) źródło pochodzenia danych osobowych.

		Art. 42 ust. 1 pkt 10 Art. 55 pkt 4	Art. 42. 1. Organ właściwy: 10) przetwarza informacje, w tym dane osobowe, dotyczące świadczonych usług kluczowych i usług cyfrowych oraz operatorów usług kluczowych lub dostawców usług cyfrowych w zakresie niezbędnym do realizacji zadań wynikających z ustawy; Art. 55. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ma prawo do: 4) przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu kontroli;
Harmonizacja minimalna Art. 3	Państwa członkowskie mogą, bez uszczerbku dla art. 16 ust. 10 oraz dla ich obowiązków wynikających z prawa Unii, przyjmować lub utrzymywać przepisy mające na celu osiągnięcie wyższego poziomu bezpieczeństwa sieci i systemów informatycznych.		Nie wymaga transpozycji
Definicje Art. 4 Art. 4 pkt 1	„sieci i systemy informatyczne” oznaczają: a) sieci łączności elektronicznej w rozumieniu art. 2 lit. a) dyrektywy 2002/21/WE; b) wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych; lub c) dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w lit. a) i b) w celu ich eksploatacji, użycia, ochrony i utrzymania;	Art. 2 pkt 14	14) system informacyjny – system teleinformatyczny, o którym mowa w ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), wraz z przetwarzanymi w nim danymi w postaci elektronicznej;
Art. 4 pkt 2	„bezpieczeństwo sieci i systemów informatycznych” 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;	Art. 2 pkt 4	4) cyberbezpieczeństwo – odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy;
Art. 4 pkt 3	„krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych” oznacza ramy zapewniające strategiczne cele i priorytety w zakresie bezpieczeństwa sieci i systemów informatycznych na poziomie krajowym;	Art. 68 ust. 1 i ust. 2 pkt 1	Art. 69. 1. Strategia określa cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. Strategia obejmuje sektory, o których mowa w załączniku nr 1 do ustawy, usługi cyfrowe oraz podmioty publiczne, o których mowa w art. 4 pkt 7-15. 2. Strategia uwzględnia w szczególności:

			1) cele i priorytety w zakresie cyberbezpieczeństwa;
Art. 4 pkt 4	„operator usług kluczowych” oznacza podmiot publiczny lub prywatny, należący do jednego z rodzajów, o których mowa w załączniku II, spełniający kryteria określone w art. 5 ust. 2;	Art. 5 ust. 1	Art. 5. 1. Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy wydał decyzję o uznaniu za operatora usługi kluczowej. Załącznik nr 1 do ustawy określa sektor, podsektor oraz rodzaj podmiotu.
Art. 4 pkt 5	„usługa cyfrowa” oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 (17), która należy do jednego z rodzajów wymienionych w załączniku III;	Art. 17 ust. 1	Art. 17. 1. Dostawcą usługi cyfrowej jest osoba prawna albo jednostka organizacyjna nie posiadająca osobowości prawnej, mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219 oraz z 2018 r. poz. 650), wymienioną w załączniku nr 2 do ustawy, z wyjątkiem przedsiębiorców, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. poz. 646). Załącznik nr 2 do ustawy określa rodzaje usług cyfrowych.
Art. 4 pkt 6	„dostawca usług cyfrowych” oznacza każdą osobę prawną, która świadczy usługi cyfrowe;	Art. 17 ust. 1	Art. 17. 1. Dostawcą usługi cyfrowej jest osoba prawna albo jednostka organizacyjna nie posiadająca osobowości prawnej, mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219 oraz z 2018 r. poz. 650), wymienioną w załączniku nr 2 do ustawy, z wyjątkiem przedsiębiorców, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. poz. 646). Załącznik nr 2 do ustawy określa rodzaje usług cyfrowych.
Art. 4 pkt 7	„incydent” oznacza każde zdarzenie, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych;	Art. 2 pkt 5 Art. 2 pkt 7-8	5) incydent – każde zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo; 7) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej; 8) incydent istotny – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi

			ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151”;
Art. 4 pkt 8	„postępowanie w przypadku incydentu” oznacza wszystkie procedury umożliwiające wykrywanie i analizowanie incydentu, ograniczenie jego skutków oraz reagowanie na niego;	Art. 2 pkt 10	10) obsługa incydentu – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych, ograniczenie skutków incydentu;
Art. 4 pkt 9	„ryzyko” oznacza każdą dającą się racjonalnie określić okoliczność lub zdarzenie, które ma potencjalny niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych;	Art. 2 pkt 12, 13 i 17	12) ryzyko – kombinacja prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji; 13) szacowanie ryzyka – całościowy proces identyfikacji, analizy i oceny ryzyka; 17) zarządzanie ryzykiem – skoordynowane działania w zakresie zarządzania cyberbezpieczeństwem w odniesieniu do oszacowanego ryzyka
Art. 4 pkt 10	„przedstawiciel” oznacza każdą osobę fizyczną lub prawną ustanowioną w Unii, wyraźnie wyznaczoną do występowania w imieniu dostawcy usług cyfrowych nieposiadającego jednostki organizacyjnej w Unii, do którego właściwy organ krajowy lub CSIRT może się zwrócić zamiast do dostawcy usług cyfrowych, w związku z obowiązkami dostawcy usług cyfrowych w ramach niniejszej dyrektywy;	Art. 17 ust. 5	5. Przedstawicielem może być osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, ustanowiona w Rzeczypospolitej Polskiej lub w innym państwie członkowskim Unii Europejskiej, wyznaczona do występowania w imieniu dostawcy usługi cyfrowej, który nie posiada jednostki organizacyjnej w Unii Europejskiej, do którego organ właściwy, CSIRT MON, CSIRT NASK lub CSIRT GOV może się zwrócić w związku z obowiązkami dostawcy usługi cyfrowej wynikającymi z ustawy.
Art. 4 pkt 11	„norma” oznacza normę w rozumieniu art. 2 pkt 1 rozporządzenia (UE) nr 1025/2012;		Nie wymaga transpozycji
Art. 4 pkt 12	„specyfikacja” oznacza specyfikację techniczną w rozumieniu art. 2 pkt 4 rozporządzenia (UE) nr 1025/2012;		Nie wymaga transpozycji
Art. 4 pkt 13	„punkt wymiany ruchu internetowego (IXP)” oznacza obiekt sieciowy, który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi systemami autonomicznymi, głównie do celów ułatwienia wymiany ruchu internetowego; IXP zapewnia połączenie międzysystemowe wyłącznie systemów autonomicznych; IXP nie wymaga, aby ruch internetowy między jakąkolwiek parą uczestniczących systemów autonomicznych przechodził przez jakikolwiek trzeci system autonomiczny, ani nie powoduje zmian w tym ruchu, ani w inny sposób w niego nie ingeruje;	Załącznik nr 1 do ustawy	Podmiot prowadzący punkt wymiany ruchu internetowego (IXP), stanowiącego obiekt sieciowy, który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi systemami autonomicznymi, głównie do celów ułatwienia wymiany ruchu internetowego.
Art. 4 pkt 14	„system nazw domen (DNS)” oznacza hierarchiczny rozproszony system nazw sieciowych, który odpowiada na zapytania o nazwy domen;		Nie wymaga transpozycji
Art. 4 pkt 15	„dostawca usług DNS” oznacza podmiot, która świadczy	Załącznik nr	Podmiot, który świadczy usługi DNS.

	w internecie usługi DNS;	1 do ustawy	
Art. 4 pkt 16	„rejestr nazw domen najwyższego poziomu” oznacza podmiot, który zarządza rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD) i dokonuje takiej rejestracji;	Załącznik nr 1 do ustawy	Podmiot zarządzający rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD).
Art.4 pkt 17	„internetowa platforma handlowa” oznacza usługę cyfrową, która umożliwia konsumentom lub przedsiębiorcom zdefiniowanym odpowiednio w art. 4 ust. 1 lit. a) i lit. b) dyrektywy Parlamentu Europejskiego i Rady 2013/11/UE ([18]) zawieranie online umów dotyczących sprzedaży lub usług z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który używa usług komputerowych świadczonych przez internetową platformę handlową;	Załącznik nr 2 do ustawy	Usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową.
Art. 4 pkt 18	„wyszukiwarka internetowa” oznacza usługę cyfrową, która umożliwia użytkownikom wyszukiwanie – co do zasady – wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania na jakikolwiek temat przez podanie słowa kluczowego, wyrażenia lub innej wartości wejściowej; w wyniku przedstawia ona odnośniki, pod którymi można znaleźć informacje związane z zadanym zapytaniem;	Załącznik nr 2 do ustawy	Usługa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiającą w wyniku odnośniki, odnoszące się do informacji związanych z zapytaniem.
Art. 4 pkt 19	„usługa przetwarzania w chmurze” oznacza usługę cyfrową umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania.	Załącznik nr 2 do ustawy	Usługa umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników.
Identyfikacja operatorów usług kluczowych Art. 5	1. W terminie do dnia 9 listopada 2018 r. w odniesieniu do każdego sektora i podsektora, o których mowa w załączniku II, państwa członkowskie identyfikują operatorów usług kluczowych posiadających jednostkę organizacyjną na ich terytorium. 2. Kryteria identyfikacji operatorów usług kluczowych, o których mowa w art. 4 pkt 4, są następujące: a) podmiot świadczy usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej; b) świadczenie tej usługi zależy od sieci i systemów informatycznych; oraz c) incydent miałby istotny skutek zakłócający dla świadczenia tej usługi.	Art. 81 Art. 5	Art. 81. Organy właściwe, w terminie do dnia 9 listopada 2018 r., wydadzą decyzje o uznaniu za operatora usługi kluczowej oraz przekażą ministrowi właściwemu do spraw informatyzacji wnioski o wpisanie operatorów usług kluczowych do wykazu, o którym mowa w art. 7. Art. 5. 1. Operatorem usługi kluczowej jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy wydał decyzję o uznaniu za operatora usługi kluczowej. Załącznik nr 1 do ustawy określa sektor, podsektor oraz rodzaj podmiotu. 2. Organ właściwy wydaje decyzję o uznaniu podmiotu za operatora usługi kluczowej, jeżeli: 1) podmiot świadczy usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, zwaną dalej „usługą kluczową”, wymienioną w wykazie usług

			kluczowych; 2) świadczenie tej usługi kluczowej zależy od systemów informacyjnych; 3) incydent miałby istotny skutek zakłócający dla świadczenia usługi kluczowej przez tego operatora. 3. Istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej, o którym mowa w ust. 2 pkt 3, określana jest na podstawie progów istotności skutku zakłócającego. 4. W przypadku, gdy podmiot świadczy usługę kluczową w innych państwach członkowskich Unii Europejskiej, organ właściwy w toku postępowania administracyjnego, za pośrednictwem Pojedynczego Punktu Kontaktowego, prowadzi konsultacje z tymi państwami w celu ustalenia, czy podmiot został w tych państwach uznany za operatora usługi kluczowej. 5. Okres na przeprowadzenie konsultacji, o których mowa w ust. 4, nie wlicza się do terminów, o których mowa w art. 35 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257 oraz z 2018 r. poz. 149 i 650). 6. W stosunku do podmiotu, który przestał spełniać warunki, o których mowa w ust. 1 i 2, organ właściwy wydaje decyzję stwierdzającą wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej. 7. Decyzje, o których mowa w ust. 2 i 6, podlegają natychmiastowemu wykonaniu.
	3. Do celów ust. 1 każde państwo członkowskie ustanawia wykaz usług, o których mowa w ust. 2 lit. a). 4. Do celów ust. 1, w przypadku gdy podmiot świadczy usługę, o której mowa w ust. 2 lit. a), w dwóch lub większej liczbie państw członkowskich, te państwa członkowskie wzajemnie się konsultują. Konsultacje te odbywają się przed podjęciem decyzji o identyfikacji. 5. Państwa członkowskie regularnie, lecz nie rzadziej niż co dwa lata, po dniu 9 maja 2018 r., dokonują przeglądu oraz, w stosownych przypadkach, aktualizują wykaz zidentyfikowanych operatorów usług kluczowych.	Art. 6	Art. 6. Rada Ministrów określi, w drodze rozporządzenia: 1) wykaz usług kluczowych, o których mowa w art. 5 ust. 2 pkt 1, kierując się przyporządkowaniem usługi kluczowej do danego sektora, podsektora i rodzaju podmiotu wymienionych w załączniku nr 1 do ustawy oraz znaczeniem usługi dla utrzymania krytycznej działalności społecznej lub gospodarczej; 2) progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w wykazie usług kluczowych, uwzględniając: a) liczbę użytkowników zależnych od usługi świadczonej przez dany podmiot, b) zależność innych sektorów, o których mowa w załączniku nr 1 do ustawy, od usługi świadczonej przez ten podmiot, c) wpływ, jaki incydent – jeżeli chodzi o skalę i czas trwania – mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne,

			d) udział podmiotu świadczącego usługę kluczową w rynku, e) zasięg geograficznego związany z obszarem, którego mógłby dotyczyć incydent, f) zdolność podmiotu dla utrzymywania wystarczającego poziomu świadczenia usługi przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia, g) inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują – kierując się potrzebą zapewnienia ochrony przed zagrożeniem życia i zdrowia ludzi, znacznymi stratami majątkowymi, obniżeniem jakości świadczonej usługi kluczowej. 4. W przypadku, gdy podmiot świadczy usługę kluczową w innych państwach członkowskich Unii Europejskiej, organ właściwy w toku postępowania administracyjnego, za pośrednictwem Pojedynczego Punktu Kontaktowego, prowadzi konsultacje z tymi państwami w celu ustalenia, czy podmiot został w tych państwach uznany za operatora usługi kluczowej. 5. Okres na przeprowadzenie konsultacji, o których mowa w ust. 4, nie wlicza się do terminów, o których mowa w art. 35 ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257 oraz z 2018 r. poz. 149).
		Art. 42 ust. 1 pkt 1-6	Art. 42. 1. Organ właściwy: 1) prowadzi bieżącą analizę podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej; 2) wydaje decyzje o uznaniu podmiotu za operatora usługi kluczowej albo decyzje stwierdzające wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej; 3) niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej przekazuje wnioski do ministra właściwego do spraw informatyzacji o wpisanie do wykazu operatorów usług kluczowych albo wykreślenie z tego wykazu; 4) składa wnioski o zmianę danych w wykazie operatorów usług kluczowych, nie później niż w terminie 6 miesięcy od zmiany tych danych; 5) przygotowuje we współpracy z CSIRT NASK, CSIRT GOV i CSIRT MON, oraz sektorowymi zespołami cyberbezpieczeństwa

		Art. 43 Art. 7	rekomendacje do działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów; 6) monitoruje stosowanie przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych; Art. 43. 1. Organ właściwy może, bez wszczynania postępowania w sprawie uznania podmiotu za operatora usługi kluczowej, wystąpić do podmiotu, o którym mowa w załączniku nr 1 do ustawy o udzielenie informacji, które umożliwią wstępną ocenę, czy dany podmiot spełnia warunki do uznania go za operatora usługi kluczowej. 2. Organ właściwy może, bez wszczynania kontroli, wystąpić do operatora usługi kluczowej o udzielenie informacji, które pozwolą na ustalenie potrzeby przeprowadzania kontroli, a także może, bez wszczynania postępowania, wystąpić do operatora usługi kluczowej o udzielenie informacji, które umożliwią wstępną ocenę, czy dany podmiot przestał spełniać warunki do uznania go za operatora usługi kluczowej. 3. Organ występując do podmiotu lub operatora usługi kluczowej, o których mowa w ust. 1 i 2, wskazuje termin udzielenia informacji. Wyznaczony termin, nie może być krótszy niż 14 dni, licząc od dnia otrzymania wystąpienia przez podmiot lub operatora usługi kluczowej. 4. Podmiot i operator usługi kluczowej, o których mowa odpowiednio w ust. 1 i 2, do którego organ skierował wystąpienie, może przekazać informacje w sprawie, której dotyczy wystąpienie lub poinformować o odmowie udzielenia informacji. 5. Wystąpienie o udzielenie informacji oraz brak udzielenia informacji przez podmiot lub operatora usługi kluczowej, o których mowa odpowiednio w ust. 1 i 2 nie wpływa na możliwości wszczęcia postępowania administracyjnego lub kontroli. 6. Informacje udzielone przez podmiot lub operatora usługi kluczowej, o których mowa w ust. 1 i 2, mogą stanowić materiał dowodowy we wszczętym postępowaniu administracyjnym lub kontroli. Brak udzielenia informacji nie wpływa na sytuację procesową strony albo kontrolowanego oraz na wszczęte postępowanie administracyjne lub kontrolę. Art. 7. 1. Minister właściwy do spraw informatyzacji prowadzi wykaz operatorów usług kluczowych. 2. Wykaz operatorów usług kluczowych zawiera: 1) nazwę (firmę) operatora usługi kluczowej;

			2) sektor, podsektor i rodzaj podmiotu; 3) siedzibę i adres; 4) numer identyfikacji podatkowej (NIP), jeżeli został nadany; 5) numer we właściwym rejestrze, jeżeli został nadany; 6) nazwę usługi kluczowej zgodną z wykazem usług kluczowych; 7) datę rozpoczęcia świadczenia usługi kluczowej; 8) informację, w których państwach członkowskich Unii Europejskiej podmiot został uznany za operatora usługi kluczowej; 9) datę zakończenia świadczenia usługi kluczowej; 10) datę wykreślenia z wykazu operatorów usług kluczowych. 3. Wpisanie do wykazu operatorów usług kluczowych i wykreślenie z tego wykazu następuje na wniosek organu właściwego, złożony niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej. Wniosek zawiera informacje, o których mowa w ust. 2 pkt 1–9. 4. Zmiana danych w wykazie operatorów usług kluczowych następuje na wniosek organu właściwego złożony, nie później niż w terminie 6 miesięcy od zmiany tych danych. 5. Wnioski, o których mowa w ust. 3 i 4, sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP. 6. Wpisanie do wykazu operatorów usług kluczowych i wykreślenie z tego wykazu oraz zmiana danych operatora usługi kluczowej w wykazie jest czynnością materialno-techniczną. 7. Dane z wykazu operatorów usług kluczowych minister właściwy do spraw informatyzacji udostępnia CSIRT MON, CSIRT NASK i CSIRT GOV oraz sektorowemu zespołowi cyberbezpieczeństwa w zakresie sektora lub podsektora, dla którego został ustanowiony, a także udostępnia operatorowi usługi kluczowej w zakresie go dotyczącym. 8. Dane z wykazu operatorów usług kluczowych, w zakresie niezbędnym do realizacji ich ustawowych zadań, minister właściwy do spraw informatyzacji udostępnia na wniosek następującym podmiotom: 1) organom właściwym; 2) Policji; 3) Żandarmerii Wojskowej; 4) Straży Granicznej; 5) Centralnemu Biuru Antykorupcyjnemu; 6) Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu;

	6. Rolą grupy współpracy jest, zgodnie z zadaniami, o których mowa w art. 11, wspieranie państw członkowskich w przyjmowaniu spójnego podejścia w procesie identyfikacji operatorów usług kluczowych. 7. Do celów przeglądu, o którym mowa w art. 23, oraz w terminie do dnia 9 listopada 2018 r., a następnie co dwa lata, państwa członkowskie przekazują Komisji niezbędne informacje, aby umożliwić jej ocenę wdrażania niniejszej dyrektywy, w szczególności spójności podejść państw członkowskich w zakresie identyfikacji operatorów usług kluczowych. Informacje te obejmują co najmniej: a) krajowe środki umożliwiające identyfikowanie operatorów usług kluczowych; b) wykaz usług, o którym mowa w ust. 3; c) liczbę zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o których mowa w załączniku II, oraz wskazanie ich znaczenia w odniesieniu do tego sektora; d) progi, jeżeli istnieją, w celu określenia odpowiedniego poziomu dostaw w powiązaniu z liczbą użytkowników zależnych od tej usługi zgodnie z art. 6 ust. 1 lit. a) lub znaczenia tego konkretnego operatora usług kluczowych zgodnie z art. 6 ust. 1 lit. f). Aby przyczynić się do dostarczania porównywalnych informacji, Komisja – w jak największym stopniu uwzględniając opinię ENISA – może przyjąć odpowiednie wytyczne techniczne dotyczące parametrów w odniesieniu do informacji, o których mowa w niniejszym ustępie.	Art. 50 Art. 80	7) Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego; 8) sądom; 9) prokuraturze; 10) organom Krajowej Administracji Skarbowej; 11) dyrektorowi Rządowego Centrum Bezpieczeństwa. Nie wymaga transpozycji. Art. 50. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej: 1) niezwłocznie informacje: a) o wyznaczonych organach właściwych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie, b) o przepisach dotyczących kar pieniężnych dotyczących krajowego systemu cyberbezpieczeństwa; 2) co 2 lata informacje umożliwiające ocenę wdrażania dyrektywy, obejmujące w szczególności: a) środki umożliwiające identyfikację operatorów usług kluczowych, b) wykaz usług kluczowych, c) liczbę zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o których mowa w załączniku nr 1 do ustawy, oraz wskazanie ich znaczenia w odniesieniu do tego sektora, d) progi istotności skutku zakłócającego dla świadczonej usługi kluczowej brane pod uwagę przy kwalifikowaniu podmiotów jako operatorów usług kluczowych; 3) informacje o zadaniach CSIRT MON, CSIRT NASK i CSIRT GOV, w tym o głównych elementach procedur postępowania w przypadku wystąpienia incydentu. Art. 80. Minister właściwy do spraw informatyzacji, po wejściu w życie ustawy, przekaże Komisji Europejskiej informacje: 1) o wyznaczonych organach właściwych, Pojedynczym Punkcie Kontaktowym oraz o ich zadaniach; 2) o zakresie zadań CSIRT MON, CSIRT NASK i CSIRT GOV, w tym o głównych elementach procedur postępowania w przypadku incydentu.

Istotny skutek zakłócający Art.6	1. Przy określaniu istotności skutku zakłócającego, o którym mowa w art. 5 ust. 2 lit. c), państwa członkowskie uwzględniają co najmniej następujące czynniki międzysektorowe: a) liczbę użytkowników zależnych od usługi świadczonej przez dany podmiot; b) zależność innych sektorów, o których mowa w załączniku II, od usługi świadczonej przez ten podmiot; c) wpływ, jaki incydenty – jeżeli chodzi o ich skalę i czas trwania – mogłyby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne; d) udział tego podmiotu w rynku; e) zasięg geograficzny związany z obszarem, którego mógłby dotyczyć incydent; f) znaczenie podmiotu w utrzymywaniu wystarczającego poziomu usługi przy uwzględnieniu dostępności alternatywnych sposobów świadczenia tej usługi. 2. W celu ustalenia, czy incydent miałby istotny skutek zakłócający, państwa członkowskie, w stosownych przypadkach, uwzględniają także czynniki sektorowe.	Art. 5 ust. 3 Art. 6	3. Istotność skutku zakłócającego incydentu dla świadczenia usługi kluczowej, o którym mowa w ust. 2 pkt 3, określana jest na podstawie progów istotności skutku zakłócającego. Art. 6. Rada Ministrów określi, w drodze rozporządzenia: 1) wykaz usług kluczowych, o których mowa w art. 5 ust. 2 pkt 1, kierując się przyporządkowaniem usługi kluczowej do danego sektora, podsektora i rodzaju podmiotu wymienionych w załączniku nr 1 do ustawy oraz znaczeniem usługi dla utrzymania krytycznej działalności społecznej lub gospodarczej; 2) progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w wykazie usług kluczowych, uwzględniając: a) liczbę użytkowników zależnych od usługi świadczonej przez dany podmiot, b) zależność innych sektorów, o których mowa w załączniku nr 1 do ustawy, od usługi świadczonej przez ten podmiot, c) wpływ, jaki incydent – jeżeli chodzi o skalę i czas trwania – mógłby mieć na działalność gospodarczą i społeczną lub bezpieczeństwo publiczne, d) udział podmiotu świadczącego usługę kluczową w rynku, e) zasięg geograficznego związany z obszarem, którego mógłby dotyczyć incydent, f) zdolność podmiotu do utrzymywania wystarczającego poziomu świadczenia usługi przy uwzględnieniu dostępności alternatywnych sposobów jej świadczenia, g) inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują – kierując się potrzebą zapewnienia ochrony przed zagrożeniem życia i zdrowia ludzi, znacznymi stratami majątkowymi, obniżeniem jakości świadczonej usługi kluczowej.
Krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych Art. 7	1. Każde państwo członkowskie przyjmuje krajową strategię w zakresie bezpieczeństwa sieci i systemów informatycznych określającą cele strategiczne i odpowiednie środki polityczne i regulacyjne mające na celu osiągnięcie i utrzymanie wysokiego poziomu bezpieczeństwa sieci i systemów informatycznych oraz obejmujące co najmniej sektory, o których mowa w załączniku II, i usługi, o których mowa w załączniku III. Krajowa strategia w zakresie bezpieczeństwa sieci i systemów informatycznych uwzględnia w szczególności	Art. 68-72	Art. 68. 1. Rada Ministrów przyjmuje w drodze uchwały Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej, zwaną dalej „Strategią”. Art. 69. 1. Strategia określa cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. Strategia obejmuje sektory, o których mowa w załączniku nr 1 do ustawy, usługi cyfrowe oraz podmioty publiczne, o których mowa w art. 4 pkt 7-15.

	następujące kwestie: a) cele i priorytety krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych; b) ramy zarządzania służące realizacji celów i priorytetów krajowej strategii w zakresie bezpieczeństwa sieci i systemów informatycznych, w tym role i zakresy obowiązków organów rządowych i innych właściwych podmiotów; c) określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym współpracy pomiędzy sektorami publicznym i prywatnym; d) wskazówki odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących do strategii w zakresie bezpieczeństwa sieci i systemów informatycznych; e) wskazówki odnoszące się do planów badawczo-rozwojowych dotyczących strategii w zakresie bezpieczeństwa sieci i systemów informatycznych; f) plan oceny ryzyka służący określeniu ryzyk; g) wykaz różnych podmiotów zaangażowanych we wdrażanie strategii w zakresie bezpieczeństwa sieci i systemów informatycznych. 2. Państwa członkowskie mogą zwrócić się do ENISA o pomoc przy opracowywaniu krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych. 3. Państwa członkowskie przekazują Komisji swoje krajowe strategie w zakresie bezpieczeństwa sieci i systemów informatycznych w ciągu trzech miesięcy od ich przyjęcia. Przekazując te strategie, państwa członkowskie mogą wyłączyć elementy strategii, które są związane z bezpieczeństwem narodowym.	Art. 85 Art. 45 pkt 1	2. Strategia uwzględnia w szczególności: 1) cele i priorytety w zakresie cyberbezpieczeństwa; 2) podmioty zaangażowane we wdrażanie i realizację Strategii; 3) środki służące realizacji celów Strategii; 4) określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy pomiędzy sektorami publicznym i prywatnym; 5) podejście do oceny ryzyka; 6) działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa; 7) działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa. 2. Strategia ustalana jest na okres pięcioletni z możliwością wprowadzenia zmian w okresie jej obowiązywania. Art. 70. 1. Projekt Strategii opracowuje minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, ministrami i właściwymi kierownikami urzędów centralnych. 2. W pracach nad projektem może uczestniczyć przedstawiciel Prezydenta Rzeczypospolitej Polskiej. Art. 71. Minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, ministrami i właściwymi kierownikami urzędów centralnych dokonuje przeglądu Strategii co dwa lata. Art. 72. Minister właściwy do spraw informatyzacji przekazuje Komisji Europejskiej Strategię w terminie trzech miesięcy od dnia jej przyjęcia przez Radę Ministrów. Art. 85. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej zostanie przyjęta do dnia 31 października 2019 r. Art. 45. 1. Minister właściwy do spraw informatyzacji jest odpowiedzialny za: 1) monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej oraz realizacji planów działań na rzecz jej wdrożenia;
Właściwe organy krajowe i pojedynczy punkt kontaktowy Art. 8	1. Każde państwo członkowskie wyznacza jeden lub większą liczbę właściwych organów krajowych ds. bezpieczeństwa sieci i systemów informatycznych (zwanych dalej „właściwym organem”), obejmujących co najmniej sektory, o których mowa w załączniku II, i usługi, o których mowa w załączniku III. Państwa członkowskie mogą do tej roli wyznaczyć istniejący organ lub istniejące organy.	Art. 41	Art. 41. Organami właściwymi do spraw cyberbezpieczeństwa są: 1) dla sektora energii – minister właściwy do spraw energii; 2) dla sektora transportu z wyłączeniem podsektora transportu wodnego – minister właściwy do spraw transportu; 3) dla podsektora transportu wodnego – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej;

			4) dla sektora bankowego i infrastruktury rynków finansowych – Komisja Nadzoru Finansowego; 5) dla sektora ochrony zdrowia z wyłączeniem podmiotów podległych lub nadzorowanych przez Ministra Obrony Narodowej – minister właściwy do spraw zdrowia; 6) dla sektora ochrony zdrowia obejmującego podmioty podległe lub nadzorowane przez Ministra Obrony Narodowej – Minister Obrony Narodowej; 7) dla sektora zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy do spraw gospodarki wodnej; 8) dla sektora infrastruktury cyfrowej z wyłączeniem podmiotów podległych lub nadzorowanych przez Ministra Obrony Narodowej – minister właściwy do spraw informatyzacji; 9) dla sektora infrastruktury cyfrowej obejmującego podmioty podległe lub nadzorowane przez Ministra Obrony Narodowej – Minister Obrony Narodowej; 10) dla dostawców usług cyfrowych z wyłączeniem podmiotów będących we właściwości Ministra Obrony Narodowej – minister właściwy do spraw informatyzacji; 11) dla dostawców usług cyfrowych będących we właściwości Ministra Obrony Narodowej – Minister Obrony Narodowej.
	2. Właściwe organy monitorują stosowanie niniejszej dyrektywy na poziomie krajowym.	Art. 42	Art. 42. 1. Organ właściwy: 1) prowadzi bieżącą analizę podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej; 2) wydaje decyzje o uznaniu podmiotu za operatora usługi kluczowej albo decyzje stwierdzające wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej; 3) niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej przekazuje wnioski do ministra właściwego do spraw informatyzacji o wpisanie do wykazu operatorów usług kluczowych albo wykreślenie z tego wykazu; 4) składa wnioski o zmianę danych w wykazie operatorów usług kluczowych, nie później niż w terminie 6 miesięcy od zmiany tych danych; 5) przygotowuje we współpracy z CSIRT NASK, CSIRT GOV i CSIRT MON, oraz sektorowymi zespołami cyberbezpieczeństwa rekomendacje do działań mających na celu wzmocnienie

			cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów; 6) monitoruje stosowanie przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych; 7) wzywa na wniosek CSIRT NASK, CSIRT GOV lub CSIRT MON operatorów usług kluczowych lub dostawców usług cyfrowych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego; 8) prowadzi kontrole operatorów usług kluczowych i dostawców usług cyfrowych; 9) może prowadzić współpracę z właściwymi organami państw członkowskich Unii Europejskiej za pośrednictwem Pojedynczego Punktu Kontaktowego; 10) przetwarza informacje, w tym dane osobowe, dotyczące świadczonych usług kluczowych i usług cyfrowych oraz operatorów usług kluczowych lub dostawców usług cyfrowych w zakresie niezbędnym do realizacji zadań wynikających z ustawy; 11) uczestniczy w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w Rzeczypospolitej Polskiej lub w Unii Europejskiej. 2. W przypadku, gdy osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, świadcząca usługi cyfrowe, nie posiada siedziby lub zarządu na terytorium Rzeczypospolitej Polskiej albo nie wyznaczyła przedstawiciela na terytorium Rzeczypospolitej Polskiej, ale jej systemy informacyjne znajdują się na terytorium Rzeczypospolitej Polskiej, i nie spełnia wymagań określonych w rozporządzeniu wykonawczym 2018/151, organ właściwy dla dostawców usług cyfrowych może przekazywać informacje oraz zwracać się o podejmowanie działań, o których mowa w art. 53 ust. 2, do organu właściwego w innym państwie członkowskim Unii Europejskiej, na terytorium którego posiada ona siedzibę lub zarząd albo został wyznaczony jej przedstawiciel. 3. Organ właściwy może powierzyć realizację, w jego imieniu, niektórych zadań, o których mowa w ust. 1, jednostkom podległym lub nadzorowanym przez ten organ. 4. Powierzenie następuje na podstawie porozumienia organu właściwego z podmiotami, o których mowa w ust. 3. 5. W porozumieniu, o którym mowa w ust. 4, określa się zasady sprawowania przez organ właściwy kontroli nad prawidłowym wykonywaniem powierzonych zadań. 6. Komunikat o zawarciu porozumienia ogłasza się w dzienniku

			urzędowym właściwego organu. W komunikacie wskazuje się informacje o: 1) adresie strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami; 2) terminie, od którego porozumienie będzie obowiązywało. 7. Organy właściwe i Pojedynczy Punkt Kontaktowy w uzasadnionych przypadkach współpracują z organami ścigania i organem właściwym do spraw ochrony danych osobowych. 8. Rekomendacje działań mające na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów, o których mowa w ust. 1 pkt 5, przygotowuje się z uwzględnieniem w szczególności Polskich Norm przenoszących normy europejskie, wspólne specyfikacje techniczne, rozumianych jako specyfikacje techniczne w dziedzinie produktów teleinformatycznych określone zgodnie z art. 13 i art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz. Urz. UE L 316 z 14.11.2012, str. 12), wytyczne Komisji Europejskiej oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA) w tym zakresie.
	3. Każde państwo członkowskie wyznacza krajowy pojedynczy punkt kontaktowy ds. bezpieczeństwa sieci i systemów informatycznych (zwany dalej „pojedynczym punktem kontaktowym”). Państwa członkowskie mogą do tej roli wyznaczyć istniejący organ. W przypadku gdy państwo członkowskie wyznacza tylko jeden właściwy organ, ten właściwy organ jest również pojedynczym punktem kontaktowym.	Art. 48	Art. 48. Minister właściwy do spraw informatyzacji prowadzi Pojedynczy Punkt Kontaktowy, do którego zadań należy: 1) odbieranie zgłoszeń incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej z pojedynczych punktów kontaktowych w innych państwach członkowskich Unii Europejskiej, a także przekazywanie tych zgłoszeń do CSIRT MON, CSIRT NASK, CSIRT GOV lub sektorowych zespołów cyberbezpieczeństwa; 2) przekazywanie, na wniosek właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV zgłoszenia incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych w innych państwach członkowskich Unii

	4. Pojedynczy punkt kontaktowy pełni funkcję łącznikową w celu zapewnienia transgranicznej współpracy organów państw członkowskich oraz współpracy z odpowiednimi organami w innych państwach członkowskich, a także z grupą współpracy, o której mowa w art. 11, i siecią CSIRT, o której mowa w art. 12. 5. Państwa członkowskie zapewniają właściwym organom i pojedynczym punktom kontaktowym odpowiednie zasoby, aby mogły one efektywnie i skutecznie wykonywać powierzone im zadania z myślą o osiągnięciu celów niniejszej dyrektywy. Państwa członkowskie zapewniają efektywną, skuteczną i bezpieczną współpracę wyznaczonych przedstawicieli w grupie współpracy.	Art. 49	Europejskiej; 3) zapewnienie reprezentacji Rzeczypospolitej Polskiej w Grupie Współpracy; 4) zapewnienie współpracy z Komisją Europejską w dziedzinie cyberbezpieczeństwa; 5) koordynacja współpracy pomiędzy organami właściwymi i organami władzy publicznej w Rzeczypospolitej Polskiej z odpowiednimi organami w państwach członkowskich Unii Europejskiej; 6) zapewnienie wymiany informacji na potrzeby Grupy Współpracy oraz Sieci CSIRT. Art. 49. 1. Pojedynczy Punkt Kontaktowy przekazuje Grupie Współpracy: 1) informacje, o których mowa w art. 45 pkt 3; 2) dobre praktyki związane ze zgłaszaniem incydentów, o których mowa w art. 45 pkt 4; 3) propozycje do programu prac Grupy Współpracy; 4) dobre praktyki krajowe dotyczące podnoszenia świadomości, szkoleń, badań i rozwoju z zakresu cyberbezpieczeństwa; 5) dobre praktyki w odniesieniu do identyfikowania operatorów usług kluczowych, w tym w odniesieniu do występujących w dwóch lub większej liczbie państw członkowskich Unii Europejskiej zależności dotyczących ryzyka i incydentów. 2. Informacje, o których mowa w ust. 1, nie obejmują informacji, które dotyczą bezpieczeństwa narodowego oraz porządku publicznego. 3. Pojedynczy Punkt Kontaktowy przekazuje organom właściwym, CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowym zespołom cyberbezpieczeństwa oraz innym organom władzy publicznej informacje pochodzące z Grupy Współpracy dotyczące: 1) ocen krajowych strategii państw członkowskich Unii Europejskiej w zakresie cyberbezpieczeństwa oraz skuteczności CSIRT, a także dobrych praktyk w zakresie cyberbezpieczeństwa; 2) działań podjętych w odniesieniu do ćwiczeń dotyczących cyberbezpieczeństwa, europejskich programów edukacyjnych i szkoleń, w tym działań Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA); 3) wytycznych o charakterze strategicznym dotyczących działalności Sieci CSIRT; 4) dobrych praktyk w zakresie wymiany informacji związanych ze zgłaszaniem w Unii Europejskiej incydentów poważnych przez

			operatorów usług kluczowych i incydentów istotnych przez dostawców usług cyfrowych; 5) dobrych praktyk w krajach członkowskich Unii Europejskiej dotyczących podnoszenia świadomości, szkolenia, zakresu badań i rozwoju w zakresie cyberbezpieczeństwa; 6) dobrych praktyk w zakresie identyfikowania operatorów usług kluczowych przez państwa członkowskie Unii Europejskiej, w tym w odniesieniu do transgranicznych zależności, dotyczących ryzyka i incydentów.
		Art. 50	Art. 50. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej: 1) niezwłocznie informacje: a) o wyznaczonych organach właściwych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie, b) o przepisach dotyczących kar pieniężnych dotyczących krajowego systemu cyberbezpieczeństwa; 2) co 2 lata informacje umożliwiające ocenę wdrażania dyrektywy, obejmujące w szczególności: a) środki umożliwiające identyfikację operatorów usług kluczowych, b) wykaz usług kluczowych, c) liczbę zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o których mowa w załączniku nr 1 do ustawy, oraz wskazanie ich znaczenia w odniesieniu do tego sektora, d) progi istotności skutku zakłócającego dla świadczonej usługi kluczowej brane pod uwagę przy kwalifikowaniu podmiotów jako operatorów usług kluczowych; 3) informacje o zadaniach CSIRT MON, CSIRT NASK i CSIRT GOV, w tym o głównych elementach procedur postępowania w przypadku wystąpienia incydentu.
	6. Właściwe organy i pojedynczy punkt kontaktowy, w stosownych przypadkach oraz zgodnie z prawem krajowym, konsultują się i współpracują z odpowiednimi krajowymi organami ścigania i krajowymi organami ochrony danych.	Art. 34	Art. 34. 1. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa współpracują z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań. 2. CSIRT MON, CSIRT NASK i CSIRT GOV koordynując obsługę incydentu, który doprowadził do naruszenia danych osobowych, współpracuje z organem właściwym do spraw ochrony danych osobowych.

	7. Każde państwo członkowskie niezwłocznie powiadamia Komisję o wyznaczeniu właściwego organu i pojedynczego punktu kontaktowego, o ich zadaniach i o wszelkich późniejszych zmianach w tym zakresie. Każde państwo członkowskie podaje do publicznej wiadomości informację o wyznaczeniu właściwego organu i pojedynczego punktu kontaktowego. Komisja publikuje wykaz wyznaczonych pojedynczych punktów kontaktowych.	Art. 50 pkt 1 lit. a Art. 80 pkt 1	Art. 50. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej: 1) niezwłocznie informacje: a) o wyznaczonych organach właściwych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie, Art. 80. Minister właściwy do spraw informatyzacji, po wejściu w życie ustawy, przekaże Komisji Europejskiej informacje: 1) o wyznaczonych organach właściwych, Pojedynczym Punkcie Kontaktowym oraz o ich zadaniach;
Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) Art. 9	1. Każde państwo członkowskie wyznacza jeden lub większą liczbę CSIRT spełniających wymogi zawarte w załączniku I pkt 1, obejmujących przynajmniej sektory, o których mowa w załączniku II, i usługi, o których mowa w załączniku III, odpowiedzialnych za postępowanie w odniesieniu do ryzyk i postępowanie w przypadku incydentu zgodnie z jasno określoną procedurą. CSIRT mogą być ustanawiane w ramach właściwego organu. 2. Państwa członkowskie zapewniają, aby CSIRT miały odpowiednie zasoby w celu skutecznej realizacji swoich zadań określonych w załączniku I pkt 2. Państwa członkowskie zapewniają skuteczną, efektywną i bezpieczną współpracę swoich CSIRT w ramach sieci CSIRT, o której mowa w art. 12.	Art. 2 pkt 1-3 Art. 26	Art. 2. Użyte w ustawie określenia oznaczają: 1) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym prowadzony przez Ministra Obrony Narodowej; 2) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy; 3) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego; Art. 26. 1. CSIRT MON, CSIRT NASK i CSIRT GOV współpracują ze sobą, z organami właściwymi, ministrem właściwym do spraw informatyzacji oraz Pełnomocnikiem, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów. 2. CSIRT MON, CSIRT NASK i CSIRT GOV w uzasadnionych przypadkach na wniosek operatorów usług kluczowych, dostawców usług cyfrowych, podmiotów publicznych, o których mowa w art. 4 pkt 7-15, sektorowych zespołów cyberbezpieczeństwa lub właścicieli, posiadaczy samoistnych albo zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, mogą zapewnić wsparcie w obsłudze incydentów.

			3. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV zgodnie z właściwością wskazaną w ust. 5-7, należy: 1) monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym; 2) szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka; 3) przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa; 4) wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa; 5) reagowanie na zgłoszone incydenty; 6) klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych; 7) zmiana klasyfikacji incydentów poważnych i incydentów istotnych; 8) przekazywanie do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacji technicznych dotyczących incydentu, którego koordynacja obsługi wymaga współpracy CSIRT; 9) przeprowadzanie, w uzasadnionych przypadkach, badania lub oceny bezpieczeństwa stosowania sprzętu lub oprogramowania oraz składanie wniosków w sprawie rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa dotyczących stosowania sprzętu lub oprogramowania, w szczególności w zakresie wpływu stosowania sprzętu lub oprogramowania na bezpieczeństwo publiczne lub istotne interesy bezpieczeństwa państwa, zwanych dalej „rekomendacjami dotyczącymi sprzętu lub oprogramowania”; 10) współpraca z sektorowymi zespołami cyberbezpieczeństwa w zakresie koordynowania obsługi incydentów poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej i incydentów krytycznych oraz wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa; 11) przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej, i przyjmowanie z tych państw informacji o incydentach poważnych i incydentach istotnych dotyczących dwóch lub większej liczby państw członkowskich, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego i istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej; 12) przekazywanie w terminie do dnia 30 maja każdego roku do

			Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednim roku kalendarzowym przez operatorów usług kluczowych incydentów poważnych mających wpływ na ciągłość świadczenia przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczenia przez nich usług kluczowych w państwach członkowskich Unii Europejskiej, a także zestawienia zgłoszonych w poprzednim roku kalendarzowym przez dostawców usług cyfrowych incydentów istotnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej; 13) wspólne opracowywanie i przekazywanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego, o którym mowa w art. 5a ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, dotyczącego cyberbezpieczeństwa; 14) zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego, które w szczególności: a) prowadzi zaawansowane analizy złośliwego oprogramowania oraz analizy podatności, b) monitoruje wskaźniki zagrożeń cyberbezpieczeństwa, c) rozwija narzędzia i metody do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa, d) prowadzi analizy i opracowuje standardy, rekomendacje i dobre praktyki w zakresie cyberbezpieczeństwa, e) wspiera podmioty krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa, f) prowadzi działania z zakresu budowania świadomości w obszarze cyberbezpieczeństwa, g) współpracuje w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa; 15) zapewnienie możliwości dokonywania zgłoszeń i przekazywania informacji, o których mowa w art. 11 ust. 1 pkt 4, art. 13 ust. 1, art. 18 ust. 1 pkt 4, art. 20, art. 22 ust. 1 pkt 2, art. 24 i art. 30 ust. 1 oraz udostępnienie i obsługa środków komunikacji pozwalających na dokonywanie tych zgłoszeń; 16) udział w Sieci CSIRT składającej się z przedstawicieli CSIRT państw członkowskich Unii Europejskiej, CSIRT właściwego dla instytucji Unii Europejskiej, Komisji Europejskiej oraz Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA). 4. CSIRT MON, CSIRT NASK i CSIRT GOV wspólnie opracowują główne elementy procedur postępowania w przypadku incydentu, którego koordynacja obsługi wymaga współpracy CSIRT, oraz

			określą, we współpracy z sektorowymi zespołami cyberbezpieczeństwa, sposób współdziałania z tymi zespołami, w tym sposób koordynacji obsługi incydentu. 5. Do zadań CSIRT MON należy koordynacja obsługi incydentów zgłaszanych przez: 1) podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; 2) przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa w rozumieniu art. 5 pkt 3 ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności państwa realizowanych przez przedsiębiorców (Dz. U. poz. 1320 oraz z 2002 r. poz. 1571) jest Minister Obrony Narodowej; 3) dostawców usług cyfrowych, będących we właściwości Ministra Obrony Narodowej. 6. Do zadań CSIRT NASK należy: 1) koordynacja obsługi incydentów zgłaszanych przez: a) 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, b) jednostki podległe organom administracji rządowej lub przez nie nadzorowane, z wyjątkiem jednostek, o których mowa w ust. 7 pkt 2, c) instytuty badawcze, d) Urząd Dozoru Technicznego, e) Polską Agencję Żeglugi Powietrznej, f) Polskie Centrum Akredytacji, g) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, h) spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu ustawy z dnia 20 grudnia 1996 r. ustawy o gospodarce komunalnej, i) dostawców usług cyfrowych, z wyjątkiem wymienionych w ust. 5 pkt 3 oraz ust. 7 pkt 5, j) operatorów usług kluczowych, z wyjątkiem wymienionych w ust. 5 i ust. 7,

			k) inne podmioty niż wymienione w lit. a-j oraz ust. 5 i 7, l) osoby fizyczne; 2) tworzenie i udostępnianie narzędzi dobrowolnej współpracy i wymiany informacji o zagrożeniach cyberbezpieczeństwa i incydentach; 3) zapewnienie obsługi linii telefonicznej lub serwisu internetowego prowadzącego działalność w zakresie zgłaszania i analizy przypadków dystrybucji, rozpowszechniania lub przesyłania pornografii dziecięcej za pośrednictwem technologii informacyjno-komunikacyjnych, o których mowa w dyrektywie Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW (Dz. Urz. UE L 335 z 13.12.2011, str. 1). 7. Do zadań CSIRT GOV należy koordynacja obsługi incydentów zgłaszanych przez: 1) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8-9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyjątkiem wymienionych w ust. 5 i 6; 2) jednostki podległe Prezesowi Rady Ministrów i przez niego nadzorowane; 3) Narodowy Bank Polski; 4) Bank Gospodarstwa Krajowego; 5) inne niż wymienione w pkt 1-4 oraz ust. 5 podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; 6) podmioty, o których mowa w ust. 6, jeżeli incydent dotyczy systemów teleinformatycznych lub sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, o której mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. 8. CSIRT MON, CSIRT NASK lub CSIRT GOV, który otrzymał zgłoszenie incydentu, a nie jest właściwy do koordynacji jego obsługi, przekazuje niezwłocznie to zgłoszenie do właściwego CSIRT wraz z otrzymanymi informacjami. 9. Działalność CSIRT NASK jest finansowana w formie dotacji podmiotowej z części budżetu państwa, której dysponentem jest

	3. Państwa członkowskie zapewniają, aby ich CSIRT miały dostęp do odpowiedniej, bezpiecznej i odpornej infrastruktury komunikacyjno-informacyjnej na poziomie krajowym.	 Art. 46 Art. 84 Art. 50 pkt 3	minister właściwy do spraw informatyzacji. 10. CSIRT MON, CSIRT NASK i CSIRT GOV mogą w drodze porozumienia powierzyć sobie wzajemnie wykonywanie zadań w stosunku do niektórych rodzajów podmiotów, o których mowa w ust. 5-7. O zawarciu porozumienia CSIRT, który powierzył wykonywanie zadań, informuje podmioty, w stosunku do których nastąpiła zmiana CSIRT. 11. Komunikat o zawarciu porozumienia, o którym mowa w ust. 10, ogłasza się odpowiednio w dzienniku urzędowym Ministra Obrony Narodowej, Szefa Agencji Bezpieczeństwa Wewnętrznego albo ministra właściwego do spraw informatyzacji. W komunikacie wskazuje się informacje o: 1) adresie strony internetowej, na której zostanie zamieszczona treść porozumienia wraz ze stanowiącymi jego integralną treść załącznikami; 2) terminie, od którego porozumienie będzie obowiązywało. Art. 46. 1. Minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego: 1) współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa; 2) generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa; 3) zgłaszanie i obsługę incydentów; 4) szacowanie ryzyka na poziomie krajowym; 5) ostrzeganie o zagrożeniach cyberbezpieczeństwa. 2. CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i Prezes Urzędu Komunikacji Elektronicznej, mogą korzystać z systemu teleinformatycznego, na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji. 3. W porozumieniu określa się zakres i warunki korzystania z systemu teleinformatycznego. Art. 84. Minister właściwy do spraw informatyzacji uruchomi system teleinformatyczny, o którym mowa w art. 46 ust. 1, do dnia 1 stycznia 2021 r. Art. 50. Pojedynczy Punkt Kontaktowy przekazuje Komisji

	4. Państwa członkowskie przekazują Komisji informacje o zakresie kompetencji CSIRT, jak również o głównych elementach procedur postępowania w przypadku incydentu. 5. Państwa członkowskie mogą zwrócić się do ENISA o pomoc przy tworzeniu krajowych CSIRT.	Art. 80 pkt 2	Europejskiej: 3) informacje o zakresie kompetencji CSIRT MON, CSIRT NASK i CSIRT GOV, w tym o głównych elementach procedur postępowania w przypadku wystąpienia incydentu. Art. 80. Minister właściwy do spraw informatyzacji, po wejściu w życie ustawy, przekaże Komisji Europejskiej informacje: 2) o zakresie zadań CSIRT MON, CSIRT NASK i CSIRT GOV, w tym o głównych elementach procedur postępowania w przypadku incydentu. Nie wymaga transpozycji
Współpraca na poziomie krajowym Art. 10	1. W przypadku gdy właściwy organ, pojedynczy punkt kontaktowy i CSIRT tego samego państwa członkowskiego są oddzielne, współpracują ze sobą w zakresie wypełnienia obowiązków określonych w niniejszej dyrektywie.	Art. 26 ust. 1 Art. 28 ust. 3 Art. 42 ust. 1 pkt 5 i 9 Art. 49 ust. 3	Art. 26. 1. CSIRT MON, CSIRT NASK i CSIRT GOV współpracują ze sobą, z organami właściwymi, ministrem właściwym do spraw informatyzacji oraz Pełnomocnikiem, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów. 3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić z wnioskiem do Pojedynczego Punktu Kontaktowego o przekazanie zgłoszenia incydentu poważnego, o którym mowa w ust. 1, pojedynczym punktom kontaktowym w innych państwach członkowskich Unii Europejskiej, których dotyczy ten incydent. Art. 42. 1. Organ właściwy: 5) przygotowuje we współpracy z CSIRT NASK, CSIRT GOV i CSIRT MON, oraz sektorowymi zespołami cyberbezpieczeństwa rekomendacje do działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów; 9) może prowadzić współpracę z właściwymi organami państw członkowskich Unii Europejskiej za pośrednictwem Pojedynczego Punktu Kontaktowego; 3. Pojedynczy Punkt Kontaktowy przekazuje organom właściwym,

			CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowym zespołom cyberbezpieczeństwa oraz innym organom władzy publicznej informacje pochodzące z Grupy Współpracy dotyczące: 1) ocen krajowych strategii państw członkowskich Unii Europejskiej w zakresie cyberbezpieczeństwa oraz skuteczności CSIRT, a także dobrych praktyk w zakresie cyberbezpieczeństwa; 2) działań podjętych w odniesieniu do ćwiczeń dotyczących cyberbezpieczeństwa, europejskich programów edukacyjnych i szkoleń, w tym działań Agencji Unii Europejskiej do spraw Bezpieczeństwa Sieci i Informacji (ENISA); 3) wytycznych o charakterze strategicznym dotyczących działalności Sieci CSIRT; 4) dobrych praktyk w zakresie wymiany informacji związanych ze zgłaszaniem w Unii Europejskiej incydentów poważnych przez operatorów usług kluczowych i incydentów istotnych przez dostawców usług cyfrowych; 5) dobrych praktyk w krajach członkowskich Unii Europejskiej dotyczących podnoszenia świadomości, szkolenia, zakresu badań i rozwoju w zakresie cyberbezpieczeństwa; 6) dobrych praktyk w zakresie identyfikowania operatorów usług kluczowych przez państwa członkowskie Unii Europejskiej, w tym w odniesieniu do transgranicznych zależności, dotyczących ryzyka i incydentów.
	2. Państwa członkowskie zapewniają, aby właściwe organy albo CSIRT odbierały zgłoszenia o incydentach przekazane na mocy niniejszej dyrektywy. W przypadku gdy państwo członkowskie postanowi, że CSIRT nie będą odbierać zgłoszeń, CSIRT otrzymają, w stopniu koniecznym do wykonywania swoich zadań, dostęp do danych dotyczących incydentów zgłaszanych przez operatorów usług kluczowych na mocy art. 14 ust. 3 i 5 lub przez dostawców usług cyfrowych na mocy art. 16 ust. 3 i 6.	Art. 11 ust. 1 pkt 4 Art. 18 ust. 1 pkt 4 Art. 31	Art. 11. 1. Operator usługi kluczowej: 4) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV; Art. 18. 1. Dostawca usługi cyfrowej: 4) zgłasza incydent istotny niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV; Art. 31. 1. CSIRT MON, CSIRT NASK i CSIRT GOV określa sposób dokonywania zgłoszeń i przekazywania informacji w postaci elektronicznej, o których mowa w art. 11 ust. 1 pkt 4, art. 13 ust. 1, art. 18 ust. 1 pkt 4, art. 20, art. 22 ust. 1 pkt 2, art. 24 i art. 30 ust. 1, a także określa sposób dokonywania zgłoszeń i przekazywania informacji przy użyciu innych środków komunikacji, w przypadku braku możliwości zgłoszenia albo przekazania ich w

			postaci elektronicznej. 2. Komunikat, zawierający informacje, o których mowa w ust. 1, CSIRT MON, CSIRT NASK i CSIRT GOV publikuje na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego.
	3. Państwa członkowskie zapewniają, aby właściwe organy lub CSIRT informowały pojedyncze punkty kontaktowe o zgłoszeniach incydentów przekazanych na mocy niniejszej dyrektywy.	Art. 26 ust. 3 pkt 12	3. Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV zgodnie z właściwością wskazaną w ust. 5-7, należy: 12) przekazywanie w terminie do dnia 30 maja każdego roku do Pojedynczego Punktu Kontaktowego zestawienia zgłoszonych w poprzednim roku kalendarzowym przez operatorów usług kluczowych incydentów poważnych mających wpływ na ciągłość świadczenia przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczenia przez nich usług kluczowych w państwach członkowskich Unii Europejskiej, a także zestawienia zgłoszonych w poprzednim roku kalendarzowym przez dostawców usług cyfrowych incydentów istotnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej;
	W terminie do dnia 9 sierpnia 2018 r., a następnie raz do roku pojedynczy punkt kontaktowy przekazuje grupie współpracy sprawozdanie podsumowujące na temat otrzymanych zgłoszeń, w tym liczby zgłoszeń i charakteru zgłoszonych incydentów, oraz działań podjętych zgodnie z art. 14 ust. 3 i 5 oraz art. 16 ust. 3 i 6.	Art. 45 pkt 3	Art. 45. Minister właściwy do spraw informatyzacji jest odpowiedzialny za: 3) opracowywanie rocznych sprawozdań dotyczących: a) incydentów poważnych zgłaszanych przez operatorów usług kluczowych mających wpływ na ciągłość świadczonych przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej, b) incydentów istotnych zgłaszanych przez dostawców usług cyfrowych, w tym incydentów dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej;
		Art. 49 ust. 1 pkt 1	Art. 49. 1. Pojedynczy Punkt Kontaktowy przekazuje Grupie Współpracy: 1) informacje, o których mowa w art. 45 pkt 3;
		Art. 82	Art. 82. Minister właściwy do spraw informatyzacji, w terminie do dnia 9 sierpnia 2018 r., przekaże Grupie Współpracy sprawozdanie podsumowujące o: 1) incydentach poważnych zgłaszanych przez operatorów usług kluczowych, mających wpływ na ciągłość świadczenia przez nich

			usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczenia usług kluczowych w państwach członkowskich Unii Europejskiej; 2) zgłaszanych przez dostawców usług cyfrowych incydentów istotnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej.
		Art. 83	Art. 83. Minister właściwy do spraw informatyzacji, w terminie do dnia 9 listopada 2018 r., przekaże Komisji Europejskiej informacje o: 1) krajowych środkach umożliwiających identyfikację operatorów usług kluczowych; 2) wykazie usług kluczowych; 3) liczbie zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o którym mowa w załączniku nr 1 do ustawy, ze wskazaniem ich znaczenia w odniesieniu do tego sektora; 4) progach istotności skutku zakłócającego dla świadczonej usługi kluczowej branych pod uwagę przy kwalifikowaniu podmiotów, jako operatorów usług kluczowych .
Grupa współpracy Art. 11	1. Niniejszym ustanawia się grupę współpracy, aby wesprzeć i ułatwić strategiczną współpracę i wymianę informacji między państwami członkowskimi oraz wzmocnić zaufanie i pewność, a także z myślą o osiągnięciu wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii. Grupa współpracy wykonuje swoje zadania na podstawie dwuletnich programów prac, o których mowa w ust. 3 akapit drugi. 2. Grupa współpracy składa się z przedstawicieli państw członkowskich, Komisji i ENISA. W stosownych przypadkach grupa współpracy może zaprosić przedstawicieli odpowiednich zainteresowanych stron do udziału w swoich pracach. Komisja zapewnia sekretariat. 3. Zadania grupy współpracy są następujące: a) udzielanie strategicznych wskazówek dotyczących działalności sieci CSIRT ustanowionej na mocy art. 12; b) wymiana najlepszych praktyk dotyczących wymiany informacji związanej ze zgłaszaniem incydentów, o którym mowa w art. 14 ust. 3 i 5 i art. 16 ust. 3 i 6; c) wymiana najlepszych praktyk między państwami członkowskimi oraz, we współpracy z ENISA, pomoc państwom członkowskim w budowaniu zdolności z myślą		Nie wymaga transpozycji. Art. 45. 2. Przez Grupę Współpracy rozumie się grupę, o której mowa w decyzji wykonawczej Komisji 2017/179/UE z dnia 1 lutego 2017 r. ustanawiającej procedury niezbędne do funkcjonowania grupy współpracy zgodnie z art. 11 ust. 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 28 z 1.02.2017, str. 73).

	o zapewnieniu bezpieczeństwa sieci i systemów informatycznych; d) omawianie zdolności i gotowości państw członkowskich oraz, na zasadzie dobrowolności, ocena krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych oraz skuteczności CSIRT, a także określanie najlepszych praktyk; e) wymiana informacji i najlepszych praktyk dotyczących podnoszenia świadomości i szkolenia; f) wymiana informacji i najlepszych praktyk dotyczących badań i rozwoju w zakresie bezpieczeństwa sieci i systemów informatycznych; g) w stosownych przypadkach, wymiana doświadczeń w sprawach dotyczących bezpieczeństwa sieci i systemów informatycznych z odpowiednimi instytucjami, organami, biurami i agencjami Unii; h) omawianie z przedstawicielami odpowiednich europejskich organizacji normalizacyjnych norm i specyfikacji, o których mowa w art. 19; i) gromadzenie informacji z zakresu najlepszych praktyk dotyczących ryzyk i incydentów; j) coroczna analiza sprawozdań podsumowujących, o których mowa w art. 10 ust. 3 akapit drugi; k) omawianie prac podjętych w odniesieniu do ćwiczeń dotyczących bezpieczeństwa sieci i systemów informatycznych, programów edukacyjnych i szkoleń, w tym prac wykonywanych przez ENISA; l) przy wsparciu ENISA – wymiana najlepszych praktyk w odniesieniu do identyfikowania operatorów usług kluczowych przez państwa członkowskie, w tym w odniesieniu do transgranicznych zależności, dotyczących ryzyk i incydentów; m) omawianie zasad dotyczących sprawozdawczości w zakresie zgłaszania incydentów, o których mowa w art. 14 i 16. W terminie do dnia 9 lutego 2018 r., a następnie co dwa lata grupa współpracy opracowuje program prac w odniesieniu do działań, jakie mają zostać podjęte w celu realizacji celów i zadań, które muszą być spójne z celami niniejszej dyrektywy. 4. Na potrzeby przeglądu, o którym mowa w art. 23, w terminie do dnia 9 sierpnia 2018 r., a następnie co półtora roku grupa współpracy przygotowuje sprawozdanie oceniające doświadczenia zdobyte w ramach strategicznej współpracy		

	prowadzonej na mocy niniejszego artykułu. 5. Komisja przyjmuje akty wykonawcze określające procedury niezbędne do funkcjonowania grupy współpracy. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 22 ust. 2. Do celów akapitu pierwszego Komisja przedkłada pierwszy projekt aktu wykonawczego komitetowi, o którym mowa w art. 22 ust. 1, w terminie do dnia 9 lutego 2017 r.		
Sieć CSIRT Art. 12	1. Niniejszym ustanawia się sieć krajowych CSIRT w celu przyczyniania się do rozwoju pewności i zaufania między państwami członkowskimi oraz propagowania szybkiej i skutecznej współpracy. 2. Sieć CSIRT składa się z przedstawicieli CSIRT państw członkowskich i CERT-EU. Komisja uczestniczy w sieci CSIRT jako obserwator. ENISA zapewnia sekretariat oraz aktywnie wspiera współpracę między CSIRT. 3. Zadania sieci CSIRT są następujące: a) wymiana informacji dotyczących usług, operacji i zdolności współpracy CSIRT; b) na wniosek przedstawiciela CSIRT z państwa członkowskiego, na które potencjalnie może mieć wpływ incydent – wymiana i dyskusja dotycząca informacji innych niż szczególnie chronione informacje handlowe, związanych z tym incydentem i powiązanymi ryzykami; jednakże CSIRT każdego z państw członkowskich może odmówić wkładu w tę dyskusję, jeżeli istnieje ryzyko szkody dla postępowania przygotowawczego w sprawie incydentu; c) wymiana i udostępnienie na zasadzie dobrowolności informacji innych niż poufne, dotyczących poszczególnych incydentów; d) na wniosek przedstawiciela państwa członkowskiego – omówienie oraz, w miarę możliwości, określenie skoordynowanej reakcji na incydent, który został zidentyfikowany w ramach jurysdykcji tego państwa członkowskiego; e) zapewnianie wsparcia państw członkowskich w obsłudze incydentów transgranicznych w oparciu o ich dobrowolną wzajemną pomoc; f) omówienie, zbadanie i określenie dalszych form współpracy operacyjnej, w tym w związku z: (i) kategoriami ryzyk i incydentów; (ii) wczesnym ostrzeganiem;		Nie wymaga transpozycji.

	(iii) wzajemną pomocą; (iv) zasadami i uzgodnieniami dotyczącymi koordynacji, gdy państwa członkowskie reagują na transgraniczne ryzyka i incydenty; g) informowanie grupy współpracy o swoich działaniach i o dalszych formach współpracy operacyjnej omawianych zgodnie z lit. f) oraz zwracanie się o wskazówki w tym zakresie; h) omawianie wniosków z ćwiczeń dotyczących bezpieczeństwa sieci i systemów informatycznych, w tym ćwiczeń organizowanych przez ENISA; i) na wniosek danego CSIRT – omawianie zdolności i gotowości tego CSIRT; j) wydawanie wytycznych w celu ułatwienia konwergencji praktyk operacyjnych w odniesieniu do stosowania przepisów niniejszego artykułu dotyczących współpracy operacyjnej. 4. Na potrzeby przeglądu, o którym mowa w art. 23, w terminie do dnia 9 sierpnia 2018 r., a następnie co półtora roku, sieć CSRIT przedstawia sprawozdanie zawierające ocenę doświadczeń zdobytych w ramach współpracy operacyjnej, wraz z wnioskami i zaleceniami, prowadzonej na mocy niniejszego artykułu. Sprawozdanie to jest także przedkładane grupie współpracy. 5. Sieć CSIRT ustanawia swój regulamin wewnętrzny.		
Współpraca międzynarodowa Art. 13	Unia może zawierać umowy międzynarodowe, zgodnie z art. 218 TFUE, z państwami trzecimi lub organizacjami międzynarodowymi, umożliwiając i organizując ich udział w niektórych działaniach grupy współpracy. Takie umowy muszą uwzględniać potrzebę zapewnienia odpowiedniej ochrony danych.		Nie wymaga transpozycji.
Wymogi w zakresie bezpieczeństwa i zgłaszanie incydentów Art. 14	1. Państwa członkowskie zapewniają, aby operatorzy usług kluczowych podejmowali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są wykorzystywane przez nich sieci i systemy informatyczne. Uwzględniając najnowszy stan wiedzy, środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka. 2. Państwa członkowskie zapewniają, aby operatorzy usług kluczowych podejmowali odpowiednie środki zapobiegające	Art. 8	Art. 8. Operator usługi kluczowej wdraża system zarządzania bezpieczeństwem w systemie informacyjnym, wykorzystywanym do świadczenia usługi kluczowej, zapewniający: 1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie ryzykiem wystąpienia incydentu; 2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym: a) utrzymanie i bezpieczną eksploatację systemów informacyjnych,

	i minimalizujące wpływ incydentów dotyczących bezpieczeństwa sieci i systemów informatycznych wykorzystywanych w celu świadczenia takich usług kluczowych, z myślą o zapewnieniu ciągłości tych usług.		b) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu, c) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej, d) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz poufność, integralność, dostępność i autentyczność informacji, e) objęcie systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym; 3) zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej; 4) zarządzanie incydentami; 5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej, w tym: a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemach informacyjnych, b) dbałość o aktualizację oprogramowania, c) ochronę przed nieuprawnioną modyfikacją w systemach informacyjnych, d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa; 6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.
		Art. 9	Art. 9. 1. Operator usługi kluczowej: 1) wyznacza osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa; 2) zapewnia użytkownikowi usługi kluczowej dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami w zakresie związanym ze świadczoną usługą kluczową, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej; 3) przekazuje organowi właściwemu informacje, o których mowa w art. 7 ust. 2 pkt 8 i 9, nie później niż w terminie 3 miesięcy, od zmiany tych danych.

			2. Operator usługi kluczowej przekazuje do organu właściwego, właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowego zespołu cyberbezpieczeństwa dane osoby, o której mowa w ust. 1 pkt 1, zawierające imię i nazwisko, numer telefonu, adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych, w terminie 14 dni od dnia nastąpienia zmiany.
		Art. 10	Art. 10. 1. Operator usługi kluczowej opracowuje, stosuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. 2. Operator usługi kluczowej jest obowiązany do ustanowienia nadzoru nad dokumentacją dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zapewniającego: 1) dostępność dokumentów wyłącznie dla osób upoważnionych zgodnie z realizowanymi przez nie zadaniami; 2) ochronę dokumentów przed niewłaściwym użyciem lub utratą integralności; 3) oznaczanie kolejnych wersji dokumentów umożliwiające określenie zmian dokonanych w dokumentach. 3. Operator usługi kluczowej przechowuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przez co najmniej 2 lata od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi kluczowej, z uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r. poz. 217, 357, 398 i 650). 4. Operator usługi kluczowej będący jednocześnie właścicielem, posiadaczem samoistnym albo zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566), który posiada zatwierdzony plan ochrony infrastruktury krytycznej, uwzględniający dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej nie ma obowiązku opracowania dokumentacji, o której mowa w ust. 1. 5. Rada Ministrów określi w drodze rozporządzenia rodzaje dokumentacji, o której mowa w ust. 1, uwzględniając Polskie Normy oraz potrzebę zapewnienia cyberbezpieczeństwa podczas

			świadczenia usług kluczowych i ciągłości świadczenia tych usług.
	3. Państwa członkowskie zapewniają, aby operatorzy usług kluczowych niezwłocznie zgłaszali właściwemu organowi lub CSIRT incydenty mające istotny wpływ na ciągłość świadczonych przez nich usług kluczowych. Zgłoszenia muszą zawierać informacje umożliwiające właściwemu organowi lub CSIRT określenie transgranicznego wpływu incydentu. Zgłoszenie nie może narażać strony zgłaszającej na zwiększoną odpowiedzialność. 4. Aby określić istotność wpływu danego incydentu, uwzględnia się w szczególności następujące parametry: a) liczbę użytkowników, których dotyczy zakłócenie usługi kluczowej; b) czas trwania incydentu; c) zasięg geograficzny związany z obszarem, którego dotyczy incydent. 5. W oparciu o informacje przekazane w zgłoszeniu przez operatora usług kluczowych właściwy organ lub CSIRT informuje inne państwo członkowskie, którego dotyczy incydent, lub inne państwa członkowskie, których dotyczy incydent, czy ma on istotny wpływ na ciągłość usług kluczowych w tym państwie członkowskim. W działaniach tych właściwy organ lub CSIRT – zgodnie z prawem Unii lub prawodawstwem krajowym zgodnym z prawem Unii – chronią bezpieczeństwo i interesy handlowe operatora usług kluczowych, jak również poufność informacji przekazanych w jego zgłoszeniu. Jeżeli pozwalają na to okoliczności, właściwy organ lub CSIRT przekazują zgłaszającemu operatorowi usług kluczowych odpowiednie informacje dotyczące działań następczych jego zgłoszenia, takie jak informacje, które mogłyby wesprzeć skuteczne postępowanie w przypadku incydentu. Na wniosek właściwego organu lub CSIRT pojedynczy punkt kontaktowy przekazuje zgłoszenia, o których mowa w akapicie pierwszym, pojedynczym punktom kontaktowym w innych państwach członkowskich, których dotyczy incydent.	Art. 11 ust. 1-2 i 4 Art. 16	Art. 11. 1. Operator usługi kluczowej: 1) zapewnia obsługę incydentu; 2) zapewnia dostęp do informacji o rejestrowanych incydentach właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV w zakresie niezbędnym do realizacji jego zadań; 3) klasyfikuje incydent jako poważny na podstawie progów uznawania incydentu za poważny; 4) zgłasza incydent poważny niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV; 5) współdziała podczas obsługi incydentu poważnego lub incydentu krytycznego z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe; 6) usuwa podatności, o których mowa w art. 32 ust. 2, oraz informuje o ich usunięciu organ właściwy. 2. Zgłoszenie, o którym mowa w ust. 1 pkt 4, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji. (…) 4. Rada Ministrów określi w drodze rozporządzenia progi uznania incydentu za poważny według rodzaju zdarzenia, w poszczególnych sektorach, podsektorach określonych w załączniku nr 1 do ustawy, określając: 1) liczbę użytkowników, których dotyczy zakłócenie świadczenia usługi kluczowej, 2) czas trwania oddziaływania incydentu na świadczoną usługę, 3) zasięg geograficzny związany z obszarem, którego dotyczy incydent, 4) inne czynniki charakterystyczne dla danego sektora lub podsektora, jeżeli występują – kierując się potrzebą zapewnienia ochrony przed zagrożeniem życia i zdrowia ludzi, znacznymi stratami majątkowymi, obniżeniem jakości świadczonej usługi kluczowej. Art. 16. Operator usługi kluczowej realizuje obowiązki określone w: 1) art. 8 pkt 1 i 4, art. 9, art. 11 ust. 1-3, art. 12 i art. 14 ust. 1 – w terminie trzech miesięcy od dnia doręczenia decyzji o uznaniu za

	6. Po konsultacji ze zgłaszającym operatorem usług kluczowych właściwy organ lub CSIRT może poinformować społeczeństwo o poszczególnych incydentach, w przypadku gdy wiedza społeczeństwa jest niezbędna do tego, aby zapobiec wystąpieniu incydentu lub aby poradzić sobie z trwającym incydentem. 7. Właściwe organy, działając wspólnie w ramach grupy współpracy, mogą opracować i przyjąć wytyczne dotyczące okoliczności, w których operatorzy usług kluczowych są zobowiązani do zgłaszania incydentów, w tym parametry służące określeniu istotności wpływu incydentu, o której mowa w ust. 4.	Art. 2 pkt 7 Art. 12	operatora usługi kluczowej; 2) art. 8 pkt 2 i 3 oraz pkt 5 i 6 i art. 10 ust. 1-3 – w terminie sześciu miesięcy od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej; 3) art. 15 ust. 1 – w terminie roku od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej. 7) incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej; Art. 12. 1. Zgłoszenie incydentu poważnego, o którym mowa w art. 11 ust. 1 pkt 4, zawiera: 1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres; 2) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby składającej zgłoszenie; 3) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji; 4) opis wpływu incydentu poważnego na usługę kluczową w tym: a) usługi kluczowe zgłaszającego, na które incydent poważny miał wpływ, b) liczbę użytkowników usługi kluczowej, na których incydent poważny miał wpływ, c) moment wystąpienia i wykrycia incydentu poważnego oraz czas jego trwania, d) zasięg geograficzny, którego dotyczy incydent poważny, e) wpływ incydentu poważnego na usługi kluczowe świadczone przez innych operatorów usług kluczowych i dostawców usług cyfrowych, f) przyczynę zaistnienia incydentu poważnego oraz sposób jego przebiegu i skutki jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe; 5) informacje umożliwiające właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV określenie, czy incydent dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej; 6) w przypadku incydentu, który mógł mieć wpływ na usługi kluczowe, opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne; 7) informacje o przyczynie i źródle incydentu poważnego;

			8) informacje o podjętych działaniach zapobiegawczych; 9) informacje o podjętych działaniach naprawczych; 10) inne istotne informacje. 2. Operator usługi kluczowej przekazuje informacje znane mu w chwili zgłoszenia, które uzupełnia w trakcie obsługi incydentu poważnego. 3. Operator usługi kluczowej przekazuje w niezbędnym zakresie w zgłoszeniu, o którym mowa w ust. 1, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji zadań, zgodnie z właściwością przez CSIRT MON, CSIRT NASK lub CSIRT GOV, bądź zadań sektorowego zespołu cyberbezpieczeństwa. 4. Zgodnie z właściwością CSIRT MON, CSIRT NASK lub CSIRT GOV, bądź sektorowy zespół cyberbezpieczeństwa może zwrócić się do operatora usługi kluczowej o uzupełnienie zgłoszenia o informacje, w tym stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie. 5. W zgłoszeniu operator usługi kluczowej oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.
		Art. 14	Art. 14. 1. Operator usługi kluczowej, w celu realizacji zadań, o których mowa w art. 8, art. 9, art. 10 ust. 1-3, art. 11 ust. 1-3, art. 12 oraz art. 13, powołuje wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawiera umowę z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa. 2. Wewnętrzne struktury powołane przez operatora usługi kluczowej odpowiedzialne za cyberbezpieczeństwo oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa są obowiązane: 1) spełniać warunki organizacyjne i techniczne pozwalające na zapewnienie cyberbezpieczeństwa obsługiwanemu operatorowi usługi kluczowej; 2) dysponować pomieszczeniami służącymi do świadczenia usług z zakresu reagowania na incydenty zabezpieczonymi przed zagrożeniami fizycznymi i środowiskowymi; 3) stosować zabezpieczenia w celu zapewnienia poufności, integralności, dostępności i autentyczności przetwarzanych informacji z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów. 3. Operator usługi kluczowej informuje organ właściwy i właściwy CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowy zespół

			cyberbezpieczeństwa o podmiocie, z którym została zawarta umowa na świadczenie usług z zakresu cyberbezpieczeństwa, danych kontaktowych tego podmiotu, zakresie świadczonej usługi oraz informacje o rozwiązaniu umowy, w terminie 14 dni od zawarcia lub rozwiązania umowy. 4. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia warunki organizacyjne i techniczne dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo, uwzględniając Polskie Normy oraz konieczność zapewnienia bezpieczeństwa dla wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo i podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla operatorów usług kluczowych, a także konieczność zapewnienia bezpieczeństwa informacji przetwarzanych w tych strukturach albo podmiotach.
		Art. 37 ust. 2-4	Art. 37. 2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym operatorem usługi kluczowej, opublikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje o incydentach poważnych, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu albo zapewnić obsługę incydentu. 3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym incydent istotny dostawcą usług cyfrowych, opublikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej lub Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje o incydentach istotnych lub wystąpić do organu właściwego dla dostawcy usług cyfrowych, aby zobowiązał dostawcę usług cyfrowych do podania tych informacji do publicznej wiadomości, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę incydentu albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym. 4. Opublikowanie informacji, o której mowa w ust. 2 i 3, nie może naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych, a także przepisów o ochronie

			danych osobowych.
		Art. 45 ust. 1 pkt 3 I 6	Art. 45. 1. Minister właściwy do spraw informatyzacji jest odpowiedzialny za: 3) opracowywanie rocznych sprawozdań dotyczących: a) incydentów poważnych zgłaszanych przez operatorów usług kluczowych mających wpływ na ciągłość świadczonych przez nich usług kluczowych w Rzeczypospolitej Polskiej oraz ciągłość świadczonych usług kluczowych w państwach członkowskich Unii Europejskiej, b) incydentów istotnych zgłaszanych przez dostawców usług cyfrowych, w tym incydentów dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej; 6) udostępnianie informacji i dobrych praktyk związanych ze zgłaszaniem incydentów poważnych przez operatorów usług kluczowych i incydentów istotnych przez dostawców usług cyfrowych, uzyskanych z Grupy Współpracy, w tym: a) procedur postępowania w zakresie zarządzania incydentem, b) procedur postępowania przy zarządzaniu ryzykiem, c) klasyfikacji informacji, ryzyka i incydentów.
		Art. 47	Art. 47. 1. Minister właściwy do spraw informatyzacji może realizować zadania, o których mowa w art. 45 i 46 ust. 1, na zasadach określonych w przepisach odrębnych, za pomocą właściwych w tym zakresie jednostek podległych lub nadzorowanych przez ministra właściwego do spraw informatyzacji. 2. Zadania powierzone do realizacji podmiotowi, o którym mowa w ust. 1, są finansowane w formie dotacji celowej z części budżetu państwa, której dysponentem jest minister właściwy do spraw informatyzacji.
		Art. 28	Art. 28. 1. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV informuje, na podstawie zgłoszenia incydentu poważnego dokonanego przez operatora usługi kluczowej, inne państwa członkowskie Unii Europejskiej, których dotyczy ten incydent, za pośrednictwem Pojedynczego Punktu Kontaktowego. 2. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV przekazuje, jeżeli pozwalają na to okoliczności, operatorowi usługi kluczowej, zgłaszającemu incydent poważny, informacje dotyczące działań podjętych po zgłoszeniu tego incydentu, które mogłyby pomóc w jego obsłudze. 3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może

			wystąpić z wnioskiem do Pojedynczego Punktu Kontaktowego o przekazanie zgłoszenia incydentu poważnego, o którym mowa w ust. 1, pojedynczym punktom kontaktowym w innych państwach członkowskich Unii Europejskiej, których dotyczy ten incydent.
Wdrażanie i egzekwowanie Art. 15	1. Państwa członkowskie zapewniają, aby właściwe organy miały uprawnienia i środki niezbędne do oceny wypełniania przez operatorów usług kluczowych ich obowiązków na mocy art. 14 oraz jego skutków dla bezpieczeństwa sieci i systemów informatycznych. 2. Państwa członkowskie zapewniają, aby właściwe organy miały uprawnienia i środki, pozwalające wymagać od operatorów usług kluczowych przekazywania: a) informacji niezbędnych do oceny bezpieczeństwa ich sieci i systemów informatycznych, w tym dokumentów dotyczących polityki w zakresie bezpieczeństwa; b) dowodów skutecznej realizacji polityk w zakresie bezpieczeństwa, takich jak wyniki audytu bezpieczeństwa przeprowadzonego przez właściwy organ lub wykwalifikowanego audytora oraz, w tym ostatnim przypadku, udostępniania ich wyników – łącznie ze wspierającymi je dowodami – właściwemu organowi. Zwracając się o przekazanie takich informacji lub dowodów, właściwy organ podaje cel wniosku i określa, jakie informacje są wymagane. 3. Po dokonaniu oceny informacji lub wyników audytów bezpieczeństwa, o których mowa w ust. 2, właściwy organ może wydać operatorom usług kluczowych wiążące polecenia wprowadzenia środków zaradczych w odniesieniu do stwierdzonych uchybień.	Art. 53 ust. 1 i 2 Art. 54-59	Art. 53. 1. Nadzór w zakresie stosowania przepisów ustawy sprawują: 1) minister właściwy do spraw informatyzacji w zakresie spełniania przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa wymogów, o których mowa w art. 15 ust. 2; 2) organy właściwe w zakresie: a) wykonywania przez operatorów usług kluczowych wynikających z ustawy obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów poważnych, b) spełniania przez dostawców usług cyfrowych wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych określonych w rozporządzeniu wykonawczym 2018/151 oraz wykonywania wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych. 2. W ramach nadzoru, o którym mowa w ust. 1: 1) organ właściwy lub minister właściwy do spraw informatyzacji prowadzi kontrole w zakresie, o którym mowa w ust. 1; 2) organ właściwy nakłada kary pieniężne na operatorów usług kluczowych i dostawców usług cyfrowych. Art. 54. 1. Do kontroli, której zakres określony jest w art. 53 ust. 1 pkt 1, stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców. 2. Do kontroli, której zakres określony jest w art. 53 ust. 1 pkt 2, realizowanej wobec podmiotów: 1) będących przedsiębiorcami, stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców; 2) niebędących przedsiębiorcami, stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, określające zasady i tryb przeprowadzania kontroli. Art. 55. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ma prawo do: 1) swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki; 2) wglądu do dokumentów dotyczących działalności podmiotu kontrolowanego, pobierania za pokwitowaniem oraz zabezpieczania dokumentów związanych z zakresem kontroli, z

			zachowaniem przepisów o tajemnicy prawnie chronionej; 3) sporządzania, a w razie potrzeby żądania sporządzenia niezbędnych do kontroli kopii, odpisów lub wyciągów z dokumentów oraz zestawień lub obliczeń; 4) przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu kontroli; 5) żądania złożenia ustnych lub pisemnych wyjaśnień w sprawach dotyczących zakresu kontroli; 6) przeprowadzania oględzin urządzeń, nośników oraz systemów informacyjnych. Art. 56. 1. Kontrolowane podmioty będące przedsiębiorcami zapewniają osobie prowadzącej czynności kontrolne warunki niezbędne do sprawnego przeprowadzenia kontroli, w szczególności przez zapewnienie niezwłocznego przedstawienia żądanych dokumentów, terminowego udzielania ustnych i pisemnych wyjaśnień w sprawach objętych kontrolą, udostępniania niezbędnych urządzeń technicznych, a także sporządzania we własnym zakresie kopii lub wydruków dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub w systemach informacyjnych. 2. Podmiot kontrolowany dokonuje potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków, o których mowa w ust. 1. W przypadku odmowy potwierdzenia za zgodność z oryginałem potwierdza je osoba prowadząca czynności kontrolne, o czym czyni wzmiankę w protokole kontroli. Art. 57. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami ustala stan faktyczny na podstawie dowodów zebranych w toku kontroli, a w szczególności dokumentów, przedmiotów, oględzin oraz ustnych lub pisemnych wyjaśnień i oświadczeń. Art. 58. 1. Osoba prowadząca czynności kontrolne wobec podmiotów będących przedsiębiorcami przedstawia przebieg przeprowadzonej kontroli w protokole kontroli. 2. Protokół kontroli zawiera: 1) wskazanie nazwy albo imienia i nazwiska oraz adresu podmiotu kontrolowanego; 2) imię i nazwisko osoby reprezentującej podmiot kontrolowany oraz nazwę organu reprezentującego ten podmiot; 3) imię i nazwisko, stanowisko oraz numer upoważnienia osoba

			prowadzącej czynności kontrolne; 4) datę rozpoczęcia i zakończenia czynności kontrolnych; 5) określenie przedmiotu i zakresu kontroli; 6) opis stanu faktycznego ustalonego w toku kontroli oraz inne informacje mające istotne znaczenie dla przeprowadzonej kontroli, w tym zakres, przyczyny i skutki stwierdzonych nieprawidłowości; 7) wyszczególnienie załączników. 3. Protokół kontroli podpisują osoba prowadząca czynności kontrolne oraz osoba reprezentująca podmiot kontrolowany. 4. Przed podpisaniem protokołu podmiot kontrolowany może, w terminie 7 dni od przedstawienia mu go do podpisu, złożyć pisemne zastrzeżenia do tego protokołu. 5. W razie zgłoszenia zastrzeżeń osoba prowadząca czynności kontrolne dokonuje ich analizy i, w razie potrzeby, podejmuje dodatkowe czynności kontrolne, a w przypadku stwierdzenia zasadności zastrzeżeń zmienia lub uzupełnia odpowiednią część protokołu w formie aneksu do protokołu. 6. W razie nieuwzględnienia zastrzeżeń w całości lub w części osoba prowadząca czynności kontrolne informuje podmiot kontrolowany na piśmie. 7. O odmowie podpisania protokołu osoba prowadząca czynności kontrolne czyni wzmiankę w protokole, zawierającą datę jej dokonania. 8. Protokół w postaci papierowej sporządza się w dwóch egzemplarzach, z których jeden pozostawia się podmiotowi kontrolowanemu, a w przypadku protokołu sporządzonego w postaci elektronicznej doręcza się go podmiotowi kontrolowanemu. Art. 59. 1. Jeżeli na podstawie informacji zgromadzonych w protokole kontroli, organ właściwy lub minister właściwy do spraw informatyzacji uzna, że mogło dojść do naruszenia przepisów ustawy przez podmiot kontrolowany, przekazuje zalecenia pokontrolne dotyczące usunięcia nieprawidłowości. 2. Od zaleceń pokontrolnych nie przysługują środki odwoławcze. 3. Podmiot kontrolowany, w wyznaczonym terminie, informuje organ właściwy lub ministra właściwego do spraw informatyzacji o sposobie wykonania zaleceń.
		Art. 15	Art. 15. 1. Operator usługi kluczowej ma obowiązek zapewnić przeprowadzenie co najmniej raz na dwa lata audytu

			bezpieczeństwa systemów informacyjnych, wykorzystywanych do świadczenia usługi kluczowej, zwanego dalej „audytem”. 2. Audyt, o którym nowa w ust. 1, może być przeprowadzony przez: 1) jednostkę oceniająca zgodność, akredytowaną zgodnie z ustawą z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650) w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych; 2) co najmniej dwóch audytorów posiadających: a) certyfikaty określone w przepisach wydanych na podstawie ust. 8, lub b) co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, lub c) co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymuje się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych; 3) sektorowy zespól cyberbezpieczeństwa, ustanowiony w ramach sektora lub podsektora wymienionego w załączniku nr 1 do ustawy, jeżeli audytorzy spełniają warunki, o których mowa w pkt 2. 3. Za praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych, o której mowa w ust. 2 pkt 2 lit. b i c, uważa się udokumentowane wykonanie 3 audytów w ciągu ostatnich 3 lat w zakresie bezpieczeństwa systemów informacyjnych lub ciągłości działania albo wykonywanie audytów bezpieczeństwa systemów informacyjnych lub ciągłości działania, w wymiarze czasu pracy nie mniejszym niż 1/2 etatu, związanych z: 1) przeprowadzaniem audytu wewnętrznego pod nadzorem audytora wewnętrznego; 2) przeprowadzaniem audytu zewnętrznego pod nadzorem audytora wiodącego; 3) przeprowadzaniem audytu wewnętrznego w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne;

			4) wykonywaniem czynności kontrolnych, o których mowa w ustawie z 15 lipca 2011 r. o kontroli w administracji rządowej (Dz. U. poz. 1092); 5) wykonywaniem czynności kontrolnych, o których mowa w ustawie z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli (Dz. U. z 2017 r. poz. 524). 4. Audytorzy są obowiązani do zachowania w tajemnicy informacji uzyskanych w związku z przeprowadzanym audytem, z zachowaniem przepisów o ochronie informacji niejawnych i innych informacji prawnie chronionych. 5. Na podstawie zebranych dokumentów i dowodów audytor sporządza pisemne sprawozdanie z przeprowadzonego audytu i przekazuje je operatorowi usługi kluczowej wraz z dokumentacją z przeprowadzonego audytu. 6. Operator usługi kluczowej, u którego w danym roku, w stosunku do systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej, został przeprowadzony przez osoby spełniające warunki określone w ust. 2 pkt 2, audyt wewnętrzny w zakresie bezpieczeństwa informacji, o którym mowa w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne nie ma obowiązku przeprowadzania przez 2 lata audytu, o którym mowa w ust. 1. 7. Operator usługi kluczowej przekazuje kopię sprawozdania z przeprowadzonego audytu na uzasadniony wniosek: 1) organu właściwego; (…) 8. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia wykaz certyfikatów uprawniających do przeprowadzenia audytu, uwzględniając zakres wiedzy specjalistycznej wymaganej od osób legitymujących się poszczególnymi certyfikatami.
	4. Obsługując incydenty, które doprowadziły do naruszeń danych osobowych, właściwy organ działa w ścisłej współpracy	Art. 34 ust. 2	Art. 34. 2. CSIRT MON, CSIRT NASK i CSIRT GOV koordynując obsługę

	z organami ochrony danych.		incydentu, który doprowadził do naruszenia danych osobowych, współpracuje z organem właściwym do spraw ochrony danych osobowych.
Wymogi w zakresie bezpieczeństwa i zgłaszanie incydentów Art. 16	1. Państwa członkowskie zapewniają, aby dostawcy usług cyfrowych określali i podejmowali odpowiednie i proporcjonalne środki techniczne i organizacyjne w celu zarządzania ryzykami, na jakie narażone są sieci i systemy informatyczne wykorzystywane przez nich w kontekście oferowania usług, o których mowa w załączniku III, w Unii. Uwzględniając najnowszy stan wiedzy, środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka oraz uwzględniać następujące elementy: a) bezpieczeństwo systemów i obiektów; b) postępowanie w przypadku incydentu; c) zarządzanie ciągłością działania; d) monitorowanie, audyt i testowanie; e) zgodność z normami międzynarodowymi. 2. Państwa członkowskie zapewniają, aby dostawcy usług cyfrowych podejmowali środki zapobiegające i minimalizujące wpływ incydentów dotyczących bezpieczeństwa ich sieci i systemów informatycznych na usługi, o których mowa w załączniku III, oferowane w Unii, z myślą o zapewnieniu ciągłości tych usług. 3. Państwa członkowskie zapewniają, aby dostawcy usług cyfrowych bez zbędnej zwłoki zgłaszali właściwemu organowi lub CSIRT wszelkie incydenty mające istotny wpływ na świadczenie usługi, o której mowa w załączniku III, oferowanej przez tych dostawców w Unii. Zgłoszenia muszą zawierać informacje umożliwiające właściwemu organowi lub CSIRT określenie istotności wpływu transgranicznego. Zgłoszenie nie może narażać strony zgłaszającej na zwiększoną odpowiedzialność. 4. W celu określenia, czy wpływ incydentu jest istotny, uwzględnia się w szczególności następujące parametry: a) liczbę użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług; b) czas trwania incydentu; c) zasięg geograficzny, którego dotyczy incydent; d) zasięg zakłócenia funkcjonowania usługi; e) zasięg wpływu na działalność gospodarczą i społeczną.	Art. 18-19	Art. 18. 1. Dostawca usługi cyfrowej: 1) przeprowadza czynności umożliwiające wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów; 2) zapewnia w niezbędnym zakresie dostęp do informacji dla właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV o incydentach zakwalifikowanych jako krytyczne przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV; 3) klasyfikuje incydent jako istotny; 4) zgłasza incydent istotny niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV; 5) zapewnia obsługę incydentu istotnego i incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe; 6) usuwa podatności, o których mowa w art. 32 ust. 2; 7) przekazuje operatorowi usługi kluczowej, który świadczy usługę kluczową za pośrednictwem tego dostawcy usługi cyfrowej, informacje dotyczące incydentu mającego wpływ na ciągłość świadczenia usługi kluczowej tego operatora. 2. Dostawca usługi cyfrowej, w celu sklasyfikowania incydentu jako istotnego, uwzględnia w szczególności: 1) liczbę użytkowników, których dotyczy incydent, w szczególności użytkowników zależnych od usługi na potrzeby świadczenia ich własnych usług; 2) czas trwania incydentu; 3) zasięg geograficzny, którego dotyczy incydent; 4) zasięg zakłócenia funkcjonowania usługi; 5) zasięg wpływu incydentu na działalność gospodarczą i społeczną. 3. Dostawca usługi cyfrowej klasyfikując incydent jako istotny, ocenia istotność wpływu incydentu na świadczenie usługi cyfrowej, na podstawie parametrów, o których mowa w ust. 2, oraz progów określonych w rozporządzeniu wykonawczym 2018/151. 4. Dostawca usługi cyfrowej nie ma obowiązku dokonania zgłoszenia, o którym mowa w ust. 1 pkt 4, gdy nie posiada informacji pozwalających na ocenę istotności wpływu incydentu na świadczenie usługi cyfrowej. 5. Zgłoszenie, o którym mowa w ust. 1 pkt 4, przekazywane jest w

	Obowiązek zgłoszenia incydentu ma zastosowanie wyłącznie wówczas, gdy dostawca usług cyfrowych ma dostęp do informacji niezbędnych do oceny wpływu incydentu względem parametrów, o których mowa w akapicie pierwszym. 5. W przypadku gdy do celów świadczenia usługi, która ma istotne znaczenie dla utrzymania krytycznej działalności społecznej i gospodarczej, operator usług kluczowych jest zależny od dostawcy usług cyfrowych będącego stroną trzecią, operatorowi temu zgłasza się wszelki istotny wpływ na ciągłość usług kluczowych związany z incydentem, który dotyczy dostawcy usług cyfrowych. 6. W stosownych przypadkach, w szczególności gdy incydent, o którym mowa w ust. 3, dotyczy dwóch lub większej liczby państw członkowskich, właściwy organ lub CSIRT informuje inne państwa członkowskie, których dotyczy incydent. W działaniach tych właściwe organy, CSIRT i pojedyncze punkty kontaktowe – zgodnie z prawem Unii lub prawodawstwem krajowym zgodnym z prawem Unii – chronią bezpieczeństwo i interesy handlowe dostawcy usług cyfrowych, jak również poufność przekazywanych informacji. 7. Po konsultacji z zainteresowanym dostawcą usług cyfrowych właściwy organ lub CSIRT oraz, w stosownych przypadkach, organy lub CSIRT innych zainteresowanych państw członkowskich mogą poinformować społeczeństwo o poszczególnych incydentach lub zobowiązać dostawcę usług cyfrowych, aby to zrobił, w przypadku gdy wiedza społeczeństwa jest niezbędna, żeby zapobiec wystąpieniu incydentu lub aby poradzić sobie z trwającym incydentem lub w przypadku gdy ujawnienie incydentu z innych względów leży w interesie publicznym. 8. Komisja przyjmuje akty wykonawcze w celu dalszego doprecyzowania elementów, o których mowa w ust. 1, oraz parametrów wymienionych w ust. 4 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 22 ust. 2, w terminie do dnia 9 sierpnia 2017 r. 9. Komisja może przyjąć akty wykonawcze określające formaty i procedury mające zastosowanie do wymogów dotyczących zgłaszania. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 22 ust. 2. 10. Bez uszczerbku dla art. 1 ust. 6 państwa członkowskie nie mogą nakładać na dostawców usług cyfrowych jakichkolwiek		postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji. Art. 19. 1. Zgłoszenie incydentu istotnego, o którym mowa w art. 18 ust. 1 pkt 4, zawiera: 1) dane podmiotu zgłaszającego, w tym firmę przedsiębiorcy, numer we właściwym rejestrze, siedzibę i adres; 2) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby składającej zgłoszenie; 3) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji; 4) opis wpływu incydentu istotnego na świadczenie usługi cyfrowej, w tym: a) liczbę użytkowników, na których incydent miał wpływ, b) moment wystąpienia i wykrycia incydentu istotnego oraz czas jego trwania, c) zasięg geograficzny, którego dotyczy incydent istotny, d) zakres zakłócenia funkcjonowania usługi cyfrowej, e) zakres wpływu incydentu na działalność gospodarczą i społeczną; 5) informacje umożliwiające właściwemu CSIRT MON, CSIRT NASK lub CSIRT GOV określenie, czy incydent dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej; 6) informacje o przyczynie i źródle incydentu istotnego; 7) informacje o podjętych działaniach zapobiegawczych; 8) informacje o podjętych działaniach naprawczych; 9) inne istotne informacje. 2. Dostawca usługi cyfrowej przekazuje informacje znane mu w chwili zgłoszenia, które uzupełnia w trakcie obsługi incydentu. 3. Dostawca usługi cyfrowej przekazuje w niezbędnym zakresie w zgłoszeniu, o którym mowa w ust. 1, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji zadań, zgodnie z właściwością przez CSIRT MON, CSIRT NASK lub CSIRT GOV. 4. Zgodnie z właściwością CSIRT MON, CSIRT NASK lub CSIRT GOV może zwrócić się do dostawcy usługi cyfrowej o uzupełnienie zgłoszenia o informacje, w tym stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie.

	dalszych wymogów dotyczących bezpieczeństwa lub zgłaszania. 11. Rozdział V nie ma zastosowania do mikroprzedsiębiorstw i małych przedsiębiorstw zdefiniowanych w zaleceniu Komisji 2003/361/WE ([19]).		5. W zgłoszeniu dostawcy usług cyfrowych oznaczają informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.
		Art. 29	Art. 29. CSIRT MON, CSIRT NASK lub CSIRT GOV informuje inne państwa członkowskie Unii Europejskiej w przypadku, gdy incydent istotny dotyczy dwóch lub większej liczby państw członkowskich Unii Europejskiej, za pośrednictwem Pojedynczego Punktu Kontaktowego.
		Art. 37 ust. 3	3. Właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV może, po konsultacji ze zgłaszającym incydent istotny dostawcą usług cyfrowych, opublikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej lub Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje o incydentach istotnych lub wystąpić do organu właściwego dla dostawcy usług cyfrowych, aby zobowiązał dostawcę usług cyfrowych do podania tych informacji do publicznej wiadomości, gdy jest to niezbędne, aby zapobiec wystąpieniu incydentu lub zapewnić obsługę incydentu albo gdy z innych powodów ujawnienie incydentu jest w interesie publicznym.
Wdrażanie i egzekwowanie Art. 17	1. Państwa członkowskie zapewniają, aby właściwe organy podjęły działania, w razie konieczności, w drodze środków nadzorczych *ex post*, gdy otrzymają dowód, że dostawca usług cyfrowych nie spełnia wymogów określonych w art. 16. Taki dowód może zostać przekazany przez właściwy organ innego państwa członkowskiego, w którym usługa jest świadczona. 2. Do celów ust. 1 właściwe organy muszą mieć uprawnienia i środki niezbędne do wymagania od dostawców usług cyfrowych: a) przekazywania informacji niezbędnych do oceny bezpieczeństwa ich sieci i systemów informatycznych, w tym dokumentów dotyczących polityki w zakresie	Art. 53 ust. 1 pkt 2 lit. b oraz ust.2 i 3	Art. 53. 1. Nadzór w zakresie stosowania przepisów ustawy sprawują: 2) organy właściwe w zakresie: b) spełniania przez dostawców usług cyfrowych wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych określonych w rozporządzeniu wykonawczym 2018/151 oraz wykonywania wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych. 2. W ramach nadzoru, o którym mowa w ust. 1: 1) organ właściwy lub minister właściwy do spraw informatyzacji prowadzi kontrole w zakresie, o którym mowa w ust. 1; 2) organ właściwy nakłada kary pieniężne na operatorów usług

	bezpieczeństwa; b) eliminowania wszelkich przypadków niespełnienia wymogów określonych w art. 16. 3. Jeżeli dostawca usług cyfrowych posiada główną jednostkę organizacyjną lub przedstawiciela w jednym państwie członkowskim, ale jego sieć i systemy informatyczne są zlokalizowane w jednym lub większej liczbie innych państw członkowskich, właściwy organ państwa członkowskiego głównej jednostki organizacyjnej lub przedstawiciela oraz właściwe organy tych innych państw członkowskich współpracują ze sobą i udzielają sobie wzajemnie pomocy, odpowiednio do potrzeb. Taka pomoc i współpraca mogą obejmować wymianę informacji między zainteresowanymi właściwymi organami oraz wnioski o podjęcie środków nadzorczych, o których mowa w ust. 2.	Art. 42 ust. 2.	kluczowych i dostawców usług cyfrowych. 3. W stosunku do dostawcy usług cyfrowych, podjęcie czynności, o których mowa w ust. 2, następuje po uzyskaniu dowodu, że dostawca usług cyfrowych nie spełnia wymogów określonych w rozporządzeniu wykonawczym 2018/151 lub nie wykonuje wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych. Art. 42. 2. W przypadku, gdy osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, świadcząca usługi cyfrowe, nie posiada siedziby lub zarządu na terytorium Rzeczypospolitej Polskiej albo nie wyznaczyła przedstawiciela na terytorium Rzeczypospolitej Polskiej, ale jej systemy informacyjne znajdują się na terytorium Rzeczypospolitej Polskiej, i nie spełnia wymagań określonych w rozporządzeniu wykonawczym 2018/151, organ właściwy dla dostawców usług cyfrowych może przekazywać informacje oraz zwracać się o podejmowanie działań, o których mowa w art. 53 ust. 2, do organu właściwego w innym państwie członkowskim Unii Europejskiej, na terytorium którego posiada ona siedzibę lub zarząd albo został wyznaczony jej przedstawiciel.
Jurysdykcja i terytorialność Art. 18	1. Na potrzeby niniejszej dyrektywy uznaje się, że dostawca usług cyfrowych podlega jurysdykcji państwa członkowskiego, w którym posiada główną jednostkę organizacyjną. Uznaje się, że dostawca usług cyfrowych posiada główną jednostkę organizacyjną w państwie członkowskim, gdy ma siedzibę zarządu w tym państwie członkowskim. 2. Dostawca usług cyfrowych, który nie posiada jednostki organizacyjnej w Unii, ale oferuje usługi, o których mowa w załączniku III, w Unii, wyznacza przedstawiciela w Unii. Przedstawiciel musi posiadać jednostkę organizacyjną w jednym z tych państw członkowskich, w których oferowane są usługi. Uznaje się, że dostawca usług cyfrowych podlega jurysdykcji państwa członkowskiego, w którym przedstawiciel posiada jednostkę organizacyjną.	Art. 17 ust. 4	17. 4. Dostawca usługi cyfrowej, który nie posiada jednostki organizacyjnej w jednym z państw członkowskich Unii Europejskiej, ale oferuje usługi cyfrowe w Rzeczypospolitej Polskiej wyznacza przedstawiciela, posiadającego jednostkę organizacyjną w Rzeczypospolitej Polskiej, o ile nie wyznaczył przedstawiciela, posiadającego jednostkę organizacyjną w innym państwie członkowskim Unii Europejskiej.

	3. Wyznaczenie przedstawiciela przez dostawcę usług cyfrowych pozostaje bez uszczerbku dla działań prawnych, które mogłyby zostać podjęte przeciwko samemu dostawcy usług cyfrowych.		
Normalizacja Art.19	1. Aby wspierać spójne wdrażanie art. 14 ust. 1 i 2 oraz art. 16 ust. 1 i 2, państwa członkowskie, nie narzucając ani nie faworyzując wykorzystywania określonego rodzaju technologii, zachęcają do stosowania europejskich lub uznanych międzynarodowo norm i specyfikacji mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych. 2. ENISA, we współpracy z państwami członkowskimi, opracowuje porady i wytyczne dotyczące kwestii technicznych, które powinny zostać wzięte pod uwagę w odniesieniu do ust. 1, a także dotyczące już istniejących norm, w tym krajowych norm państw członkowskich, które pozwoliłyby na uwzględnienie tych obszarów	Art. 42 ust. 8	8. Rekomendacje działań mające na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów, o których mowa w ust. 1 pkt 5, przygotowuje się z uwzględnieniem w szczególności Polskich Norm przenoszących normy europejskie, wspólne specyfikacje techniczne, rozumianych jako specyfikacje techniczne w dziedzinie produktów teleinformatycznych określone zgodnie z art. 13 i art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1025/2012 z dnia 25 października 2012 r. w sprawie normalizacji europejskiej, zmieniające dyrektywy Rady 89/686/EWG i 93/15/EWG oraz dyrektywy Parlamentu Europejskiego i Rady 94/9/WE, 94/25/WE, 95/16/WE, 97/23/WE, 98/34/WE, 2004/22/WE, 2007/23/WE, 2009/23/WE i 2009/105/WE oraz uchylające decyzję Rady 87/95/EWG i decyzję Parlamentu Europejskiego i Rady nr 1673/2006/WE (Dz. Urz. UE L 316 z 14.11.2012, str. 12), wytyczne Komisji Europejskiej oraz Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA) w tym zakresie.
Dobrowolne zgłaszanie incydentów Art. 20	1. Bez uszczerbku dla art. 3 podmioty, które nie zostały zidentyfikowane jako operatorzy usług kluczowych i które nie są dostawcami usług cyfrowych, mogą na zasadzie dobrowolności zgłaszać incydenty mające istotny wpływ na ciągłość usług, które świadczą. 2. Przy rozpatrywaniu zgłoszeń państwa członkowskie postępują zgodnie z procedurą określoną w art. 14. Państwa członkowskie mogą rozpatrywać zgłoszenia obowiązkowe priorytetowo względem zgłoszeń dobrowolnych. Zgłoszenia dobrowolne są rozpatrywane wyłącznie wtedy, gdy takie rozpatrywanie nie stanowi nieproporcjonalnego czy nadmiernego obciążenia dla danych państw członkowskich. Zgłoszenie dobrowolne nie może skutkować nałożeniem na podmiot zgłaszający jakichkolwiek obowiązków, którym by nie podlegał, gdyby nie dokonał tego zgłoszenia.	Art. 30	Art. 30. 1. Podmioty inne niż operatorzy usług kluczowych i dostawcy usług cyfrowych, w tym osoby fizyczne, mogą zgłosić incydent do CSIRT NASK. W zgłoszeniu należy podać: 1) nazwę podmiotu lub systemu informacyjnego, w którym wystąpił incydent; 2) opis incydentu; 3) inne istotne informacje. 2. Zgłoszenia incydentów od operatorów usług kluczowych oraz dostawców usług cyfrowych są traktowane priorytetowo względem zgłoszeń, o których mowa w ust. 1. 3. Zgłoszenia, o których mowa w ust. 1, mogą zostać rozpatrzone, gdy nie stanowi to nieproporcjonalnego czy nadmiernego obciążenia dla CSIRT NASK. 4. Podmiot, o którym mowa w ust. 1, oznacza w zgłoszeniu informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.
Sankcje Art. 21	Państwa członkowskie ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszeń krajowych przepisów przyjętych na podstawie niniejszej dyrektywy i podejmują wszystkie niezbędne środki w celu zapewnienia ich	Art. 73-75	Art. 73. 1. Karze pieniężnej podlega operator usługi kluczowej, który: 1) nie przeprowadza systematycznego szacowania ryzyka lub nie zarządza ryzykiem wystąpienia incydentu, o których mowa w art. 8

	wykonania. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach do dnia 9 maja 2018 r., a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą		pkt 1; 2) nie wdrożył środków technicznych i organizacyjnych uwzględniających wymagania, o których mowa w art. 8 pkt 2 lit. a-e; 3) nie stosuje środków, o których mowa w art. 8 pkt 5 lit. a-d; 4) nie wyznaczył osoby, o której mowa w art. 9 ust. 1 pkt 1; 5) nie wykonuje obowiązku, o którym mowa w art. 10 ust. 1; 6) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 1; 7) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 4; 8) nie wykonuje obowiązku, o którym mowa w art. 11 ust. 1 pkt 5; 9) nie wykonuje obowiązku o którym mowa w art. 11 ust. 1 pkt 6; 10) nie wykonuje obowiązku, o którym mowa wart. 14 ust. 1; 11) nie przeprowadza audytu, o którym mowa w art. 15 ust. 1; 12) uniemożliwia lub utrudnia wykonywanie kontroli, o której mowa w art. 53 ust. 2 pkt 1; 13) nie wykonał w wyznaczonym terminie zaleceń pokontrolnych, o których mowa w art. 59 ust. 1. 2. Karze pieniężnej podlega dostawca usługi cyfrowej, który: 1) nie wykonuje obowiązku, wynikającego z art. 18 ust. 1 pkt 4; 2) nie wykonuje obowiązku wynikającego z art. 18 ust. 1 pkt 5; 3) nie wykonuje obowiązku wynikającego z art. 18 ust. 1 pkt 6; 3. Wysokość kary pieniężnej, o której mowa w: 1) ust. 1 pkt 1 wynosi do 150 000 złotych; 2) ust. 1 pkt 2 wynosi do 100 000 złotych; 3) ust. 1 pkt 3 wynosi do 50 000 złotych; 4) ust. 1 pkt 4 wynosi do 15 000 złotych; 5) ust. 1 pkt 5 wynosi do 50 000 złotych; 6) ust. 1 pkt 6 wynosi do 15 000 złotych za każdy stwierdzony przypadek zaniechania obsługi incydentu; 7) ust. 1 pkt 7 wynosi do 20 000 złotych za każdy stwierdzony przypadek niezgłoszenia incydentu poważnego; 8) ust. 1 pkt 8 i 9 wynosi do 20 000 złotych; 9) ust. 1 pkt 10 wynosi 100 000 złotych; 10) ust. 1 pkt 11 i 13 wynosi do 200 000 złotych; 11) ust. 1 pkt 12 wynosi do 50 000 złotych; 12) ust. 2 pkt 1 wynosi do 20 000 złotych za każdy stwierdzony przypadek niezgłoszenia incydentu istotnego; 13) ust. 2 pkt 2 i 3 wynosi do 20 000 złotych. 4. Jeżeli w wyniku kontroli organ właściwy stwierdzi, że operator usługi kluczowej bądź dostawca usługi cyfrowej uporczywie narusza przepisy ustawy powodując: 1) bezpośrednie i poważne zagrożenie cyberbezpieczeństwa dla

			obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego lub życia i zdrowia ludzi, 2) zagrożenie wywołania poważnej szkody majątkowej lub poważnych utrudnień w świadczeniu usług kluczowych – organ właściwy nakłada karę w wysokości do 1 000 000 złotych. Art. 74. 1. Karę pieniężną, o której mowa w art. 73, nakłada w drodze decyzji organ właściwy. 2. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73, stanowią dochód budżetu państwa. 3. Kara, o której mowa w: 1) art. 73 ust. 1 pkt 4 nie może być niższa niż 1 000 złotych; 2) art. 73 ust. 1 pkt 1-3, 6-9 i 12 nie może być niższa niż 5 000 złotych; 3) art. 73 ust. 1 pkt 5, 10, 11 i 13 nie może być niższa niż 15 000 złotych. 4. Organ właściwy może nałożyć karę pieniężną na kierownika operatora usługi kluczowej w przypadku gdy nie dochował należytej staranności celem spełnienia obowiązków, o których mowa w art. 8 pkt 1, art. 9 ust. 1 pkt 1 oraz art. 15 ust. 1, z tym że kara ta może być wymierzona w kwocie nie większej niż 200% jego miesięcznego wynagrodzenia. 5. Kara, o której mowa w art. 73, może zostać nałożona również w przypadku gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli organ właściwy uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia. Art. 75. W sprawach nakładania lub wymierzania administracyjnej kary pieniężnej lub udzielania ulg w jej wykonaniu stosuje się przepisy działu IVa – ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego.
		Art. 50	Art. 50. Pojedynczy Punkt Kontaktowy przekazuje Komisji Europejskiej: 1) niezwłocznie informacje: a) o wyznaczonych organach właściwych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie, b) o przepisach dotyczących kar pieniężnych dotyczących krajowego systemu cyberbezpieczeństwa;
Procedura komitetowa Art. 22	1. Komisję wspomaga Komitet ds. Bezpieczeństwa Sieci i Systemów Informatycznych. Komitet ten jest komitetem w rozumieniu rozporządzenia (UE) nr 182/2011. 2. W przypadku odesłania do niniejszego ustępu stosuje się		Nie wymaga transpozycji.

	art. 5 rozporządzenia (UE) nr 182/2011.		
Przegląd Art. 23	1. W terminie do dnia 9 maja 2019 r. Komisja przedkłada Parlamentowi Europejskiemu i Radzie sprawozdanie, w którym oceni spójność podejścia przyjętego przez państwa członkowskie do identyfikacji operatorów usług kluczowych. 2. Komisja dokonuje okresowego przeglądu funkcjonowania niniejszej dyrektywy i składa Parlamentowi Europejskiemu i Radzie sprawozdania na ten temat. W tym celu oraz z myślą o dalszym rozwijaniu współpracy strategicznej i operacyjnej Komisja bierze pod uwagę sprawozdania grupy współpracy i sieci CSIRT na temat doświadczeń zdobytych na poziomie strategicznym i operacyjnym. W swoim przeglądzie Komisja oceni również wykazy zawarte w załącznikach II i III oraz spójność w identyfikacji operatorów usług kluczowych oraz usług w sektorach, o których mowa w załączniku II. Pierwsze sprawozdanie zostanie przedłożone w terminie do dnia 9 maja 2021 r.		Nie wymaga transpozycji.
Środki przejściowe Art. 24	1. Bez uszczerbku dla art. 25 oraz w celu zapewnienia państwom członkowskim dodatkowych możliwości odpowiedniej współpracy podczas okresu transpozycji grupa współpracy i sieć CSIRT rozpoczynają wykonywanie swoich zadań określonych, odpowiednio, w art. 11 ust. 3 i art. 12 ust. 3 w terminie do dnia 9 lutego 2017 r. 2. W okresie od dnia 9 lutego 2017 r. do dnia 9 listopada 2018 r. oraz w celu wspierania państw członkowskich w przyjmowaniu spójnego podejścia w procesie identyfikacji operatorów usług kluczowych grupa współpracy omawia ten proces, treść i rodzaj środków krajowych umożliwiających identyfikację operatorów usług kluczowych w danym sektorze zgodnie z kryteriami określonymi w art. 5 i 6. Grupa współpracy omawia również, na wniosek państwa członkowskiego, konkretne projekty środków krajowych tego państwa członkowskiego, umożliwiając identyfikację operatorów usług kluczowych w danym sektorze zgodnie z kryteriami określonymi w art. 5 i 6. 3. W terminie do dnia 9 lutego 2017 r. oraz do celów niniejszego artykułu państwa członkowskie zapewnią właściwą reprezentację w grupie współpracy i w sieci CSIRT.		Nie wymaga transpozycji.
Transpozycja Art. 25	1. Państwa członkowskie przyjmują i publikują w terminie do dnia 9 maja 2018 r. przepisy ustawowe, wykonawcze i administracyjne niezbędne do wykonania niniejszej dyrektywy. Niezwłocznie powiadamiają o tym Komisję.	Art. 88 Art. 50	Art. 88. Ustawa wchodzi w życie po upływie 14 dni od dnia ogłoszenia. Art. 50. Pojedynczy Punkt Kontaktowy przekazuje Komisji

	Państwa członkowskie stosują te środki od dnia 10 maja 2018 r. Przepisy przyjęte przez państwa członkowskie zawierają odniesienie do niniejszej dyrektywy lub odniesienie takie towarzyszy ich urzędowej publikacji. Metody dokonywania takiego odniesienia określane są przez państwa członkowskie. 2. Państwa członkowskie przekazują Komisji teksty podstawowych przepisów prawa krajowego przyjętych w dziedzinie objętej niniejszą dyrektywą.		Europejskiej: 1) niezwłocznie informacje: a) o wyznaczonych organach właściwych, Pojedynczym Punkcie Kontaktowym, ich zadaniach oraz późniejszych zmianach w tym zakresie, b) o przepisach dotyczących kar pieniężnych dotyczących krajowego systemu cyberbezpieczeństwa; 2) co 2 lata informacje umożliwiające ocenę wdrażania dyrektywy, obejmujące w szczególności: a) środki umożliwiające identyfikację operatorów usług kluczowych, b) wykaz usług kluczowych, c) liczbę zidentyfikowanych operatorów usług kluczowych w każdym z sektorów, o których mowa w załączniku nr 1 do ustawy, oraz wskazanie ich znaczenia w odniesieniu do tego sektora, d) progi istotności skutku zakłócającego dla świadczonej usługi kluczowej brane pod uwagę przy kwalifikowaniu podmiotów jako operatorów usług kluczowych; 3) informacje o zadaniach CSIRT MON, CSIRT NASK i CSIRT GOV, w tym o głównych elementach procedur postępowania w przypadku wystąpienia incydentu.
Wejście w życie Art. 26	Niniejsza dyrektywa wchodzi w życie dwudziestego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.		Nie wymaga transpozycji.
Adresaci Art. 27	Niniejsza dyrektywa skierowana jest do państw członkowskich.		Nie wymaga transpozycji.
Załącznik I			Nie wymaga transpozycji
Załącznik II		Załącznik nr 1 do ustawy	Załącznik nr 1 do ustawy.

Załącznik III	RODZAJE USŁUG CYFROWYCH DO CELÓW ART. 4 PKT 5 1. Internetowa platforma handlowa. 2. Wyszukiwarka internetowa. 3. Usługa przetwarzania w chmurze.	Art. 17 ust. 1 Załącznik nr 2 do ustawy	Art. 17. 1. Dostawcą usługi cyfrowej jest osoba prawna albo jednostka organizacyjna nie posiadająca osobowości prawnej, mająca siedzibę lub zarząd na terytorium Rzeczypospolitej Polskiej albo przedstawiciela mającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, świadcząca usługę cyfrową w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219 oraz z 2018 r. poz. 650), wymienioną w załączniku nr 2 do ustawy, z wyjątkiem przedsiębiorców, o których mowa w art. 7 ust. 1 pkt 1 i 2 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców (Dz. U. poz. 646). Załącznik nr 2 do ustawy określa rodzaje usług cyfrowych. Usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową. Usługa umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników. Usługa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiającą w wyniku odnośniki, odnoszące się do informacji związanych z zapytaniem.

ODWRÓCONA TABELA ZGODNOŚCI
dla projektu ustawy o krajowym systemie cyberbezpieczeństwa

Tytuł projektu	Projekt ustawy o krajowym systemie cyberbezpieczeństwa
Tytuł wdrażanego aktu prawnego	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, zwana dalej „Dyrektywą NIS”

Jednostka redakcyjna	**Treść przepisu projektu ustawy**	**Uzasadnienie wprowadzenia przepisu**
Art. 2 pkt 6 i 9	6) incydent krytyczny – incydent, skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV; 9) incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7-15;	Ustawa rozróżnia incydenty poważne i istotne, których obowiązek zgłoszenia wynika z Dyrektywy NIS. Dodatkowo wprowadzono kategorie niewystępujące w Dyrektywie NIS tj. incydenty krytyczne – takie, które mogą zaowocować sytuacją kryzysową w rozumieniu ustawy o zarządzaniu kryzysowym oraz incydenty w podmiotach publicznych ze względu na podnoszenie cyberbezpieczeństwa na poziomie krajowym. W tym miejscu warto też wskazać, że definicja incydentu zwykłego jest szersza niż przewidziana w Dyrektywie NIS - odnosząca się do każdego zdarzenia, które ma rzeczywiście niekorzystny wpływ na bezpieczeństwo sieci i systemów informatycznych. W opinii projektodawcy ta definicja jest za wąska, ponieważ wyklucza wszelkie zdarzenia, które zostały powstrzymane przez skuteczne zastosowanie zabezpieczeń (np. odparty atak rozproszonej odmowy dostępu), jak również nieudolne lub niewłaściwie przeprowadzone ataki (np. ściągnięcie malware’u infekującego OS Windows na sprzęt korzystający z Linuksa). Wobec tego poszerzono definicję incydentu zwykłego także o potencjalne zdarzenia o niekorzystnym wpływie. Spowodowało to również rozszerzenie definicji incydentu poważnego.
Art. 1 ust. 2 pkt 3	Art. 1. 2. Ustawy nie stosuje się do: 3) podmiotów wykonujących działalność leczniczą tworzonych przez Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Agencji Wywiadu.	Konieczne było wyłączenie spod zakresu ustawy podmiotów wykonujących działalność leczniczą prowadzonych przez ABW i AW na mocy odrębnych ustaw.

Art. 2 pkt 11 i 15	11) podatność – właściwość systemu informacyjnego, która może być wykorzystana przez zagrożenie cyberbezpieczeństwa; 15) zagrożenie cyberbezpieczeństwa – potencjalną przyczynę incydentu;	Włączenie do ustawy pojęć „podatność" i „zagrożenie cyberbezpieczeństwa" służy przypisaniu ról podmiotom wchodzących w skład krajowego systemu cyberbezpieczeństwa wobec zdarzeń, które nie są incydentami, ale mogą się w nie przeobrazić. Rozwiązanie to czyni system bardziej elastycznym i stwarza szersze spektrum możliwych działań jeszcze przed wystąpieniem incydentu.
Art. 2 pkt 16	16) zarządzanie incydentem – obsługę incydentu, wyszukiwanie powiązań pomiędzy incydentami, usuwanie przyczyn ich wystąpienia oraz opracowanie wniosków z obsługi incydentu;	Zdefiniowanie pojęcia „zarządzanie incydentem" jest konieczne w celu określenia zadań podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa. Jest ono szersze niż obsługa incydentu (w dyrektywie NIS – „postępowanie z incydentem", „incident handling"), gdyż obejmuje również czynności dotyczące wyszukiwania powiązań, usuwania przyczyn i opracowywania wniosków z obsługi incydentu (tzw. „lessons learnt").
Art. 3 i 4	Art. 3. Krajowy system cyberbezpieczeństwa ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Art. 4. Krajowy system cyberbezpieczeństwa obejmuje: 1) operatorów usług kluczowych; 2) dostawców usług cyfrowych; 3) CSIRT MON; 4) CSIRT NASK; 5) CSIRT GOV; 6) sektorowe zespoły cyberbezpieczeństwa; 7) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1-6, 8 i 9 oraz 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62); 8) instytuty badawcze; 9) Narodowy Bank Polski; 10) Bank Gospodarstwa Krajowego; 11) Urząd Dozoru Technicznego; 12) Polską Agencję Żeglugi Powietrznej; 13) Polskie Centrum Akredytacji; 14) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej;	Projekt ustawy zapewnia implementację Dyrektywy NIS i dodatkowo ma na celu ustanowienie krajowego systemu cyberbezpieczeństwa, obejmującego nie tylko CSIRT i wskazane w Dyrektywie NIS podmioty publiczne lub prywatne należące do jednego z rodzajów, o których mowa w Załączniku II do Dyrektywy NIS, ale również administrację publiczną, przedsiębiorców telekomunikacyjnych i inne podmioty wymienione w art. 4 projektu ustawy. Podmioty określone w art. 4 pkt 1-5 oraz 17-18 projektu są wprost wymienione w Dyrektywie NIS, jako współpracujące na poziomie krajowym, natomiast podmioty wymienione w art. 4 pkt 7-15 są podmiotami publicznymi, którym zgodnie z motywem 45 Dyrektywy powinno być zapewnione cyberbezpieczeństwo. Aby zapewnić wysoki poziom cyberbezpieczeństwa konieczne jest objęcie regulacją także innych niż wymienione w Dyrektywie podmiotów. Podmioty wymienione w pkt 6 i 16 wspierają operatorów

	15) spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu ustawy z dnia 20 grudnia 1996 r. ustawy o gospodarce komunalnej (Dz. U. z 2017 r. poz. 827); 16) podmioty świadczące usługi z zakresu cyberbezpieczeństwa; 17) organy właściwe do spraw cyberbezpieczeństwa; 18) Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa, zwany dalej „Pojedynczym Punktem Kontaktowym"; 19) Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, zwany dalej „Pełnomocnikiem"; 20) Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium".	usług kluczowych i dostawców usług cyfrowych. Podmioty wymienione w art. pkt 19 i 20 nie są wymienione w Dyrektywie NIS. Celem ich powołania jest koordynacja działań i wymiana informacji w warstwie strategiczno-politycznej pomiędzy instytucjami odpowiedzialnymi za cyberbezpieczeństwo w sferze cywilnej, wojskowej, sektorów usług kluczowych oraz instytucji odpowiedzialnych za zwalczanie cyberprzestępczości.
Art. 11 ust. 3	Art. 11. 3. W przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa operator usługi kluczowej, niezależnie od zadań określonych w ust. 1: 1) przekazuje jednocześnie w postaci elektronicznej zgłoszenie, o którym mowa w ust. 1 pkt 4, do sektorowego zespołu cyberbezpieczeństwa; 2) współdziała na poziomie sektora lub podsektora z tym zespołem podczas obsługi incydentu poważnego lub incydentu krytycznego, przekazując niezbędne dane, w tym dane osobowe; 3) zapewnia sektorowemu zespołowi cyberbezpieczeństwa dostęp do informacji o rejestrowanych incydentach, w zakresie niezbędnym do realizacji jego zadań.	Określono obowiązek przekazywania (równoległego) zgłoszeń do sektorowych zespołów cyberbezpieczeństwa (utworzone na mocy art. 44 poniżej). Pozwoli to na sprawną wymianę informacji pomiędzy uczestnikami procesu obsługi incydentu, bez tworzenia poziomu pośredniego.
Art. 13	Art. 13. 1. Operator usługi kluczowej może przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacje: 1) o innych incydentach; 2) o zagrożeniach cyberbezpieczeństwa; 3) dotyczące szacowania ryzyka; 4) o podatnościach; 5) o wykorzystywanych technologiach. 2. Informacje, o których mowa w ust. 1, są przekazywane w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji. 3. W przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa, operator usługi kluczowej może przekazywać jednocześnie w postaci elektronicznej informacje, o których mowa w ust. 1, do sektorowego zespołu cyberbezpieczeństwa. 4. Operator usługi kluczowej oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.	Zgodnie z Dyrektywą NIS, obowiązek zgłaszania dotyczy tylko incydentów poważnych. Operatorzy usług kluczowych mogą zgodnie z art. 13 zgłaszać także inne incydenty, pozostaje to jednak w ich gestii. Pozwoli to na zasilanie systemu innymi danymi, istotnymi dla osiągnięcia wysokiego poziomu cyberbezpieczeństwa, na zasadzie dobrowolności i współpracy pomiędzy poszczególnymi podmiotami.
Art. 15 ust. 7 pkt 2 i 3	7. Operator usługi kluczowej przekazuje kopię sprawozdania z przeprowadzonego audytu na uzasadniony wniosek: (…) 2) dyrektora Rządowego Centrum Bezpieczeństwa w przypadku gdy operator usługi kluczowej jest jednocześnie właścicielem, posiadaczem samoistnym albo zależnym obiektów, instalacji lub urządzeń wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym; 3) Szefa Agencji Bezpieczeństwa Wewnętrznego.	Ze względu na objęcie przepisami projektu ustawy podmiotów, których część objęta jest także przepisami dotyczącymi zarządzania kryzysowego konieczne było zapewnienie, aby dyrektor Rządowego Centrum Bezpieczeństwa otrzymywał kopię sprawozdania z przeprowadzonego audytu w przypadku, gdy operator usługi kluczowej jest jednocześnie

		operatorem infrastruktury krytycznej. Pozwoli to dyrektorowi RCB na sprawniejsze wykonywanie jego zadań dotyczących ochrony infrastruktury krytycznej w zakresie cyberbezpieczeństwa oraz ujednolici rekomendacje i polecenia dla operatorów usług kluczowych, będących jednocześnie operatorami infrastruktury krytycznej.
Art. 20	Art. 20. Dostawca usługi cyfrowej może przekazywać, zgodnie z właściwością do właściwego CSIRT MON, CSIRT NASK lub CESIRT GOV informacje, o których mowa w art. 13 ust. 1. Informacje te przekazywane są w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.	Zgodnie z Dyrektywą NIS, obowiązek zgłaszania incydentów przez dostawców usług cyfrowych dotyczy tylko incydentów istotnych. Dostawcy usług cyfrowych mogą zgodnie z art. 21 zgłaszać także inne incydenty, pozostaje to jednak w ich gestii. Pozwoli to na zasilanie systemu innymi danymi, istotnymi dla osiągnięcia wysokiego poziomu cyberbezpieczeństwa, na zasadzie dobrowolności i współpracy pomiędzy poszczególnymi podmiotami.
Art. 21-25	Art. 21. 1. Podmiot publiczny, o którym mowa w art. 4 pkt 7-15, realizujący zadanie publiczne zależne od systemów informacyjnych jest obowiązany do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. 2. Organ administracji publicznej, może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki jemu podległe lub przez niego nadzorowane. 3. Jednostka samorządu terytorialnego może wyznaczyć jedną osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jej jednostki organizacyjne. Art. 22. 1. Podmiot publiczny, o którym mowa w art. 4 pkt 7-15, realizujący zadanie publiczne zależne od systemów informacyjnych: 1) zapewnia zarządzanie incydentem w podmiocie publicznym; 2) zgłasza incydent w podmiocie publicznym niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV; 3) zapewnia obsługę incydentu w podmiocie publicznym oraz incydentu krytycznego we współpracy z właściwym CSIRT MON, CSIRT NASK lub CSIRT GOV, przekazując niezbędne dane, w tym dane osobowe; 4) zapewnia osobom, na rzecz których zadanie publiczne jest realizowane, dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i stosowanie skutecznych sposobów	Ze względu na potrzebę zapewnienia cyberbezpieczeństwa na poziomie krajowym konieczne było wprowadzenie przepisów stawiających wymogi podmiotom publicznym w zakresie cyberbezpieczeństwa. Uznano, że dotychczasowe wymagania, wynikające z ustawy o informatyzacji[1] nie są wystarczające (m.in. szczątkowo regulują obowiązek zgłaszania incydentów, bez regulacji w jakim czasie i jakiej formie) i należy je rozszerzyć zwłaszcza o obowiązki w zakresie obsługi i zgłaszania incydentów.

[1] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570).

	zabezpieczania się przed tymi zagrożeniami, w szczególności przez publikowanie informacji w tym zakresie na swojej stronie internetowej; 5) przekazuje do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV dane osoby, o której mowa w art. 21, zawierające imię i nazwisko, numer telefonu, adres poczty elektronicznej, w terminie 14 dni od dnia jej wyznaczenia, a także informacje o zmianie tych danych w terminie 14 dni od dnia nastąpienia zmiany. 2. Zgłoszenie, o którym mowa w ust. 1 pkt 2, przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji. Art. 23. 1. Zgłoszenie incydentu w podmiocie publicznym, o którym mowa w art. 22 ust. 1 pkt 2, zawiera: 1) dane podmiotu zgłaszającego, w tym nazwę podmiotu, numer we właściwym rejestrze, siedzibę i adres; 2) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby składającej zgłoszenie; 3) imię i nazwisko, numer telefonu, adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji; 4) opis wpływu incydentu w podmiocie publicznym na realizowane zadanie publiczne, w tym: a) wskazanie zadania publicznego, na które incydent miał wpływ, b) liczbę osób, na które incydent miał wpływ, c) moment wystąpienia i wykrycia incydentu oraz czas jego trwania, d) zasięg geograficzny, którego dotyczy incydent, e) przyczynę zaistnienia incydentu oraz sposób jego przebiegu i skutki jego oddziaływania na systemy informacyjne podmiotu publicznego; 5) informacje o przyczynie i źródle incydentu; 6) informacje o podjętych działaniach zapobiegawczych; 7) informacje o podjętych działaniach naprawczych; 8) inne istotne informacje. 2. Podmiot publiczny, o którym mowa w art. 4 pkt 7-15, przekazuje informacje znane mu w chwili zgłoszenia, które uzupełnia w trakcie obsługi incydentu. 3. Podmiot publiczny, o którym mowa w art. 4 pkt 7-15, przekazuje w niezbędnym zakresie w zgłoszeniu, o którym mowa w ust. 1, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji zadań, zgodnie z właściwością przez CSIRT MON, CSIRT NASK lub CSIRT GOV. 4. Zgodnie z właściwością CSIRT MON, CSIRT NASK lub CSIRT GOV może zwrócić się do podmiotu publicznego, o którym mowa w art. 4 pkt 7-15, o uzupełnienie zgłoszenia o informacje, w tym stanowiące tajemnice prawnie chronione, w zakresie niezbędnym do realizacji zadań, o których mowa w ustawie. 5. W zgłoszeniu podmiot publiczny, o którym mowa w art. 4 pkt 7-15, oznacza informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa.	

	Art. 24. Podmiot publiczny, o którym mowa w art. 4 pkt 7-15, realizujący zadania publiczne zależne od systemów informacyjnych może przekazywać do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacje, o których mowa w art. 13 ust. 1. Informacje te przekazywane są w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji. Art. 25. Do podmiotu publicznego, o którym mowa w art. 4 pkt 7-15, wobec którego wydana została decyzja o uznaniu za operatora usługi kluczowej, stosuje się przepisy rozdziału 3 w zakresie świadczenia usługi kluczowej, w związku z świadczeniem której został uznany za operatora usługi kluczowej.	
Art. 26 ust. 2	2. CSIRT MON, CSIRT NASK i CSIRT GOV w uzasadnionych przypadkach na wniosek operatorów usług kluczowych, dostawców usług cyfrowych, podmiotów publicznych, o których mowa w art. 4 pkt 7-15, sektorowych zespołów cyberbezpieczeństwa lub właścicieli, posiadaczy samoistnych albo zależnych obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej ujętych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, mogą zapewnić wsparcie w obsłudze incydentów.	Dodatkowa regulacja pozwalająca na obsługę incydentu przez CSIRT – w określonych okolicznościach i wskazanych podmiotów. Jest to wyjątek od ogólnej zasady, że CSIRT wspierają i koordynują obsługę, ale nie prowadzą jej bezpośrednio.
Art. 26 ust. 3 pkt 13	Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV należy: 13) wspólne opracowywanie i przekazywanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego, o którym mowa w art. 5a ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, dotyczącego cyberbezpieczeństwa;	Uznano, że w celu stworzenia spójnego i jednolitego systemu konieczne jest wytworzenie syntetycznej informacji o stanie bezpieczeństwa państwa, zasilającej „Raport o zagrożeniach bezpieczeństwa narodowego”, o którym mowa w art. 5a ustawy o zarządzaniu kryzysowym. Raport będzie zawierał m.in. wskazanie najważniejszych zagrożeń przez stworzenie mapy ryzyka, określenie celów strategicznych oraz określenie priorytetów w reagowaniu na określone zagrożenia, wskazanie sił i środków niezbędnych do osiągnięcia celów strategicznych.
Art. 27	Art. 27. 1. CSIRT GOV jest właściwy w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 2 pkt 7 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 r. poz. 452). 2. CSIRT MON jest właściwy w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 5 ust. 1 pkt 2a ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2017 r. poz. 1978 i 2405). 3. W przypadku stwierdzenia, że incydent, którego obsługa jest koordynowana przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV jest związany ze zdarzeniami, o których mowa w ust. 1 i 2, koordynację obsługi incydentu przejmuje właściwy CSIRT MON lub CSIRT GOV.	Konieczne było ustanowienie przepisów dotyczących zdarzeń terrorystycznych. Jest to uzupełnienie przepisów o właściwości CSIRT oraz powiązanie przepisów niniejszego projektu z ustawą o działaniach antyterrorystycznych.
Art. 32	Art. 32. 1. CSIRT MON, CSIRT NASK i CSIRT GOV mogą wykonywać niezbędne działania techniczne, związane z analizą zagrożeń, koordynacją obsługi incydentu poważnego, incydentu istotnego i incydentu krytycznego. 2. W trakcie koordynacji obsługi incydentu poważnego, incydentu istotnego lub krytycznego CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić do organu właściwego z wnioskiem o wezwanie	Poza zadaniami określonymi w projekcie ustawy wynikającymi z implementacji Dyrektywy NIS, projektodawca uznał za konieczne umożliwienie CSIRT także realizację innych czynności, które pozwolą na skuteczną realizację zadań z zakresu

	operatora usługi kluczowej lub dostawcy usługi cyfrowej, aby w wyznaczonym terminie usunął podatności, które doprowadziły lub mogłyby doprowadzić do incydentu poważnego, istotnego lub krytycznego. 3. CSIRT MON, CSIRT NASK lub CSIRT GOV może wystąpić bezpośrednio do operatora usługi kluczowej o udostępnienie informacji technicznych związanych z incydentem poważnym lub krytycznym, które będą niezbędne do przeprowadzenia analizy lub koordynacji obsługi takiego incydentu. 4. CSIRT MON, CSIRT NASK, CSIRT GOV lub sektorowe zespoły cyberbezpieczeństwa na podstawie informacji, o których mowa w art. 13 ust. 1 pkt 3 i 5, uzyskanych od operatora usługi kluczowej, dostawcy usługi cyfrowej lub podmiotu publicznego, o którym mowa w art. 4 pkt 7-15, może przekazywać im informacje o podatnościach i sposobie usunięcia podatności w wykorzystywanych technologiach.	zapewnienia cyberbezpieczeństwa oraz zapobiegania wystąpieniu negatywnych skutków incydentu.
Art. 33, art. 62 ust. 1 pkt 6 oraz art. 65 ust. 1 pkt 6	Art. 33. 1. CSIRT MON, CSIRT NASK lub CSIRT GOV może przeprowadzić badanie lub ocenę bezpieczeństwa stosowania sprzętu lub oprogramowania, na podstawie którego składa wniosek do Pełnomocnika w sprawie wydania, zmiany lub odwołania rekomendacji dotyczących sprzętu lub oprogramowania. 2. Pełnomocnik, po uzyskaniu opinii Kolegium, decyduje o wydaniu, zmianie lub odwołaniu rekomendacji dotyczących sprzętu lub oprogramowania. 3. Podmiot krajowego systemu cyberbezpieczeństwa może wnieść do Pełnomocnika zastrzeżenia do zakresu stosowania rekomendacji dotyczących sprzętu lub oprogramowania z uwagi na ich negatywny wpływ na świadczone usługi lub realizowane zadania publiczne, niezwłocznie, jednak nie później niż w terminie 7 dni od dnia ich otrzymania. 4. Pełnomocnik odnosi się do zastrzeżeń otrzymanych w trybie ust. 3 niezwłocznie, jednak nie później niż w terminie 14 dni od dnia ich otrzymania, 5. Podmioty krajowego systemu cyberbezpieczeństwa informują Pełnomocnika, na jego wniosek, o sposobie i zakresie stosowania rekomendacji dotyczących sprzętu lub oprogramowania lub ich niestosowaniu. 6. Pełnomocnik może przekazać do organu sprawującego nadzór nad podmiotem krajowego systemu cyberbezpieczeństwa informację o sposobie i zakresie stosowania rekomendacji dotyczących sprzętu lub oprogramowania albo ich niestosowaniu przez ten podmiot. Art. 62. 1. W ramach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa do zadań Pełnomocnika należy: 6) wydawanie rekomendacji dotyczących sprzętu lub oprogramowania na wniosek CSIRT MON, CSIRT NASK lub CSIRT GOV. Art. 65. 1. Do zadań Kolegium należy wyrażanie opinii w sprawach: 6) wniosków CSIRT MON, CSIRT NASK lub CSIRT GOV w sprawie rekomendacji dotyczących sprzętu lub oprogramowania.	Nowe uprawnienie pozwoli CSIRT wykonywać badania i ocenę sprzętu lub oprogramowania, na podstawie których Pełnomocnik (po zasięgnięciu opinii Kolegium) będzie mógł wydać rekomendację dotyczącą stosowania danego sprzętu lub oprogramowania przez podmioty krajowego systemu cyberbezpieczeństwa.
Art. 35	Art. 35. 1. CSIRT MON, CSIRT NASK i CSIRT GOV informują się wzajemnie oraz informują Rządowe Centrum Bezpieczeństwa o incydencie krytycznym. 2. Informacja, o której mowa w ust. 1, zawiera:	Ze względu na fakt, że niektóre incydenty mogą wywołać sytuacje kryzysową konieczne było uregulowanie zasad współpracy pomiędzy CSIRT

	1) wstępną analizę potencjalnych skutków incydentu z uwzględnieniem w szczególności: a) liczby użytkowników, których dotyczy incydent, w szczególności jeśli zakłóca świadczenie usługi kluczowej, b) momentu wystąpienia i wykrycia incydentu oraz czas jego trwania, c) zasięgu geograficznego, którego dotyczy incydent; 2) rekomendację w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego, o którym mowa w art. 8 ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. 3. Informacja, o której mowa w ust. 1, może zawierać wniosek o zwołanie Zespołu do spraw Incydentów Krytycznych, o którym mowa w art. 36 ust. 1. 4. W przypadku uzyskania informacji o zagrożeniach cyberbezpieczeństwa CSIRT MON, CSIRT NASK i CSIRT GOV mogą informować się wzajemnie oraz informować Rządowe Centrum Bezpieczeństwa. Przepisy ust. 2 i 3 stosuje się odpowiednio. 5. CSIRT MON, CSIRT NASK i CSIRT GOV mogą publikować na stronie podmiotowej Biuletynu Informacji Publicznej odpowiednio Ministra Obrony Narodowej, Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego lub Agencji Bezpieczeństwa Wewnętrznego informacje, w niezbędnym zakresie, o podatnościach i incydentach, o których mowa w ust. 1, oraz o zagrożeniach cyberbezpieczeństwa, o ile przekazywanie informacji przyczyni się do zwiększenia cyberbezpieczeństwa systemów informacyjnych użytkowanych przez obywateli i przedsiębiorców lub zapewnienia bezpiecznego korzystania z tych systemów. Publikowane informacje nie mogą naruszać przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych, a także przepisów o ochronie danych osobowych.	a Rządowym Centrum Bezpieczeństwa na wypadek wystąpienia sytuacji kryzysowej.
Art. 36	Art. 36. 1. Tworzy się Zespół do spraw Incydentów Krytycznych, zwany dalej „Zespołem”, jako organ pomocniczy w sprawach obsługi incydentów krytycznych zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV i koordynujący działania podejmowane przez CSIRT MON, CSIRT NASK, CSIRT GOV oraz Rządowe Centrum Bezpieczeństwa. 2. W skład Zespołu wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizujący zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa. 3. Dyrektor Rządowego Centrum Bezpieczeństwa przewodniczy pracom Zespołu. 4. Obsługę prac Zespołu zapewnia Rządowe Centrum Bezpieczeństwa. 5. Do udziału w pracach Zespołu, z głosem doradczym, członkowie Zespołu mogą zapraszać przedstawicieli organów właściwych lub jednostek im podległych lub przez nie nadzorowanych, organów ścigania, wymiaru sprawiedliwości lub służb specjalnych. 6. W przypadku, o którym mowa w art. 35 ust. 3, albo na wniosek członka Zespołu lub z własnej inicjatywy po uzyskaniu informacji, o której mowa w art. 35 ust. 2, dyrektor Rządowego Centrum Bezpieczeństwa zawiadamia niezwłocznie członków Zespołu o terminie i miejscu posiedzenia Zespołu. Udział w posiedzeniu Zespołu może odbywać się za pośrednictwem środków komunikacji elektronicznej. 7. Zespół na posiedzeniu: 1) wyznacza jednomyślnie CSIRT koordynujący obsługę incydentu, którego dotyczy informacja, o której mowa w art. 35 ust. 2; 2) określa role pozostałych CSIRT oraz Rządowego Centrum Bezpieczeństwa w obsłudze incydentu,	Istnieje potrzeba ustanowienia zespołu, który stanowił będzie pośredni poziom pomiędzy CSIRT a Rządowym Zespołem Zarządzania Kryzysowego. Zespół do spraw Incydentów Krytycznych będzie stanowił organ pomocniczy dla obsługi incydentów, które mogą stać się incydentami krytycznymi.

	którego dotyczy informacja, o której mowa w art. 35 ust. 2; 3) określa sposób wymiany informacji technicznych dotyczących incydentu krytycznego obsługiwanego wspólnie przez CSIRT MON, CSIRT NASK lub Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV; 4) podejmuje decyzję o wystąpieniu przez dyrektora Rządowego Centrum Bezpieczeństwa z wnioskiem do Prezesa Rady Ministrów w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego; 5) w przypadku incydentu krytycznego, który może spowodować zagrożenie wystąpienia zdarzenia o charakterze terrorystycznym, dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej, o którym mowa w art. 15 ust. 2 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, przygotowuje w zakresie takiego incydentu informacje i wnioski dla ministra właściwego do spraw wewnętrznych i Szefa Agencji Bezpieczeństwa Wewnętrznego.	
Art. 37 ust. 1 i art. 38	Art. 37. 1. Do udostępnienia informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2016 r. poz. 1764 oraz z 2017 r. poz. 933 i 1033). Art. 38. Nie udostępnia się informacji przetwarzanych na podstawie ustawy, jeżeli ich ujawnienie naruszyłoby ochronę interesu publicznego w odniesieniu do bezpieczeństwa lub porządku publicznego, a także negatywnie wpłynęłoby na prowadzenie postępowań przygotowawczych w sprawie przestępstw, ich wykrywanie i ściganie.	Istnieje potrzeba uregulowania kwestii dotyczących informacji o podatnościach na incydenty, incydentach i zagrożeniach cyberbezpieczeństwa oraz o poziomie ryzyka wystąpienia incydentów w taki sposób, aby informacje te nie były udostępniane na podstawie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2016 r. poz. 1764 oraz z 2017 r. poz. 1033). Uregulowano również, że udostępnianie informacji nie może odbywać się w sposób, który naruszyłby ochronę interesu publicznego.
Art. 40.	Art. 40. 1. CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa i minister właściwy do spraw informatyzacji przetwarzają informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne dla realizacji zadań, o których mowa w ustawie. 2. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa przekazują dane, o których mowa w ust. 1, organom ścigania w związku z incydentem wyczerpującym znamiona przestępstwa. 3. CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa zobowiązane są do zachowania w tajemnicy informacji, w tym informacji stanowiących tajemnice prawnie chronione, uzyskanych w związku z realizacją zadań, o których mowa w ustawie.	Ze względu na konieczność przetwarzania w niezbędnym zakresie tajemnic prawnie chronionych przez CSIRT podczas obsługi incydentu, pojawiła się konieczność regulacji przetwarzania nie tylko danych osobowych, ale i tajemnic prawnie chronionych. Wiąże się to z obowiązkiem przekazywania tych danych organom ścigania oraz zachowania tajemnicy informacji, które również nałożono na CSIRT.
Art. 44.	Art. 44. 1. Organ właściwy może ustanowić, zgodnie z odrębnymi przepisami, sektorowy zespół cyberbezpieczeństwa dla danego sektora lub podsektora wymienionego w załączniku nr 1 do ustawy, odpowiedzialny w szczególności za: 1) przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów; 2) wspieranie operatorów usług kluczowych w wykonywaniu obowiązków określonych w art. 8, art. 9, art. 10 ust. 1-3, art. 11 ust. 1-3, art. 12 i art. 13;	Określono, w formie katalogu otwartego, zadania dla sektorowych zespołów cyberbezpieczeństwa, które mają mieć funkcję wspierającą dla operatorów usług kluczowych.

	3) analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowanie wniosków z obsługi incydentu; 4) współpracę z właściwym CSIRT MON, CSIRT NASK i CSIRT GOV w zakresie koordynowania obsługi incydentów poważnych. 2. Sektorowy zespół cyberbezpieczeństwa może przekazywać do innych państw, w tym państw członkowskich Unii Europejskiej i przyjmować z tych państw informacje o incydentach poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej. 3. Sektorowy zespół cyberbezpieczeństwa może otrzymywać zgłoszenia incydentu poważnego z innego państwa członkowskiego Unii Europejskiej dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej. Sektorowy zespół cyberbezpieczeństwa przekazuje te zgłoszenie do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV oraz Pojedynczego Punktu Kontaktowego. 4. W przypadku ustanowienia sektorowego zespołu cyberbezpieczeństwa, organ właściwy informuje operatorów usług kluczowych w danym sektorze oraz CSIRT MON, CSIRT NASK i CSIRT GOV o ustanowieniu tego zespołu i zakresie realizowanych zadań.	
Art. 45 pkt 2, 4 i 5	Art. 45. 1. Minister właściwy do spraw informatyzacji jest odpowiedzialny za: 2) rekomendowanie obszarów współpracy z sektorem prywatnym w celu zwiększenia cyberbezpieczeństwa Rzeczypospolitej Polskiej; 4) prowadzenie działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników; 5) gromadzenie informacji o incydentach poważnych, które dotyczą lub zostały przekazane przez inne państwo członkowskie Unii Europejskiej;	W projektowanym przepisie zawarto zadania ministra właściwego do spraw informatyzacji. Zadanie określone w pkt 2 wynika z potrzeby łączenia wysiłków sektora prywatnego i publicznego, zwłaszcza poprzez partnerstwo publiczno-prywatne; pkt 4 jest realizacją zadań informacyjnych, niezwiązanych bezpośrednio z incydentami, ale istotnych dla podwyższanie poziomu cyberbezpieczeństwa, gdyż pozwoli na podnoszenie świadomości użytkowników Internetu, poprzez edukację i szkolenia. Realizacja obowiązku określonego w pkt 5 wyposaży ministra i inne podmioty systemu w pogłębioną wiedzę dotyczący zagrożeń na obszarze UE, które potencjalnie mogą bezpośrednio lub pośrednio dotknąć też RP.
Art. 51-52	Art. 51. Minister Obrony Narodowej jest odpowiedzialny za: 1) współpracę Sił Zbrojnych Rzeczypospolitej Polskiej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej i organizacji międzynarodowych w obszarze obrony narodowej w zakresie cyberbezpieczeństwa; 2) zapewnienie zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa, powodującego konieczność działań obronnych; 3) rozwijanie umiejętności Sił Zbrojnych Rzeczypospolitej Polskiej w zakresie zapewnienia cyberbezpieczeństwa poprzez organizację specjalistycznych przedsięwzięć szkoleniowych; 4) pozyskiwanie i rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych RP; 5) kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego, o którym	Przepisy te wykraczają poza zakres Dyrektywy NIS, która dotyczy funkcjonowania rynku wewnętrznego UE, bowiem konieczne było również uregulowanie kwestii obronnych będących w zakresie kompetencji Ministra Obrony Narodowej. Przepisy te określają zadania Ministra Obrony Narodowej: współpraca z właściwymi podmiotami NATO, UE i innych organizacji międzynarodowych, zapewnienie Siłom Zbrojnym RP cyberbezpieczeństwa i zdolności do działań obronnych w cyberprzestrzeni, przeprowadzanie

	mowa w ustawie z dnia 22 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2017 r. poz. 1932); 6) ocenę wpływu incydentów na system obrony państwa; 7) ocenę zagrożeń cyberbezpieczeństwa w czasie stanu wojennego oraz przedstawianie właściwym organom propozycji dotyczących działań obronnych; 8) koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego, dotyczących działań obronnych w przypadku zagrożenia cyberbezpieczeństwa. Art. 52. Minister Obrony Narodowej prowadzi Narodowy Punkt Kontaktowy do współpracy z Organizacją Traktatu Północnoatlantyckiego, do którego zadań należy: 1) zapewnienie współpracy w obszarze obrony narodowej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego w zakresie cyberbezpieczeństwa; 2) koordynacja działań w zakresie wzmacniania zdolności obronnych w przypadku zagrożenia cyberbezpieczeństwa; 3) zapewnienie współpracy pomiędzy narodowymi i sojuszniczymi siłami zbrojnymi w zakresie zapewnienia cyberbezpieczeństwa; 4) rozwijanie systemów wymiany informacji o zagrożeniach cyberbezpieczeństwa w obszarze obrony narodowej; 5) udział w realizacji celów Organizacji Traktatu Północnoatlantyckiego w obszarze cyberbezpieczeństwa i kryptologii.	szkoleń specjalistycznych, kierowanie działaniami związanymi z obsługą incydentów i ocena zagrożeń cyberbezpieczeństwa w czasie stanu wojennego, ocena wpływu incydentów na system obrony państwa oraz prowadzenie Narodowego Punktu Kontaktowego do współpracy z NATO, a także uregulowanie odpowiedzialności za sferę militarną krajowego systemu cyberbezpieczeństwa oraz uwzględnienie funkcjonowania tego systemu w czasie obowiązywania stanu wojennego.
Art. 60-67	Art. 60. Koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej powierza się Pełnomocnikowi. Art. 61. 1. Pełnomocnika powołuje i odwołuje Prezes Rady Ministrów. 2. Pełnomocnik podlega Radzie Ministrów. 3. Pełnomocnikiem jest sekretarz stanu albo podsekretarz stanu. 4. Obsługę merytoryczną, organizacyjno-prawną, techniczną i kancelaryjno-biurową Pełnomocnika zapewnia ministerstwo lub inny urząd administracji rządowej, w którym powołano Pełnomocnika. Art. 62. 1. W ramach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa do zadań Pełnomocnika należy: 1) analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji publicznej, organów właściwych, CSIRT MON, CSIRT NASK i CSIRT GOV; 2) nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych, CSIRT MON, CSIRT NASK i CSIRT GOV; 3) opiniowanie dokumentów rządowych, w tym projektów aktów prawnych, mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa;	W celu należytej koordynacji krajowego systemu cyberbezpieczeństwa oraz zapewnienia jego spójności i efektywności powołuje się Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Kolegium do Spraw Cyberbezpieczeństwa. Funkcjonowania tych podmiotów nie przewiduje Dyrektywa NIS.

	4) upowszechnianie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym; 5) inicjowanie krajowych ćwiczeń z zakresu cyberbezpieczeństwa; 6) wydawanie rekomendacji dotyczących sprzętu lub oprogramowania na wniosek CSIRT MON, CSIRT NASK lub CSIRT GOV. 2. Do zadań Pełnomocnika wykonywanymi w porozumieniu z właściwymi ministrami należy również: 1) współpraca w sprawach związanych z cyberbezpieczeństwem z innymi państwami, organizacjami oraz instytucjami międzynarodowymi; 2) podejmowanie działań mających na celu wspieranie badań naukowych i rozwój technologii z zakresu cyberbezpieczeństwa; 3) podejmowanie działań mających na celu podnoszenie świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z Internetu. Art. 63. 1. Pełnomocnik opracowuje i przedkłada Radzie Ministrów, w terminie do dnia 31 marca każdego roku, sprawozdanie za poprzedni rok kalendarzowy, zawierające informację o prowadzonej działalności w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym. 2. Pełnomocnik może przekazywać Radzie Ministrów wnioski oraz rekomendacje dotyczące działań, które powinny podejmować podmioty krajowego systemu cyberbezpieczeństwa w celu zapewnienia cyberbezpieczeństwa na poziomie krajowym i przeciwdziałania zagrożeniom w tym zakresie. Art. 64. Przy Radzie Ministrów działa Kolegium, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych. Art. 65. 1. Do zadań Kolegium należy wyrażanie opinii w sprawach: 1) kierunków i planów na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa; 2) wykonywania przez CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego realizującego zadania w ramach CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa oraz organy właściwe powierzonych im zadań zgodnie z kierunkami i planami na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa; 3) współdziałania organów prowadzących lub nadzorujących CSIRT MON, CSIRT GOV i CSIRT NASK; 4) współdziałania podmiotów CSIRT MON, CSIRT NASK, Szefa Agencji Bezpieczeństwa Wewnętrznego oraz ministra-członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych, sektorowych zespołów cyberbezpieczeństwa i organów właściwych; 5) organizacji wymiany informacji istotnych dla cyberbezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej między organami administracji rządowej; 6) wniosków CSIRT MON, CSIRT NASK lub CSIRT GOV w sprawie rekomendacji dotyczących sprzętu lub oprogramowania. 2. Do zadań Kolegium należy opracowywanie rekomendacji dla Rady Ministrów, dotyczących działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym, o których mowa w	

	art. 67. Art. 66. 1. W skład Kolegium wchodzą: 1) przewodniczący Kolegium – Prezes Rady Ministrów; 2) Pełnomocnik; 3) sekretarz Kolegium; 4) członkowie Kolegium: a) minister właściwy do spraw wewnętrznych, b) minister właściwy do spraw informatyzacji, c) Minister Obrony Narodowej, d) minister właściwy do spraw zagranicznych, e) Szef Kancelarii Prezesa Rady Ministrów, f) Szef Biura Bezpieczeństwa Narodowego, jeżeli został wyznaczony przez Prezydenta Rzeczypospolitej Polskiej, g) minister-członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych lub osoba przez niego upoważniona w randze sekretarza stanu albo podsekretarza stanu, a jeżeli minister-członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego. 2. Prezes Rady Ministrów może upoważnić Pełnomocnika do pełnienia funkcji przewodniczącego Kolegium. 3. Członkowie Kolegium, o których mowa w ust. 1 pkt 4 lit. a-e, mogą być zastępowani przez upoważnionych przedstawicieli w randze sekretarza stanu albo podsekretarza stanu. 4. W posiedzeniach Kolegium uczestniczą również: 1) Dyrektor Rządowego Centrum Bezpieczeństwa; 2) Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca; 3) Szef Służby Kontrwywiadu Wojskowego albo jego zastępca; 4) Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego. 5. Przewodniczący Kolegium: 1) zwołuje posiedzenia Kolegium; 2) może zapraszać do udziału w posiedzeniach Kolegium przewodniczących właściwych komisji sejmowych, przedstawicieli organów państwowych, przedstawicieli organów właściwych oraz inne osoby, których uczestnictwo jest niezbędne ze względu na tematykę obrad. 6. Sekretarza Kolegium powołuje Prezes Rady Ministrów spośród osób spełniających wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli "tajne". Sekretarza Kolegium odwołuje Prezes Rady Ministrów. 7. Sekretarz Kolegium organizuje pracę Kolegium i w tym zakresie może występować do CSIRT MON, CSIRT GOV i CSIRT NASK, sektorowych zespołów cyberbezpieczeństwa, organów właściwych oraz organów administracji rządowej o przedstawienie informacji niezbędnych w sprawach rozpatrywanych przez Kolegium. 8. Obsługę Kolegium zapewnia ministerstwo lub inny urząd administracji rządowej, które obsługuje Pełnomocnika. 9. Rada Ministrów określi, w drodze rozporządzenia, zakres działania oraz tryb pracy Kolegium,	

	mając na uwadze charakter zadań Kolegium oraz konieczność zapewnienia jego sprawnej pracy. Art. 67. 1. Prezes Rady Ministrów w celu koordynacji działań administracji rządowej w zakresie cyberbezpieczeństwa może, na podstawie rekomendacji Kolegium, wydawać wiążące wytyczne dotyczące zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz funkcjonowania krajowego systemu cyberbezpieczeństwa, a także żądać informacji i opinii w tym zakresie od: 1) ministra właściwego do spraw wewnętrznych – w odniesieniu do działalności Policji i Straży Granicznej; 2) Ministra Obrony Narodowej – w odniesieniu do działalności CSIRT MON; 3) Szefa Agencji Bezpieczeństwa Wewnętrznego – w odniesieniu do działalności CSIRT GOV; 4) Dyrektora Rządowego Centrum Bezpieczeństwa – w odniesieniu do zadań realizowanych zgodnie z ustawą; 5) Dyrektora Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego – w odniesieniu do działalności CSIRT NASK; 6) ministra właściwego do spraw informatyzacji – w odniesieniu do zadań realizowanych zgodnie z ustawą. 2. Prezes Rady Ministrów wydaje wiążące wytyczne dla CSIRT MON, CSIRT GOV i CSIRT NASK w zakresie obsługi incydentów krytycznych, w tym wskazuje CSIRT odpowiedzialny za obsługę incydentu krytycznego.	
Art. 76	Art. 76. W ustawie z dnia 7 września 1991 r. o systemie oświaty (Dz. U. z 2017 r. poz. 2198, 2203 i 2361) w art. 90u: 1) w ust. 1 pkt 6 otrzymuje brzmienie: „6) rozwijanie kompetencji, zainteresowań i uzdolnień dzieci i młodzieży oraz innych grup społecznych, w tym wspomaganie organów prowadzących szkoły lub placówki w realizacji przedsięwzięć w tym obszarze, w szczególności w zakresie bezpiecznego korzystania z technologii informacyjno-komunikacyjnych;”; 2) w ust. 4 pkt 6 otrzymuje brzmienie: „6) szczegółowe warunki, formy i tryb realizacji przedsięwzięć w zakresie rozwijania kompetencji, zainteresowań i uzdolnień dzieci i młodzieży oraz innych grup społecznych, a także warunki i tryb wspomagania organów prowadzących szkoły lub placówki w realizacji przedsięwzięć w tym obszarze, w szczególności w zakresie bezpiecznego korzystania z technologii informacyjno-komunikacyjnych, uwzględniając konieczność rozwijania umiejętności ułatwiających przystosowanie się do zmian zachodzących w życiu społecznym i gospodarczym, możliwość udzielenia wsparcia finansowego organów prowadzących szkoły lub placówki oraz wymóg skuteczności i efektywności wydatkowania środków budżetowych;”.	W celu realizacji zadania, o którym mowa w art. 45 pkt 4 projektu wobec uczniów szkół, planowane jest nawiązanie współpracy z ministrem właściwym do spraw oświaty. Projektodawca nie widzi potrzeby zmian w obecnej podstawie programowej – wystarczające cele można osiągnąć poprzez rozwinięcie istniejących programów rządowych, o których mowa w art. 90u ustawy o systemie oświaty.
	Art. 77. W ustawie z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2017 r. poz. 888, z późn. zm.) wprowadza się następujące zmiany: 1) w art. 12a w ust. 1 pkt 10 otrzymuje brzmienie: ,,10) bezpieczeństwo cyberprzestrzeni w wymiarze cywilnym;"; 2) w art. 19 w ust. 1 po pkt 1 dodaje się pkt 1a w brzmieniu: „1a) bezpieczeństwo cyberprzestrzeni w wymiarze militarnym,".	Celem uniknięcia potencjalnych sporów kompetencyjnych na tle realizacji zadań ustawowych konieczne jest rozdzielenie kompetencji i uprawnień wśród członków Rady Ministrów.

Art. 78	Art. 78. W ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne wprowadza się następujące zmiany: 1) w art. 175a: a) po ust. 1 dodaje się ust. 1a i 1b w brzmieniu: „1a. Prezes UKE przekazuje informacje, o których mowa w ust. 1, jeżeli dotyczą one zdarzeń będących incydentami w rozumieniu ustawy z dnia …. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …), CSIRT właściwemu dla zgłaszającego przedsiębiorcy telekomunikacyjnego zgodnie z art. 26 ust. 5-7 tej ustawy, z wyłączeniem informacji stanowiących tajemnicę przedsiębiorstwa zastrzeżonych na podstawie art. 9. 1b. Informacje, o których mowa w ust. 1a, przekazywane są w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej – przy użyciu innych dostępnych środków komunikacji.”, b) po ust. 2 dodaje się ust. 2a w brzmieniu: „2a. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, kryteria uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług, biorąc pod uwagę w szczególności wartość procentową użytkowników, na których naruszenie bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych miało wpływ, czas trwania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych powodującego niedostępność lub ograniczenie dostępności sieci lub usług telekomunikacyjnych oraz rekomendacje i wytyczne Europejskiej Agencji do spraw Bezpieczeństwa Sieci i Informacji (ENISA).”; 2) w art. 176a: a) w ust. 1 pkt 3 otrzymuje brzmienie: „3) bezpośrednich zagrożeń dla bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej przedsiębiorcy lub świadczonych przez niego usług”, b) w ust. 2 pkt 4 otrzymuje brzmienie: „4) technicznych i organizacyjnych środków zapewnienia bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i świadczonych usług, w tym ochrony przed wystąpieniem incydentów w rozumieniu ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa;”; 3) w art. 209 w ust. 1 po pkt 27 dodaje się pkt 27^1 w brzmieniu: „27^1) nie wypełnia obowiązku, o którym mowa w art. 175a ust. 1,”.	Wprowadzona zmiana ma na celu zobowiązanie Prezesa UKE do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na ich funkcjonowanie, które to informacje uzyskuje od przedsiębiorców telekomunikacyjnych. Gromadzenie wiedzy o wszystkich incydentach pozwoli na stworzenie spójnego systemu cyberbezpieczeństwa na poziomie krajowym.
Art. 79	Art. 79. W ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym wprowadza się następujące zmiany: 1) w art. 5a ust. 2 otrzymuje brzmienie: „2. Koordynację przygotowania Raportu zapewnia dyrektor Rządowego Centrum Bezpieczeństwa, natomiast w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego, a w części dotyczącej zagrożeń cyberbezpieczeństwa, mogących doprowadzić do sytuacji kryzysowej, Pełnomocnik Rządu do spraw Cyberbezpieczeństwa.”; 2) w art. 6 po ust. 5a dodaje się ust. 5b w brzmieniu: „5b. Właściciele, posiadacze samoistni i zależni, o których mowa w ust. 5, będący jednocześnie operatorami usług kluczowych w rozumieniu ustawy z dnia … o krajowym systemie	Wprowadzane zmiany mają na celu ujęcie Pełnomocnika Rządu do spraw Cyberbezpieczeństwa w systemie zarządzania kryzysowego oraz wyeliminowanie sytuacji, w której operator usługi kluczowej będący jednocześnie operatorem infrastruktury krytycznej musiałby opracowywać plan ochrony infrastruktury krytycznej i jednocześnie dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych. Wprowadzone

	cyberbezpieczeństwa (Dz. U. poz. …), uwzględniają w planach ochrony infrastruktury krytycznej, dokumentację dotyczącą cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych, zgodnie z zakresem informacji określonym w przepisach wydanych na podstawie art. 11 ust. 3 ustawy z dnia … o krajowym systemie cyberbezpieczeństwa."; 3) w art. 8 w ust. 3 dodaje się pkt 15 w brzmieniu: „15) Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa."; 4) w art. 11 po ust. 1 dodaje się ust. 1a w brzmieniu: „1a. Centrum zapewnia obsługę Zespołu do spraw Incydentów Krytycznych, o którym mowa w art. 37 ust. 1 ustawy z dnia …..o krajowym systemie cyberbezpieczeństwa.".	przepisy przewidują, że wystarczającym będzie uwzględnienie w planie ochrony infrastruktury krytycznej dokumentacji dotyczącej cyberbezpieczeństwa. Ponadto, projektowane przepisy przewidują współdziałanie RCB z CSIRT.
Art. 86	Art. 86. Dotychczasowe przepisy wykonawcze wydane na podstawie art. 90u ust. 4 pkt 6 ustawy zmienianej w art. 76 zachowują moc do dnia wejścia w życie przepisów wykonawczych wydanych na podstawie art. 90u ust. 4 pkt 6 ustawy, o której mowa w art. 76 w brzmieniu nadanym niniejszą ustawą, nie dłużej jednak niż do dnia 1 grudnia 2019 r., i mogą być zmieniane na podstawie tych przepisów.	Przepis dostosowujący.
Art. 87	(pominięto)	Zgodnie z art. 50 ust. 4 ustawy o finansach publicznych, konieczne było umieszczenie w projekcie ustawy reguły wydatkowej.

Warszawa, 26 kwietnia 2018 r.

[redacted]

Minister
Spraw Zagranicznych

DPUE.920.1777.2017 / 22 / ar

dot.: RM-10-64-18 z dn. 20.04.2018 r.

Pani Jolanta Rusiniak
Sekretarz Rady Ministrów

Opinia
o zgodności z prawem Unii Europejskiej *projektu ustawy o krajowym systemie cyberbezpieczeństwa*, wyrażona przez ministra właściwego do spraw członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej

Szanowna Pani Minister,

w związku z przedłożonym projektem pozwalam sobie wyrazić poniższą opinię

Projektowany art. 39 ma na celu wdrożenie art. 2 ust 1 *dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, zgodnie z którym przetwarzanie danych osobowych na mocy tej dyrektywy odbywa się zgodnie z *rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych*. Wskazać należy, że dyrektywa 2016/1148 nie przewiduje w tym zakresie żadnych wyłączeń i ograniczeń od stosowania przepisów rozporządzenia 2016/679 jeśli chodzi o sposób i zasady przetwarzania danych osobowych przez krajowe CSIRT.

W projekcie przekazanym do rozpatrzenia przez Radę Ministrów wprowadzone zostały zmiany polegające na wyłączeniu CSIRT GOV z niektórych obowiązków wynikających z projektowanego art. 39 (ust. 2, 5, 6, 8, 9). Regulacje te budzą wątpliwości odnośnie do zgodności z art. 2 ust. 1 dyrektywy 2016/1148. Większość obowiązków określonych w projektowanym art. 39, z których realizacji wyłącza się CSIRT GOV, gwarantuje bowiem zgodność przetwarzania danych osobowych z przepisami rozporządzenia 2016/679. W konsekwencji w przypadku CSIRT GOV projekt nie zapewnia, że CSIRT ten będzie przetwarzał dane osobowe zgodnie z rozporządzeniem 2016/679.

W konsekwencji projektowany art. 39 nie zapewnia pełnej transpozycji art. 2 ust. 1 dyrektywy 2016/1148.

Projekt ustawy, z zastrzeżeniem uwagi zgłoszonej w niniejszej opinii, jest zgodny z prawem Unii Europejskiej.

Z poważaniem

Do wiadomości:
Pan Marek Zagórski
Minister Cyfryzacji

Kancelaria Prezesa Rady Ministrów
Departament Rady Ministrów
wpłynęło 26 -04- 2018

z up. Ministra Spraw Zagranicznych
Piotr Wawrzyk
Podsekretarz Stanu

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie wykazu usług kluczowych wraz z progami istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych[1)]

Na podstawie art. 6 ustawy z dnia ... o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …) zarządza się, co następuje:

§ 1. Określa się wykaz usług kluczowych, o których mowa w art. 5 ust. 2 pkt 1 ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa, wraz z progami istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, stanowiący załącznik do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie z dniem…...

PREZES RADY MINISTRÓW

---

1) Niniejsze rozporządzenie w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1).

Załącznik
do rozporządzenia
Rady Ministrów
z dnia ... (poz. …)

WYKAZ USŁUG KLUCZOWYCH ORAZ PROGI ISTOTNOŚCI SKUTKU ZAKŁÓCAJĄCEGO INCYDENTU DLA ŚWIADCZENIA USŁUG KLUCZOWYCH

Sektor	**Podsektor**	**Rodzaj podmiotu**	**Usługa kluczowa**	Próg istotności skutku zakłócającego incydentu dla usługi kluczowej
Energia	Wydobycie kopalin	Podmioty prowadzące działalność gospodarczą w zakresie wydobywania gazu ziemnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze (Dz. U. z 2017 r. poz. 2126 oraz z 2018 r. poz. 650 i 723).	Wydobywanie gazu ziemnego	
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania ropy naftowej na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.	Wydobywanie ropy naftowej	
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla brunatnego na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.	Wydobywanie węgla brunatnego	
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania węgla kamiennego na podstawie koncesji, o	Wydobywanie węgla kamiennego	

		której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.		
		Podmioty prowadzące działalność gospodarczą w zakresie wydobywania pozostałych kopalin na podstawie koncesji, o której mowa w art. 22 ust. 1 ustawy z dnia 9 czerwca 2011 r. – Prawo geologiczne i górnicze.	Wydobywanie pozostałych kopalin	
	Energia elektryczna	Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne (Dz. U. z 2018 r. poz. 755), posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania energii elektrycznej.	Wytwarzanie energii elektrycznej	Wytwarzanie minimum … MW (megawatów) rocznie.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania energii elektrycznej.	Przesyłanie energii elektrycznej	Przesyłanie minimum … GWh (gigawatogodzin) rocznie.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji energii elektrycznej.	Dystrybucja energii elektrycznej	Dystrybucja minimum … GWh (gigawatogodzin) rocznie.
		Przedsiębiorstwo	Obrót energią	Obrót na rynku energii elektrycznej o

		energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu energią elektryczną.	elektryczną	minimalnym wolumenie … TWh (terawatogodzin) rocznie.
		Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność gospodarczą w zakresie przetwarzania albo magazynowania energii elektrycznej.	Przetwarzanie energii elektrycznej	Przetwarzanie minimum … MW (megawatów) rocznie.
		Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność gospodarczą w zakresie przetwarzania albo magazynowania energii elektrycznej.	Magazynowanie energii elektrycznej	Magazynowanie minimum … MW (megawatów) rocznie.
		Podmioty prowadzące działalność gospodarczą w zakresie świadczenia usług systemowych, jakościowych i zarządzania infrastrukturą energetyczną.	Usługi systemowe, jakościowe i zarządzanie infrastrukturą energetyczną	
	Ciepło	Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania ciepła.	Wytwarzanie ciepła	Wytwarzanie … GWh (gigawatogodzin) rocznie.
		Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z	Przesyłanie ciepła	Przesyłanie … GWh (gigawatogodzin) rocznie.

		dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania ciepła.		
		Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie dystrybucji ciepła.	Dystrybucja ciepła	Minimum 250 tys. podłączonych gospodarstw domowych.
		Przedsiębiorstwo energetyczne, o którym w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu ciepłem.	Obrót ciepłem	Minimum 250 tys. podłączonych gospodarstw domowych.
	Ropa naftowa	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie wytwarzania paliw ciekłych, o której mowa w art. 32 ust. 1 ustawy – Prawo energetyczne.	Wytwarzanie paliw ciekłych	Wytwarzanie minimum … miliona litrów paliw ciekłych rocznie.
		Podmioty prowadzące działalność gospodarczą w zakresie przesyłania ropy naftowej.	Przesyłanie ropy naftowej	Przesyłanie minimum … miliona ton ropy naftowej rocznie.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. –	Przesyłanie paliw ciekłych	Przesyłanie minimum … miliona litrów paliw ciekłych rocznie.

		Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie przesyłania paliw ciekłych siecią rurociągów, o którym mowa w art. 32 ust. 1 ustawy - Prawo energetyczne.		
		Podmiot prowadzący działalność gospodarczą w zakresie magazynowania ropy naftowej, w tym w zakresie bezzbiornikowego podziemnego magazynowania ropy naftowej, o którym mowa w art. 22 ust. 1 ustawy – Prawo geologiczne i górnicze (Dz. U. z 2017 r. poz. 2126).	Magazynowanie ropy naftowej	Magazynowanie minimum … miliona ton ropy naftowej rocznie.
		Podmioty prowadzące działalność gospodarczą w zakresie przeładunku ropy naftowej.	Przeładunek ropy naftowej	Przeładunek minimum … miliona ton ropy naftowej rocznie.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie magazynowania paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy – Prawo energetyczne oraz podmiot prowadzący działalność w zakresie bezzbiornikowego podziemnego magazynowania paliw ciekłych, o którym mowa w art. 22 ust. 1 ustawy – Prawo geologiczne i górnicze.	Magazynowanie paliw ciekłych	Magazynowanie minimum … miliona litrów paliw ciekłych rocznie.

		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie przeładunku paliw ciekłych, o którym mowa w art. 32 ust. 1 ustawy – Prawo energetyczne.	Przeładunek paliw ciekłych	Przeładunek minimum … miliona litrów paliw ciekłych rocznie.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, wykonujące działalność gospodarczą w zakresie obrotu paliwami ciekłymi lub w zakresie obrotu paliwami ciekłymi z zagranicą, o którym mowa w art. 32 ust. 1 ustawy – Prawo energetyczne.	Obrót paliwami ciekłymi i obrót paliwami ciekłymi z zagranicą	Spełnienie co najmniej jednego z trzech kryteriów: 1. Obrót w kraju minimum … miliona litrów paliw ciekłych rocznie. 2. Obrót z zagranicą minimum … miliona litrów paliw ciekłych rocznie. 3. Obrót łącznie w kraju i z zagranicą minimum … miliona litrów paliw ciekłych rocznie.
		Podmioty prowadzące działalność gospodarczą w zakresie wytwarzania paliw syntetycznych.	Wytwarzanie paliw syntetycznych	
	Gaz	Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, prowadzące działalność w zakresie wytwarzania paliw gazowych, o którym mowa w art. 3 pkt 45 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne.	Wytwarzanie paliw gazowych	Wytwarzanie energii z paliw gazowych w wysokości minimum … GWh (gigawatogodzin) rocznie.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 24 ustawy z dnia 10 kwietnia 1997 r. –	Przesyłanie paliw gazowych	Przesyłanie energii z paliw gazowych w wysokości minimum … GWh (gigawatogodzin) rocznie.

		Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu przesyłowego gazowego.		
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 25 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu dystrybucyjnego gazowego.	Dystrybucja paliw gazowych	Dystrybucja energii z paliw gazowych w wysokości minimum … GWh (gigawatogodzin) rocznie.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 12 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, posiadające koncesję na wykonywanie działalności gospodarczej w zakresie obrotu gazem ziemnym z zagranicą lub na wykonywanie działalności gospodarczej w zakresie obrotu paliwami gazowymi.	Obrót paliwami gazowymi i obrót gazem ziemnym z zagranicą	Spełnienie co najmniej jednego z trzech kryteriów: 1. Obrót w kraju energią z paliw gazowych w wysokości minimum … GWh (gigawatogodzin) rocznie. 2. Obrót z zagranicą energią z paliw gazowych w wysokości minimum … GWh (gigawatogodzin) rocznie. 3. Obrót łącznie w kraju i z zagranicą energią z paliw gazowych w wysokości minimum … GWh (gigawatogodzin) rocznie.
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 26 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu	Magazynowanie paliw gazowych	Magazynowanie energii z paliw gazowych w wysokości minimum … GWh (gigawatogodzin) rocznie.

		Regulacji Energetyki operatorem systemu magazynowania paliw gazowych.		
		Przedsiębiorstwo energetyczne, o którym mowa w art. 3 pkt 27 ustawy z dnia 10 kwietnia 1997 r. – Prawo energetyczne, będące wyznaczonym przez Prezesa Urzędu Regulacji Energetyki operatorem systemu skraplania gazu ziemnego.	Skraplanie i regazyfikacja LNG oraz sprowadzanie i wyładunek	
	Dostawy i usługi dla sektora energii	Podmioty prowadzące działalność gospodarczą w zakresie dostaw systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenia usług na rzecz sektora energii.	Dostawy systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenie usług na rzecz sektora energii	
	Jednostki nadzorowane i podległe	Jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane.	Utrzymywanie rezerw strategicznych i zapasów ropy naftowej, produktów naftowych i gazu ziemnego.	
		Jednostki organizacyjne podległe ministrowi właściwemu do spraw energii lub przez niego nadzorowane.	Unieszkodliwianie odpadów promieniotwórczych	
		Jednostki organizacyjne podległe ministrowi właściwemu do spraw gospodarki złożami kopalin lub przez niego nadzorowane.	Optymalne zagospodarowanie złóż kopalin oraz ograniczenie uciążliwości oddziaływania górnictwa na ludzi i środowisko	
Transport	Transport lotniczy	Przewoźnik lotniczy, o którym mowa w art. 3 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady	Transport lotniczy pasażerski	Obsługa minimum 500 tyś. pasażerów rocznie.

		(WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002 (Dz. Urz. UE. L 2008 Nr 97, str. 72).		
		Przewoźnik lotniczy, o którym mowa w art. 3 pkt 4 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 300/2008 z dnia 11 marca 2008 r. w sprawie wspólnych zasad w dziedzinie ochrony lotnictwa cywilnego i uchylające rozporządzenie (WE) nr 2320/2002.	Transport lotniczy towarów	Spełnienie co najmniej jednego z dwóch kryteriów: 1. Realizacja przewozu ładunku cargo przy równoczesnym świadczeniu transportu pasażerskiego. 2. Minimum 25% udział procentowy realizowanych lotów transportu towarów w skali rynku krajowego obliczony na podstawie danych statystycznych za rok poprzedzający wydanie decyzji o uznaniu za operatora usługi kluczowej.
		Przedsiębiorca, o którym mowa w art. 177 ust. 2 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2017 poz. 959 i 1089 oraz z 2018 r. poz. 138 i 650), wykonujący dla przewoźników lotniczych oraz innych użytkowników statków powietrznych jedną lub więcej kategorii usług, o których mowa w art. 176 tej ustawy oraz przedsiębiorca, o którym mowa w art. 186b ust. 1 pkt 2) ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze wykonujący dla	Działalność usługowa wspomagająca transport lotniczy	Zarejestrowani Agenci - Spełnienie co najmniej jednego z dwóch kryteriów: 1. Realizacja przez podmiot kontroli bezpieczeństwa ładunku lub poczty lotniczej wraz z nadawaniem skontrolowanym ładunkom statusów SPX, SCO oraz SHR w myśl rozporządzenia wykonawczego Komisji (UE) 2015/1998 z dnia 5 listopada 2015 r. ustanawiającego szczegółowe środki w celu wprowadzenia

		przewoźników lotniczych zadania związane z kontrolą bezpieczeństwa.		w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego (Dz. Urz. UE L 2015 Nr 299, str. 1). 2. Świadczenie usługi elektronicznego przekazu informacji o statusie ochrony nadanym przesyłce, przekazywanej drogą lotniczą do punktu docelowego. Agenci handlingowi: Istnienie zależności pomiędzy prawidłowym działaniem innych usług kluczowych od usług świadczonych przez agenta handlingowego.
		Zarządzający lotniskiem, o którym mowa w art. 2 pkt 7 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.		Obsługa minimum 500 tyś. pasażerów rocznie.
		Instytucja zapewniająca służby żeglugi powietrznej, o której mowa w art. 127 ust. 1 ustawy z dnia 3 lipca 2002 r. – Prawo lotnicze.		Spełnienie co najmniej dwóch z poniższych kryteriów: 1. Świadczenie usługi na obszarze całego kraju. 2. Brak alternatywy dla świadczonej usługi i możliwości jej realizowania przez inną służbę w przypadku wystąpienia incydentu. 3. Usługa zapewniana jest dla więcej niż 10 000 lotów rocznie, niezależnie od

				maksymalnej masy startowej i liczby miejsc pasażerskich w statku powietrznym, przy lotach liczonych jako suma startów i lądowań oraz obliczanych jako średnia z ubiegłych trzech lat.
	Transport kolejowy	Zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym (Dz. U. z 2017 r. poz. 2117 i 2361 oraz z 2018 r. poz. 650), z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1b tej ustawy, infrastruktury prywatnej, o której mowa w art. 4 pkt 1c oraz infrastruktury kolei wąskotorowej, o której mowa w art. 4 pkt 1d tej ustawy.	Udostępnianie dróg kolejowych	
		Zarządca infrastruktury kolejowej w rozumieniu art. 4 pkt 7 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, z wyłączeniem zarządców wyłącznie infrastruktury nieczynnej, o której mowa w art. 4 pkt 1b tej ustawy, infrastruktury prywatnej, o której mowa w art. 4 pkt 1c oraz infrastruktury kolei wąskotorowej, o której mowa w art. 4 pkt 1d tej ustawy.	Prowadzenie ruchu kolejowego	Spełnienie co najmniej jednego z trzech kryteriów głównych, a w obrębie kryterium głównego co najmniej jednego z kryteriów szczegółowych. 1. Zależność co najmniej jednego z sektorów: a) energetyczny, b) drogowy, c) paliwowy, d) transport publiczny. 2. Co najmniej jeden z czynników mających wpływ na działalność gospodarczą i społeczną lub bezpieczeństwo

				publiczne: a) strata finansowa z tytułu niezrealizowania przewozu: 500 000 PLN/dzień, b) brak możliwości uruchomienia pociągów: 5000/dzień, c) brak możliwości realizacji dostaw paliw kopalnych (węgiel), płynnych (paliwa), d) brak możliwości realizacji przejazdów pociągów pasażerskich (transport publiczny). 3. Udział w rynku wśród zarządców infrastruktury kolejowej: 90%
		Przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, którego działalność podlega licencjonowaniu oraz operator obiektu infrastruktury usługowej, o którym mowa w art. 4 pkt 52 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, jeżeli przedsiębiorca wykonujący funkcję operatora jest jednocześnie przewoźnikiem kolejowym.	Transport kolejowy pasażerski	
		Przewoźnik kolejowy, o którym mowa w art. 4 pkt 9 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, którego działalność podlega licencjonowaniu oraz operator obiektu infrastruktury usługowej, o którym mowa w art. 4	Transport kolejowy towarów	

		pkt 52 ustawy z dnia 28 marca 2003 r. o transporcie kolejowym, jeżeli przedsiębiorca wykonujący funkcję operatora jest jednocześnie przewoźnikiem kolejowym.		
	Transport wodny	Armator w transporcie morskim pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych (Dz. Urz. UE. L 2004 Nr 129, str. 6), z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy.	Transport morski pasażerski	
		Armator w transporcie morskim pasażerów i towarów zgodnie z definicją dla transportu morskiego w załączniku I do rozporządzenia (WE) nr 725/2004 Parlamentu Europejskiego i Rady dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych, z wyłączeniem poszczególnych statków, na których prowadzą działalność ci armatorzy.	Transport morski towarów	
		Armator, o którym mowa w art. 5 ust. 1 pkt 2 ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej.	Transport wodny śródlądowy pasażerski	
		Armator, o którym mowa w art. 5 ust. 1 pkt 2	Transport wodny śródlądowy towarów	

		ustawy z dnia 21 grudnia 2000 r. o żegludze śródlądowej.		
		1. Podmiot zarządzający portem, o którym mowa w art. 2 pkt 6 ustawy z dnia 20 grudnia 1996 r. o portach i przystaniach morskich (Dz.U. z 2017 r. poz. 1933). 2. Podmiot zarządzający obiektem portowym, o którym mowa w art. 2 pkt 11 rozporządzenia (WE) 725/2004 Parlamentu Europejskiego i Rady z dnia 31 marca 2004 r. w sprawie podniesienia ochrony statków i obiektów portowych. 3. Podmioty prowadzące na terenie portu działalność wspomagającą transport morski.	Działalność usługowa wspomagająca transport morski	
		VTS (Służba Kontroli Ruchu Statków) – aparat pomocniczy dyrektora urzędu morskiego powołany w celu monitorowania ruchu statków i przekazywania informacji, stanowiący część składową Narodowego Systemu SafeSeaNet, o którym mowa w art. 91 ustawy z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2018 r. poz. 181).	Monitorowanie ruchu statków	
	Transport drogowy	Organy, o których mowa w art. 19 ust. 2, 5, 5a, ustawy z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z	Zarządzanie drogami	Spełnienie co najmniej jednego z poniższych kryteriów: 1. Obsługa minimum

		2017 r. poz. 2222 oraz z 2018 r. poz. 12, 138, 159 i 317).		500 tyś. użytkowników dróg krajowych rocznie. 2. Wystąpienie zagrożenia dla bezpieczeństwa ruchu spowodowane niewłaściwym funkcjonowaniem systemów zarządzania drogami (ruchem drogowym). 3. Minimum 15% udział procentowy wszystkich dróg krajowych objętych danym systemem zarządzania drogami (ruchem drogowym).
		Podmioty, o których mowa w art. 43a ust. 1 ustawy z dnia 21 marca 1985 r. o drogach publicznych.	Inteligentne systemy transportowe	Spełnienie co najmniej jednego z poniższych kryteriów: 1. Obsługa minimum 500 tyś. użytkowników dróg krajowych rocznie. 2. Zagrożenie dla bezpieczeństwa ruchu spowodowane niewłaściwym funkcjonowaniem inteligentnych systemów transportowych albo brak wpływów z tytułu opłat za przejazd drogami krajowymi. 3. Minimum 15% udział procentowy wszystkich dróg krajowych objętych danym Inteligentnym Systemem Transportowym.
Bankowość i infrastruktura rynków finansowych		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2017 r. 1876, 2361 i 2491 oraz z 2018 r. poz. 62,106, 138, 650, 685 i 723).	Obsługa posiadaczy rachunków	

		Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy – Prawo bankowe. Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz. U. z 2017 r. poz. 2065, 2486 i 2491 oraz z 2018 r. poz. 62, 106, 138, 650, 723 i 771).		
		Instytucja kredytowa, o której mowa w art. 4 ust. 1 pkt 17 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe. Oddział instytucji kredytowej, o którym mowa w art. 4 ust. 1 pkt 18 ustawy – Prawo bankowe. Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe. Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy – Prawo bankowe. Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych.	Usługi kredytowe dla MSP	.
		Bank krajowy, o którym mowa w art. 4 ust. 1 pkt 1 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe. Oddział banku zagranicznego, o którym mowa w art. 4 ust. 1 pkt 20 ustawy – Prawo bankowe. Spółdzielcze kasy oszczędnościowo-kredytowe w rozumieniu ustawy z dnia 5 listopada 2009 r. o spółdzielczych	Wypłata środków pieniężnych z bankomatu	

		kasach oszczędnościowo-kredytowych.		
		Podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2017 r. poz. 1768, 2486 i 2491 oraz z 2018 r. poz. 106, 138, 650, 685, 723 i 771).	Prowadzenie rynku regulowanego lub innej działalności w zakresie organizowania obrotu instrumentami finansowymi oraz giełdy towarowej	
		Podmiot prowadzący rynek regulowany, o którym mowa w art. 14 ust. 1 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi. Podmiot, o którym mowa w art. 3 pkt 49 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.	Organizowanie alternatywnego systemu obrotu instrumentami finansowymi	
		Podmiot, o którym mowa w art. 48 ust. 7 ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi.	Prowadzenie rozliczeń i transakcji i rozrachunku transakcji zawieranych w obrocie instrumentami finansowymi bądź zawartych na giełdach towarowych.	
Ochrona zdrowia		Podmiot leczniczy, o którym mowa w art. 4 ust. 1 ustawy z dnia 15 kwietnia 2011 r. o działalności leczniczej (Dz. U. z 2018 r. poz. 160, 138 i 650).		
		Podmioty związane z obrotem produktami leczniczymi w rozumieniu przepisów ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne (Dz. U. z 2017 r. poz. 2211 oraz z 2018 r. poz. 650 i 697).		
		Jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia.		
		Narodowy Fundusz Zdrowia		
		Podmiot leczniczy w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej, w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo		

		farmaceutyczne.		
		Podmiot leczniczy w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.		
		Przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.		
		Przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim Unii Europejskiej lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) – strony umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego.		
		Importer produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.		
		Wytwórca produktu leczniczego/substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne..		
		Importer równoległy w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.		
		Dystrybutor substancji czynnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.		
		Przedsiębiorca prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu ustawy z dnia 6 września 2001 r. – Prawo farmaceutyczne.		
Zaopatrzenie w wodę pitną i jej		Przedsiębiorstwo wodociągowo-kanalizacyjne, o którym	Pobór wody	Pobór wody dla minimum 500 tys. podłączonych

dystrybucja		mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków (Dz. U. z 2017 r. poz. 328, 1566 i 2180 oraz z 2018 r. poz. 650).		mieszkańców.
		Przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków.	Uzdatnianie wody	Uzdatnianie wody dla minimum 500 tys. podłączonych mieszkańców.
		Przedsiębiorstwo wodociągowo-kanalizacyjne, o którym mowa w art. 2 pkt 4 ustawy z dnia 7 czerwca 2001 r. o zbiorowym zaopatrzeniu w wodę i zbiorowym odprowadzaniu ścieków.	Dostarczanie wody	Zaopatrywanie w wodę pitną w ilości 22 milionów m3 minimalnie w ujęciu rocznym.
Infrastruktura cyfrowa		Podmiot prowadzący punkt wymiany ruchu internetowego (IXP), stanowiącego obiekt sieciowy, który umożliwia połączenie międzysystemowe pomiędzy więcej niż dwoma niezależnymi systemami autonomicznymi, głównie do celów ułatwienia wymiany ruchu internetowego.	Prowadzenie punktu wymiany ruchu internetowego (IXP) w Polsce	Ilość podłączonych systemów autonomicznych w ilości 300 w ujęciu minimalnym (średnia roczna).
		Podmiot, który świadczy usługi DNS.	Prowadzenie autorytatywnego serwera DNS	Minimalnie 250 tys. ilości domen , dla których serwer jest autorytatywny.
		Podmiot zarządzający rejestracją internetowych nazw domen w ramach domeny najwyższego poziomu (TLD).	Prowadzenie rejestru domeny najwyższego poziomu (TLD)	

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie delegacji art. 6 ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa (Dz. U. poz.....) i określa wykaz usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, zwanych dalej usługami kluczowymi wraz z progami istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w wykazie usług kluczowych. Wykaz usług kluczowych został sporządzony w oparciu o:

1) rodzaje działalności usługowych wskazane w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) (Dz. U. poz. 1885, z późn. zm.), które mogą być świadczone co najmniej przez przedsiębiorców bądź inne podmioty, objęte zakresem ustawy o krajowym systemie cyberbezpieczeństwa;
2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego;
3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu w sprawie Polskiej Klasyfikacji Działalności;
4) weryfikację pozycji pkt 1–3 przez organy właściwe.

Progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w wykazie zostały sporządzone w oparciu o dane przekazane przez organy właściwe oraz najlepszymi międzynarodowymi praktykami prezentowanymi w materiałach Grupy Współpracy ustanowionej na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L Nr 194 z 19.07.2016, str. 1), której to dyrektywy niniejsze rozporządzenie i ustawa o krajowym systemie cyberbezpieczeństwa stanowią transpozycję do polskiego porządku prawnego. Wykaz usług kluczowych będący załącznikiem do niniejszego rozporządzenia uwzględnia podział na sektory, podsektory, rodzaje podmiotów określone w załączniku do ustawy oraz progi istotności skutku zakłócającego incydentu dla usługi kluczowej.

Wykaz usług kluczowych będzie wykorzystywany w procesie wydawania decyzji administracyjnych przez organy właściwe w sprawie uznania za operatora usługi kluczowej przedsiębiorcy bądź podmiotu należącego do jednego z sektorów wymienionych w załączniku do ustawy. W procesie wydawania decyzji administracyjnych organy właściwe

będą dokonywać oceny, czy określona usługa znajduje się w załączniku do niniejszego rozporządzenia. W kolejnych krokach w oparciu o stworzony wykaz organ właściwy będzie określał, czy świadczenie usługi kluczowej zależy od systemów informacyjnych oraz jaki jest poziom skutku zakłócającego dla świadczonej usługi kluczowej.

Podstawowym założeniem projektodawcy jest zapewnienie, aby na początkowym etapie wydawania decyzji administracyjnej w sprawie uznania za operatora usługi kluczowej organ właściwy miał możliwość wstępnej weryfikacji w oparciu o dane ze stosownych rejestrów, a więc dane z Krajowego Rejestru Sądowego, czy Centralnej Ewidencji i Informacji o Działalności Gospodarczej (CEIDG) lub na podstawie analizy rynku dokonywanej przez organy regulacyjne i nadzoru rynku w poszczególnych sektorach. Wykorzystanie nomenklatury Polskiej Klasyfikacji Działalności umożliwia również identyfikację podmiotów publicznych, które nie znajdują się w rejestrach gospodarczych, a będą mogły być uznane za operatora usługi kluczowej w oparciu o nomenklaturę PKD. Dla podsektora transportu drogowego projektodawca wskazał bezpośrednio usługi z zakresu zarządu dróg z uwagi na fakt, że PKD nie odwołuje się bezpośrednio do tego rodzaju działalności. W przypadku sektora finansowego, oprócz nomenklatury PKD uwzględniono również rodzaje działalności ustalone przez ustawodawcę europejskiego, które należy uwzględnić w procesie wydawania decyzji administracyjnych w zakresie operatorów usług kluczowych. Należy podkreślić, iż ustalenie wykazu usług kluczowych oraz progów istotności skutku zakłócającego nastąpiło we współpracy z organami właściwymi.

Projektowane rozporządzenie wejdzie w życie w dniu wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa.

Przedmiot projektowanej regulacji jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2018 r. poz. 362).

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania konsultacji lub uzgodnienia.

Projekt został udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Nazwa projektu Rozporządzenie Rady Ministrów z dnia ….w sprawie wykazu usług kluczowych wraz z progami istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Karol Okoński, Podsekretarz Stanu w Ministerstwie Cyfryzacji **Kontakt do opiekuna merytorycznego projektu** Andrzej Szyszko, Departament Cyberbezpieczeństwa, Zastępca Dyrektora, tel. (22) 245 57 05, e-mail: andrzej.szyszko@mc.gov.pl	**Data sporządzenia** 19 kwietnia 2018 r. **Źródło:** Art. 6 ustawy o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …) **Nr w wykazie prac legislacyjnych Rady Ministrów**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projektowane rozporządzenie stanowi wykonanie delegacji art. 6 ustawy z dnia ... o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …) i określa wykaz usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, zwanych dalej usługami kluczowymi wraz z progami istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w ww. wykazie usług kluczowych. Artykuł 7 ww. ustawy zobowiązuje ministra właściwego do spraw informatyzacji do prowadzenia wykazu operatorów usług kluczowych. Wykaz ten zostanie utworzony z uwzględnieniem podziału na sektory, podsektory i rodzaje podmiotów, który wprowadza ustawa. Wpis do wykazu lub wykreślenie z niego ma charakter deklaratoryjny i będzie czynnością materialno-techniczną, realizowaną w oparciu o decyzje administracyjne organów właściwych (właściwych działowo ministrów), w zakresie identyfikacji operatorów usług kluczowych we właściwych sektorach. Rozporządzenie wraz z załącznikiem będącym wykazem usług kluczowych wraz z progami istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w ww. wykazie jest jednym z elementów niezbędnych do wydania ww. decyzji administracyjnej.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Wykaz usług kluczowych został sporządzony w oparciu o:

1) rodzaje działalności usługowych wskazane w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) (Dz. U. poz. 1885, z późn. zm.), które mogą być świadczone co najmniej przez przedsiębiorców bądź inne podmioty, objęte zakresem ustawy o krajowym systemie cyberbezpieczeństwa;
2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego;
3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu w sprawie Polskiej Klasyfikacji Działalności;
4) weryfikację pozycji pkt 1-3 przez organy właściwe.

Wykaz usług kluczowych wraz z progami istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych zawartych w ww. wykazie jest elementem niezbędnym w procedurze wyłaniania operatora usług kluczowej. Wyłonienie operatora usługi kluczowej odbywa się poprzez podjęcie decyzji administracyjnej.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Ustawa o krajowym systemie cyberbezpieczeństwa stanowiąca implementację dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, zwanej dalej „dyrektywą 2016/1148/UE", jest w trakcie transpozycji w innych państwach członkowskich UE, podobnie jak i akty wykonawcze do ustawy implementujące zapisy dyrektywy 2016/1148/UE.

Za dokument referencyjny dla przedstawienia rozwiązań w innych państwach UE uznać można opracowanie przygotowane w ramach prac grupy roboczej utworzonej decyzją Grupy Współpracy (instytucja utworzona na mocy dyrektywy 2016/1148/UE, w jej skład wchodzą przedstawiciele państw członkowskich) – *Identification of Operators of Essential Services. Sharing of good practice related to the criteria defining the criticality of an operator pursuant to art 5(2) of the directive by means of guidelines.* Dokument został zatwierdzony przez Grupę Współpracy i przedstawia wytyczne dotyczące identyfikacji operatorów usług kluczowych uwzględniając element wykazu usług kluczowych oraz progu istotności skutku zakłócającego incydentu dla świadczonej usługi kluczowej, które są niezbędne do skutecznego przeprowadzenia procesu identyfikacji. W dokumencie zawarte są

również przykłady dobrych praktyk w ww. obszarze. Dokument zakłada przyjęcie podziału na sektory, podsektory i rodzaj podmiotu z załącznika nr 2 do dyrektywy 2016/1148/UE, który odpowiada załącznikowi do ustawy o krajowym systemie cyberbezpieczeństwa. Wykaz usług kluczowych obejmuje zatem przynajmniej następujące sektory i podsektory: energia (energia elektryczna, gaz, ropa naftowa), transport (drogowy, lotniczy, wodny, kolejowy), bankowość i infrastruktura rynków finansowych, ochrona zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa. Analiza prac nad wykazem usług w państwach UE wykazała, iż państwa poza ww. sektorami i podsektorami wyróżniają również i inne kluczowe dla utrzymania krytycznej działalności społecznej lub gospodarczej w danym państwie (np. sektor produktów żywnościowych, sektor przemysłu, sektor ochrony środowiska). Ponadto niektóre państwa członkowskie zrównują przymiotnik „kluczowy" z „krytyczny" i odwołują się przy identyfikacji usług kluczowych do metodologii wykorzystywanej przy identyfikacji infrastruktury krytycznej. Dokument sugeruje jednak, aby państwa które zdecydowały się na taką metodologię sprawdziły czy odpowiada ona tej przyjętej w dyrektywie 2016/1148/UE. Określenie wykazu usług kluczowych i progów istotności skutku zakłócającego incydentu dla świadczonej usługi kluczowej odbywa się w ramach różnych procedur w państwach UE. Jedne z nich określają wykaz w drodze eksperckich konsultacji sektora publicznego z prywatnym. Inne zdecydowały się na rozesłanie ankiet do sektorów i połączenie ich z konsultacjami z danym sektorem. W efekcie powstawały eksperckie zespoły złożone z przedstawicieli sektora, odpowiedniego dla sektora ministerstwa i agencji odpowiedzialnych za infrastrukturę krytyczną.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Sektor energii, podsektor wydobycie kopalin,	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe wydobycia gazu ziemnego, ropy naftowej, węgla brunatnego, węgla kamiennego, pozostałych kopalin	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	Wykaz usług kluczowych jest elementem procedury wyznaczania operatora usługi kluczowej.
Sektor energii, podsektor elektroenergetyczny	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe wytwarzania, przesyłania, dystrybucji, obrotu, przetwarzania, magazynowania energii elektrycznej oraz usługi systemowe, jakościowe i zarządzanie infrastrukturą energetyczną	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności	

		(PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor energii, podsektor ciepło	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe wytwarzania, przesyłania, dystrybucji, obrotu ciepłem	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor energii, podsektor ropy naftowej	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe wytwarzania paliw ciekłych, przesyłania ropy naftowej, przesyłania paliw ciekłych, magazynowania ropy naftowej, przeładunku ropy naftowej, magazynowanie paliw ciekłych, przeładunek paliw ciekłych, obrót paliwami ciekłymi i obrót paliwami ciekłymi z zagranicą, wytwarzanie paliw syntetycznych	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor energii, podsektor gazu	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe wytwarzania, przesyłania, dystrybucji paliw gazowych, obrót paliwami gazowymi i obrót gazem ziemnym z zagranicą, magazynowanie paliw gazowych, skraplanie i regazyfikacja LNG oraz sprowadzanie i wyładunek	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w	

		rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor energii w zakresie dostaw i usług dla sektora energii oraz jednostki nadzorowane i podległe ministrowi właściwemu do spraw energii	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe dostawy systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenie usług na rzecz sektora energii; utrzymywanie rezerw strategicznych i zapasów ropy naftowej, produktów naftowych i gazu ziemnego; unieszkodliwianie odpadów promieniotwórczych; Optymalne zagospodarowanie złóż kopalin oraz ograniczenie uciążliwości oddziaływania górnictwa na ludzi i środowisko.	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD; 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor transportu, podsektor transport lotniczy	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe transport lotniczy pasażerski, transport lotniczy towarów, działalność usługowa wspomagająca transport lotniczy	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego, 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor transportu, podsektor transport kolejowy	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe udostępnianie dróg kolejowych, prowadzenie ruchu kolejowego, transport kolejowy towarowy	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma	

		określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor transport, podsektor transport wodny (dotyczącym transportu morskiego)	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe transport morski pasażerski, towarowy, działalność usługowa wspomagająca transport morski, monitorowanie ruchu statków	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor transport, podsektor transport wodny (dotyczącym transportu śródlądowego)	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe transport wodny śródlądowy pasażerski, towarowy;	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor transport, podsektor transport drogowy	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe zarządzanie drogami, inteligentne systemy transportowe	Szacunki oparte na załączniku do projektu ustawy oraz danych MI (jeden zarządca dróg krajowych, szesnastu zarządców dróg wojewódzkich, dwóch operatorów systemów ITS na poziomie krajowym i pięciu w miastach). Jest możliwe poszerzenie tej	

		grupy o zarządców dróg powiatowych i gminnych, jednak nie były brane pod uwagę w szacunkach.	
Sektor bankowość i infrastruktura rynków finansowych	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa	Szacunki oparte na załączniku do projektu ustawy oraz danych KNF (dwadzieścia największych banków, dziesięć największych banków spółdzielczych, Krajowa SKOK, dziesięć największych SKOK, , dziesięć największych instytucji płatniczych, dwa banki państwowe, jedna giełda, dwaj operatorzy systemu obrotu i jeden kontrahent centralny)	
Sektor zaopatrzenie w wodę pitną i jej dystrybucja	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe pobór, uzdatnianie, dostarczanie wody	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor ochrona zdrowia	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor infrastruktura	Szacunki – OSR do ustawy o	1) rozporządzenie Rady	

cyfrowa	krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe prowadzenie punktu wymiany ruchu internetowego (IXP) w Polsce, prowadzenie autorytatywnego serwera DNS, prowadzenie rejestru domeny najwyższego poziomu (TLD)	Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Przeprowadzono ustalenia z ministerstwami, które uczestniczyły w pracach międzyresortowego zespołu roboczego ds. przygotowania ustawy (skład osobowy bazował na zespole ds. opracowania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017–2022). Organy właściwe według ustawy o krajowym systemie cyberbezpieczeństwa (właściwe działowo ministerstwa) otrzymały od Ministerstwa Cyfryzacji wykaz usług kluczowych sporządzony w oparciu o rodzaje działalności usługowych wskazane w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) które mogą być świadczone co najmniej przez przedsiębiorców bądź inne podmioty, objęte zakresem ustawy o krajowym systemie cyberbezpieczeństwa; rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu w sprawie Polskiej Klasyfikacji Działalności. W następnym etapie odbywały się konsultacje z poszczególnymi organami właściwymi zweryfikowanych przez nich list powstałych w oparciu o ww. dokumenty.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2018 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	Łącznie (0–10)
Dochody ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Fundusz Ubezpieczeń Społecznych												
Fundusz Pracy												
Narodowy Fundusz Zdrowia												
Wydatki ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Fundusz Ubezpieczeń Społecznych												
Fundusz Pracy												
Narodowy Fundusz Zdrowia												

Źródła finansowania	Rozporządzenie nie generuje finansowych obciążeń.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0–10)
W ujęciu pieniężnym	-	-	-	-	-	-	-	-
W ujęciu niepieniężnym	zidentyfikowani m.in. w oparciu o wykaz usług kluczowych jako operatorzy usług kluczowych	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w ustawie.						
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

9. Wpływ na rynek pracy

O ile na podstawie wykazu usług kluczowych podmiot zostanie zidentyfikowany jako operator usługi kluczowej będzie zobowiązany do utworzenia u operatora usługi kluczowej stanowiska ds. cyberbezpieczeństwa a to z kolei wpłynie na certyfikację tego typu kompetencji.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☒ zdrowie

Omówienie wpływu	Wykaz usług kluczowych jest niezbędnym elementem procedury administracyjnej mającej wyłonić operatorów usług kluczowych.
11. Planowane wykonanie przepisów aktu prawnego	
Rozporządzenie wejdzie w życie z dniem….	
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?	
Każdorazowe zakończenie procedury postępowania administracyjnego, skutkujące wydaniem decyzji, będzie wpływało na aktualizację wykazu operatorów usług kluczowych oraz wykaz usług kluczowych.	
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)	
-	

76/04/rch

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych

Na podstawie art. 10 ust. 5 ustawy z dnia ... o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …) zarządza się, co następuje:

§ 1. Rozporządzenie określa rodzaje dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych.

§ 2. W skład dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej wchodzą:

1) dokumentacja normatywna;
2) dokumentacja operacyjna.

§ 3. W skład dokumentacji, o której mowa w § 2 pkt 1 wchodzi w szczególności:

1) dokumentacja systemu zarządzania bezpieczeństwem informacji wytworzona zgodnie z wymaganiami normy PN ISO/IEC 27001;
2) plan ochrony infrastruktury, z wykorzystaniem której świadczona jest usługa kluczowa;
3) plan zapewnienia ciągłości działania usługi kluczowej wytworzony zgodnie z wymaganiami normy PN-EN ISO 22301;
4) dokumentacja techniczna systemu teleinformatycznego wykorzystywanego do świadczenia usługi kluczowej;
5) inna dokumentacja, której potrzeba istnienia wynika ze specyfiki świadczonej usługi kluczowej.

§ 4. 1. Plan ochrony, o którym mowa w § 3 pkt 2 zawiera w szczególności:

1) charakterystykę wykorzystywanych obiektów infrastruktury;
2) analizę stopnia zagrożenia dla wykorzystywanych obiektów infrastruktury;
3) ocenę aktualnego stanu ochrony;
4) opis zabezpieczeń technicznych obiektu;
5) zasady organizacji i wykonywania ochrony fizycznej;

6) dane dotyczące specjalistycznej uzbrojonej formacji ochronnej, jeśli występuje.

2. W przypadku gdy obiekt podlega obowiązkowej ochronie zastosowanie mają przepisy ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2017 r. poz. 2213 oraz z 2018 r. poz. 138 i 650).

§ 5. 1. W skład dokumentacji, o której mowa w § 2 pkt 2 wchodzą w szczególności:

1) procedury oraz instrukcje wynikające z dokumentacji normatywnej;
2) wzory zapisów dokumentujących wykonanie procedury;
3) zapisy dokumentujące każdorazowe wykonanie procedury.

2. Zapisy, o których mowa w ust. 1 pkt 3, mogą być tworzone zarówno w postaci papierowej, jak i w postaci elektronicznej.

§ 6. Rozporządzenie wchodzi w życie z dniem ……..

PREZES RADY MINISTRÓW

UZASADNIENIE

Projekt rozporządzenia Rady Ministrów w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych stanowi wykonanie delegacji ustawowej, zamieszczonej w art. 10 ust. 5 projektu ustawy o krajowym systemie cyberbezpieczeństwa, określanej dalej jako „ustawa”.

Celem projektowanych przepisów jest określenie wymagań dla dokumentacji technicznej, opisującej zasady oraz metody zapewniania cyberbezpieczeństwa systemów informacyjnych wykorzystywanych dla realizacji usług kluczowych, o których mowa w art. 5 ust. 2 pkt 1 ustawy, zaś ich adresatami są przedsiębiorcy oraz podmioty publiczne w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), będący operatorami usług kluczowych w rozumieniu ustawy.

W ślad za praktyką stosowaną w zarządzaniu dokumentacja określona w projekcie rozporządzenia dzieli się na dwie podstawowe klasy: dokumentację normatywną i dokumentację operacyjną. Dokumentację normatywną stanowią przepisy prawa powszechnego oraz wewnętrzne akty normatywne wydawane na przykład w postaci zarządzeń i decyzji przez kierownictwo danego podmiotu. Drugą z klas dokumentacji jest dokumentacja operacyjna, sporządzana w ramach prowadzenia bieżącej działalności danego podmiotu, a w szczególności dokumentacja w postaci zapisów z wykonanych czynności, stanowiąca ślad audytowy, na podstawie którego można stwierdzić prawidłowość wykonywania nałożonych obowiązków. Podział taki został uwzględniony w treści projektowanego § 2.

W § 3 wskazany został minimalny zakres dokumentacji normatywnej, która musi być prowadzona przez operatora usługi kluczowej. Zakres tej dokumentacji mieści się w ramach dokumentacji, którą musi prowadzić operator infrastruktury krytycznej w rozumieniu przepisów o zarządzaniu kryzysowym. Oznacza to, że operator usługi kluczowej, który jest jednocześnie operatorem infrastruktury krytycznej, nie musi tworzyć odrębnej dokumentacji na podstawie projektowanego rozporządzenia. Mając na uwadze cel prowadzenia dokumentacji normatywnej na podkreślenie zasługuje konieczność prowadzenia dokumentacji związanej z systemem zarządzania bezpieczeństwem informacji oraz zarządzaniem ciągłością działania zgodnie z powszechnie stosowanymi w tym zakresie Polskimi Normami.

W § 4 wskazany został minimalny zakres informacji, które powinien zawierać plan ochrony infrastruktury operatora usługi kluczowej. Zakres ten jest tożsamy z zakresem informacji dotyczącym planów ochrony obiektów podlegających obowiązkowej ochronie, o którym mowa w art. 7 ust. 2 ustawy z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2017 r. poz. 2213 oraz z 2018 r. poz. 138 i 650).

W § 5 wyszczególniony został minimalny zakres dokumentacji operacyjnej. Szczególne znaczenie mają zapisy stanowiące ślad audytowy, które pozwalają audytorom i kontrolerom na stwierdzenie poprawności funkcjonowania podmiotu w zakresie zapewniania cyberbezpieczeństwa co do realizacji usługi kluczowej.

Przewiduje się, że dokumenty poświadczające każdorazowe wykonanie procedury mogą być prowadzone w postaci papierowej lub elektronicznej, zależnie od okoliczności. Ustanawia się obowiązek sprawowania nadzoru nad dokumentacją przez operatora i definiuje minimalny zakres czynności nadzorczych.

Mając na uwadze treść przepisu art. 19 ust. 1 dyrektywy Parlamentu Europejskiego i Rady (UE) nr 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1), zgodnie z którym, w celu zapewnienia spójnego wdrażania poszczególnych przepisów dyrektywy dopuszczalnym jest odwoływanie się do stosowania europejskich lub uznanych międzynarodowo norm i specyfikacji mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych, w przepisach projektu zamieszczono wskazania odpowiednich norm, co powinno przyczynić się do bardziej precyzyjnego określenia wymogów dokumentacji, jakie mają spełnić operatorzy usług kluczowych.

Projekt rozporządzenia podlega uproszczonej notyfikacji w trybie przepisu § 8 ust. 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597).

Projekt został udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie dokumentacji cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Kontakt do opiekuna merytorycznego projektu**	**Data sporządzenia** **Źródło:** Art. 10 ust. 5 ustawy……..... o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …) **Nr w wykazie prac …….**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Na mocy art. 10 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa na operatorach usług kluczowych spoczywają wymogi opracowania, wdrożenia i aktualizacji dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych – projektowane rozporządzenia ma dookreślić kształt i charakter tej dokumentacji, potrzebnej dla zapewnienia odpowiedniego poziomu bezpieczeństwa systemów.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rozwiązaniem problemu jest opracowanie stosownych przepisów, zgodnie z upoważnieniem zamieszczonym w art. 10 ust. 5 ustawy o krajowym systemie cyberbezpieczeństwa.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Nie dotyczy.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze elektroenergetycznym	20	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (OSP, pięciu największych OSD dla gospodarstw domowych, dziewięciu największych OSD dla przedsiębiorców, pięciu największych sprzedawców prądu)	Spełnienie wszystkich wymogów nałożonych przepisami rozporządzenia
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze ropy naftowej	4	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (OSP oraz czterej najwięksi przedsiębiorcy posiadający koncesję na dystrybucję, wytwarzanie, magazynowanie lub przeładunek paliw ciekłych oraz na obrót paliwami ciekłymi)	
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze gazu	22	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (OSP, OSD, przedsiębiorcy dostarczający lub magazynujący gaz lub gaz ziemny oraz dziesięć największych przedsiębiorstw gazowych w rozumieniu art. 2 pkt 1 dyrektywy 2009/73/WE)	

Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu lotniczego	28	Szacunki oparte na załączniku do projektu ustawy oraz danych ULC (jeden przewoźnik lotniczy, zarządzający ośmioma największymi portami lotniczymi, pięć podmiotów obsługujących urządzenia pomocnicze znajdujące się w portach lotniczych oraz służba kontroli ruchu lotniczego)	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu kolejowego	10	Szacunki oparte na załączniku do projektu ustawy oraz danych UTK (trzech największych zarządców infrastruktury kolejowej, czterech największych przewoźników kolejowych osobowych oraz trzech największych przewoźników kolejowych towarowych). Nie wzięto pod uwagę liczby operatorów infrastruktury usługowej ze względu na fakt, że rejestr obiektów infrastruktury usługowej zostanie utworzony przez Prezesa UTK do 30 czerwca 2018 r.	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu wodnego (dotyczącym transportu morskiego)	17	Szacunki oparte na załączniku do projektu ustawy oraz danych MGMiŻŚ (założyliśmy objęcie dziesięciu największych armatorów, pięciu portów morskich oraz operatora SafeSeaNet)	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu wodnego (dotyczącym transportu śródlądowego)	4	Szacunki oparte na załączniku do projektu ustawy oraz danych MGMiŻŚ (założyliśmy objęcie trzech największych armatorów i jednego portu śródlądowego)	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu drogowego	24	Szacunki oparte na załączniku do projektu ustawy oraz danych MIiB (jeden zarządca dróg krajowych, szesnastu zarządców dróg wojewódzkich, dwóch operatorów systemów ITS na poziomie krajowym i pięciu w miastach). Jest możliwe poszerzenie tej grupy o zarządców dróg powiatowych i gminnych, jednak nie były brane pod	

		uwagę w szacunkach.	
Podmioty świadczące usługi kluczowe w sektorze bankowości i infrastruktury rynków finansowych	47	Szacunki oparte na załączniku do projektu ustawy oraz danych KNF (dwadzieścia największych banków, dziesięć największych banków spółdzielczych, Krajowa SKOK, dziesięć największych SKOK, dwa banki państwowe, jedna giełda, dwaj operatorzy systemu obrotu i jeden kontrahent centralny)	
Podmioty świadczące usługi kluczowe w sektorze zaopatrzenia w wodę pitną i jej dystrybucję	31	Przedsiębiorstwa wodno-kanalizacyjne na wykazie IK.	
Podmioty świadczące usługi kluczowe w sektorze służby zdrowia	131	Liczba podmiotów realizujących świadczenia szpitalne, które miały więcej niż 18 000 hospitalizacji rocznie (dane MZ) Dolnośląskie – 12 Kujawsko-pomorskie – 8 Lubelskie – 8 Lubuskie – 3 Łódzkie – 8 Małopolskie – 10 Mazowieckie – 18 Opolskie – 3 Podkarpackie – 8 Podlaskie – 8 Pomorskie – 5 Śląskie – 15 Świętokrzyskie – 5 Warmińsko-mazurskie – 3 Wielkopolskie – 12 Zachodniopomorskie – 5	
Podmioty świadczące usługi kluczowe w sektorze infrastruktury cyfrowej	8	Szacunki oparte na analizie informacji rynkowych	

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W ramach konsultacji i opiniowania projekt zostanie przesłany do:

1) Prezes Urzędu Komunikacji Elektronicznej,
2) Prezes Urzędu Ochrony Konkurencji i Konsumentów,
3) Generalnego Inspektora Ochrony Danych Osobowych,
4) Prezesa Głównego Urzędu Statystycznego,
5) Polskiej Izby Informatyki i Telekomunikacji,
6) Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji,
7) Polskiej Izby Komunikacji Elektronicznej,
8) Krajowej Izby Gospodarczej,

9) Krajowej Izby Komunikacji Ethernetowej,
10) Polskiej Izby Radiodyfuzji Cyfrowej,
11) Polskiej Izby Handlu,
12) Fundacji Bezpieczna Cyberprzestrzeń,
13) Polskiego Towarzystwa Informatycznego,
14) Fundacji Nowoczesna Polska,
15) Fundacji Projekt Polska,
16) Internet Society Poland,
17) Stowarzyszenia Inżynierów Telekomunikacji,
18) Fundacji Panoptykon,
19) Rady Dialogu Społecznego,
20) Business Centre Club – Związku Pracodawców,
21) Niezależnego Samorządowego Związku Zawodowego „Solidarność”,
22) Ogólnopolskiego Porozumienia Związków Zawodowych,
23) Forum Związków Zawodowych,
24) Pracodawców Rzeczypospolitej Polskiej,
25) Konfederacji Lewiatan,
26) Związku Przedsiębiorców i Pracodawców,
27) Związku Rzemiosła Polskiego,
28) Związku Pracodawców Mediów Publicznych,
29) Związku Pracodawców Branży Internetowej IAB Polska,
30) Federacji Związków Zawodowych Pracowników Telekomunikacji,
31) Federacji Konsumentów.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt został udostępniony na stronie podmiotowej Biuletynu Informacji Publicznej Ministra Cyfryzacji oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0-10)
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w rozporządzeniu.						
	sektor mikro-, małych i średnich przedsiębiorstw	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w rozporządzeniu.						
	rodzina, obywatele oraz gospodarstwa domowe	Rodziny, obywatele, gospodarstwa domowe – regulacje zamieszczone w rozporządzeniu przyczynią się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele.						
Niemierzalne	-	Nie dotyczy.						

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

Wymogi wprowadzane rozporządzeniem nie będą stanowiły znaczącego obciążenia dla podmiotów, gdyż większość z nich powinna mieć już wdrożone analogiczne rozwiązania, ponieważ podlegają również przepisom ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566), wobec czego posiadają analogiczną dokumentację i będą mogły ją wykorzystać, bez potrzeby opracowywania dokumentacji od początku.

9. Wpływ na rynek pracy		
Pozytywny – przepisy przyczynią się do wzrostu zatrudnienia w obszarze cyberbezpieczeństwa, gdyż operatorzy mogą stworzyć nowe miejsca pracy dla pracowników wykonujących obowiązki dotyczące właściwego prowadzenia dokumentacji cyberbezpieczeństwa.		
10. Wpływ na pozostałe obszary		
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Przepisy rozporządzenia przyczynią się do zwiększenia poziomu cyberbezpieczeństwa, co będzie miało pozytywny wpływ na przedsiębiorców i obywateli.	
11.Planowane wykonanie przepisów aktu prawnego		
Po upływie vacatio legis.		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
100% operatorów posiada i stosuje odpowiednią dokumentację, po roku od wejścia w życie przepisów.		
13.Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie progów uznania incydentu za poważny[1)]

Na podstawie art. 11 ust. 4 ustawy z dnia ... o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …..) zarządza się, co następuje:

§ 1. Rozporządzenie określa progi uznania incydentu za poważny według rodzaju zdarzeń, w poszczególnych sektorach i podsektorach określonych w załączniku nr 1 do ustawy z dnia ... o krajowym systemie cyberbezpieczeństwa.

§ 2. Progi mają zastosowanie w odniesieniu do zdarzeń dotyczących systemów informacyjnych w procesie uznania incydentu za poważny przez operatora usługi kluczowej z danego sektora bądź podsektora, w przypadku wystąpienia co najmniej jednego z następujących zdarzeń:

1) usługa kluczowa świadczona przez operatora usług kluczowych była niedostępna dla co najmniej 100 000 użytkowników w czasie 1 godziny;
2) incydent doprowadził do poważnego obniżenia jakości świadczonej usługi kluczowej, które dotknęło ponad 100 000 użytkowników w Polsce i/lub innym państwie członkowskim Unii Europejskiej;
3) incydent spowodował ryzyko dla zdrowia lub życia ludzi;
4) incydent spowodował straty finansowe co najmniej jednego użytkownika przekraczające 1 000 000 zł.

§ 3. Czynniki charakterystyczne dla poszczególnych sektorów uznania incydentu za poważny określa załącznik do rozporządzenia.

[1)] Niniejsze rozporządzenie w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1).

§ 4. Rozporządzenie wchodzi w życie z dniem ……...

PREZES RADY MINISTRÓW

Załącznik
do rozporządzenia
Rady Ministrów
z dnia … (poz. …)

Sektor	Podsektor	Zdarzenie	Progi
Energia	Wydobycie kopalin		
	Energia elektryczna	Incydent dotyczący obciążenia obszarów synchronizowanych.	1. Energia nie dostarczona po rozłączeniu synchronizacji odpowiada od 1 do 10% szacowanego obciążenia operatora systemu przesyłowego bezpośrednio przed wystąpieniem incydentu. 2. Incydent trwa dłużej niż trzy minuty. 3. Rozłączenie synchronizacji jest większe niż 200 MW.
		Incydent dotyczący obciążenia.	Zmniejszenie obciążenia od 5 do 15% w czasie trwania incydentu, niezależnie od czasu trwania incydentu.
		Incydent dotyczący elementów sieci przesyłowej.	Końcowe wyłączenie samoczynne lub ręczne awaryjne rozłączenie sprzętu zasilającego znajdującego się na liście rezerwowej przeznaczonych na wypadek sytuacji wyjątkowych i wywołujące skutki w obszarze odpowiedzialności i/lub dla przesyłu transgranicznego.
		Incydent dotyczący zmniejszenia możliwości operacyjnych.	Operator systemu przesyłowego traci kontrolę nad systemami sterowania na dłużej niż 30 minut.
		Incydent dotyczący niezawodności oddzielenia od zasilania.	Incydent prowadzi do wydzielenia istotnych części od zasilania, w którego skład wchodzi co najmniej jeden obszar odpowiedzialności operatora systemu przesyłowego.
		Incydent dotyczący utraty kontroli nad systemami sterowania.	Operator systemu przesyłowego całkowicie utracił kontrolę nad systemami sterowania na dłużej niż 30 minut.
		Incydent blackoutu (przerwania dostawy energii elektrycznej) dla obszarów synchronizowanych.	Operator systemu przesyłowego: 1. Ogłosił blackout (przerwanie dostawy energii elektrycznej). 2. Utracił synchronizację na ponad 50% obszaru odpowiedzialności. 3. Miał całkowitą utratę napięcia w

			systemie na dłużej niż 3 minuty.
		Incydent blackoutu (przerwania dostawy energii elektrycznej) dla systemów wyizolowanych.	Utrata 70% synchronizacji w czasie incydentu lub całkowita utrata mocy.
	Ciepło	Incydent dotyczący wytwarzania ciepła.	
		Incydent dotyczący przesyłania ciepła.	
		Incydent dotyczący dystrybucji ciepła.	
		Incydent dotyczący obrotu ciepłem.	
	Ropa naftowa i Gaz	Incydent dotyczący przesyłu ropy naftowej, paliw ciekłych i gazu ziemnego rurociągami.	1. Nieplanowany wyciek ropy naftowej, gazu lub innych substancji niebezpiecznych, niezależnie od tego, czy doszło do zapłonu. 2. Incydent skutkuje niemożliwością prawidłowego dostarczania i przesyłu ropy naftowej i gazu ziemnego.
		Incydenty dotyczące produkcji, wydobywania, wytwarzania paliw ciekłych, magazynowania ropy naftowej, przeładunku ropy naftowej, magazynowania paliw ciekłych, przeładunku paliw ciekłych, obrotu paliwami ciekłymi i obrotu paliwami ciekłymi z zagranicą, wytwarzania paliw syntetycznych.	1. Znacząca utrata integralności, lub utrata ochrony przeciwko efektom eksplozji, lub utrata stacji utrzymania w przypadku instalacji mobilnych. 2. Incydent skutkuje zakłóceniem w produkcji, rafinacji, funkcjonowaniu urządzeń przetwarzających, magazynowaniu i przesyłaniu ropy naftowej.
		Incydenty dotyczące przedsiębiorstw zajmujących się wytwarzaniem paliw gazowych, przesyłaniem paliw gazowych, dystrybucją paliw gazowych, obrotem	1. Nieplanowany wyciek ropy naftowej, gazu lub innych substancji niebezpiecznych, niezależnie od tego, czy doszło do zapłonu, znacząca utrata integralności, lub utrata ochrony przeciwko efektom eksplozji, lub utrata stacji utrzymania w przypadku instalacji mobilnych.

		paliwami gazowymi i obrót gazem ziemnym z zagranicą, magazynowaniem paliw gazowych, skraplaniem i regazyfikacją LNG oraz sprowadzaniem i wyładunkiem LNG.	2. Incydent skutkuje niemożliwością prawidłowego dostarczania i przesyłu gazu ziemnego, a także zakłóceniem w produkcji, rafinacji, funkcjonowaniu urządzeń przetwarzających, magazynowaniu i przesyłaniu gazu ziemnego.
	Dostawy i usługi dla sektora energii	Incydent dotyczący dostaw systemów, maszyn, urządzeń, materiałów, surowców oraz świadczenia usług na rzecz sektora energii.	
		Incydent dotyczący utrzymywania rezerw strategicznych i zapasów ropy naftowej, produktów naftowych i gazu ziemnego.	
		Incydent dotyczący unieszkodliwiania odpadów promieniotwórczych.	
Transport	Transport lotniczy	Incydent dotyczący transportu lotniczego pasażerskiego.	
		Incydent dotyczący transport lotniczego towarów.	
		Incydent dotyczący działalności usługowej wspomagającej transport lotniczy.	
	Transport kolejowy	Incydenty dotyczące systemów informacyjnych zarządców infrastruktury kolejowej, przewoźników kolejowych i usług kolejowych.	1) kolizja pociągu z pojazdem szynowym; 2) kolizja pociągu z przeszkodą; 3) wykolejenie się pociągu; 4) pożar w pociągu; 5) awaria pociągu; 6) uszkodzenia torów lub trakcji; 7) awaria sygnalizacji; 8) awaria systemów ostrzegania – w wyniku których: a) doszło do zatrzymania ruchu pociągów na znacznym obszarze,

			b) lub liczba ofiar i rannych przekracza 100 osób; 9) wypadek z udziałem co najmniej jednego pojazdu szynowego transportującego niebezpieczne towary, w których doszło do uwolnienia substancji niebezpiecznych.
	Transport wodny	Incydent dotyczący armatorów morskich i śródlądowych transportu pasażerów i towarów.	1. Zniszczenie statku lub systemów informacyjnych kluczowych dla sterowania i funkcjonowania statku. 2. Utrata kontroli. 3. Uszkodzenie kadłuba. 4. Zalanie bądź zatopienie. 5. Kolizja. 6. Wywrócenie lub przechył. 7. Utrata kontroli.
		Incydent dotyczący organów zarządzających portami.	Niedostępność portu bądź ograniczona dostępność portu.
	Transport drogowy	Incydent dotyczący zarządzania drogami.	
		Incydent dotyczący Inteligentnych systemów transportowych.	
Bankowość i infrastruktura rynków finansowych		Incydent dotyczący funkcjonowania banków, instytucji kredytowych i infrastruktury rynków finansowych.	1. Wiedza o incydencie jest powszechnie dostępna i/lub mógł on spowodować istotną szkodę wizerunkową. 2. Szacowany finansowy wpływ incydentu przekracza 5 mln EUR lub 0,1% kapitału skapitalizowanego. 3. Incydent rozprzestrzenia się wewnętrznie aż do poziomu kierownika do spraw informatyzacji (bądź równoważnego stanowiska kierowniczego). 4. Incydent będzie prowadzić do naruszenia prawa bądź prawnych zobowiązań. 5. Incydent doprowadził do uruchomienia procedur zarządzania kryzysowego. 6. Incydent został zgłoszony do właściwego CSIRT lub policji.

		Incydent dotyczący transakcji.	Incydent obejmuje 25% płatności realizowanych przez dostawcę usług płatniczych (pod względem liczby transakcji) lub 5 mln EUR.
		Incydent dotyczący użytkowników usług płatniczych.	Incydent obejmuje 50 000 użytkowników lub 25% płatności realizowanych przez użytkowników.
Służba zdrowia			Incydentem dotkniętych zostało ponad 30% funkcjonalności usługi.
			Incydent dotknął ponad 100 użytkowników usługi i trwał ponad 4 godziny.
			Strata finansowa spowodowana incydentem jest większa niż 10 000 EUR.
Zaopatrzenie w wodę pitną i jej dystrybucja		Incydent dotyczący poboru wody.	
		Incydent dotyczący uzdatniania wody.	
		Incydent dotyczący dostarczania wody.	
Infrastruktura cyfrowa		Incydent dotyczący prowadzenia punktu wymiany ruchu internetowego (IXP) w Polsce.	1. Incydent doprowadził do braku dostępności usługi. 2. Incydent doprowadził do braku poufności usługi. 3. Incydent doprowadził do braku integralności usługi.
		Incydent dotyczący prowadzenia autorytatywnego serwera DNS.	1. Incydent doprowadził do braku dostępności usługi. 2. Incydent doprowadził do braku poufności usługi. 3. Incydent doprowadził do braku integralności usługi.
		Incydent dotyczący prowadzenia rejestru domeny najwyższego poziomu (TLD).	1. Incydent doprowadził do braku dostępności usługi. 2. Incydent doprowadził do braku poufności usługi. 3. Incydent doprowadził do braku integralności usługi.

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie delegacji art. 11 ust. 4 ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …) i określa progi uznania incydentu za poważny w odniesieniu do usługi kluczowej świadczonej przez operatora usługi kluczowej.

Rozporządzenie będzie wykorzystywane przez operatorów usług kluczowych w procesie zgłaszania i obsługi incydentu. Operatorzy będą zobowiązani do identyfikacji incydentu, jego rejestracji oraz klasyfikacji na podstawie progów uznawania incydentu za poważny. Określono progi, które będą wspólne dla wszystkich sektorów usług kluczowych wskazanych w załączniku nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa. Dotyczą one okresu przez jaki usługa kluczowa była niedostępna lub nastąpiło jej krytyczne obniżenie jakości, liczby użytkowników na których incydent miał wpływ, a także strat finansowych oraz oddziaływania na inne państwa członkowskie UE. Drugim rodzajem progów są progi sektorowe, charakterystyczne dla każdego sektora, a w niektórych przypadkach także dla podsektorów.

Rozporządzenie wskazuje rodzaj zdarzenia powodujący uznanie incydentu za poważny, natomiast klasyfikacja incydentów jest elementem procesu obsługi incydentu wykonywana przez operatorów usług kluczowych w oparciu o najlepsze praktyki z zakresu cyberbezpieczeństwa[2], oraz sektorowe wytyczne dotyczące zgłaszania incydentów, opracowywane zgodnie z ustawą przez organy właściwe we współpracy z CSIRT poziomu krajowego.

Podmioty wskazane jako operatorzy usług kluczowych będą w stanie skutecznie stosować progi określone w niniejszym rozporządzaniu, po spełnieniu wymogów, jakie ustawa o krajowym systemie cyberbezpieczeństwa nakłada na operatorów usług kluczowych. Ponadto w niektórych sektorach istnieją odrębne przepisy dotyczące ciągłości działania i analizy ryzyka, np. w ustawie z dnia 10 kwietnia 2017 r. – Prawo energetyczne (Dz. U. z 2018 r. poz. 755, 650, 685 i 771), ustawie z dnia 3 lipca 2002 r. – Prawo lotnicze (Dz. U. z 2017 r. poz. 959 i 1089 oraz z 2018 r. poz. 138 i 650), czy ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2017 r. poz. 1876, z późn. zm.)

---

[2] Np. ENISA: „Reference Incident Classification Taxonomy: Task Force Status and Way Forward”, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

Przy określaniu progów kierowano się najlepszymi międzynarodowymi praktykami prezentowanymi w materiałach Grupy Współpracy ustanowionej na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1), której to dyrektywy niniejsze rozporządzenie i ustawa o krajowym systemie cyberbezpieczeństwa stanowią transpozycję do polskiego porządku prawnego.

Założeniem projektodawcy jest wprowadzenie w rozporządzeniu wyłącznie wartości parametrycznych, natomiast potencjalne rodzaje incydentów byłyby określone przez organy właściwe zgodnie z art. 42 ust. 1 pkt 5 ustawy o krajowym systemie cyberbepieczeństwa w wytycznych sektorowych dotyczących zgłaszania incydentów[3].

Projektowane rozporządzenie wejdzie w życie w dniu wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa.

Przedmiot projektowanej regulacji jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2018 r. poz. 362).

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej oraz Europejskiemu Bankowi Centralnemu w celu uzyskania opinii, dokonania konsultacji lub uzgodnienia.

Projekt zostanie udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

---

[3] Dobrym przykładem jest tutaj „Common Taxonomy for the National Network of CSIRTs”, wydanym przez EC3.

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny	**Data sporządzenia** 19 kwietnia 2018 r.
Ministerstwo wiodące i ministerstwa współpracujące Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Karol Okoński, Podsekretarz Stanu w Ministerstwie Cyfryzacji	**Źródło:** Art. 11 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …)
Kontakt do opiekuna merytorycznego projektu Andrzej Szyszko, Departament Cyberbezpieczeństwa, Zastępca Dyrektora, tel. (22) 245 57 05, e-mail: andrzej.szyszko@mc.gov.pl	**Nr w wykazie prac legislacyjnych Rady Ministrów**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projektowane rozporządzenie stanowi wykonanie delegacji art. 11 ust. 4 ustawy z dnia ... o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. ...) i określa progi uznania incydentu za poważny w odniesieniu do usługi kluczowej świadczonej przez operatora usługi kluczowej. Rozporządzenie będzie wykorzystywane przez operatorów usług kluczowych w procesie klasyfikacji, zgłaszania i obsługi incydentu. Operatorzy będą zobowiązani do identyfikacji incydentu, jego rejestracji oraz klasyfikacji na podstawie progów uznawania incydentu za poważny. W projekcie rozporządzenia określono progi , które będą wspólne dla wszystkich sektorów usług kluczowych wskazanych w załączniku do ustawy o krajowym systemie cyberbezpieczeństwa. Dotyczą one okresu przez jaki usługa kluczowa była niedostępna lub nastąpiło jej krytyczne obniżenie jakości, liczy użytkowników na których incydent miał wpływ; strat finansowych oraz oddziaływania na inne państwa członkowskie UE. Drugim rodzajem progów są progi sektorowe, charakterystyczne dla każdego sektora, a w niektórych przypadkach także dla podsektorów.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Progi zostały określone przy wykorzystaniu projektu opracowania pt. "Reference document on Incident Notification for Operators of Essential Services" i załączników do tego dokumentu. Zostały one przygotowane przez grupę roboczą w ramach Grupy Współpracy, która została ustanowiona na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1), zwanej dalej „dyrektywą 2016/1148/UE”. Ustawa o krajowym systemie cyberbezpieczeństwa i rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny stanowią transpozycję dyrektywy 2016/1148/UE do polskiego porządku prawnego.

Ponadto w części dotyczącej progów horyzontalnych wykorzystano metodykę zastosowaną rozporządzeniu wykonawczym Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE)

2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48).

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Ustawa o krajowym systemie cyberbezpieczeństwa stanowiąca implementację dyrektywy 2016/1148/UE, jest w trakcie transpozycji w innych państwach członkowskich UE, podobnie jak i akty wykonawcze do ustawy implementujące zapisy dyrektywy 2016/1148/UE.
Za dokument referencyjny dla przedstawienia rozwiązań w innych państwach UE uznać można projekt opracowania przygotowanego w ramach prac grupy roboczej utworzonej decyzją Grupy Współpracy (instytucja utworzona na mocy dyrektywy 2016/1148/UE, w jej skład wchodzą przedstawiciele państw członkowskich) – "Reference document on Incident Notification for Operators of Essential Services" i załączników. Dokumenty te przedstawiają propozycje i rekomendacje dotyczące wyznaczania progów dla incydentów dotyczących sektorów i podsektorów wymienionych w załączniku II do dyrektywy 2016/1148/UE oraz odpowiadającemu mu załącznikowi nr 1 do ustawy o krajowym systemie cyberbezpieczeństwa: energia elektryczna, ropa naftowa i gaz, transport kolejowy, transport wodny, transport drogowy, bankowość i infrastruktura rynków finansowych, ochrona zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa).
Większość państw członkowskich wciąż prowadzi prace nad krajowymi przepisami wdrażającymi dyrektywę 2016/1148/UE.

Załączniki przedstawiają najlepsze praktyki dla poszczególnych sektorów i podsektorów, które są już obecnie stosowane, bądź wynikają z już istniejących regulacji dla poszczególnych sektorów, np. rozporządzenia 1093/2010/UE dotyczącego Europejskiego Nadzoru Bankowego czy dyrektywy 2015/2366/UE dotyczącej usług płatniczych dla sektora Bankowość i infrastruktura rynków finansowych oraz rozporządzenia 714/2009/UE w sprawie warunków dostępu do sieci w odniesieniu do transgranicznej wymiany energii elektrycznej dla podsektora Energia elektryczna.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Sektor energii, podsektor wydobycie kopalin,	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe wydobycia gazu ziemnego, ropy naftowej, węgla brunatnego, węgla kamiennego, pozostałych kopalin	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) (Dz. U. poz. 1885, z 2009 r. poz. 489 oraz z 2017 r. poz. 2440; 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego, 3) usługi z zakresu zarządu	Wyznaczeni operatorzy usług kluczowych będą zobowiązani klasyfikować i zgłaszać incydenty poważne na podstawie progów określonych rozporządzeniu.

		dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor energii, podsektor elektroenergetyczny	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe wytwarzania, przesyłania, dystrybucji, obrotu, przetwarzania, magazynowania energii elektrycznej oraz usługi systemowe, jakościowe i zarządzanie infrastrukturą energetyczną	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor energii, podsektor ciepło	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe wytwarzania, przesyłania, dystrybucji, obrotu ciepłem	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy	

		właściwe.	
Sektor energii, podsektor ropy naftowej	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe wytwarzania paliw ciekłych, przesyłania ropy naftowej, przesyłania paliw ciekłych, magazynowania ropy naftowej, przeładunku ropy naftowej, magazynowanie paliw ciekłych, przeładunek paliw ciekłych, obrót paliwami ciekłymi i obrót paliwami ciekłymi z zagranicą, wytwarzanie paliw syntetycznych	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor energii, podsektor gazu	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe wytwarzania, przesyłania, dystrybucji paliw gazowych, obrót paliwami gazowymi i obrót gazem ziemnym z zagranicą, magazynowanie paliw gazowych, skraplanie i regazyfikacja LNG oraz sprowadzanie i wyładunek	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor energii w zakresie dostaw i usług dla sektora energii oraz jednostki nadzorowane i podległe ministrowi właściwemu do spraw energii	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe dostawy systemów, maszyn,	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności	

	urządzeń, materiałów, surowców oraz świadczenie usług na rzecz sektora energii; badania naukowe, prace rozwojowe i wdrożenia w dziedzinie pozostałych nauk przyrodniczych i technicznych; utrzymywanie rezerw strategicznych i zapasów ropy naftowej, produktów naftowych i gazu ziemnego; unieszkodliwianie odpadów promieniotwórczych; poprawa bezpieczeństwa pracy i ochrony zdrowia górników, optymalne zagospodarowanie złóż kopalin oraz ograniczenie uciążliwości oddziaływania górnictwa na ludzi i środowisko.	usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor transportu, podsektor transport lotniczy	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe transport lotniczy pasażerski, transport lotniczy towarów, działalność usługowa wspomagająca transport lotniczy	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	

Sektor transportu, podsektor transport kolejowy	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe udostępnianie dróg kolejowych, prowadzenie ruchu kolejowego, transport kolejowy towarowy	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor transport, podsektor transport wodny (dotyczący transportu morskiego)	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe transport morski pasażerski, towarowy, działalność usługowa wspomagająca transport morski	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor transport, podsektor transport wodny (dotyczący transportu śródlądowego)	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe transport wodny śródlądowy pasażerski, towarowy;	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora	

	działalność usługowa wspomagająca transport śródlądowy	finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor transport, podsektor transport drogowy	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe zarządzanie drogami, inteligentne systemy transportowe	Szacunki oparte na załączniku do projektu ustawy oraz danych MI (jeden zarządca dróg krajowych, szesnastu zarządców dróg wojewódzkich, dwóch operatorów systemów ITS na poziomie krajowym i pięciu w miastach). Jest możliwe poszerzenie tej grupy o zarządców dróg powiatowych i gminnych, jednak nie były brane pod uwagę w szacunkach.	
Sektor bankowość i infrastruktura rynków finansowych	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe produkcja znaków pieniężnych i innych środków płatniczych; realizacja polityki kursowej; realizacja polityki pieniężnej; emisja papierów wartościowych; prowadzenie rejestru papierów wartościowych; agent emisji papierów wartościowych; przechowywanie i obróbka znaków pieniężnych; wypłata środków gwarantowanych	Szacunki oparte na załączniku do projektu ustawy oraz danych KNF (dwadzieścia największych banków, dziesięć największych banków spółdzielczych, Krajowa SKOK, dziesięć największych SKOK, dziesięć największych krajowych zakładów ubezpieczeń, dziesięć największych instytucji płatniczych, dwa banki państwowe, jedna giełda, PWPW, dwaj operatorzy systemu obrotu i jeden kontrahent centralny)	

	deponentom; udzielanie pomocy finansowej bankom; zaspokojenie roszczeń z tytułu obowiązkowych ubezpieczeń od odpowiedzialności cywilnej; rozliczenia międzybankowe; rozrachunek międzybankowy; zarządzanie rezerwami walutowymi; obsługa posiadaczy rachunków; prowadzenie rynku regulowanego lub innej działalności w zakresie organizowania obrotu instrumentami finansowymi oraz giełdy towarowej; organizowanie alternatywnego systemu obrotu instrumentami finansowymi; ewidencjonowanie oraz klasyfikacja informacji przekazywanych w ramach wykonywania przez spółki publiczne obowiązków informacyjnych i publikacyjnych; dystrybucja (przeliczanie i wypłata) świadczeń emerytalno-rentowych i zasiłków; przeciwdziałanie praniu pieniędzy oraz finansowaniu terroryzmu; zarządzanie długiem Skarbu Państwa, w tym finansowanie potrzeb pożyczkowych budżetu państwa; realizacja podstawowych		

	procesów związanych z obsługą budżetu państwa (planowanie, wykonywanie oraz sprawozdawczość); pobór podatków i należności pieniężnych; prowadzenie centralnego depozytu papierów wartościowych (w tym nadzorowanie zgodności wielkości emisji oraz obsługa realizacji zobowiązań emitentów wobec uprawnionych z papierów wartościowych); prowadzenie rozliczeń transakcji zawieranych w obrocie instrumentami finansowymi bądź zawartych na giełdach towarowych; prowadzenie rozrachunku transakcji zawieranych w obrocie instrumentami finansowymi bądź zawartych na giełdach towarowych; wypłata środków pieniężnych z bankomatu; acquiring; obsługa umów ubezpieczenia i wypłata odszkodowań lub świadczeń; usługi kredytowe dla MSP		
Sektor zaopatrzenie w wodę pitną i jej dystrybucja	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe pobór, uzdatnianie, dostarczanie wody	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu	

		dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor ochrona zdrowia	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego, 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt 1–3 przez organy właściwe.	
Sektor infrastruktura cyfrowa	Szacunki – OSR do ustawy o krajowym systemie cyberbezpieczeństwa obejmujące usługi kluczowe prowadzenie punktu wymiany ruchu internetowego (IXP) w Polsce, prowadzenie autorytatywnego serwera DNS, prowadzenie rejestru domeny najwyższego poziomu (TLD)	1) rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 2) rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; 3) usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD); 4) weryfikację pozycji pkt	

		1–3 przez organy właściwe.	

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Przeprowadzono ustalenia z ministerstwami, które uczestniczyły w pracach międzyresortowego zespołu roboczego ds. przygotowania ustawy (skład osobowy bazował na zespole ds. opracowania Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017–2022). Organy właściwe według ustawy o krajowym systemie cyberbezpieczeństwa (właściwe działowo ministerstwa) otrzymały od Ministerstwa Cyfryzacji wykaz usług kluczowych sporządzony w oparciu o rodzaje działalności usługowych wskazane w rozporządzeniu Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) które mogą być świadczone co najmniej przez przedsiębiorców bądź inne podmioty, objęte zakresem ustawy o krajowym systemie cyberbezpieczeństwa; rodzaje działalności usługowych dla sektora finansowego i infrastruktury rynków finansowych wynikające z ustawodawstwa unijnego; usługi z zakresu zarządu dróg, dla której nie ma określonej podklasy w rozporządzeniu w sprawie Polskiej Klasyfikacji Działalności. W następnym etapie odbywały się konsultacje z poszczególnymi organami właściwymi zweryfikowanych przez nich list powstałych w oparciu o ww. dokumenty.

6. Wpływ na sektor finansów publicznych

(ceny stałe z 2018 r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Fundusz Ubezpieczeń Społecznych												
Fundusz Pracy												
Narodowy Fundusz Zdrowia												
Wydatki ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem	-	-	-	-	-	-	-	-	-	-	-	-
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Fundusz Ubezpieczeń Społecznych												
Fundusz Pracy												
Narodowy Fundusz Zdrowia												

Źródła finansowania	Rozporządzenie nie generuje finansowych obciążeń.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym	-	-	-	-	-	-	-	-
W ujęciu niepieniężnym	Zidentyfikowani m.in. w oparciu o wykaz usług kluczowych jako operatorzy usług kluczowych	Operatorzy usług kluczowych będą zobowiązani do zgłaszania incydentów poważnych na podstawie progów określonych w rozporządzeniu.						
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

9. Wpływ na rynek pracy

Podmioty zidentyfikowane jako operatorzy usługi kluczowej będą zobowiązane klasyfikować i zgłaszać incydenty poważne, co wpłynie na wzrost zainteresowania usługami z zakresu cyberbezpieczeństwa oraz będzie się to wiązało potrzebą zatrudnienia specjalistów z zakresu cyberbezpieczeństwa.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☒ zdrowie
Omówienie wpływu	Wskazanie progów, jakie należy wziąć pod uwagę w celu uznania incydentu za poważny jest niezbędne dla umożliwienia realizowanie ustawowego obowiązku klasyfikowania i zgłaszania incydentów poważnych.	
11. Planowane wykonanie przepisów aktu prawnego		
Projektowane rozporządzenie wejdzie w życie z dniem……		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
Na podstawie rocznych sprawozdań dotyczących incydentów poważnych zgłaszanych przez operatorów usług kluczowych mających wpływ na ciągłość działania świadczonych przez nich usług kluczowych w Rzeczpospolitej Polskiej oraz ciągłość działania usług kluczowych w państwach członkowskich Unii Europejskiej, które minister właściwy do spraw informatyzacji będzie zobowiązany sporządzać na podstawie art. 45 ust. 1 pkt 3 lit. a ustawy o krajowym systemie cyberbezpieczeństwa.		
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		
-		

Projekt

R O Z P O R Z Ą D Z E N I E

M I N I S T R A C Y F R Y Z A C J I [1)]

z dnia

w sprawie warunków organizacyjnych i technicznych dla wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo oraz podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla operatorów usług kluczowych

Na podstawie art. 14 ust. 4 ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. ……) zarządza się, co następuje:

§ 1. Rozporządzenie określa warunki organizacyjne i techniczne dla odpowiedzialnych za cyberbezpieczeństwo wewnętrznych struktur organizacyjnych operatorów usług kluczowych oraz dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa usług kluczowych.

§ 2. Użyte w rozporządzeniu określenia oznaczają:

1) wewnętrzna struktura organizacyjna odpowiedzialna za cyberbezpieczeństwo – wewnętrzną komórkę organizacyjną przedsiębiorcy będącego operatorem usługi kluczowej albo przedsiębiorcę zależnego od operatora usługi kluczowej, świadczącego usługi w zakresie reagowania na incydenty wyłącznie na rzecz tego operatora;
2) podmiot świadczący usługi z zakresu cyberbezpieczeństwa – przedsiębiorcę niezależnego od operatora usługi kluczowej, świadczącego usługi w zakresie reagowania na incydenty dla jednego lub wielu operatorów usług kluczowych;
3) zespół reagowania – wewnętrzną strukturę organizacyjną operatora usługi kluczowej odpowiedzialną za cyberbezpieczeństwo lub podmiot świadczący usługi z zakresu cyberbezpieczeństwa;
4) usługa reagowania na incydenty – działania polegające na rejestrowaniu i obsłudze zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych.

[1)] Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 20 kwietnia 2018 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 761).

§ 3. Podmiot świadczący usługi z zakresu cyberbezpieczeństwa, w zakresie warunków organizacyjnych odnoszących się do tej działalności jest obowiązany:

1) posiadać i utrzymywać w aktualności system zarządzania bezpieczeństwem informacji spełniający wymagania Polskiej Normy PN ISO/IEC 27001;
2) zapewnić ciągłość działania usłudze reagowania na incydenty zgodnie z wymaganiami Polskiej Normy PN-EN ISO 22301;
3) upublicznić w języku polskim i angielskim deklarację swojej polityki działania w zakresie określonym dokumentem RFC 2350 publikowanym przez Internet Engineering Task Force (IETF);
4) zapewnić wsparcie operatorowi usługi kluczowej w trybie całodobowym przez wszystkie dni w roku, z czasem reakcji adekwatnym do charakteru usługi kluczowej;
5) dysponować personelem posiadającym umiejętności i doświadczenie w zakresie:
   a) identyfikowania zagrożeń w odniesieniu do systemów teleinformatycznych,
   b) analizowania oprogramowania szkodliwego i określania jego wpływu na system teleinformatyczny operatora usługi kluczowej,
   c) zabezpieczania śladów kryminalistycznych na potrzeby postępowań prowadzonych przez organy ścigania.

§ 4. Podmiot prowadzący działalność zespołu reagowania jest obowiązany dysponować pomieszczeniami, do których posiada wyłączne prawo użytkowania, wyposażonymi w zabezpieczenia techniczne adekwatne do przeprowadzonego szacowania ryzyka, w tym co najmniej:

1) system sygnalizacji włamania i napadu klasy 2 według Polskiej Normy PN-EN 50131-1;
2) system kontroli dostępu klasy 2 według Polskiej Normy PN-EN 60839-11-1, zapewniający osobie przyznanie dostępu do pomieszczenia poprzez rzecz posiadaną przez tą osobę oraz zapamiętanie zdarzenia przyznania dostępu danej osobie wraz z datą i czasem;
3) system wykrywania i sygnalizacji pożaru z powiadamianiem do centrum odbiorczego alarmów pożarowych;
4) szafy służące do przechowywania dokumentów oraz informatycznych nośników danych, o istotnym znaczeniu dla prowadzonej działalności, klasy S1 spełniającymi wymagania Polskiej Normy PN-EN 14450, chyba że inne przepisy wymagają wyższej klasy odporności szaf;

5) zewnętrzne drzwi wejściowe do pomieszczeń o klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627, wyposażone w zamki o klasie nie niższej niż klasa odporności drzwi;
6) wewnętrzne drzwi do pomieszczeń o klasie odporności RC2 według wymagań Polskiej Normy PN-EN 1627, wyposażone w zamki o klasie nie niższej niż klasa odporności drzwi;
7) okna o klasie odporności RC4 według wymagań Polskiej Normy PN-EN 1627, o ile na podstawie przeprowadzonego szacowania ryzyka dostęp do nich rodziłby nieakceptowalne ryzyko nieuprawnionego wejścia do pomieszczenia.

§ 5. W przypadku, gdy obiekt, w którym znajdują się pomieszczenia zespołu reagowania nie jest wyposażony w system, o którym mowa w § 4 pkt 3, dopuszcza się, po wykonaniu szacowania ryzyka i w braku przeciwwskazań wynikających z innych przepisów, wyposażenie tych pomieszczeń w czujki wykrywające pożar podłączone do systemu sygnalizacji włamania i napadu, o ile stacja monitorująca alarmy z tego systemu będzie w stanie ustalić przyczynę poszczególnych alarmów.

§ 6. Podmiot prowadzący zespół reagowania w zakresie spełnienia warunków technicznych dysponuje:
1) sprzętem komputerowym oraz specjalizowanymi narzędziami informatycznymi umożliwiającymi:
   a) automatyczne rejestrowanie zgłoszeń incydentów,
   b) analizę kodu oprogramowania uznanego za szkodliwe,
   c) badanie odporności systemów teleinformatycznych na przełamanie zabezpieczeń;
2) środkami łączności umożliwiającymi wymianę informacji z podmiotem, dla którego świadczy usługi oraz właściwym Zespołem Reagowania na Incydenty Bezpieczeństwa Komputerowego działającym na poziomie krajowym.

§ 7. Podmiot świadczący usługi z zakresu cyberbezpieczeństwa, o ile świadczy usługi dla operatora usługi kluczowej będącego jednocześnie operatorem infrastruktury krytycznej w rozumieniu art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566) jest obowiązany posiadać ważne świadectwo bezpieczeństwa przemysłowego, o którym mowa w art. 54 ust. 2 ustawy z dnia z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2018 r. poz. 412 i 650), stosownie do klauzuli informacji niejawnej, z dostępem do której wiązałaby się obsługa incydentu.

§ 8. Zespoły reagowania, które rozpoczęły świadczenie usług przed dniem wejścia w życie przepisów niniejszego rozporządzenia dostosują się do jego wymagań w terminie 6 miesięcy od dnia wejścia w życie rozporządzenia.

§ 9. Rozporządzenie wchodzi w życie z dniem ……

MINISTER CYFRYZACJI

UZASADNIENIE

Projekt rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo oraz podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla operatorów usług kluczowych stanowi wykonanie delegacji ustawowej, zamieszczonej w art. 14 ust. 4 ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …), określanej dalej jako „ustawa”.

Celem projektowanych przepisów jest określenie wymagań dla wewnętrznych struktur organizacyjnych operatorów usług kluczowych oraz podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla tych operatorów, mających wykonywać zadania nałożone na nich przez art. 8, art. 9, art. 10 ust. 1, art. 11 ust. 1 oraz art. 13 ust. 1 ustawy. Chodzi tu o obowiązkowe elementy schematu organizacyjnego mającego zapewnić cyberbezpieczeństwo systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych.

Adresatami projektu są przedsiębiorcy oraz podmioty publiczne w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), będący operatorami usług kluczowych w rozumieniu ustawy oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa.

Definiując zakres podmiotowy projektowanego aktu prawnego przyjęto w § 2 pkt 1, że wewnętrzna struktura organizacyjna operatora usługi kluczowej odpowiedzialna za cyberbezpieczeństwo może być wewnętrzną komórką organizacyjną przedsiębiorcy albo podmiotem zależnym od tego przedsiębiorcy, jednak z tym zastrzeżeniem, że usługi takiego podmiotu zależnego świadczone są wyłącznie na potrzeby przedsiębiorcy, od którego dany podmiot zależy. W przypadku gdyby podmiot zależny od przedsiębiorcy świadczył usługi bezpieczeństwa również dla innych podmiotów, podmiot taki staje się podmiotem świadczącym usługi cyberbezpieczeństwa w rozumieniu definicji zawartej w § 2 pkt 2. Każda ze wskazanych powyżej form organizacyjnych, w przypadku gdy celem jej istnienia jest świadczenie usług w zakresie reagowania na incydenty, staje się zespołem reagowania § 2 pkt 3 projektu.

Projektowany przepis § 3 pkt 1 określa, że podmiot świadczący usługi w zakresie cyberbezpieczeństwa dla operatorów usług kluczowych musi posiadać i utrzymywać

w aktualności system zarządzania bezpieczeństwem informacji. System zarządzania bezpieczeństwem informacji stanowi narzędzie zarządcze, pozwalające w uporządkowany sposób zapewnić bezpieczeństwo informacji w zakresie dostępności, integralności, poufności i autentyczności, z uwzględnieniem bezpieczeństwa osobowego, eksploatacji i architektury systemów oraz pozwala sprawować skuteczny nadzór nad bezpieczeństwem. Powszechnie uznaje się, że spełnienie przez system zarządzania bezpieczeństwem informacji wymagań międzynarodowej normy ISO/IEC 27001 jest najlepszym sposobem osiągnięcia celu w tym zakresie. Wspomniana międzynarodowa norma została wprowadzona do polskiego systemu prawa jako Polska Norma PN ISO/IEC 27001. Mając na względzie przepis art. 5 ust. 4 ustawy z dnia 12 września 2002 r. o normalizacji (Dz. U. 2015 r. poz. 1483) uprawnione jest bezpośrednie przywołanie tej normy w projektowanym rozporządzeniu. Każdorazowo zastosowanie będzie miała aktualna wersja normy.

Mając na względzie to, że Polska Norma PN ISO/IEC 27001 jedynie w sposób ogólny formułuje wymagania dotyczące zarządzania ciągłością działania, a także z uwagi na to, że zapewnienie przez podmiot świadczący usługi cyberbezpieczeństwa ciągłości wsparcia świadczonego dla operatora usługi kluczowej jest istotnym elementem zapewnienia bezpieczeństwa samej usługi kluczowej, w § 3 pkt 2 projektu przywołano wymagania zawarte w Polskiej Normie PN-EN ISO 22301, która uściśla wymagania dotyczące zapewnienia ciągłości działania.

Dobrą praktyką podmiotów świadczących usługi reagowania na incydenty jest upublicznianie deklaracji polityki swojego działania. Powszechnie przyjęto, że deklaracja taka opracowywana jest zgodnie z wymaganiami określonymi przez dokument RFC 2350 opracowany przez organizację Internet Engineering Task Force, który to dokument jest dostępny w sieci Internet, na witrynie pod adresem https://www.ietf.org/rfc/rfc2350.txt. Również dobrą praktyką jest to, aby tekst deklaracji dostępny był nie tylko w języku narodowym, ale również w języku angielskim, wobec czego wymóg takiej deklaracji zawarty został w § 3 pkt 3.

Z uwagi na to, że zwykle usługi kluczowe świadczone są w systemie całodobowym, przez wszystkie dni w roku, operator takiej usługi musi mieć wsparcie w taki samym układzie czasowym, co zostało wskazane w § 3 pkt 4 projektu.

Niezbędnym elementem sprawnego funkcjonowania usług wsparcia dla operatorów usług kluczowych w zakresie cyberbezpieczeństwa jest dysponowanie przez podmiot

zapewniający te usługi personelem o odpowiednich kwalifikacjach. Wymagane kalifikacje, niezbędne do właściwego wykonywania przez personel podmiotu zadań z zakresu usług wsparcia, wskazane zostały w § 3 pkt 5.

Podmiot prowadzący działalność zespołu reagowania musi zapewnić bezpieczeństwo fizyczne i środowiskowe dla lokalizacji, w której świadczone są usługi. Służą temu wymagania sformułowane w § 4. Na wymagania te składają się zarówno wymagania dotyczące bezpieczeństwa prawnego jak i wymagania dotyczące zabezpieczeń technicznych. Mając na względzie to, że wymagania dotyczące systemów zabezpieczenia technicznego znajdują odzwierciedlenie w polskim systemie normatywnym uzasadnione jest przywoływanie odpowiednich Polskich Norm w treści § 4. Jednocześnie, aby uniknąć nadmiernych obciążeń nakładanych przepisami prawa na podmiot świadczący usługi bezpieczeństwa, proponowany jest w § 5 zapis dopuszczający, w uzasadnionych przypadkach, odstępstwo od konieczności posiadania systemu sygnalizacji pożaru.

Przepisy § 6 określają minimalne wymagania, jakie podmiot świadczący usługi reagowania na incydenty musi spełnić w zakresie posiadanego potencjału technicznego.

Podmiot świadczący usługi z zakresu cyberbezpieczeństwa na rzecz operatora usługi kluczowej, który jednocześnie jest operatorem infrastruktury krytycznej w rozumieniu art. 3 pkt 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566), musi posiadać uprawnienie do przetwarzania informacji niejawnych i wymaganie takie określone zostało w § 7. W przypadku wewnętrznej struktury organizacyjnej odpowiedzialnej za cyberbezpieczeństwo zastosowanie mają przepisy ustawy o ochronie informacji niejawnych, które normują przetwarzanie informacji niejawnych w danym podmiocie, wobec czego nie jest konieczne ich dookreślanie w projektowanym rozporządzeniu.

W przypadku podmiotów, które rozpoczęły swoją działalność przed wejściem w życie projektowanego rozporządzenia wprowadza się sześciomiesięczny okres przejściowy na dostosowanie się do jego przepisów.

Mając na względzie przepis art. 19 ust. 1 dyrektywy Parlamentu Europejskiego i Rady UE 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa NIS) (Dz. Urz. UE L Nr 194, str. 1) dopuszczalne jest odwoływanie się do stosowania

europejskich lub uznanych międzynarodowo norm i specyfikacji mających znaczenie dla bezpieczeństwa sieci i systemów informatycznych.

Proponuje się, aby rozporządzenie weszło w życie jednocześnie z wejściem w życie ustawy upoważniającej.

Rozporządzenie podlega uproszczonej notyfikacji w trybie przepisu § 8 ust. 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. z 2002 r. poz. 2039 oraz z 2004 r. poz. 597)

Projekt został udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Nazwa projektu Projekt rozporządzenia Ministra Cyfryzacji w sprawie warunków organizacyjnych i technicznych dla wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo oraz podmiotów świadczących usługi z zakresu cyberbezpieczeństwa dla operatorów usług kluczowych **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **Kontakt do opiekuna merytorycznego projektu**	**Data sporządzenia** **Źródło:** Art. 14 ust. 4 ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. ...) **Nr w wykazie prac …….**

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Na mocy art. 8, art. 9, art. 10 ust. 1, art. 11 ust. 1 oraz art. 13 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa na operatorów usług kluczowych nałożono obowiązki związane z wdrożeniem i zapewnieniem właściwego funkcjonowania systemu zarządzania bezpieczeństwem w systemach informacyjnych, wykorzystywanych do świadczenia usług kluczowych. Dla wykonania tych zadań każdy operator winien powołać wewnętrzne struktury odpowiedzialne za cyberbezpieczeństwo lub zawrzeć umowę z podmiotem świadczącym usługi z tego zakresu. Projektowane rozporządzenie ma określać wymagania, które powinny spełnić te struktury bądź podmioty, w celu właściwej i skutecznej realizacji zadań z zakresu cyberbezpieczeństwa.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Rozwiązaniem problemu jest opracowanie stosownych przepisów, zgodnie z upoważnieniem zamieszczonym w art. 14 ust. 4 ustawy o krajowym systemie cyberbezpieczeństwa.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Nie dotyczy.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze elektroenergetycznym	20	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (OSP, pięciu największych OSD dla gospodarstw domowych, dziewięciu największych OSD dla przedsiębiorców, pięciu największych sprzedawców prądu)	Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze elektroenergetycznym
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze ropy naftowej	4	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (OSP oraz czterej najwięksi przedsiębiorcy posiadający koncesję na dystrybucję, wytwarzanie, magazynowanie lub przeładunek paliw ciekłych oraz na obrót paliwami ciekłymi)	Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze ropy naftowej
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze gazu	22	Szacunki oparte na załączniku do projektu ustawy oraz danych URE (OSP, OSD, przedsiębiorcy dostarczający	Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze gazu

		lub magazynujący gaz lub gaz ziemny oraz dziesięć największych przedsiębiorstw gazowych w rozumieniu art. 2 pkt 1 dyrektywy 2009/73/WE)	
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu lotniczego	28	Szacunki oparte na załączniku do projektu ustawy oraz danych ULC (jeden przewoźnik lotniczy, zarządzający ośmioma największymi portami lotniczymi, pięć podmiotów obsługujących urządzenia pomocnicze znajdujące się w portach lotniczych oraz służba kontroli ruchu lotniczego)	Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu lotniczego
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu kolejowego	10	Szacunki oparte na załączniku do projektu ustawy oraz danych UTK (trzech największych zarządców infrastruktury kolejowej, czterech największych przewoźników kolejowych osobowych oraz trzech największych przewoźników kolejowych towarowych). Nie wzięto pod uwagę liczby operatorów infrastruktury usługowej ze względu na fakt, że rejestr obiektów infrastruktury usługowej zostanie utworzony przez Prezesa UTK do 30 czerwca 2018 r.	Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu kolejowego

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W ramach konsultacji i opiniowania projekt zostanie przesłany do:

1) Prezes Urzędu Komunikacji Elektronicznej,
2) Prezes Urzędu Ochrony Konkurencji i Konsumentów,
3) Generalnego Inspektora Ochrony Danych Osobowych,
4) Prezesa Głównego Urzędu Statystycznego,
5) Polskiej Izby Informatyki i Telekomunikacji,
6) Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji,
7) Polskiej Izby Komunikacji Elektronicznej,
8) Krajowej Izby Gospodarczej,
9) Krajowej Izby Komunikacji Ethernetowej,
10) Polskiej Izby Radiodyfuzji Cyfrowej,
11) Polskiej Izby Handlu,
12) Fundacji Bezpieczna Cyberprzestrzeń,
13) Polskiego Towarzystwa Informatycznego,
14) Fundacji Nowoczesna Polska,
15) Fundacji Projekt Polska,
16) Internet Society Poland,

17) Stowarzyszenia Inżynierów Telekomunikacji,
18) Fundacji Panoptykon,
19) Rady Dialogu Społecznego,
20) Business Centre Club – Związku Pracodawców,
21) Niezależnego Samorządowego Związku Zawodowego „Solidarność”,
22) Ogólnopolskiego Porozumienia Związków Zawodowych,
23) Forum Związków Zawodowych,
24) Pracodawców Rzeczypospolitej Polskiej,
25) Konfederacji Lewiatan,
26) Związku Przedsiębiorców i Pracodawców,
27) Związku Rzemiosła Polskiego,
28) Związku Pracodawców Mediów Publicznych,
29) Związku Pracodawców Branży Internetowej IAB Polska,
30) Federacji Związków Zawodowych Pracowników Telekomunikacji,
31) Federacji Konsumentów.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt został udostępniony na stronie podmiotowej Biuletynu Informacji Publicznej MC oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0–10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	0	0	0	0	0	0	0
	sektor mikro-, małych i średnich przedsiębiorstw	0	0	0	0	0	0	0
	rodzina, obywatele oraz gospodarstwa domowe	0	0	0	0	0	0	0
W ujęciu niepieniężnym	duże przedsiębiorstwa	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w rozporządzeniu.						
	sektor mikro-, małych i średnich przedsiębiorstw	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w rozporządzeniu.						
	rodzina, obywatele oraz gospodarstwa domowe	Rodziny, obywatele, gospodarstwa domowe – regulacje zamieszczone w rozporządzeniu przyczynią się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele.						
Niemierzalne	-	Nie dotyczy.						
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☒ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

9. Wpływ na rynek pracy

Pozytywny – przepisy przyczynią się do wzrostu zatrudnienia w obszarze cyberbezpieczeństwa.

10. Wpływ na pozostałe obszary		
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Przepisy rozporządzenia przyczynią się do zwiększenia poziomu cyberbezpieczeństwa, co będzie miało pozytywny wpływ na przedsiębiorców i obywateli.	
11. Planowane wykonanie przepisów aktu prawnego		
Po upływie okresów przewidzianych na wprowadzenie odpowiednich rozwiązań (vacatio legis) bądź dostosowanie istniejących przez adresatów aktu.		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
100% operatorów ma wdrożone odpowiednie rozwiązania, po roku od wejścia w życie przepisów.		
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		
–		

Projekt

R O Z P O R Z Ą D Z E N I E

M I N I S T R A C Y F R Y Z A C J I [1)]

z dnia

w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu

Na podstawie art. 15 ust. 8 ustawy z dnia ... o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. ...) zarządza się, co następuje:

§ 1. Rozporządzenie określa wykaz certyfikatów uprawniających do przeprowadzenia audytu w rozumieniu art. 15 ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa, stanowiący załącznik do rozporządzenia.

§ 2. Rozporządzenie wchodzi w życie z dniem …

MINISTER CYFRYZACJI

[1)] Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 20 kwietnia 2018 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 761)

Załącznik
do rozporządzenia
Ministra Cyfryzacji
z dnia ….. (poz. ….)

W Y K A Z C E R T Y F I K A T Ó W U P R A W N I A J Ą C Y C H D O P R Z E P R O W A D Z E N I A A U D Y T U

1) Certified Internal Auditor (CIA);
2) Certified Information System Auditor (CISA);
3) Certified Information Security Manager (CISM);
4) Certified in Risk and Information Systems Control (CRISC);
5) Certified in the Governance of Enterprise IT (CGEIT);
6) Certified Information Systems Security Professional (CISSP);
7) Systems Security Certified Practitioner (SSCP);
8) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN ISO/IEC 27001;
9) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN ISO 22301.

UZASADNIENIE

Projekt rozporządzenia Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu został przygotowany na podstawie delegacji ustawowej, zamieszczonej w art. 15 ust. 8 projektu ustawy o krajowym systemie cyberbezpieczeństwa, określanej dalej jako „ustawa”.

Celem projektowanych przepisów jest określenie wymagań uprawniających do przeprowadzania audytu bezpieczeństwa u Operatora usługi kluczowej. Wymienione certyfikaty swoimi wymaganiami uwzględniają zakres wiedzy specjalistycznej od osób się nimi legitymującymi. Obowiązek przeprowadzania audytu określony jest w art. 15 ust. 1 ustawy i powinien odbywać się co najmniej raz na dwa lata.

Projektując rozporządzenie wzięto pod uwagę następujące uznane certyfikaty:

1. Certified Internal Auditor (CIA), który jest międzynarodowym certyfikatem wydawanym przez Instytut Audytorów Wewnętrznych (Institute of Internal Auditors, IIA). Certyfikat CIA potwierdza standardy i kompetencje zawodowe audytorów wewnętrznych, a egzamin sprawdza wiedzę, umiejętności i kwalifikacje niezbędne do wykonywania zawodu audytora wewnętrznego.
2. Certified Information System Auditor (CISA), który jest certyfikatem wydawanym przez Stowarzyszenie ds. Audytu i Kontroli Systemów Informatycznych (Information Systems Audit and Control Association, ISACA), przeznaczonym dla osób odpowiedzialnych za zapewnienie bezpieczeństwa IT organizacji oraz monitorowanie, zarządzanie i ochronę systemów biznesowych. Certyfikat CISA jest uznawanym na całym świecie standardem gwarantującym odpowiednią wiedzę i umiejętności audytorów IT w zakresie oceny luk w zabezpieczeniach i wdrażania mechanizmów kontrolnych w przedsiębiorstwach.
3. Certified Information Security Manager (CISM), który jest certyfikatem w zakresie zarządzania bezpieczeństwem informacji, wydawanym przez Stowarzyszenie ds. Audytu i Kontroli Systemów Informatycznych (Information Systems Audit and Control Association, ISACA). Celem certyfikacji jest upowszechnienie wspólnego zasobu wiedzy dla osób zarządzających bezpieczeństwem informacji. CISM koncentruje się na zarządzaniu ryzykiem jako podstawą bezpieczeństwa informacji. Dotyczy również szerszych zagadnień, takich jak zarządzanie bezpieczeństwem informacji, a także kwestii

praktycznych, takich jak zarządzanie programami w zakresie bezpieczeństwa informacji i zarządzanie incydentami bezpieczeństwa.

4. Certified in Risk and Information Systems Control (CRISC), który jest certyfikatem przeznaczonym dla osób zajmujących się problematyką IT i zarządzaniem ryzkiem w przedsiębiorstwach. Wydawanie certyfikatów jest akredytowane przez instytucję ustalającą normy techniczne obowiązujące w USA - American National Standards Institute (ANSI) pod oznaczeniem ISO/IEC 17024:2012. Norma ta dotyczy ogólnych wymagań dla jednostek certyfikujących osoby oraz zawiera zasady i wymagania dotyczące jednostki certyfikującej osoby w odniesieniu do specyficznych wymagań, łącznie z opracowywaniem i utrzymywaniem programu certyfikacji osób.

5. Certified in the Governance of Enterprise IT (CGEIT), który jest certyfikatem przeznaczonym dla osób zajmujących się kwestiami IT w przedsiębiorstwie, a także osób odpowiedzialnych za doradztwo związane z IT. Gwarantuje on wiedzę, umiejętności i praktyczne doświadczanie osób go posiadających w zakresie testowania, sprawdzania poprawności i poświadczania w obszarze zarządzania IT.

   Za rozwój, utrzymanie, testowanie i monitorowanie odpowiada Stowarzyszenie ds. Audytu i Kontroli Systemów Informatycznych (Information Systems Audit and Control Association, ISACA).

6. Certified Information Systems Security Professional (CISSP), który jest certyfikatem gwarantującym niezależne i obiektywne świadectwo eksperckie w dziedzinie bezpieczeństwa teleinformatycznego. Certyfikat spełnia standard ISO 17024:2003 oraz akredytowany jest przez ANSI (American National Standards Institute).

7. Systems Security Certified Practitioner (SSCP), który jest certyfikatem dla osób zajmujących się bezpieczeństwem IT. Jego uzyskanie potwierdza zdolność wdrażania, monitorowania i administrowania infrastrukturą IT w zgodności polityką bezpieczeństwa informatycznego i procedurami, które zapewniają poufność, integralność i dostępność danych.

8. Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN ISO/IEC 27001. Niniejsza międzynarodowa norma określa wymagania dotyczące ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu zarządzania bezpieczeństwem informacji w odniesieniu do organizacji. Norma obejmuje

również wymagania dotyczące szacowania i postępowania z ryzykiem dotyczącym bezpieczeństwa informacji, dostosowanych do potrzeb organizacji. Wymogi określone w niniejszej normie są ogólne i mają zastosowanie do wszystkich organizacji, niezależnie od typu, wielkości i charakteru.

9. Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN ISO 22301. Niniejsza norma określa wymagania dotyczące planowania, ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i ciągłego doskonalenia udokumentowanego systemu zarządzania, aby zmniejszyć prawdopodobieństwo wystąpienia uciążliwych incydentów, przygotować się na ich wystąpienia, odpowiedzieć na ich działanie i wyjść z kryzysu gdy się pojawiają.

Projektowane rozporządzenie wejdzie w życie w dniu wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa.

Przedmiot projektowanej regulacji jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2018 r. poz. 362).

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej oraz Europejskiemu Bankowi Centralnemu w celu uzyskania opinii, dokonania konsultacji lub uzgodnienia.

Projekt zostanie udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Nazwa projektu Rozporządzenie Ministra Cyfryzacji w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Podsekretarz Stanu – Karol Okoński **Kontakt do opiekuna merytorycznego projektu** Andrzej Szyszko, Departament Cyberbezpieczeństwa, Zastepca Dyrektora, tel. (22) 245 57 05, e-mail: andrzej.szyszko@mc.gov.pl	**Data sporządzenia** 19 kwietnia 2018 r. **Źródło:** art. 15 ust. 8 ustawy z dnia ……. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …) **Nr w wykazie prac legislacyjnych Rady Ministrów** XXX

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W związku z regulacją zawartą w art. 15 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa, która normuje obowiązek operatora usługi kluczowej do przeprowadzania, co najmniej raz na dwa lata, audytu bezpieczeństwa systemów informacyjnych, wykorzystywanych do świadczenia usługi kluczowej, zwany dalej „audytem", powstała konieczność przeprowadzania audytu przez osoby posiadające certyfikaty, które zakresem swojego programu certyfikacyjnego dają rękojmię właściwego przeprowadzenia audytu.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Określenie właściwych certyfikatów:

1) Certified Internal Auditor (CIA).
2) Certified Information System Auditor (CISA).
3) Certified Information Security Manager (CISM).
4) Certified in Risk and Information Systems Control (CRISC).
5) Certified in the Governance of Enterprise IT (CGEIT).
6) Certified Information Systems Security Professional (CISSP).
7) Systems Security Certified Practitioner (SSCP).
8) Certyfikat audytora wiodącego systemu zarządzania bezpieczeństwem informacji według normy PN ISO/IEC 27001.
9) Certyfikat audytora wiodącego systemu zarządzania ciągłością działania PN ISO 22301.

Wymienione wyżej rozwiązania powinny w sposób skuteczny i kompleksowy zapewnić właściwe przeprowadzenie audytu.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Ze względu na szczegółowość projektowanej regulacji, odstąpiono od przeprowadzenia analiz prawnoporównawczych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze elektroenergetycznym	20	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych URE (OSP, pięciu największych OSD dla gospodarstw domowych, dziewięciu największych OSD dla przedsiębiorców, pięciu największych sprzedawców prądu).	Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze elektroenergetycznym
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze ropy naftowej	4	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych URE (OSP oraz czterej najwięksi przedsiębiorcy posiadający koncesję na dystrybucję, wytwarzanie,	Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze ropy naftowej

		magazynowanie lub przeładunek paliw ciekłych oraz na obrót paliwami ciekłymi).	
Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze gazu	22	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych URE (OSP, OSD, przedsiębiorcy dostarczający lub magazynujący gaz lub gaz ziemny oraz dziesięć największych przedsiębiorstw gazowych w rozumieniu art. 2 pkt 1 dyrektywy 2009/73/WE).	Podmioty świadczące usługi kluczowe w sektorze energetycznym w podsektorze gazu
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu lotniczego	28	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych ULC (jeden przewoźnik lotniczy, zarządzający ośmioma największymi portami lotniczymi, pięć podmiotów obsługujących urządzenia pomocnicze znajdujące się w portach lotniczych oraz służba kontroli ruchu lotniczego).	Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu lotniczego
Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu kolejowego	10	Szacunki oparte na załączniku nr 1 do projektu ustawy oraz danych UTK (trzech największych zarządców infrastruktury kolejowej, czterech największych przewoźników kolejowych osobowych oraz trzech największych przewoźników kolejowych towarowych). Nie wzięto pod uwagę liczby operatorów infrastruktury usługowej ze względu na fakt, że rejestr obiektów infrastruktury usługowej zostanie utworzony przez Prezesa UTK do 30 czerwca 2018 r.	Podmioty świadczące usługi kluczowe w sektorze transportu w podsektorze transportu kolejowego

Projekt rozporządzenia oddziałuje na przedsiębiorców, jak również na osoby fizyczne, które będą chciały świadczyć usługi w zakresie wykonywania audytów. Koszty uzyskania uprawnień wynikających z rozporządzenia należy traktować jako zwykłe koszty związane z prowadzenia działalności gospodarczej lub zawodowej.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W ramach konsultacji i opiniowania projekt zostanie przesłany do:
1) Prezes Urzędu Komunikacji Elektronicznej,
2) Prezes Urzędu Ochrony Konkurencji i Konsumentów,
3) Generalnego Inspektora Ochrony Danych Osobowych,
4) Prezesa Głównego Urzędu Statystycznego,
5) Polskiej Izby Informatyki i Telekomunikacji,
6) Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji,
7) Polskiej Izby Komunikacji Elektronicznej,
8) Krajowej Izby Gospodarczej,
9) Krajowej Izby Komunikacji Ethernetowej,
10) Polskiej Izby Radiodyfuzji Cyfrowej,

11) Polskiej Izby Handlu,
12) Fundacji Bezpieczna Cyberprzestrzeń,
13) Polskiego Towarzystwa Informatycznego,
14) Fundacji Nowoczesna Polska,
15) Fundacji Projekt Polska,
16) Internet Society Poland,
17) Stowarzyszenia Inżynierów Telekomunikacji,
18) Fundacji Panoptykon,
19) Rady Dialogu Społecznego,
20) Business Centre Club – Związku Pracodawców,
21) Niezależnego Samorządowego Związku Zawodowego „Solidarność”,
22) Ogólnopolskiego Porozumienia Związków Zawodowych,
23) Forum Związków Zawodowych,
24) Pracodawców Rzeczypospolitej Polskiej,
25) Konfederacji Lewiatan,
26) Związku Przedsiębiorców i Pracodawców,
27) Związku Rzemiosła Polskiego,
28) Związku Pracodawców Mediów Publicznych,
29) Związku Pracodawców Branży Internetowej IAB Polska,
30) Federacji Związków Zawodowych Pracowników Telekomunikacji,
31) Federacji Konsumentów.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz.U. z 2017 r. poz. 248) projekt zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny oraz na stronach internetowych Ministerstwa Cyfryzacji.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)												

Źródła finansowania	Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0–10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …. r.)								
	sektor przedsiębiorstw – przedsiębiorcy, będący operatorami usług kluczowych – szacunkowy koszt dla przedsiębiorcy							
	sektor przedsiębiorstw – przedsiębiorcy, którzy chcą świadczyć usługi z zakresu reagowania na incydenty – szacunkowy koszt dla przedsiębiorcy							
W ujęciu niepieniężnym	duże przedsiębiorstwa	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w rozporządzeniu.						
	sektor mikro-, małych i średnich przedsiębiorstw	Operatorzy usług kluczowych będą zobowiązani do spełnienia wymogów określonych w rozporządzeniu.						
	rodzina, obywatele oraz gospodarstwa domowe	Rodziny, obywatele, gospodarstwa domowe – regulacje zamieszczone w rozporządzeniu przyczynią się do zwiększenia bezpieczeństwa usług, z których korzystają wszyscy obywatele.						
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń								

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☒ nie dotyczy

9. Wpływ na rynek pracy

Pozytywny – przepisy przyczynią się do wzrostu zatrudnienia w obszarze cyberbezpieczeństwa.

10. Wpływ na pozostałe obszary		
☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie
Omówienie wpływu	Przepisy rozporządzenia przyczynią się do zwiększenia poziomu cyberbezpieczeństwa, co będzie miało pozytywny wpływ na przedsiębiorców i obywateli.	
11. Planowane wykonanie przepisów aktu prawnego		
Po upływie okresów przewidzianych na wprowadzenie odpowiednich rozwiązań (vacatio legis) bądź dostosowanie istniejących przez adresatów aktu.		
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?		
Nie jest planowana ewaluacja.		
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)		

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa

Na podstawie art. 66 ust. 9 ustawy z dnia ... o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. ...) zarządza się, co następuje:

§ 1. 1. Kolegium do Spraw Cyberbezpieczeństwa, zwane dalej „Kolegium", rozpatruje sprawy, należące do jego właściwości, na posiedzeniach zwołanych przez Przewodniczącego Kolegium, w terminach określonych w planie pracy Kolegium.

2. Przewodniczący Kolegium może, z własnej inicjatywy lub na wniosek członka Kolegium albo osoby, o której mowa w art. 66 ust. 1 ustawy z dnia … o krajowym systemie cyberbezpieczeństwa, zwanej dalej „ustawą", zwołać posiedzenie Kolegium w innym, niż określony w planie pracy Kolegium, terminie.

§ 2. 1. Zawiadomienie o terminie posiedzenia Kolegium, wraz z porządkiem obrad, powinno być doręczone przez sekretarza Kolegium uczestnikom posiedzenia najpóźniej na pięć dni przed wyznaczonym terminem posiedzenia.

2. W przypadku zwołania posiedzenia, o którym mowa w § 1 ust. 2, zawiadomienie o terminie posiedzenia Kolegium, wraz z porządkiem obrad, powinno być doręczone uczestnikom posiedzenia niezwłocznie po podjęciu przez Przewodniczącego Kolegium decyzji o zwołaniu posiedzenia.

3. Przewodniczący Kolegium może w trakcie posiedzenia wprowadzić do porządku obrad sprawy nieprzewidziane w tym porządku.

§ 3. 1. Posiedzenia Kolegium mają charakter niejawny.

2. Przewodniczący Kolegium przed posiedzeniem Kolegium określa, które z osób wymienionych w art. 66 ust. 5 pkt 2 ustawy uczestniczą w całości lub określonej części posiedzenia.

§ 4. Szczegółową organizację działania Kolegium określa regulamin pracy uchwalony przez Kolegium i zatwierdzony przez Przewodniczącego Kolegium.

§ 5. 1. W szczególnie uzasadnionych przypadkach, za zgodą Przewodniczącego Kolegium, w posiedzeniu Kolegium może brać udział osoba wskazana przez osobę, o której mowa w art. 66 ust. 4 ustawy, zastępująca ją w pełnieniu obowiązków na stanowisku, którego zajmowanie uprawnia go do udziału w posiedzeniach Kolegium.

2. Osoby, o których mowa w art. 66 ust. 1 i ust. 4 ustawy, mogą uczestniczyć w posiedzeniu Kolegium pod warunkiem spełnienia przez te osoby wymagań w zakresie dostępu do informacji niejawnych.

§ 6. 1. Kolegium wyraża swoje stanowisko w formie ocen lub opinii.

2. Ustalenia stanowiska Kolegium dokonuje się w drodze uzgodnienia. W przypadku gdy osiągnięcie uzgodnienia nie jest możliwe, Przewodniczący Kolegium przeprowadza głosowanie. O treści stanowiska decyduje większość głosów, a w razie równej liczby głosów rozstrzyga głos Przewodniczącego.

3. Członkowie Kolegium mogą zgłosić do protokołu zdanie odrębne w stosunku do przyjętego stanowiska.

4. W sprawach wymagających decyzji Rady Ministrów Przewodniczący Kolegium przedstawia Radzie Ministrów oceny lub opinie Kolegium.

§ 7. 1. Z posiedzenia Kolegium sporządza się protokół oraz pełny zapis jego przebiegu, z zachowaniem przepisów o ochronie informacji niejawnych.

2. Protokół powinien zawierać w szczególności:

1) porządek obrad;
2) listę obecności osób biorących udział w posiedzeniu;
3) wnioski osób biorących udział w posiedzeniu;
4) przyjęte przez Kolegium oceny lub opinie;
5) dokumenty stanowiące przedmiot obrad;
6) stenogram zawierający pełny zapis przebiegu posiedzenia Kolegium.

3. Protokół podpisuje Przewodniczący Kolegium i sekretarz Kolegium.

4. W terminie siedmiu dni od dnia podpisania protokołu, osoby biorące udział w posiedzeniu mogą wnieść sprostowanie do zamieszczonych w protokole sformułowań własnych wypowiedzi i wniosków. Sprostowanie, podpisane przez osobę, która je wniosła, umieszcza się w aneksie do protokołu.

§ 8. 1. W uzasadnionych przypadkach Przewodniczący Kolegium może powołać, w ramach Kolegium, zespół o charakterze doraźnym, którego zadaniem będzie szczegółowe rozpatrzenie danej sprawy.

2. Przewodniczący Kolegium określa skład zespołu, o którym mowa w ust. 1, oraz zakres jego zadań.

§ 9 1. Sekretarz Kolegium zapewnia obsługę organizacyjną i techniczną prac Kolegium oraz wykonywanie zadań wynikających z wyrażonych przez Kolegium stanowisk i decyzji Przewodniczącego Kolegium.

2. Do obowiązków sekretarza Kolegium należy:

1) przygotowanie projektów planów pracy Kolegium;
2) koordynacja przygotowania oraz dostarczenia materiałów i projektów dokumentów przeznaczonych do rozpatrzenia przez Kolegium;
3) informowanie członków Kolegium oraz innych uczestników posiedzenia Kolegium o terminie posiedzenia oraz o jego porządku obrad;
4) przygotowywanie analiz materiałów i dokumentów przekazanych do Kolegium celem ich rozpatrzenia;
5) sporządzanie protokołów posiedzeń Kolegium i przedstawianie ich do podpisu Przewodniczącemu Kolegium;
6) prowadzenie rejestru ocen lub opinii Kolegium i decyzji Przewodniczącego Kolegium oraz harmonogramu ich realizacji;
7) gromadzenie i przechowywanie dokumentacji Kolegium, z zachowaniem zasad ochrony informacji niejawnych;
8) zapewnienie właściwego przygotowania i sprawnej obsługi posiedzeń Kolegium;
9) sporządzanie projektu rocznego sprawozdania z działalności Kolegium i przedstawianie go Przewodniczącemu Kolegium;
10) wykonywanie innych zadań zleconych przez Kolegium i Przewodniczącego Kolegium.

§ 10 Rozporządzenie wchodzi w życie z dniem ……

PREZES RADY MINISTRÓW

UZASADNIENIE

Projekt ustawy przewiduje powołanie Kolegium do Spraw Cyberbezpieczeństwa jako organu opiniodawczo-doradczego w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych. Potrzebę utworzenia ciała opiniodawczo-doradczego sygnalizowano w trakcie uzgadniania i opiniowania projektu z podmiotami, które będą wchodzić w skład systemu. Tryb pracy oraz zasady działania Kolegium określa niniejsze rozporządzenie.

Art. 65 projektu określa zakres spraw w jakich Kolegium formułuje oceny lub wyraża opinie, w tym w stosunku do zadań wykonywanych przez zespoły CSIRT, sektorowe zespoły cyberbezpieczeństwa oraz organy właściwe. Na czele Kolegium stoi Prezes Rady Ministrów, ponadto w jego skład wchodzą sekretarz Kolegium (powoływany przez Prezesa Rady Ministrów spośród osób posiadających poświadczenie bezpieczeństwa o klauzuli "tajne"), oraz członkowie, którymi są minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej (ww. ministrowie mogą być reprezentowani przez swoich zastępców), Szef Biura Bezpieczeństwa Narodowego (jeżeli został wyznaczony przez Prezydenta RP), minister-członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, a jeżeli nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego. W posiedzeniach Kolegium uczestniczą także: Dyrektor RCB, Szef ABW, Szef Służby Kontrwywiadu Wojskowego i Dyrektor NASK. Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach Kolegium także inne osoby. Obsługę Kolegium zapewnia ministerstwo lub inny urząd administracji rządowej, które obsługuje Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.

Projektowane rozporządzenie wejdzie w życie w dniu wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa.

Przedmiot projektowanej regulacji jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2018 r. poz. 362).

Projekt nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania konsultacji lub uzgodnienia.

Projekt został udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministerstwa Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Nazwa projektu Rozporządzenie Rady Ministrów w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** **xxx** **Kontakt do opiekuna merytorycznego projektu** xxx	**Data sporządzenia** xx.xxx.xxxx **Źródło:** art. 66 ust. 9 ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …) **Nr w wykazie prac:** xxx

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W związku z powstaniem regulacji zawartej w art. 64 ustawy o krajowym systemie cyberbezpieczeństwa, treścią którego przy Radzie Ministrów działa Kolegium do Spraw Cyberbezpieczeństwa, zgodnie z dyspozycją art. 66 ust. 9 Rada Ministrów określa w drodze rozporządzenia, szczegółowy tryb i zasady funkcjonowania Kolegium oraz zakres czynności sekretarza Kolegium.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Niniejszy projekt określa zasady działania Kolegium oraz tryb jego pracy. Posiedzenia mają charakter niejawny a w skład Kolegium wchodzą osoby wymienione w art. 66 ust. 1 oraz ust. 4 i ust. 5 ustawy.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Ze względu na szczegółowość projektowanej regulacji, odstąpiono od przeprowadzenia analiz prawnoporównawczych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Prezes Rady Ministrów	1		Uczestnictwo w posiedzeniach
Minister właściwy do spraw wewnętrznych	1		Uczestnictwo w posiedzeniach
Minister właściwy do spraw informatyzacji	1		Uczestnictwo w posiedzeniach
Minister Obrony Narodowej	1		Uczestnictwo w posiedzeniach
Szef Biura Bezpieczeństwa Narodowego	1		Uczestnictwo w posiedzeniach
Minister-członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych	1		Uczestnictwo w posiedzeniach
Szef Agencji Bezpieczeństwa Wewnętrznego	1		Uczestnictwo w posiedzeniach
Dyrektor Rządowego Centrum Bezpieczeństwa	1		Uczestnictwo w posiedzeniach
Szef Służby Kontrwywiadu Wojskowego	1		Uczestnictwo w posiedzeniach
Dyrektor Naukowej i	1		Uczestnictwo w posiedzeniach

Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego			

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

W ramach konsultacji i opiniowania projekt zostanie przesłany do:

1) Prezes Urzędu Komunikacji Elektronicznej;
2) Polskiej Izby Informatyki i Telekomunikacji;
3) Krajowej Izby Gospodarczej Elektroniki i Telekomunikacji;
4) Polskiej Izby Komunikacji Elektronicznej;
5) Krajowej Izby Komunikacji Ethernetowej;
6) Polskiej Izby Radiodyfuzji Cyfrowej;
7) Fundacji Bezpieczna Cyberprzestrzeń;
8) Polskiego Towarzystwa Informatycznego;
9) Fundacji Nowoczesna Polska;
10) Fundacji Projekt Polska;
11) Internet Society Poland;
12) Stowarzyszenia Inżynierów Telekomunikacji;
13) Fundacji Panoptykon;
14) Związku Pracodawców Branży Internetowej IAB Polska;
15) Federacji Związków Zawodowych Pracowników Telekomunikacji.

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt został udostępniony na stronie podmiotowej Biuletynu Informacji Publicznej MC oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	0	0	0	0	0	0	0	0	0	0	*Łącznie (0-10)*
Dochody ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Wydatki ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0
Saldo ogółem	0	0	0	0	0	0	0	0	0	0	0	0
budżet państwa	0	0	0	0	0	0	0	0	0	0	0	0
JST	0	0	0	0	0	0	0	0	0	0	0	0
pozostałe jednostki (oddzielnie)	0	0	0	0	0	0	0	0	0	0	0	0

Źródła finansowania	Przyjęte rozwiązania nie spowodują dodatkowych skutków finansowych dla sektora finansów publicznych, w tym budżetu państwa i budżetów jednostek samorządu terytorialnego.

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	0	0	0	0	0	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł, ceny stałe z …… r.)	duże przedsiębiorstwa	-	-	-	-	-	-	-
	sektor mikro-, małych i średnich przedsiębiorstw	-	-	-	-	-	-	-
	rodzina, obywatele oraz gospodarstwa domowe	-	-	-	-	-	-	-
	Przedsiębiorstwa wykorzystujące częstotliwości w celach badawczych i eksperymentalnych	-	-	-	-	-	-	-
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☐ nie ☒ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☒ nie dotyczy

9. Wpływ na rynek pracy
Projekt ustawy nie będzie miał wpływu na rynek pracy.
10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	

11. Planowane wykonanie przepisów aktu prawnego
Po upływie okresów przewidzianych na wprowadzenie odpowiednich rozwiązań (vacatio legis) bądź dostosowanie istniejących przez adresatów aktu.
12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?
Nie jest planowana ewaluacja.
13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)
-

Projekt

R O Z P O R Z Ą D Z E N I E

M I N I S T R A C Y F R Y Z A C J I [1)]

z dnia

w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług

Na podstawie art. 175a ust. 2a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138, 650) zarządza się, co następuje:

§ 1. Rozporządzenie określa kryteria, na podstawie których przedsiębiorcy telekomunikacyjni uznają naruszenie bezpieczeństwa lub integralności sieci lub usług za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług.

§ 2. Naruszenie bezpieczeństwa lub integralności sieci lub usług, o którym mowa w § 1, ma istotny wpływ na funkcjonowanie sieci lub usług, w przypadku spełnienia co najmniej jednego z następujących kryteriów:

1) wartość procentowa użytkowników z ogólnej liczby użytkowników danego przedsiębiorcy, na których naruszenie wywarło wpływ, jest większa niż 5%;
2) czas trwania naruszenia (okres niedostępności lub niepełnej dostępności sieci lub usług jest dłuższy niż 4 godziny;
3) obszar, na którym wystąpiło naruszenie jest większy niż obszar jednego powiatu;
4) naruszenie miało wpływ na połączenia z numerami alarmowymi;
5) naruszenie miało wpływ na obowiązek zachowania tajemnicy telekomunikacyjnej;
6) naruszenie miało wpływ na możliwość realizacji zadań lub obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

[1)] Minister Cyfryzacji kieruje działem administracji rządowej – informatyzacja, na podstawie § 1 ust. 2 rozporządzenia Prezesa Rady Ministrów z dnia 20 kwietnia 2018 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 761).

§ 3. Rozporządzenie wchodzi w życie z dniem ……

MINISTER CYFRYZACJI

UZASADNIENIE

Projektowane rozporządzenie stanowi wykonanie upoważnienia ustawowego zawartego w art. 175a ust. 2a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907 i 2201 oraz z 2018 r. poz. 106, 138 i 650) i określa kryteria uznania naruszenia bezpieczeństwa lub integralności sieci lub usług za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług. Wprowadzenie wskazanej delegacji ustawowej nastąpiło przez uchwalenie ustawy z dnia …… o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. …), która w art. 78 wprowadziła zmiany do ustawy – Prawo telekomunikacyjne.

Projektowane rozporządzenie będzie wykorzystywane przez przedsiębiorców telekomunikacyjnych przy wykonywaniu zadań, które nakłada na nich ustawa – Prawo telekomunikacyjne w art. 175a. Przedsiębiorcy telekomunikacyjni będą zobowiązani do identyfikacji naruszenia bezpieczeństwa lub integralności sieci lub usług na podstawie kryteriów uznania naruszenia za mające istotny wpływ na funkcjonowanie sieci lub usług. Projektowane rozporządzenie wskazuje kryteria ustalenia, czy naruszenie ma istotny wpływ na funkcjonowanie sieci lub usługi: wartość procentową użytkowników danego przedsiębiorcy, których dotyczy naruszenie bezpieczeństwa lub integralności sieci lub usługi; czas trwania naruszenia na bezpieczeństw lub integralność sieci lub usługi; obszaru, na którym wystąpiło naruszenie bezpieczeństwa lub integralności sieci lub usługi; wpływ na połączenia z numerami alarmowymi; wpływ na naruszenie ochrony tajemnicy telekomunikacyjnej; wpływ na możliwość realizacji zadań lub obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Rozporządzenie wejdzie w życie z dniem wejścia w życie ustawy z dnia ... o krajowym systemie cyberbezpieczeństwa.

Projekt rozporządzenia jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2018 r. poz. 362).

Projekt rozporządzenia nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt zostanie udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Nazwa projektu Rozporządzenie Ministra Cyfryzacji w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług **Ministerstwo wiodące i ministerstwa współpracujące** Ministerstwo Cyfryzacji **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Podsekretarz Stanu - Karol Okoński **Kontakt do opiekuna merytorycznego projektu** Andrzej Szyszko, Departament Cyberbezpieczeństwa, Zastępca Dyrektora, tel. (22) 245 57 05, e-mail: andrzej.szyszko@mc.gov.pl	**Data sporządzenia** 19 kwietnia 2018 **Źródło:** Art. 175a ust. 2a ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907, z późn. zm.) **Nr w wykazie prac legislacyjnych Rady Ministrów** XXX

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

W związku z regulacją zawartą w art. 175a ust. 1 ustawy – Prawo telekomunikacyjne, normującą obowiązek przedsiębiorcy telekomunikacyjnego niezwłocznego informowania Prezesa UKE o naruszeniu bezpieczeństwa lub integralności sieci lub usług, które miało istotny wpływ na funkcjonowanie sieci lub usług, na skutek wprowadzenia ust. 2e, zachodzi konieczność określenia kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Naruszenie bezpieczeństwa lub integralności sieci lub usług, o którym mowa w § 1 rozporządzenia, ma istotny wpływ na funkcjonowanie sieci lub usług, w przypadku spełnienia co najmniej jednego z następujących kryteriów:

1) wartość procentowa użytkowników, z ogólnej liczby użytkowników danego przedsiębiorcy, na których naruszenie wywarło wpływ jest większa niż 5%;
2) czas trwania naruszenia (okres niedostępności lub niepełnej dostępności sieci lub usług jest dłuższy niż 4 godziny;
3) obszar, na którym wystąpiło naruszenie jest większy niż obszar jednego powiatu;
4) naruszenie miało wpływ na połączenia z numerami alarmowymi;
5) naruszenie miało wpływ na obowiązek zachowania tajemnicy telekomunikacyjnej;
6) naruszenie miało wpływ na możliwość realizacji zadań lub obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.

Wymienione wyżej rozwiązania powinny w sposób skuteczny i kompleksowy zapewnić właściwe przeprowadzenie obowiązku zgłaszania przez przedsiębiorców telekomunikacyjnych informacji o zaistniałych poważnych naruszeniach bezpieczeństwa lub integralności sieci lub usług.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Ze względu na szczegółowość projektowanej regulacji, odstąpiono od przeprowadzenia analiz prawnoporównawczych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie

Projekt rozporządzenia oddziałuje na przedsiębiorców telekomunikacyjnych, jak również na osoby fizyczne.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248) projekt zostanie udostępniony w Biuletynie Informacji Publicznej na stronie podmiotowej Rządowego Centrum Legislacji, w serwisie Rządowy Proces Legislacyjny oraz na stronie podmiotowej Ministra Cyfryzacji.

6. Wpływ na sektor finansów publicznych

(ceny stałe z … r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]

											Łącznie (0–10)
Dochody ogółem											
budżet państwa											
JST											
pozostałe jednostki (oddzielnie)											
Wydatki ogółem											
budżet państwa											
JST											
pozostałe jednostki (oddzielnie)											
Saldo ogółem											
budżet państwa											
JST											
pozostałe jednostki (oddzielnie)											

Źródła finansowania	Projektowane rozporządzenie reguluje kryteria uznane przez przedsiębiorców telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług, naruszeń bezpieczeństwa lub integralności sieci lub usług, i jako takie nie będzie powodować skutków dla sektora finansów publicznych.
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	Łącznie (0–10)
W ujęciu pieniężnym (w mln zł, ceny stałe z 2017 r.)								
	sektor przedsiębiorstw – przedsiębiorcy, będący operatorami usług kluczowych – szacunkowy koszt dla przedsiębiorcy							
	sektor przedsiębiorstw – przedsiębiorcy, którzy chcą świadczyć usługi z zakresu reagowania na incydenty – szacunkowy koszt dla przedsiębiorcy							
W ujęciu niepieniężnym	duże przedsiębiorstwa							
	sektor mikro-, małych i średnich przedsiębiorstw							
	rodzina, obywatele oraz gospodarstwa domowe							

Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☐ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☒ tak ☐ nie ☐ nie dotyczy

9. Wpływ na rynek pracy

Projektowane rozporządzenie nie wpłynie na rynek pracy.

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☒ informatyzacja ☐ zdrowie

Omówienie wpływu	Przyspieszenie obiegu informacji o incydentach związanych z naruszeniem bezpieczeństwa lub integralności sieci lub usług przez przedsiębiorców telekomunikacyjnych.

11. Planowane wykonanie przepisów aktu prawnego

Przewiduje się wejście w życie rozporządzenia z dniem wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Nie jest planowana ewaluacja.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Projekt

R O Z P O R Z Ą D Z E N I E

R A D Y M I N I S T R Ó W

z dnia

zmieniające rozporządzenie w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego

Na podstawie art. 5a ust. 6 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566) zarządza się, co następuje:

§ 1. W rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. poz. 540) wprowadza się następujące zmiany:

1) w § 4 w pkt 1 w lit. d średnik zastępuje się przecinkiem i dodaje się lit. e w brzmieniu:
„e) cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej;”;
2) po § 8 dodaje się § 8a w brzmieniu:
„8a. Przepisy § 7 ust. 1, 5 i 6 oraz § 8 ust. 2 i 3 w zakresie dotyczącym uzgadniania raportu cząstkowego z Szefem ABW oraz jego aktualizacji, stosuje się odpowiednio do uzgadniania raportu cząstkowego z Pełnomocnikiem Rządu do spraw Cyberbezpieczneństwa w przypadku zagrożenia, o którym mowa w § 4 pkt 1 lit. e.”;
3) w § 9 po ust. 2 dodaje się ust. 2a w brzmieniu:
„2a. Przepis ust. 1 stosuje się odpowiednio do Pełnomocnika Rządu do spraw Cyberbezpieczeństwa w zakresie koordynacji opracowania Raportu w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej.”.

§ 2. Dyrektor Centrum dokona aktualizacji Raportu uwzględniającej zagrożenia, o których mowa w § 4 pkt 1 lit. e, w terminie 12 miesięcy od dnia wejścia w życie rozporządzenia.

§ 3. Rozporządzenie wchodzi w życie z dniem ……

PREZES RADY MINISTRÓW

UZASADNIENIE

Projekt zmian w rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. poz. 540) dotyczy dodania instytucji Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, tworzonego projektem ustawy o krajowym systemie cyberbezpieczeństwa, który będzie odpowiadać za koordynację przygotowań Raportu o zagrożeniach bezpieczeństwa narodowego (dalej „Raport") w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej.

Pozostałe kwestie dotyczące koordynacji czynności umożliwiających sporządzenie Raportu pozostają bez zmian – tak jak dotychczas dyrektor Rządowego Centrum Bezpieczeństwa (RCB) będzie koordynował całość przygotowania Raportu jak również przedkładał ten dokument do rozpatrzenia Radzie Ministrów, a cześć dotyczącą zagrożeń o charakterze terrorystycznym mogących doprowadzić do sytuacji kryzysowej nadal będzie koordynował Szef Agencji Bezpieczeństwa Wewnętrznego (ABW).

Elementy składające się na opracowywane przez ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów raporty cząstkowe, zostały wyszczególnione w § 4 zmienianego rozporządzenia. Na strukturę raportu cząstkowego składa się m.in. wskazanie najważniejszych zagrożeń i skutków ich wystąpienia przez stworzenie mapy ryzyka, o której mowa w art. 3 pkt 10 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566), obejmującej wyszczególnienie rodzajów i charakterystyki zagrożeń. Dlatego też w § 4 w pkt 1 zmienianego rozporządzenia konieczne jest jednoznaczne wskazanie zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej.

Propozycje zmian polegające na dodaniu § 8a oraz ust. 2a w § 9 wynikają z konieczności wskazania uprawnień Pełnomocnika Rządu do spraw Cyberbezpieczneństwa w zakresie koordynacji Raportu, analogicznych do obecnie posiadanych przez dyrektora RCB oraz Szefa ABW.

Ponadto w § 2 rozporządzenia zmieniającego nałożono na dyrektora RCB obowiązek dokonania aktualizacji Raportu w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej, w terminie 12 miesięcy od dnia wejścia w życie rozporządzenia zmieniającego.

Projektowane rozporządzenie wejdzie w życie z dniem wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa.

Przedmiot projektowanej regulacji jest zgodny z prawem Unii Europejskiej.

Projektowana regulacja nie zawiera przepisów technicznych w rozumieniu rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. poz. 2039 oraz z 2004 r. poz. 597) i nie podlega notyfikacji Komisji Europejskiej.

Projektowana regulacja nie będzie wymagała notyfikacji Komisji Europejskiej w trybie ustawy z dnia 30 kwietnia 2004 r. o postępowaniu w sprawach dotyczących pomocy publicznej (Dz. U. z 2018 r. poz. 362).

Projekt rozporządzenia nie wymaga przedłożenia instytucjom i organom Unii Europejskiej, w tym Europejskiemu Bankowi Centralnemu, w celu uzyskania opinii, dokonania powiadomienia, konsultacji albo uzgodnienia.

Projekt rozporządzenia zostanie udostępniony na stronie Rządowego Centrum Legislacji w serwisie „Rządowy Proces Legislacyjny” oraz w Biuletynie Informacji Publicznej na stronie podmiotowej Ministra Cyfryzacji, zgodnie z art. 5 ustawy z dnia 7 lipca 2005 r. o działalności lobbingowej w procesie stanowienia prawa (Dz. U. z 2017 r. poz. 248).

Nazwa projektu Rozporządzenie Rady Ministrów zmieniające rozporządzenie w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego **Ministerstwo wiodące i ministerstwa współpracujące** Rządowe Centrum Bezpieczeństwa **Osoba odpowiedzialna za projekt w randze Ministra, Sekretarza Stanu lub Podsekretarza Stanu** Pan Marek Kubiak, Dyrektor Rządowego Centrum Bezpieczeństwa **Kontakt do opiekuna merytorycznego projektu** Pani Beata Janowczyk, Szef Wydziału Oceny Ryzyka i Planowania RCB (tel. 22 23 65 930 lub mail: beata.janowczyk@rcb.gov.pl)	**Data sporządzenia** 19.04.2018 r. **Źródło:** Art. 5a ust. 6 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209 i 1566) **Nr w wykazie prac:** ----------

OCENA SKUTKÓW REGULACJI

1. Jaki problem jest rozwiązywany?

Projekt zmian w rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego (Dz. U. poz. 540) dotyczy dodania instytucji Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, tworzonego projektem ustawy o krajowym systemie cyberbezpieczeństwa, który będzie odpowiadać za koordynację przygotowań Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej.

2. Rekomendowane rozwiązanie, w tym planowane narzędzia interwencji, i oczekiwany efekt

Elementy składające się na opracowywane przez ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów raporty cząstkowe, zostały wyszczególnione w § 4 zmienianego rozporządzenia. Na strukturę raportu cząstkowego składa się m.in. wskazanie najważniejszych zagrożeń i skutków ich wystąpienia przez stworzenie mapy ryzyka, o której mowa w art. 3 pkt 10 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, obejmującej wyszczególnienie rodzajów i charakterystyki zagrożeń. Dlatego też w § 4 w pkt 1 zmienianego rozporządzenia konieczne jest jednoznaczne wskazanie zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej.

Propozycje zmian polegające na dodaniu § 8a oraz ust. 2a w § 9 wynikają z konieczności wskazania uprawnień Pełnomocnika Rządu do spraw Cyberbezpieczneństwa w zakresie koordynacji Raportu analogicznych do obecnie posiadanych przez dyrektora RCB oraz Szefa ABW.

Ponadto w § 2 rozporządzenia zmieniającego nałożono na dyrektora RCB obowiązek dokonania aktualizacji Raportu w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej, w terminie 12 miesięcy od dnia wejścia w życie rozporządzenia zmieniającego.

3. Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich OECD/UE?

Brak danych.

4. Podmioty, na które oddziałuje projekt

Grupa	Wielkość	Źródło danych	Oddziaływanie
Ministrowie	19		Opracowywanie, zgodnie z właściwością, raportów cząstkowych.
Kierownicy urzędów centralnych	40		Opracowywanie, zgodnie z właściwością, raportów cząstkowych.
Wojewodowie	16		Opracowywanie, zgodnie z właściwością, raportów cząstkowych.
Dyrektor RCB	1		Koordynacja przygotowania Raportu o zagrożeniach bezpieczeństwa narodowego oraz przedłożenie raportu

			Radzie Ministrów.
Szef ABW	1		Koordynacja przygotowania Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń o charakterze terrorystycznym mogących doprowadzić do sytuacji kryzysowej.
Pełnomocnik Rządu do spraw Cyberbezpieczeństwa	1		Koordynacja przygotowania Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej.

5. Informacje na temat zakresu, czasu trwania i podsumowanie wyników konsultacji

Brak konsultacji publicznych.

6. Wpływ na sektor finansów publicznych

(ceny stałe z …… r.)	Skutki w okresie 10 lat od wejścia w życie zmian [mln zł]											
	0	1	2	3	4	5	6	7	8	9	10	*Łącznie (0-10)*
Dochody ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Wydatki ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												
Saldo ogółem												
budżet państwa												
JST												
pozostałe jednostki (oddzielnie)												

Źródła finansowania	
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projekt rozporządzenia nie będzie mieć wpływu na sektor finansów publicznych, w tym budżet państwa i budżety jednostek samorządu terytorialnego.

7. Wpływ na konkurencyjność gospodarki i przedsiębiorczość, w tym funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe

		Skutki						
Czas w latach od wejścia w życie zmian		0	1	2	3	5	10	*Łącznie (0-10)*
W ujęciu pieniężnym (w mln zł,	duże przedsiębiorstwa	nd	nd	nd	nd	nd	nd	nd
	sektor mikro-, małych i średnich przedsiębiorstw	nd	nd	nd	nd	nd	nd	nd

ceny stałe z …… r.)	rodzina, obywatele oraz gospodarstwa domowe	nd	nd	nd	nd	nd	nd	nd
W ujęciu niepieniężnym	duże przedsiębiorstwa	nd						
	sektor mikro-, małych i średnich przedsiębiorstw	nd						
	rodzina, obywatele oraz gospodarstwa domowe	nd						
Niemierzalne								
Dodatkowe informacje, w tym wskazanie źródeł danych i przyjętych do obliczeń założeń	Projektowane rozporządzenie nie wpłynie na konkurencyjność gospodarki i przedsiębiorczość, w tym na funkcjonowanie przedsiębiorców oraz na rodzinę, obywateli i gospodarstwa domowe.							

8. Zmiana obciążeń regulacyjnych (w tym obowiązków informacyjnych) wynikających z projektu

☐ nie dotyczy

Wprowadzane są obciążenia poza bezwzględnie wymaganymi przez UE (szczegóły w odwróconej tabeli zgodności).	☐ tak ☒ nie ☐ nie dotyczy
☐ zmniejszenie liczby dokumentów ☐ zmniejszenie liczby procedur ☐ skrócenie czasu na załatwienie sprawy ☐ inne:	☐ zwiększenie liczby dokumentów ☒ zwiększenie liczby procedur ☐ wydłużenie czasu na załatwienie sprawy ☐ inne:
Wprowadzane obciążenia są przystosowane do ich elektronizacji.	☐ tak ☐ nie ☒ nie dotyczy

Komentarz: Rozporządzenie powoduje zmianę obciążeń regulacyjnych przez zwiększenie liczby procedur.

9. Wpływ na rynek pracy

Brak wpływu

10. Wpływ na pozostałe obszary

☐ środowisko naturalne ☐ sytuacja i rozwój regionalny ☐ inne:	☐ demografia ☐ mienie państwowe	☐ informatyzacja ☐ zdrowie

Omówienie wpływu	Nie przewiduje się wpływu projektowanego rozporządzenia na ww. obszary.

11. Planowane wykonanie przepisów aktu prawnego

Wejście w życie rozporządzenia powinno nastąpić równocześnie z dniem wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa.

12. W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Zakres projektu rozporządzenia uniemożliwia zastosowanie mierników.

13. Załączniki (istotne dokumenty źródłowe, badania, analizy itp.)

Brak załącznika.