Parlament Europejski
2019-2024

Komisja Rynku Wewnętrznego i Ochrony Konsumentów

2020/0359(COD)

14.7.2021

OPINIA

Komisji Rynku Wewnętrznego i Ochrony Konsumentów

dla Komisji Przemysłu, Badań Naukowych i Energii

w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Sprawozdawca komisji opiniodawczej: Morten Løkkegaard

PA_Legam

ZWIĘZŁE UZASADNIENIE

Ogólnie sprawozdawca pozytywnie ocenia wniosek ustawodawczy dotyczący dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS 2). Uważa, że w coraz bardziej cyfrowym świecie bezpieczeństwo online ma kluczowe znaczenie w środowisku cyfrowym oraz dla funkcjonowania jednolitego rynku, na którym konsumenci i podmioty gospodarcze mogą swobodnie prowadzić działalność.

Wniosek dotyczący NIS 2 zapewnia istotną poprawę w stosunku do dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (NIS 1). Wymieniono w nim kluczowe braki NIS 1, takie jak niski poziom cyberodporności przedsiębiorstw i sektorów, a także niespójna odporność i niski poziom wspólnej orientacji sytuacyjnej i reagowania kryzysowego w państwach członkowskich i między nimi. Sprawozdawca pochwala zamiar skorygowania tych niedociągnięć za pośrednictwem NIS 2.

Zakres stosowania

Sprawozdawca docenia rozszerzony zakres stosowania wniosku dotyczącego NIS 2, w szczególności objęcie nim nowych sektorów, np. administracji publicznej. Jasna lista sektorów i usług z pewnością ograniczy swobodę państw członkowskich w określaniu konkretnych podmiotów podlegających dyrektywie i tym samym zmniejszy fragmentację jednolitego rynku.

Komisja zaproponowała zasadę maksymalnej wielkości jako jednolite kryterium wyboru podmiotów objętych zakresem stosowania analizowanej dyrektywy. Niewątpliwie pozwoli ono zagwarantować pewność prawa, a jednocześnie zmniejszyć rozbieżności między państwami członkowskimi.

Sprawozdawca z zadowoleniem przyjmuje rozszerzenie zakresu sektorowego, jest jednak zdania, że należy połączyć to ogólne kryterium z oceną poziomu krytyczności podmiotów w poszczególnych sektorach. Pozwoliłoby to wyłączyć z zakresu stosowania dyrektywy średnie i duże podmioty, jeżeli po ocenie ryzyka uznano, że charakteryzują się niskim poziomem krytyczności i zależności od innych podmiotów krytycznych.

Sprawozdawca podkreśla, że nie należy tego postrzegać jako furtki do rozbieżnych interpretacji między państwami członkowskimi. Aby zagwarantować, że nie spowoduje to fragmentarycznego wdrażania przepisów w państwach członkowskimi, zachęcamy Komisję do wydania jasnych wytycznych na ten temat.

Ponadto, choć sprawozdawca uznaje wyłączenie mikroprzedsiębiorstw i małych przedsiębiorstw z zakresu stosowania dyrektywy za godne pochwały, uważa, że należy je zachęcać do dobrowolnego stosowania jej przepisów, ponieważ mikroprzedsiębiorstwa i małe podmioty również są narażone na cyberataki.

Skoordynowane ramy regulacyjne w dziedzinie cyberbezpieczeństwa

Sprawozdawca pochwala rozdział, w którym określono różne elementy krajowych strategii cyberbezpieczeństwa i krajowe narzędzia zarządzania kryzysowego. W ramach krajowej strategii cyberbezpieczeństwa proponujemy, aby państwa członkowskie przyjęły politykę

promującą stosowanie kryptografii i szyfrowania, zwłaszcza przez MŚP.

Sprawozdawca wyraża zadowolenie, że ENISA stworzyła europejski rejestr podatności, uważa jednak, że przy rejestracji należy dochować tajemnicy przedsiębiorstwa i tajemnicy handlowej. Nie można też niepotrzebnie obciążać podmiotów.

Współpraca między państwami członkowskimi

Szczególnie godna pochwały jest bardziej ustrukturyzowana współpraca między państwami członkowskimi w Grupie Współpracy, sieci CSIRT i nowo utworzonej grupy ds. incydentów na dużą skalę w związku z NIS 2. Konieczny jest jednak większy poziom zaufania i gotowości do wymiany informacji między państwami członkowskimi, ponieważ skuteczność tej współpracy ma kluczowe znaczenie dla wysokiego poziomu cyberbezpieczeństwa w UE.

W związku z tym przygotowano szereg poprawek, aby wzmocnić rolę sieci. Sprawozdawca uważa w szczególności, że wzajemna ocena może zwiększyć obopólne zaufanie państw członkowskich i powinna odgrywać kluczową rolę w ocenie skuteczności polityki poszczególnych państw członkowskich w dziedzinie cyberbezpieczeństwa.

Zarządzanie ryzykiem w cyberprzestrzeni

Sprawozdawca docenia rozszerzenie oceny ryzyka na cały łańcuch dostaw (art. 18 i 19), podkreśla jednak, że kwestia ta wymaga wyjaśnienia, aby zapewnić jasne wytyczne podmiotom objętym tym wymogiem i państwom członkowskim podczas skoordynowanej oceny ryzyka dla bezpieczeństwa szczególnie krytycznych sektorów lub łańcuchów dostaw.

Obowiązki w zakresie zgłaszania incydentów

Sprawozdawca uważa, że należy lepiej sprecyzować konkretne elementy zmienionej dyrektywy, głównie niektóre obowiązki nałożone na przedsiębiorstwa w NIS 2. Mając na uwadze ostateczny cel, tj. skuteczne wdrożenie tej dyrektywy, sprawozdawca starał się ograniczyć biurokrację i ułatwić przedsiębiorstwom przestrzeganie nowych przepisów.

Sprawozdawca proponuje wydłużyć proponowany 24-godzinny termin w ramach obowiązków sprawozdawczych w przypadku pierwszych zgłoszeń do 72 godzin, aby przedsiębiorstwa mogły skutecznie odeprzeć trwający cyberatak przed zgłoszeniem. Ponadto proponuje skreślenie wszelkich odniesień do obowiązkowego zgłaszania tzw. potencjalnych incydentów.

POPRAWKI

Komisja Rynku Wewnętrznego i Ochrony Konsumentów zwraca się do Komisji Przemysłu, Badań Naukowych i Energii, jako komisji przedmiotowo właściwej, o wzięcie pod uwagę następujących poprawek:

Poprawka 1
Wniosek dotyczący dyrektywy
Motyw 5

Tekst proponowany przez Komisję	*Poprawka*
(5) Wszystkie te rozbieżności pociągają za sobą fragmentację rynku wewnętrznego i mogą mieć szkodliwy wpływ na jego funkcjonowanie, oddziałując w szczególności na transgraniczne świadczenie usług i poziom odporności pod względem cyberbezpieczeństwa ze względu na stosowanie różnych norm. Celem ***niniejszej*** dyrektywy jest zatem wyeliminowanie ***takich*** rozbieżności między państwami członkowskimi, w szczególności ***przez określenie minimalnych przepisów dotyczących*** funkcjonowania skoordynowanych ram regulacyjnych, ***ustanowienie mechanizmów*** skutecznej współpracy między odpowiedzialnymi organami w każdym państwie członkowskim, ***dokonanie*** aktualizacji wykazu sektorów i działań podlegających obowiązkom w zakresie cyberbezpieczeństwa oraz ***ustanowienie skutecznych środków naprawczych*** i ***sankcji***, które są kluczowe dla skutecznego egzekwowania tych obowiązków. Dyrektywę (UE) 2016/1148 należy zatem uchylić i zastąpić niniejszą dyrektywą.	(5) Wszystkie te rozbieżności pociągają za sobą fragmentację rynku wewnętrznego i mogą mieć szkodliwy wpływ na jego funkcjonowanie, oddziałując w szczególności na transgraniczne świadczenie usług i poziom odporności pod względem cyberbezpieczeństwa ze względu na stosowanie różnych norm. Celem dyrektywy jest zatem wyeliminowanie rozbieżności między państwami członkowskimi ***i wzmocnienie rynku wewnętrznego***, w szczególności ***dzięki minimalnym przepisom dotyczącym*** funkcjonowania skoordynowanych ram regulacyjnych, ***mechanizmom*** skutecznej współpracy między odpowiedzialnymi organami w każdym państwie członkowskim, aktualizacji wykazu sektorów i działań podlegających obowiązkom w zakresie cyberbezpieczeństwa oraz ***skutecznym środkom naprawczym*** i ***sankcjom***, które są kluczowe dla skutecznego egzekwowania tych obowiązków. Dyrektywę (UE) 2016/1148 należy zatem uchylić i zastąpić niniejszą dyrektywą.

Poprawka 2
Wniosek dotyczący dyrektywy
Motyw 6 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(6a) Dyrektywa nie narusza obowiązujących przepisów UE o ochronie danych osobowych.

Poprawka 3
Wniosek dotyczący dyrektywy
Motyw 9

Tekst proponowany przez Komisję	*Poprawka*
(9) Zakres niniejszej dyrektywy powinien jednak obejmować także małe podmioty lub mikropodmioty spełniające określone kryteria, które wskazują na zasadnicze znaczenie tych podmiotów dla gospodarek lub społeczeństw państw członkowskich lub dla konkretnych sektorów lub rodzajów usług. Państwa członkowskie powinny być odpowiedzialne za ustanowienie wykazu takich podmiotów i powinny przedłożyć go Komisji.	(9) Zakres niniejszej dyrektywy powinien jednak obejmować także małe podmioty lub mikropodmioty spełniające określone kryteria, które wskazują na zasadnicze znaczenie tych podmiotów dla gospodarek lub społeczeństw państw członkowskich lub dla konkretnych sektorów lub rodzajów usług. Państwa członkowskie powinny być odpowiedzialne za ustanowienie wykazu takich podmiotów i powinny przedłożyć go Komisji. ***Komisja powinna przedstawić jasne wytyczne dotyczące kryteriów określających, które małe lub mikroprzedsiębiorstwa zostaną uznane za niezbędne lub istotne, zwłaszcza w przypadku firm świadczących usługi w kilku państwach członkowskich.***

Poprawka 4
Wniosek dotyczący dyrektywy
Motyw 10

Tekst proponowany przez Komisję	*Poprawka*
(10) Komisja, ***we współpracy*** z Grupą Współpracy, ***może*** sformułować wytyczne dotyczące wdrażania kryteriów mających zastosowanie do mikroprzedsiębiorstw i małych przedsiębiorstw.	(10) Komisja, ***wraz*** z Grupą Współpracy, ***powinna*** sformułować wytyczne dotyczące wdrażania kryteriów mających zastosowanie do mikroprzedsiębiorstw i małych przedsiębiorstw.

Poprawka 5
Wniosek dotyczący dyrektywy
Motyw 12 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(12a) Rozszerzenie zakresu stosowania dyrektywy pociąga za sobą włączenie

podmiotów podlegających regulacjom sektorowym. Aby uniknąć powielania przepisów i nadmiernych obciążeń regulacyjnych, Komisja powinna dopilnować, aby akty sektorowe wymagające od niezbędnych lub istotnych podmiotów przyjęcia środków zarządzania ryzykiem w cyberprzestrzeni albo zgłaszania incydentów lub poważnych cyberzagrożeń były spójne z dyrektywą.

Poprawka 6
Wniosek dotyczący dyrektywy
Motyw 12 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(12b) Komisja powinna opublikować jasne wytyczne towarzyszące dyrektywie, aby pomóc w harmonizacji we wdrażaniu przepisów w państwach członkowskich i uniknięciu fragmentacji.

Poprawka 7
Wniosek dotyczący dyrektywy
Motyw 12 c (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(12c) Komisja powinna również opracować wytyczne, aby wesprzeć państwa członkowskie w prawidłowym wdrażaniu przepisów dotyczących zakresu stosowania oraz aby ocenić proporcjonalność obowiązków określonych w dyrektywie, biorąc pod uwagę poziom krytyczności podmiotów objętych zakresem stosowania, zwłaszcza w przypadku podmiotów o złożonych modelach biznesowych lub środowiskach operacyjnych, przy czym podmiot może jednocześnie spełniać kryteria niezbędnego, jak i istotnego podmiotu, lub może jednocześnie prowadzić działalność, która jest tylko częściowo objęta zakresem dyrektywy. Jeżeli główna działalność

	podmiotów wykracza poza zakres dyrektywy, ale w jej zakres wchodzi inna, drugorzędna działalność, przepisy powinny mieć zastosowanie wyłącznie na poziomie funkcji lub jednostki podmiotu, które wchodzą w zakres dyrektywy.

Poprawka 8
Wniosek dotyczący dyrektywy
Motyw 14

Tekst proponowany przez Komisję	*Poprawka*
(14) Biorąc pod uwagę powiązania między cyberbezpieczeństwem a bezpieczeństwem fizycznym podmiotów, należy zapewnić spójność pod względem podejścia między dyrektywą Parlamentu Europejskiego i Rady (UE) XXX/XXX [17] a niniejszą dyrektywą. W tym celu państwa członkowskie powinny zapewnić, aby podmioty krytyczne, oraz równoważne podmioty, zgodnie z dyrektywą (UE) XXX/XXX uznawano za podmioty niezbędne w rozumieniu niniejszej dyrektywy. Państwa członkowskie powinny także zapewnić, aby ich strategie dotyczące cyberbezpieczeństwa obejmowały ramy polityki na rzecz zwiększonej koordynacji między właściwym organem na mocy niniejszej dyrektywy a właściwym organem na mocy dyrektywy (UE) XXX/XXX w kontekście udostępniania informacji na temat incydentów i cyberzagrożeń oraz w kontekście wykonywania zadań nadzorczych. Organy na mocy obu dyrektyw powinny ze sobą współpracować i prowadzić wymianę informacji, w szczególności w odniesieniu do identyfikacji podmiotów krytycznych, cyberzagrożeń, ryzyka w cyberprzestrzeni, incydentów wpływających na podmioty krytyczne, a także w odniesieniu do środków w zakresie cyberbezpieczeństwa przyjmowanych przez podmioty krytyczne. Na wniosek właściwych organów na mocy dyrektywy (UE) XXX/XXX właściwym	(14) Biorąc pod uwagę powiązania między cyberbezpieczeństwem a bezpieczeństwem fizycznym podmiotów, należy zapewnić spójność pod względem podejścia między dyrektywą Parlamentu Europejskiego i Rady (UE) XXX/XXX [17] a niniejszą dyrektywą. W tym celu państwa członkowskie powinny zapewnić, aby podmioty krytyczne, oraz równoważne podmioty, zgodnie z dyrektywą (UE) XXX/XXX uznawano za podmioty niezbędne w rozumieniu niniejszej dyrektywy. Państwa członkowskie powinny także zapewnić, aby ich ***krajowe*** strategie dotyczące cyberbezpieczeństwa obejmowały ramy polityki na rzecz zwiększonej koordynacji między właściwym organem na mocy niniejszej dyrektywy a właściwym organem na mocy dyrektywy (UE) XXX/XXX w kontekście ***zgłaszania incydentów,*** udostępniania informacji na temat incydentów***, zdarzeń potencjalnie wypadkowych*** i cyberzagrożeń oraz w kontekście wykonywania zadań nadzorczych. Organy na mocy obu dyrektyw powinny ze sobą współpracować i prowadzić wymianę informacji, w szczególności w odniesieniu do identyfikacji podmiotów krytycznych, cyberzagrożeń, ryzyka w cyberprzestrzeni, incydentów wpływających na podmioty krytyczne, a także w odniesieniu do środków w zakresie cyberbezpieczeństwa przyjmowanych przez podmioty krytyczne. Na wniosek właściwych organów na mocy

organom na mocy niniejszej dyrektywy należy zezwolić na wykonywanie swoich uprawnień w zakresie nadzoru i egzekwowania przepisów względem podmiotu niezbędnego zidentyfikowanego jako podmiot krytyczny. Właściwe organy na mocy obu dyrektyw powinny w tej kwestii współpracować i prowadzić wymianę informacji.	dyrektywy (UE) XXX/XXX właściwym organom na mocy niniejszej dyrektywy należy zezwolić na wykonywanie swoich uprawnień w zakresie nadzoru i egzekwowania przepisów względem podmiotu niezbędnego zidentyfikowanego jako podmiot krytyczny. Właściwe organy na mocy obu dyrektyw powinny w tej kwestii współpracować i prowadzić wymianę informacji.
[17] [wstawić pełny tytuł i odniesienie do publikacji w Dzienniku Urzędowym, kiedy już będą znane]	[17] [wstawić pełny tytuł i odniesienie do publikacji w Dzienniku Urzędowym, kiedy już będą znane]

Poprawka 9
Wniosek dotyczący dyrektywy
Motyw 15

Tekst proponowany przez Komisję	*Poprawka*
(15) Utrzymywanie i zachowanie wiarygodnego, odpornego i bezpiecznego systemu nazw domen (DNS) odgrywa decydującą rolę w utrzymaniu integralności internetu oraz ma istotne znaczenie dla jego nieprzerwanego i stabilnego działania, od którego zależą gospodarka cyfrowa i społeczeństwo cyfrowe. W związku z tym niniejsza dyrektywa powinna mieć zastosowanie do wszystkich dostawców usług DNS w całym łańcuchu rozwiązywania nazw DNS, z uwzględnieniem operatorów głównych serwerów nazw, serwerów nazw domen najwyższego poziomu (TLD), autorytatywnych serwerów nazw dla nazw domen i rekurencyjnych resolwerów.	(15) Utrzymywanie i zachowanie wiarygodnego, odpornego i bezpiecznego systemu nazw domen (DNS) odgrywa decydującą rolę w utrzymaniu integralności internetu oraz ma istotne znaczenie dla jego nieprzerwanego i stabilnego działania, od którego zależą gospodarka cyfrowa***, rynek wewnętrzny*** i społeczeństwo cyfrowe. W związku z tym niniejsza dyrektywa powinna mieć zastosowanie do wszystkich dostawców usług DNS w całym łańcuchu rozwiązywania nazw DNS, z uwzględnieniem operatorów głównych serwerów nazw, serwerów nazw domen najwyższego poziomu (TLD), autorytatywnych serwerów nazw dla nazw domen i rekurencyjnych resolwerów***, dostawców usług w zakresie rejestracji prywatności lub serwerów proxy, brokerów lub odsprzedawców domen oraz wszelkich innych usług związanych z rejestracją nazw domen***.

Poprawka 10
Wniosek dotyczący dyrektywy
Motyw 20

Tekst proponowany przez Komisję	*Poprawka*
(20) Te coraz większe współzależności wynikają z coraz bardziej transgranicznej i współzależnej sieci świadczenia usług, wykorzystującej kluczową infrastrukturę w całej Unii w sektorach energetyki, transportu, infrastruktury cyfrowej, wody pitnej i ścieków, zdrowia, niektórych aspektów administracji publicznej, a także przestrzeni kosmicznej, jeżeli chodzi o świadczenie niektórych usług zależnych od naziemnej infrastruktury będącej własnością państw członkowskich albo podmiotów prywatnych oraz która jest zarządzana i obsługiwana przez państwa członkowskie albo podmioty prywatne, a zatem nieobejmującej infrastruktury będącej własnością Unii bądź zarządzanej lub obsługiwanej przez Unię lub w jej imieniu w ramach jej programów kosmicznych. Wspomniane współzależności oznaczają, że każde zakłócenie, nawet początkowo ograniczające się do jednego podmiotu lub jednego sektora, może wywołać szerzej zakrojony efekt kaskadowy, którego potencjalne negatywne skutki dla świadczenia usług na całym rynku wewnętrznym mogą być dalekosiężne i długotrwałe. Pandemia COVID-19 uwydatniła podatność naszych coraz bardziej współzależnych społeczeństw w obliczu ryzyka o niskim prawdopodobieństwie wystąpienia.	(20) Te coraz większe współzależności wynikają z coraz bardziej transgranicznej i współzależnej sieci świadczenia usług, wykorzystującej kluczową infrastrukturę w całej Unii w sektorach energetyki, transportu, infrastruktury cyfrowej, wody pitnej i ścieków, zdrowia, niektórych aspektów administracji publicznej, a także przestrzeni kosmicznej, jeżeli chodzi o świadczenie niektórych usług zależnych od naziemnej infrastruktury będącej własnością państw członkowskich albo podmiotów prywatnych oraz która jest zarządzana i obsługiwana przez państwa członkowskie albo podmioty prywatne, a zatem nieobejmującej infrastruktury będącej własnością Unii bądź zarządzanej lub obsługiwanej przez Unię lub w jej imieniu w ramach jej programów kosmicznych. Wspomniane współzależności oznaczają, że każde zakłócenie, nawet początkowo ograniczające się do jednego podmiotu lub jednego sektora, może wywołać szerzej zakrojony efekt kaskadowy, którego potencjalne negatywne skutki dla świadczenia usług na całym rynku wewnętrznym mogą być dalekosiężne i długotrwałe. Pandemia COVID-19 uwydatniła podatność naszych coraz bardziej współzależnych społeczeństw w obliczu ryzyka o niskim prawdopodobieństwie wystąpienia ***oraz potrzebę ochrony rynku wewnętrznego poprzez wspólne strategie i działania na szczeblu Unii***.

Poprawka 11
Wniosek dotyczący dyrektywy
Motyw 23

Tekst proponowany przez Komisję	*Poprawka*
(23) Właściwe organy lub CSIRT powinny otrzymywać zgłoszenia incydentów od podmiotów w ***sposób*** efektywny i skuteczny. Pojedynczym punktom kontaktowym należy powierzyć zadanie przekazywania zgłoszeń incydentów pojedynczym punktom kontaktowym innych państw członkowskich, których incydent dotyczy. ***Na szczeblu organów państw członkowskich,*** aby zapewnić w każdym państwie członkowskim jeden pojedynczy punkt kontaktowy, pojedyncze punkty kontaktowe powinny być również adresatem stosownych informacji na temat incydentów dotyczących podmiotów sektora finansowego przekazywanych przez właściwe organy na mocy rozporządzenia XXXX/XXXX, które to informacje punkty te powinny być w stanie przekazywać, stosownie do przypadku, odpowiednim właściwym organom krajowym lub CSIRT na mocy niniejszej dyrektywy.	(23) Właściwe organy lub CSIRT powinny otrzymywać zgłoszenia incydentów od podmiotów w ***znormalizowany,*** efektywny i skuteczny ***sposób***. Pojedynczym punktom kontaktowym należy powierzyć zadanie przekazywania zgłoszeń incydentów pojedynczym punktom kontaktowym innych państw członkowskich, których incydent dotyczy. Aby zapewnić w każdym państwie członkowskim jeden pojedynczy punkt kontaktowy, pojedyncze punkty kontaktowe powinny być również adresatem stosownych informacji na temat incydentów dotyczących podmiotów sektora finansowego przekazywanych przez właściwe organy na mocy rozporządzenia XXXX/XXXX, które to informacje punkty te powinny być w stanie przekazywać, stosownie do przypadku, odpowiednim właściwym organom krajowym lub CSIRT na mocy niniejszej dyrektywy.

Poprawka 12
Wniosek dotyczący dyrektywy
Motyw 25

Tekst proponowany przez Komisję	*Poprawka*
(25) Jeżeli chodzi o dane osobowe, CSIRT powinny być w stanie zapewnić – zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679[19] – w imieniu i na wniosek podmiotu w rozumieniu niniejszej dyrektywy **–** ***proaktywne*** skanowanie sieci i systemów informatycznych wykorzystywanych przez te podmioty do świadczenia usług. Państwa członkowskie powinny dążyć do zapewnienia równego poziomu zdolności technicznych wszystkich sektorowych CSIRT. Państwa członkowskie mogą zwrócić się do Agencji Unii Europejskiej	(25) Jeżeli chodzi o ***wykrywanie i ograniczanie specyficznych zagrożeń godzących w*** dane osobowe ***i zapobieganie im***, CSIRT powinny być w stanie zapewnić – zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679[19] – w imieniu i na wniosek podmiotu w rozumieniu niniejszej dyrektywy**,** skanowanie sieci i systemów informatycznych wykorzystywanych przez te podmioty do świadczenia usług. Państwa członkowskie powinny dążyć do zapewnienia równego poziomu zdolności technicznych wszystkich sektorowych

ds. Cyberbezpieczeństwa (ENISA) o pomoc przy tworzeniu krajowych CSIRT.	CSIRT. Państwa członkowskie mogą zwrócić się do Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) o pomoc przy tworzeniu krajowych CSIRT.
[19] 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. L 119 z 4.5.2016, s. 1).	[19] 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. L 119 z 4.5.2016, s. 1).

Poprawka 13
Wniosek dotyczący dyrektywy
Motyw 26 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(26a) W krajowych strategiach cyberbezpieczeństwa państw członkowskich powinny się znaleźć strategie polityczne dotyczące promocji i integracji inteligentnych systemów do zapobiegania cyberincydentom i cyberzagrożeniom oraz ich wykrywania. Państwa członkowskie powinny, zgodnie ze swoimi krajowymi strategiami cyberbezpieczeństwa, zadbać o podnoszenie świadomości w dziedzinie cyberbezpieczeństwa i umiejętności w tej dziedzinie w celu ochrony konsumentów. Proces przyjmowania krajowych strategii cyberbezpieczeństwa w państwach członkowskich powinien odbywać się w taki sposób, aby zapewnić legalny dostęp do informacji.

Poprawka 14
Wniosek dotyczący dyrektywy
Motyw 27

Tekst proponowany przez Komisję	*Poprawka*
(27) Zgodnie z załącznikiem do zalecenia Komisji (UE) 2017/1548 w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę („plan”)[20] incydent na dużą skalę powinien oznaczać incydent mający znaczący wpływ na co najmniej dwa państwa członkowskie lub taki, który powoduje na tyle duże zakłócenia, że dotknięte nimi państwo członkowskie nie jest samo w stanie na nie skutecznie zareagować. W zależności od przyczyny i wpływu incydenty na dużą skalę mogą przerodzić się w prawdziwy kryzys uniemożliwiający prawidłowe funkcjonowanie rynku wewnętrznego. Biorąc pod uwagę szeroki zakres oraz, w większości przypadków, transgraniczny charakter takich incydentów, państwa członkowskie i odpowiednie instytucje, organy i agencje Unii powinny współpracować na poziomie technicznym, operacyjnym i politycznym w celu odpowiedniej koordynacji reakcji w całej Unii.	(27) Zgodnie z załącznikiem do zalecenia Komisji (UE) 2017/1548 w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę („plan”)[20] incydent na dużą skalę powinien oznaczać incydent mający znaczący wpływ na co najmniej dwa państwa członkowskie lub taki, który powoduje na tyle duże zakłócenia, że dotknięte nimi państwo członkowskie nie jest samo w stanie na nie skutecznie zareagować***, co tym samym zagraża rynkowi wewnętrznemu***. W zależności od przyczyny i wpływu incydenty na dużą skalę mogą przerodzić się w prawdziwy kryzys uniemożliwiający prawidłowe funkcjonowanie rynku wewnętrznego. Biorąc pod uwagę szeroki zakres oraz, w większości przypadków, transgraniczny charakter takich incydentów, państwa członkowskie i odpowiednie instytucje, organy i agencje Unii powinny współpracować na poziomie technicznym, operacyjnym i politycznym w celu odpowiedniej koordynacji reakcji w całej Unii.
[20] Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L 239 z 19.9.2017, s. 36).	[20] Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L 239 z 19.9.2017, s. 36).

Poprawka 15
Wniosek dotyczący dyrektywy
Motyw 28

Tekst proponowany przez Komisję	*Poprawka*
(28) Ponieważ wykorzystywanie podatności sieci i systemów informatycznych może powodować znaczące zakłócenia i szkody, ważnym czynnikiem w ograniczaniu ryzyka	(28) Ponieważ wykorzystywanie podatności sieci i systemów informatycznych może powodować znaczące zakłócenia i szkody ***dla przedsiębiorstw i konsumentów***, ważnym

w cyberprzestrzeni jest szybkie identyfikowanie takich podatności i ich eliminowanie. Podmioty, które opracowują takie systemy, powinny zatem ustanowić odpowiednie procedury postępowania w przypadku wykrycia takich podatności. Ponieważ podatności często są wykrywane i zgłaszane (ujawniane) przez osoby trzecie (podmioty zgłaszające), producent lub dostawca produktów lub usług ICT również powinien wprowadzić niezbędne procedury regulujące odbieranie od osób trzecich informacji na temat podatności. W tym względzie normy międzynarodowe ISO/IEC 30111 i ISO/IEC 29417 zawierają wytyczne dotyczące, odpowiednio, postępowania w przypadku wykrycia podatności i ujawniania podatności. Jeśli chodzi o ujawnianie podatności, szczególnie ważna jest koordynacja między podmiotami zgłaszającymi a producentami lub dostawcami produktów lub usług ICT. Skoordynowane ujawnianie podatności to ustrukturyzowany proces, w ramach którego podatności są zgłaszane organizacjom w sposób umożliwiający organizacji zdiagnozowanie i wyeliminowanie danej podatności, zanim szczegółowe informacje dotyczące podatności zostaną ujawnione osobom trzecim lub podane do wiadomości publicznej. Skoordynowane ujawnianie podatności powinno także obejmować koordynację między podmiotem zgłaszającym a organizacją w odniesieniu do terminarza eliminowania podatności i podania ich do wiadomości publicznej.	czynnikiem w ograniczaniu ryzyka w cyberprzestrzeni jest szybkie identyfikowanie takich podatności i ich eliminowanie. Podmioty, które opracowują takie systemy, powinny zatem ustanowić odpowiednie procedury postępowania w przypadku wykrycia takich podatności. Ponieważ podatności często są wykrywane i zgłaszane (ujawniane) przez osoby trzecie (podmioty zgłaszające), producent lub dostawca produktów lub usług ICT również powinien wprowadzić niezbędne procedury regulujące odbieranie od osób trzecich informacji na temat podatności. W tym względzie normy międzynarodowe ISO/IEC 30111 i ISO/IEC 29417 zawierają wytyczne dotyczące, odpowiednio, postępowania w przypadku wykrycia podatności i ujawniania podatności. Jeśli chodzi o ujawnianie podatności, szczególnie ważna jest koordynacja między podmiotami zgłaszającymi a producentami lub dostawcami produktów lub usług ICT. Skoordynowane ujawnianie podatności to ustrukturyzowany proces, w ramach którego podatności są zgłaszane organizacjom w sposób umożliwiający organizacji zdiagnozowanie i wyeliminowanie danej podatności, zanim szczegółowe informacje dotyczące podatności zostaną ujawnione osobom trzecim lub podane do wiadomości publicznej. Skoordynowane ujawnianie podatności powinno także obejmować koordynację między podmiotem zgłaszającym a organizacją w odniesieniu do terminarza eliminowania podatności i podania ich do wiadomości publicznej.

Poprawka 16
Wniosek dotyczący dyrektywy
Motyw 28 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(28a) Komisja, ENISA i państwa członkowskie powinny nadal wspierać międzynarodowe dostosowanie do norm i

	istniejących najlepszych praktyk branżowych w dziedzinie zarządzania ryzykiem, na przykład w obszarach oceny bezpieczeństwa łańcucha dostaw, wymiany informacji i ujawniania podatności.

Poprawka 17
Wniosek dotyczący dyrektywy
Motyw 30

Tekst proponowany przez Komisję	*Poprawka*
(30) Dostęp do prawidłowych i terminowych informacji na temat podatności dotyczących produktów i usług ICT pozwala usprawnić zarządzanie ryzykiem w cyberprzestrzeni. W tym względzie ważnym narzędziem dla podmiotów i ich użytkowników, ale również dla właściwych organów krajowych i CSIRT są źródła publicznie dostępnych informacji na temat podatności. Z tego powodu ENISA powinna ustanowić ***rejestr*** podatności, w ***którym*** podmioty niezbędne i istotne oraz ich dostawcy, a także podmioty, które nie są objęte zakresem stosowania niniejszej dyrektywy, mogą na zasadzie dobrowolności ujawniać podatności i przekazywać informacje na temat podatności, dzięki którym użytkownicy mogą wprowadzać odpowiednie środki ograniczające ryzyko.	(30) Dostęp do prawidłowych i terminowych informacji na temat podatności dotyczących produktów i usług ICT pozwala usprawnić zarządzanie ryzykiem w cyberprzestrzeni. W tym względzie ważnym narzędziem dla podmiotów i ich użytkowników, ale również dla właściwych organów krajowych i CSIRT są źródła publicznie dostępnych informacji na temat podatności. Z tego powodu ENISA powinna ustanowić ***bazę danych dotyczących*** podatności, w ***której*** podmioty niezbędne i istotne oraz ich dostawcy, a także podmioty, które nie są objęte zakresem stosowania niniejszej dyrektywy, mogą na zasadzie dobrowolności ujawniać podatności i przekazywać informacje na temat podatności, dzięki którym użytkownicy mogą wprowadzać odpowiednie środki ograniczające ryzyko.

Poprawka 18
Wniosek dotyczący dyrektywy
Motyw 31

Tekst proponowany przez Komisję	*Poprawka*
(31) Choć istnieją podobne rejestry podatności lub bazy danych dotyczących podatności, są one prowadzone i utrzymywane przez podmioty, które nie mają siedziby w Unii. ***Europejski rejestr***	(31) Choć istnieją podobne rejestry podatności lub bazy danych dotyczących podatności, są one prowadzone i utrzymywane przez podmioty, które nie mają siedziby w Unii. ***Europejska baza***

podatności ***utrzymywany*** przez ENISA ***zapewniłby*** lepszą przejrzystość w odniesieniu do procesu publikacji poprzedzającego oficjalne ujawnienie podatności, a także odporność w przypadku zakłóceń lub przerw w świadczeniu podobnych usług. Aby uniknąć powielania podejmowanych działań i dążyć do jak największej komplementarności, ENISA powinna zbadać możliwość zawarcia umów o współpracy strukturalnej z ***podobnymi rejestrami*** w jurysdykcjach państw trzecich.	***danych dotyczących*** podatności ***utrzymywana*** przez ENISA ***zapewniłaby*** lepszą przejrzystość w odniesieniu do procesu publikacji poprzedzającego oficjalne ujawnienie podatności, a także odporność w przypadku zakłóceń lub przerw w świadczeniu podobnych usług. Aby uniknąć powielania podejmowanych działań i dążyć do jak największej komplementarności, ENISA powinna zbadać możliwość zawarcia umów o współpracy strukturalnej z ***rejestrami podatności lub bazami danych dotyczących podatności*** w jurysdykcjach państw trzecich ***i przekazywania sprawozdań do odpowiednich rejestrów, pod warunkiem że takie działania nie naruszają ochrony poufności i tajemnicy handlowej***.

Poprawka 19
Wniosek dotyczący dyrektywy
Motyw 32

Tekst proponowany przez Komisję	*Poprawka*
(32) Co dwa lata Grupa Współpracy powinna opracowywać program prac obejmujący działania, które mają zostać podjęte przez Grupę w celu realizacji jej celów i zadań. Aby uniknąć potencjalnych zakłóceń w pracy Grupy, ramy czasowe pierwszego programu przyjętego na podstawie niniejszej dyrektywy należy zharmonizować z ramami czasowymi ostatniego programu przyjętego na podstawie dyrektywy (UE) 2016/1148.	(32) Co dwa lata Grupa Współpracy powinna ***omawiać priorytety polityczne i główne wyzwania dotyczące cyberbezpieczeństwa oraz*** opracowywać program prac obejmujący działania, które mają zostać podjęte przez Grupę w celu realizacji jej celów i zadań. Aby uniknąć potencjalnych zakłóceń w pracy Grupy, ramy czasowe pierwszego programu przyjętego na podstawie niniejszej dyrektywy należy zharmonizować z ramami czasowymi ostatniego programu przyjętego na podstawie dyrektywy (UE) 2016/1148.

Poprawka 20
Wniosek dotyczący dyrektywy
Motyw 32 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(32a) Grupa Współpracy powinna składać się z przedstawicieli państw członkowskich, Komisji i ENISA.

Poprawka 21
Wniosek dotyczący dyrektywy
Motyw 34

Tekst proponowany przez Komisję	*Poprawka*
(34) Grupa Współpracy powinna pozostać elastycznym forum i być w stanie reagować na zmieniające się i nowe priorytety i wyzwania polityczne, przy jednoczesnym uwzględnieniu dostępności zasobów. Powinna ona organizować regularne wspólne spotkania z odpowiednimi zainteresowanymi stronami z sektora prywatnego z całej Unii w celu omawiania działań realizowanych przez Grupę i gromadzenia informacji na temat pojawiających się wyzwań w zakresie polityki. Aby zacieśnić współpracę na szczeblu unijnym, Grupa powinna rozważyć zaproszenie organów i agencji unijnych zaangażowanych w kształtowanie polityki cyberbezpieczeństwa, takich jak Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3), Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA) oraz Agencja Unii Europejskiej ds. Programu Kosmicznego, do uczestnictwa w pracach Grupy.	(34) Grupa Współpracy powinna pozostać elastycznym forum i być w stanie reagować na zmieniające się i nowe priorytety i wyzwania polityczne, przy jednoczesnym uwzględnieniu dostępności zasobów. Powinna ona organizować regularne wspólne spotkania z odpowiednimi zainteresowanymi stronami z sektora prywatnego z całej Unii w celu omawiania działań realizowanych przez Grupę i gromadzenia informacji na temat pojawiających się wyzwań w zakresie polityki. Aby zacieśnić współpracę na szczeblu unijnym, Grupa powinna rozważyć zaproszenie organów i agencji unijnych zaangażowanych w kształtowanie polityki cyberbezpieczeństwa, takich jak Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3), Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA) oraz Agencja Unii Europejskiej ds. Programu Kosmicznego, do uczestnictwa w pracach Grupy ***oraz inne odpowiednie organy i agencje unijne***.

Poprawka 22
Wniosek dotyczący dyrektywy
Motyw 35

Tekst proponowany przez Komisję	*Poprawka*
(35) Właściwe organy i CSIRT powinny być upoważnione do uczestniczenia w programach wymiany dla urzędników z innych państw członkowskich w celu usprawnienia współpracy. Właściwe organy powinny podejmować działania niezbędne do zapewnienia urzędnikom z innych państw członkowskich możliwości efektywnego angażowania się w działalność przyjmującego właściwego organu.	(35) Właściwe organy i CSIRT powinny być upoważnione do uczestniczenia w programach wymiany ***i wspólnych programach szkoleniowych*** dla urzędników z innych państw członkowskich w celu usprawnienia współpracy ***i zwiększenia zaufania między państwami członkowskimi***. Właściwe organy powinny podejmować działania niezbędne do zapewnienia urzędnikom z innych państw członkowskich możliwości efektywnego angażowania się w działalność przyjmującego właściwego organu ***lub CSIRT***.

Poprawka 23
Wniosek dotyczący dyrektywy
Motyw 39

Tekst proponowany przez Komisję	*Poprawka*
(39) Na potrzeby niniejszej dyrektywy termin „zdarzenie potencjalnie wypadkowe" powinien odnosić się do zdarzenia, które może spowodować szkodę, ale którego pełnemu wystąpieniu udało się skutecznie zapobiec.	***skreśla się***

Poprawka 24
Wniosek dotyczący dyrektywy
Motyw 45 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(45a) Dodatkowo podmioty powinny również dbać o odpowiednie kształcenie i szkolenie w dziedzinie cyberbezpieczeństwa personelu wszystkich szczebli.

Poprawka 25
Wniosek dotyczący dyrektywy
Motyw 46

Tekst proponowany przez Komisję	*Poprawka*
(46) Aby w większym stopniu ograniczyć kluczowe ryzyka w łańcuchu dostaw i wesprzeć podmioty działające w sektorach objętych niniejszą dyrektywą w odpowiednim zarządzaniu ryzykiem w cyberprzestrzeni związanym z łańcuchem dostaw i dostawcami, Grupa Współpracy przy udziale odpowiednich organów krajowych, we współpracy z Komisją i ENISA, powinna przeprowadzić skoordynowane sektorowe oceny ryzyka w łańcuchach dostaw, tak jak to miało już miejsce w przypadku sieci 5G w następstwie zalecenia (UE) 2019/534 w sprawie cyberbezpieczeństwa sieci 5G[21], aby zidentyfikować w każdym sektorze krytyczne usługi, systemy lub produkty ICT, istotne zagrożenia i podatności.	*(Nie dotyczy polskiej wersji językowej)*

[21] Zalecenie Komisji (UE) 2019/534 z dnia 26 marca 2019 r. Cyberbezpieczeństwo sieci 5G (Dz.U. L 88 z 29.3.2019, s. 42).

Poprawka 26
Wniosek dotyczący dyrektywy
Motyw 47

Tekst proponowany przez Komisję	*Poprawka*
(47) W świetle specyfiki danego sektora w ocenach ryzyka w łańcuchu dostaw należy uwzględnić zarówno czynniki techniczne, jak i – w stosownych przypadkach – pozatechniczne, w tym te określone w zaleceniu (UE) 2019/534, w unijnej skoordynowanej ocenie ryzyka w zakresie bezpieczeństwa sieci 5G oraz w unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G uzgodnionym przez Grupę Współpracy. Aby zidentyfikować łańcuchy dostaw,	(47) W świetle specyfiki danego sektora ***i jego poziomu krytyczności*** w ocenach ryzyka w łańcuchu dostaw należy uwzględnić zarówno czynniki techniczne, jak i – w stosownych przypadkach – pozatechniczne, w tym te określone w zaleceniu (UE) 2019/534, w unijnej skoordynowanej ocenie ryzyka w zakresie bezpieczeństwa sieci 5G oraz w unijnym zestawie narzędzi na potrzeby cyberbezpieczeństwa sieci 5G uzgodnionym przez Grupę Współpracy.

które należy poddać skoordynowanej ocenie ryzyka, należy wziąć pod uwagę następujące kryteria: (i) zakres, w jakim podmioty niezbędne i istotne wykorzystują konkretne krytyczne usługi, systemy lub produkty ICT i na nich polegają; (ii) znaczenie konkretnych krytycznych usług, systemów lub produktów ICT dla wykonywania krytycznych lub wrażliwych funkcji, w tym przetwarzania danych osobowych; (iii) dostępność alternatywnych usług, systemów lub produktów ICT; (iv) odporność całego łańcucha dostaw usług, systemów lub produktów ICT na zdarzenia powodujące zakłócenia oraz (v) w przypadku pojawiających się usług, systemów lub produktów ICT – ich potencjalne przyszłe znaczenie dla działalności podmiotów.

Aby zidentyfikować łańcuchy dostaw, które należy poddać skoordynowanej ocenie ryzyka, należy wziąć pod uwagę następujące kryteria: (i) zakres, w jakim podmioty niezbędne i istotne wykorzystują konkretne krytyczne usługi, systemy lub produkty ICT i na nich polegają; (ii) znaczenie konkretnych krytycznych usług, systemów lub produktów ICT dla wykonywania krytycznych lub wrażliwych funkcji, w tym przetwarzania danych osobowych; (iii) dostępność alternatywnych usług, systemów lub produktów ICT; (iv) odporność całego łańcucha dostaw usług, systemów lub produktów ICT na zdarzenia powodujące zakłócenia oraz (v) w przypadku pojawiających się usług, systemów lub produktów ICT – ich potencjalne przyszłe znaczenie dla działalności podmiotów.

Poprawka 27
Wniosek dotyczący dyrektywy
Motyw 51

Tekst proponowany przez Komisję	*Poprawka*
(51) Rynek wewnętrzny jest bardziej niż kiedykolwiek uzależniony od funkcjonowania internetu. Usługi niemal wszystkich podmiotów niezbędnych i istotnych zależą od usług świadczonych przez internet. Aby zapewnić sprawne świadczenie usług przez podmioty niezbędne i istotne, publiczne sieci łączności elektronicznej, jak na przykład internetowe sieci szkieletowe czy podmorskie kable telekomunikacyjne, powinny wprowadzić odpowiednie środki w zakresie cyberbezpieczeństwa i zgłaszać incydenty w tym zakresie.	(51) Rynek wewnętrzny jest bardziej niż kiedykolwiek uzależniony od funkcjonowania internetu. Usługi niemal wszystkich podmiotów niezbędnych i istotnych zależą od usług świadczonych przez internet***, a konsumenci polegają na nich w najważniejszych aspektach codziennego życia***. Aby zapewnić sprawne świadczenie usług przez podmioty niezbędne i istotne, publiczne sieci łączności elektronicznej, jak na przykład internetowe sieci szkieletowe czy podmorskie kable telekomunikacyjne, powinny wprowadzić odpowiednie środki w zakresie cyberbezpieczeństwa i zgłaszać incydenty w tym zakresie.

Poprawka 28
Wniosek dotyczący dyrektywy
Motyw 52

Tekst proponowany przez Komisję	*Poprawka*
(52) ***W stosownych przypadkach podmioty powinny informować*** odbiorców swoich usług o szczególnych i istotnych zagrożeniach oraz o środkach, które odbiorcy ci mogą zastosować w celu ograniczenia wynikłego ryzyka, na jakie są sami narażeni***. Wymóg informowania tych odbiorców o takich zagrożeniach*** nie ***powinien*** zwalniać podmiotu z obowiązku zastosowania na własny koszt odpowiednich i natychmiastowych środków w celu zapobieżenia lub zaradzenia wszelkim cyberzagrożeniom oraz przywrócenia normalnego poziomu bezpieczeństwa danej usługi. Udzielanie odbiorcom takich informacji na temat zagrożeń bezpieczeństwa powinno odbywać się bezpłatnie.	(52) ***Podmioty powinny dążyć do informowania*** odbiorców swoich usług o szczególnych i istotnych zagrożeniach oraz o środkach, które odbiorcy ci mogą zastosować w celu ograniczenia wynikłego ryzyka, na jakie są sami narażeni***, zwłaszcza jeżeli takie środki mogą zwiększyć ochronę konsumentów.*** Nie ***powinno to*** zwalniać podmiotu z obowiązku zastosowania na własny koszt odpowiednich i natychmiastowych środków w celu zapobieżenia lub zaradzenia wszelkim cyberzagrożeniom oraz przywrócenia normalnego poziomu bezpieczeństwa danej usługi. Udzielanie odbiorcom takich informacji na temat zagrożeń bezpieczeństwa powinno odbywać się bezpłatnie ***i w przystępnym języku***.

Poprawka 29
Wniosek dotyczący dyrektywy
Motyw 53

Tekst proponowany przez Komisję	*Poprawka*
(53) W szczególności dostawcy publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej powinni informować odbiorców usługi o szczególnych i istotnych cyberzagrożeniach oraz o środkach, które mogą zastosować ***w celu ochrony bezpieczeństwa*** swoich ***środków*** łączności, na przykład ***przez zastosowanie*** szczególnych rodzajów oprogramowania lub technologii szyfrowania.	(53) W szczególności dostawcy publicznych sieci łączności elektronicznej lub publicznie dostępnych usług łączności elektronicznej powinni informować odbiorców usługi o szczególnych i istotnych cyberzagrożeniach oraz o ***dodatkowych*** środkach, które mogą zastosować***, aby chronić bezpieczeństwo*** swoich ***urządzeń i*** łączności, na przykład ***za pomocą*** szczególnych rodzajów oprogramowania lub technologii szyfrowania.

Poprawka 30
Wniosek dotyczący dyrektywy
Motyw 54

Tekst proponowany przez Komisję	*Poprawka*
(54) Aby zagwarantować bezpieczeństwo sieci i usług łączności elektronicznej, należy promować korzystanie z szyfrowania, w szczególności szyfrowania end-to-end, a w razie konieczności uczynić je obowiązkowym dla dostawców takich usług i sieci zgodnie z zasadą uwzględniania bezpieczeństwa i prywatności w sposób domyślny i na etapie projektowania do celów ***art. 18***. Korzystanie z szyfrowania end-to-end ***należy pogodzić z uprawnieniami*** państw członkowskich ***w zakresie zapewnienia ochrony*** ich podstawowych interesów bezpieczeństwa i bezpieczeństwa publicznego, a także ***w zakresie umożliwiania wykrywania*** i ***ścigania*** przestępstw oraz ***prowadzenia*** dochodzeń w ich sprawie zgodnie z prawem Unii. Rozwiązania zapewniające zgodny z prawem dostęp do informacji przesyłanych z wykorzystaniem transmisji szyfrowanej end-to-end powinny gwarantować zachowanie skuteczności szyfrowania pod względem ochrony prywatności i bezpieczeństwa łączności, zapewniając jednocześnie możliwość skutecznego reagowania na przestępstwa.	(54) Aby zagwarantować bezpieczeństwo sieci i usług łączności elektronicznej, należy promować korzystanie z szyfrowania, w szczególności szyfrowania end-to-end, a w razie konieczności uczynić je obowiązkowym dla dostawców takich usług i sieci zgodnie z zasadą uwzględniania bezpieczeństwa i prywatności w sposób domyślny i na etapie projektowania do celów ***zarządzania ryzykiem w cyberprzestrzeni***. Korzystanie z szyfrowania end-to-end ***nie narusza uprawnień, polityki i procedur*** państw członkowskich***, które służą ochronie*** ich podstawowych interesów bezpieczeństwa i bezpieczeństwa publicznego, a także ***umożliwiają wykrywanie*** i ***ściganie*** przestępstw oraz ***prowadzenie*** dochodzeń w ich sprawie zgodnie z prawem Unii. Rozwiązania zapewniające zgodny z prawem dostęp do informacji przesyłanych z wykorzystaniem transmisji szyfrowanej end-to-end powinny gwarantować zachowanie skuteczności szyfrowania pod względem ochrony prywatności i bezpieczeństwa łączności, zapewniając jednocześnie możliwość skutecznego reagowania na przestępstwa. ***Podejmowane działania muszą być ściśle zgodne z zasadami proporcjonalności i pomocniczości.***

Poprawka 31
Wniosek dotyczący dyrektywy
Motyw 55

Tekst proponowany przez Komisję	*Poprawka*
(55) W niniejszej dyrektywie określono ***dwuetapowe*** podejście do zgłaszania incydentów w celu zapewnienia odpowiedniej równowagi między szybkim	(55) W niniejszej dyrektywie określono ***stopniowe*** podejście do zgłaszania incydentów w celu zapewnienia odpowiedniej równowagi między szybkim

zgłaszaniem, co pomoże zahamować potencjalne rozprzestrzenianie się incydentów i pozwoli podmiotom zwrócić się o wsparcie, a szczegółowym zgłaszaniem, co umożliwi wyciągnięcie cennych wniosków z poszczególnych incydentów i z czasem przyczyni się do zwiększenia odporności poszczególnych przedsiębiorstw i całych sektorów na cyberzagrożenia. W przypadku gdy podmioty powezmą wiedzę o incydencie, powinny mieć obowiązek dokonania wstępnego zgłoszenia w ciągu ***24*** godzin, a następnie przedłożenia – ***w terminie nie dłuższym niż miesiąc*** – sprawozdania końcowego. Wstępne zgłoszenie powinno zawierać jedynie informacje absolutnie niezbędne do tego, by poinformować właściwe organy o wystąpieniu incydentu i umożliwić podmiotowi zwrócenie się o wsparcie, jeśli zachodzi taka potrzeba. W stosownych przypadkach w takim zgłoszeniu należy wskazać, czy, jak przypuszcza się, incydent został wywołany działaniem bezprawnym lub działaniem w złym zamiarze. Państwa członkowskie powinny zapewnić, aby wymóg dokonania wstępnego zgłoszenia nie powodował przekierowania zasobów podmiotu zgłaszającego z działań podejmowanych w reakcji na incydent, które to działania powinny mieć charakter priorytetowy. Aby dodatkowo zapobiec sytuacji, w której obowiązki w zakresie zgłaszania incydentów ograniczą zdolność podmiotu do podjęcia reakcji na incydent albo w inny sposób osłabią działania podmiotu w tym zakresie, państwa członkowskie powinny również przewidzieć – w należycie uzasadnionych przypadkach i w porozumieniu z właściwymi organami lub CSIRT – możliwość odstąpienia w przypadku danego podmiotu od ***terminu 24 godzin na dokonanie wstępnego zgłoszenia i terminu jednego miesiąca na przedłożenie sprawozdania końcowego***.

zgłaszaniem, co pomoże zahamować potencjalne rozprzestrzenianie się incydentów i pozwoli podmiotom zwrócić się o wsparcie, a szczegółowym zgłaszaniem, co umożliwi wyciągnięcie cennych wniosków z poszczególnych incydentów i z czasem przyczyni się do zwiększenia odporności poszczególnych przedsiębiorstw i całych sektorów na cyberzagrożenia. W przypadku gdy podmioty powezmą wiedzę o incydencie ***lub zdarzeniu potencjalnie wypadkowym***, powinny mieć obowiązek dokonania wstępnego zgłoszenia w ciągu ***72*** godzin, a następnie przedłożenia – ***najpóźniej trzy miesiące po wstępnym zgłoszeniu – wyczerpującego raportu i*** sprawozdania końcowego ***najpóźniej po upływie miesiąca po ograniczeniu incydentu***. Wstępne zgłoszenie powinno zawierać jedynie informacje absolutnie niezbędne do tego, by poinformować właściwe organy o wystąpieniu incydentu i umożliwić podmiotowi zwrócenie się o wsparcie, jeśli zachodzi taka potrzeba. W stosownych przypadkach w takim zgłoszeniu należy wskazać, czy, jak przypuszcza się, incydent został wywołany działaniem bezprawnym lub działaniem w złym zamiarze. Państwa członkowskie powinny zapewnić, aby wymóg dokonania wstępnego zgłoszenia nie powodował przekierowania zasobów podmiotu zgłaszającego z działań podejmowanych w reakcji na incydent, które to działania powinny mieć charakter priorytetowy. ***Wstępne zgłoszenie powinno być poprzedzone wczesnym ostrzeżeniem w ciągu pierwszych 24 godzin bez konieczności ujawniania dodatkowych informacji. Wczesne ostrzeżenie należy przekazać jak najszybciej, co umożliwi podmiotom szybkie zwrócenie się o wsparcie do właściwych organów lub CSIRT, oraz umożliwi właściwym organom lub CSIRT ograniczenie potencjalnego rozprzestrzeniania się zgłaszanego incydentu, a także posłuży jako narzędzie orientacji sytuacyjnej***

CSIRT. Aby dodatkowo zapobiec sytuacji, w której obowiązki w zakresie zgłaszania incydentów ograniczą zdolność podmiotu do podjęcia reakcji na incydent albo w inny sposób osłabią działania podmiotu w tym zakresie, państwa członkowskie powinny również przewidzieć – w należycie uzasadnionych przypadkach i w porozumieniu z właściwymi organami lub CSIRT – możliwość odstąpienia w przypadku danego podmiotu od ***przewidzianych terminów***.

Poprawka 32
Wniosek dotyczący dyrektywy
Motyw 56

Tekst proponowany przez Komisję	*Poprawka*
(56) Podmioty niezbędne i istotne znajdują się często w sytuacji, w której konkretny incydent, ze względu na jego cechy, należy zgłosić różnym organom w wyniku istnienia obowiązków w zakresie zgłaszania przewidzianych w różnych instrumentach prawnych. Takie przypadki powodują dodatkowe obciążenie, a ponadto mogą rodzić niepewność dotyczącą formatu i procedur dokonywania takich zgłoszeń. W związku z tym i w celu uproszczenia zgłaszania incydentów bezpieczeństwa państwa członkowskie powinny ustanowić pojedynczy punkt kontaktowy na potrzeby wszystkich zgłoszeń wymaganych na podstawie niniejszej dyrektywy, a także na podstawie innych przepisów unijnych, takich jak rozporządzenie (UE) 2016/679 i dyrektywa 2002/58/WE. ENISA, we współpracy z Grupą Współpracy, powinna opracować wspólne wzory zgłoszeń w formie wytycznych, które ułatwiłyby i usprawniły zgłaszanie informacji wymaganych zgodnie z prawem Unii oraz zmniejszyłyby obciążenia spoczywające na przedsiębiorstwach.	(56) Podmioty niezbędne i istotne znajdują się często w sytuacji, w której konkretny incydent, ze względu na jego cechy, należy zgłosić różnym organom w wyniku istnienia obowiązków w zakresie zgłaszania przewidzianych w różnych instrumentach prawnych. Takie przypadki powodują dodatkowe obciążenie, a ponadto mogą rodzić niepewność dotyczącą formatu i procedur dokonywania takich zgłoszeń. W związku z tym i w celu uproszczenia zgłaszania incydentów bezpieczeństwa ***oraz utrzymania zasady jednorazowości*** państwa członkowskie powinny ustanowić pojedynczy punkt kontaktowy na potrzeby wszystkich zgłoszeń wymaganych na podstawie niniejszej dyrektywy, a także na podstawie innych przepisów unijnych, takich jak rozporządzenie (UE) 2016/679 i dyrektywa 2002/58/WE. ENISA, we współpracy z Grupą Współpracy, powinna opracować wspólne wzory zgłoszeń w formie wytycznych, które ułatwiłyby i usprawniły zgłaszanie informacji wymaganych zgodnie z prawem Unii oraz zmniejszyłyby obciążenia spoczywające na przedsiębiorstwach.

Poprawka 33
Wniosek dotyczący dyrektywy
Motyw 59

Tekst proponowany przez Komisję	*Poprawka*
(59) Prowadzenie prawidłowych i kompletnych baz danych zawierających nazwy domen i dane rejestracyjne („dane WHOIS”) oraz zapewnienie zgodnego z prawem dostępu do takich danych jest niezbędne do zapewnienia bezpieczeństwa, stabilności i odporności systemu nazw domen (DNS), co z kolei przyczynia się do wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii. Gdy przetwarzanie dotyczy danych osobowych, powinno być ono zgodne z unijnymi przepisami o ochronie danych.	(59) Prowadzenie prawidłowych***, zweryfikowanych*** i kompletnych baz danych zawierających nazwy domen i dane rejestracyjne („dane WHOIS”) oraz zapewnienie zgodnego z prawem dostępu do takich danych jest niezbędne do zapewnienia bezpieczeństwa, stabilności i odporności systemu nazw domen (DNS), co z kolei przyczynia się do wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii. Gdy przetwarzanie dotyczy danych osobowych, powinno być ono zgodne z unijnymi przepisami o ochronie danych.

Poprawka 34
Wniosek dotyczący dyrektywy
Motyw 61

Tekst proponowany przez Komisję	*Poprawka*
(61) W celu zapewnienia dostępności prawidłowych i kompletnych danych dotyczących rejestracji nazw domen rejestry TLD i podmioty świadczące usługi rejestracji nazw domen ***dla TLD (tzw. rejestratorzy***) powinny gromadzić dane dotyczące rejestracji nazw domen oraz zapewniać ich integralność i dostępność. W szczególności rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD powinny ustanowić polityki i procedury na potrzeby gromadzenia i utrzymywania prawidłowych i kompletnych danych rejestracyjnych, a także przeciwdziałać powstawaniu nieprawidłowych danych rejestracyjnych i poprawiać je zgodnie z unijnymi przepisami o ochronie danych.	(61) W celu zapewnienia dostępności prawidłowych i kompletnych danych dotyczących rejestracji nazw domen rejestry TLD i podmioty świadczące usługi rejestracji nazw domen ***(w tym usługi świadczone przez rejestry nazw domen i rejestratorów, dostawców usług w zakresie rejestracji prywatności lub serwerów proxy, brokerów lub odsprzedawców domen oraz wszelkie inne usługi związane z rejestracją nazw domen***) powinny gromadzić dane dotyczące rejestracji nazw domen oraz zapewniać ich integralność i dostępność. W szczególności rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD powinny ustanowić polityki i procedury na potrzeby gromadzenia i utrzymywania prawidłowych i kompletnych danych rejestracyjnych, a także przeciwdziałać

powstawaniu nieprawidłowych danych rejestracyjnych i poprawiać je zgodnie z unijnymi przepisami o ochronie danych.

Poprawka 35
Wniosek dotyczący dyrektywy
Motyw 68

Tekst proponowany przez Komisję	*Poprawka*
(68) Należy zachęcać podmioty do wspólnego wykorzystywania ich indywidualnej wiedzy i praktycznego doświadczenia na szczeblu strategicznym, taktycznym i operacyjnym w celu wzmocnienia ich zdolności w zakresie odpowiedniego oceniania i monitorowania cyberzagrożeń, obrony przed nimi i reagowania na nie. Należy zatem umożliwić powstawanie na poziomie Unii mechanizmów dobrowolnej wymiany informacji. W tym celu państwa członkowskie powinny aktywnie wspierać również odpowiednie podmioty nieobjęte zakresem niniejszej dyrektywy i zachęcać je do uczestnictwa w takich mechanizmach wymiany informacji. Mechanizmy te powinny funkcjonować w pełnej zgodności z unijnymi regułami konkurencji oraz z unijnymi przepisami dotyczącymi ochrony danych osobowych.	(68) Należy zachęcać podmioty do wspólnego wykorzystywania ich indywidualnej wiedzy i praktycznego doświadczenia na szczeblu strategicznym, taktycznym i operacyjnym w celu wzmocnienia ich zdolności w zakresie odpowiedniego oceniania i monitorowania cyberzagrożeń, obrony przed nimi i reagowania na nie***, a państwa członkowskie powinny je w tym wspierać***. Należy zatem umożliwić powstawanie na poziomie Unii mechanizmów dobrowolnej wymiany informacji. W tym celu państwa członkowskie powinny aktywnie wspierać również odpowiednie podmioty nieobjęte zakresem niniejszej dyrektywy i zachęcać je do uczestnictwa w takich mechanizmach wymiany informacji. Mechanizmy te powinny funkcjonować w pełnej zgodności z unijnymi regułami konkurencji oraz z unijnymi przepisami dotyczącymi ochrony danych osobowych.

Poprawka 36
Wniosek dotyczący dyrektywy
Motyw 69

Tekst proponowany przez Komisję	*Poprawka*
(69) Należy uznać, że przetwarzanie danych osobowych ***w zakresie*** bezwzględnie ***niezbędnym*** i ***proporcjonalnym*** do zapewnienia bezpieczeństwa sieci i informacji przez podmioty, organy publiczne, CERT, CSIRT oraz dostawców technologii i usług	(69) Należy uznać, że przetwarzanie danych osobowych***, które należy ograniczyć to tego, co jest*** bezwzględnie ***niezbędne*** i ***proporcjonalne*** do zapewnienia bezpieczeństwa sieci i informacji ***oraz ochrony konsumentów*** przez podmioty, organy publiczne, CERT,

z zakresu bezpieczeństwa stanowi prawnie uzasadniony interes zainteresowanego administratora danych w rozumieniu rozporządzenia (UE) 2016/679. Powinno to obejmować środki związane z zapobieganiem incydentom, wykrywaniem i analizowaniem ich oraz reagowaniem na nie, środki zwiększające świadomość konkretnych cyberzagrożeń, wymianę informacji w kontekście usuwania oraz skoordynowanego ujawniania podatności, a także dobrowolną wymianę informacji na temat tych incydentów, a także na temat cyberzagrożeń i podatności, oznak naruszenia integralności systemu, taktyk, technik i procedur, ostrzeżeń dotyczących cyberbezpieczeństwa i narzędzi konfiguracji. Takie środki mogą wiązać się z koniecznością przetwarzania następujących rodzajów danych osobowych: adresów IP, ujednoliconych formatów adresowania zasobów (URL), nazw domen i adresów e-mail.

CSIRT oraz dostawców technologii i usług z zakresu bezpieczeństwa**,** stanowi prawnie uzasadniony interes zainteresowanego administratora danych w rozumieniu rozporządzenia (UE) 2016/679. Powinno to obejmować środki związane z zapobieganiem incydentom, wykrywaniem i analizowaniem ich oraz reagowaniem na nie, środki zwiększające świadomość konkretnych cyberzagrożeń, wymianę informacji w kontekście usuwania oraz skoordynowanego ujawniania podatności, a także dobrowolną wymianę informacji na temat tych incydentów, a także na temat cyberzagrożeń i podatności, oznak naruszenia integralności systemu, taktyk, technik i procedur, ostrzeżeń dotyczących cyberbezpieczeństwa i narzędzi konfiguracji. Takie środki mogą wiązać się z koniecznością przetwarzania następujących rodzajów danych osobowych: adresów IP, ujednoliconych formatów adresowania zasobów (URL), nazw domen i adresów e-mail.

Poprawka 37
Wniosek dotyczący dyrektywy
Motyw 70

Tekst proponowany przez Komisję	*Poprawka*
(70) Aby wzmocnić uprawnienia i działania nadzorcze, które pomagają zapewnić efektywną zgodność z przepisami, w niniejszej dyrektywie należy przewidzieć minimalny wykaz działań i środków nadzorczych, za pomocą których właściwe organy mogą sprawować nadzór nad podmiotami niezbędnymi i istotnymi. Ponadto w niniejszej dyrektywie należy wprowadzić rozróżnienie systemów nadzoru mających zastosowanie do podmiotów niezbędnych i podmiotów istotnych w celu zapewnienia sprawiedliwej równowagi pod względem obowiązków zarówno po stronie podmiotów, jak i właściwych organów.	(70) Aby wzmocnić uprawnienia i działania nadzorcze, które pomagają zapewnić efektywną zgodność z przepisami ***i osiągnąć wysoki wspólny poziom bezpieczeństwa w sektorze cyfrowym, w tym przez zapobieganie ryzyku dla użytkowników lub innych sieci, systemów informatycznych i usług***, w niniejszej dyrektywie należy przewidzieć minimalny wykaz działań i środków nadzorczych, za pomocą których właściwe organy mogą sprawować nadzór nad podmiotami niezbędnymi i istotnymi. Ponadto w niniejszej dyrektywie należy wprowadzić rozróżnienie systemów nadzoru mających zastosowanie do

Podmioty niezbędne należy zatem objąć pełnym systemem nadzoru (ex ante i ex post), natomiast podmioty istotne należy objąć uproszczonym systemem nadzoru (wyłącznie ex post). W przypadku tego drugiego systemu podmioty istotne nie powinny mieć obowiązku systematycznego dokumentowania spełniania wymogów dotyczących zarządzania ryzykiem w cyberprzestrzeni, natomiast właściwe organy powinny realizować nadzór w oparciu o podejście reaktywne w trybie ex post, a zatem nie powinny mieć ogólnego obowiązku prowadzenia nadzoru nad tymi podmiotami.	podmiotów niezbędnych i podmiotów istotnych w celu zapewnienia sprawiedliwej równowagi pod względem obowiązków zarówno po stronie podmiotów, jak i właściwych organów. Podmioty niezbędne należy zatem objąć pełnym systemem nadzoru (ex ante i ex post), natomiast podmioty istotne należy objąć uproszczonym systemem nadzoru (wyłącznie ex post)***, z uwzględnieniem podejścia opartego na analizie ryzyka***. W przypadku tego drugiego systemu podmioty istotne nie powinny mieć obowiązku systematycznego dokumentowania spełniania wymogów dotyczących zarządzania ryzykiem w cyberprzestrzeni, natomiast właściwe organy powinny realizować nadzór w oparciu o podejście reaktywne w trybie ex post, a zatem nie powinny mieć ogólnego obowiązku prowadzenia nadzoru nad tymi podmiotami***, z wyjątkiem przypadków dającego się udowodnić naruszenia obowiązków***.

Poprawka 38
Wniosek dotyczący dyrektywy
Motyw 76

Tekst proponowany przez Komisję	*Poprawka*
(76) Aby jeszcze bardziej wzmocnić skuteczność i odstraszający charakter sankcji mających zastosowanie do naruszeń obowiązków przewidzianych w niniejszej dyrektywie, właściwe organy powinny być uprawnione do stosowania sankcji polegających na zawieszeniu certyfikacji lub zezwolenia dotyczących ***części lub całości*** usług świadczonych przez podmiot niezbędny ***oraz na nałożeniu tymczasowego zakazu sprawowania funkcji zarządczych przez osobę fizyczną***. Zważywszy na dotkliwość takich sankcji i ich wpływ na działalność podmiotów, a ostatecznie na ich konsumentów, należy je stosować proporcjonalnie do powagi naruszenia	(76) Aby jeszcze bardziej wzmocnić skuteczność i odstraszający charakter sankcji mających zastosowanie do naruszeń obowiązków przewidzianych w niniejszej dyrektywie, właściwe organy powinny być uprawnione do stosowania sankcji polegających na zawieszeniu certyfikacji lub zezwolenia dotyczących ***odpowiednich*** usług świadczonych przez podmiot niezbędny. Zważywszy na dotkliwość takich sankcji i ich wpływ na działalność podmiotów, a ostatecznie na ich konsumentów, należy je stosować proporcjonalnie do powagi naruszenia i z uwzględnieniem konkretnych okoliczności danej sprawy, w tym faktu, czy naruszenie ma charakter umyślny czy

i z uwzględnieniem konkretnych okoliczności danej sprawy, w tym faktu, czy naruszenie ma charakter umyślny czy też wynika z niedbalstwa, oraz działań podjętych, aby zapobiec szkodom lub stratom lub je ograniczyć. Takie sankcje należy stosować wyłącznie w ostateczności, po wyczerpaniu przewidzianych w niniejszej dyrektywie pozostałych stosownych działań z zakresu egzekwowania przepisów i wyłącznie dopóki podmioty, na które nałożono sankcje, nie podejmą niezbędnych działań w celu usunięcia nieprawidłowości lub nie spełnią wymogów właściwego organu, z których tytułu zastosowano takie sankcje. Nakładanie takich sankcji powinno przebiegać z zastrzeżeniem odpowiednich gwarancji proceduralnych zgodnych z ogólnymi zasadami prawa Unii i z Kartą praw podstawowych Unii Europejskiej, w tym skutecznej ochrony prawnej, prawa do rzetelnego procesu sądowego, domniemania niewinności oraz prawa do obrony.	też wynika z niedbalstwa, oraz działań podjętych, aby zapobiec szkodom lub stratom lub je ograniczyć. Takie sankcje należy stosować wyłącznie w ostateczności, po wyczerpaniu przewidzianych w niniejszej dyrektywie pozostałych stosownych działań z zakresu egzekwowania przepisów i wyłącznie dopóki podmioty, na które nałożono sankcje, nie podejmą niezbędnych działań w celu usunięcia nieprawidłowości lub nie spełnią wymogów właściwego organu, z których tytułu zastosowano takie sankcje. Nakładanie takich sankcji powinno przebiegać z zastrzeżeniem odpowiednich gwarancji proceduralnych zgodnych z ogólnymi zasadami prawa Unii i z Kartą praw podstawowych Unii Europejskiej, w tym skutecznej ochrony prawnej, prawa do rzetelnego procesu sądowego, domniemania niewinności oraz prawa do obrony.

Poprawka 39
Wniosek dotyczący dyrektywy
Motyw 79

Tekst proponowany przez Komisję	*Poprawka*
(79) Należy wprowadzić mechanizm wzajemnej oceny umożliwiający przeprowadzanie przez ekspertów wyznaczonych przez państwa członkowskie oceny wdrożenia polityk cyberbezpieczeństwa, w tym poziomu zdolności państw członkowskich oraz dostępnych w nich zasobów.	(79) Należy wprowadzić mechanizm wzajemnej oceny umożliwiający przeprowadzanie przez ekspertów wyznaczonych przez państwa członkowskie ***i ENISA*** oceny wdrożenia polityk cyberbezpieczeństwa, w tym poziomu zdolności państw członkowskich oraz dostępnych w nich zasobów***, a także wymianę najlepszych praktyk***.

Poprawka 40
Wniosek dotyczący dyrektywy
Motyw 80

Tekst proponowany przez Komisję	*Poprawka*
(80) W celu uwzględnienia nowych cyberzagrożeń, postępu technologicznego lub specyfiki sektora należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 TFUE w odniesieniu do elementów związanych ze środkami zarządzania ryzykiem przewidzianymi w niniejszej dyrektywie. Komisja powinna być również uprawniona do ***przyjęcia*** aktów delegowanych określających***, które kategorie podmiotów niezbędnych mają obowiązek uzyskać certyfikację i*** na ***podstawie których konkretnych europejskich programów certyfikacji cyberbezpieczeństwa mają ją uzyskać***. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[26]. W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.	(80) W celu uwzględnienia nowych cyberzagrożeń, postępu technologicznego lub specyfiki sektora należy przekazać Komisji uprawnienia do przyjęcia aktów zgodnie z art. 290 TFUE w odniesieniu do elementów związanych ze środkami zarządzania ryzykiem przewidzianymi w niniejszej dyrektywie. Komisja powinna być ***uprawniona do przyjmowania aktów delegowanych określających elementy techniczne związane ze środkami zarządzania ryzykiem. Komisja powinna być*** również uprawniona do ***przyjmowania*** aktów delegowanych określających ***rodzaj informacji przekazywanych przez niezbędne i istotne podmioty w odniesieniu do każdego incydentu mającego poważny wpływ*** na ***świadczenie usług lub zdarzenia potencjalnie wypadkowego, a także określających przypadki, w których incydent należy uznać za poważny***. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[26]. W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.
[26] Dz.U. L 123 z 12.5.2016, s. 1.	[26] Dz.U. L 123 z 12.5.2016, s. 1.

Poprawka 41
Wniosek dotyczący dyrektywy
Motyw 81

Tekst proponowany przez Komisję	*Poprawka*
(81) Aby zapewnić jednolite warunki wdrażania odpowiednich przepisów niniejszej dyrektywy dotyczących procedur niezbędnych do funkcjonowania Grupy Współpracy, ***elementów technicznych związanych ze środkami zarządzania ryzykiem lub rodzaju zgłaszanych informacji,*** formatu i procedury dokonywania zgłoszeń incydentów, należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[27].	(81) Aby zapewnić jednolite warunki wdrażania odpowiednich przepisów niniejszej dyrektywy dotyczących procedur niezbędnych do funkcjonowania Grupy Współpracy, formatu i procedury dokonywania zgłoszeń incydentów, należy powierzyć Komisji uprawnienia wykonawcze. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[27].
[27] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).	[27] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

Poprawka 42
Wniosek dotyczący dyrektywy
Artykuł 1 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Niniejszą dyrektywą ustanawia się środki mające na celu zapewnienie wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii.	1. Niniejszą dyrektywą ustanawia się środki mające na celu zapewnienie wysokiego wspólnego poziomu cyberbezpieczeństwa w Unii***, aby stworzyć godne zaufania środowisko cyfrowe dla konsumentów i podmiotów gospodarczych oraz poprawić funkcjonowanie rynku wewnętrznego dzięki usunięciu barier je utrudniających***.

Poprawka 43
Wniosek dotyczący dyrektywy
Artykuł 2 – ustęp 2 – akapit 1 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
2. Niniejsza dyrektywa ma jednak zastosowanie do podmiotów, o których mowa w załącznikach I i II, niezależnie od ich wielkości, w przypadku gdy:	2. Niniejsza dyrektywa ma jednak zastosowanie do ***rodzajów*** podmiotów, o których mowa w załącznikach I i II, niezależnie od ich wielkości, w przypadku gdy:

Poprawka 44
Wniosek dotyczący dyrektywy
Artykuł 2 – ustęp 2 – akapit 2 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	Komisja wydaje wytyczne, aby wesprzeć państwa członkowskie we właściwym wdrażaniu przepisów dotyczących zakresu, jak również aby przyznać ewentualne odstępstwa konkretnym istotnym podmiotom wyłączonym z zakresu dyrektywy lub niektórych jej przepisów, z uwagi na ich niski poziom krytyczności w ich konkretnym sektorze lub niski poziom zależności od innych sektorów lub rodzajów usług. Państwa członkowskie, w pełni uwzględniając wytyczne Komisji, powiadamiają Komisję o swoich uzasadnionych decyzjach w tym zakresie.

Poprawka 45
Wniosek dotyczący dyrektywy
Artykuł 4 – akapit 1 – punkt 4

Tekst proponowany przez Komisję	*Poprawka*
4) „krajowa strategia cyberbezpieczeństwa” oznacza spójne ramy państwa członkowskiego zapewniające strategiczne cele i priorytety w zakresie bezpieczeństwa sieci i systemów informatycznych w tym	4) „krajowa strategia cyberbezpieczeństwa” oznacza spójne ramy państwa członkowskiego zapewniające strategiczne cele i priorytety w zakresie bezpieczeństwa sieci i systemów informatycznych w tym

państwie członkowskim;	państwie członkowskim***, a także polityki niezbędne do ich realizacji***;

Poprawka 46
Wniosek dotyczący dyrektywy
Artykuł 4 – akapit 1 – punkt 5 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	5a) „incydent transgraniczny" oznacza każdy incydent, który ma wpływ na operatorów pod nadzorem właściwych organów krajowych z co najmniej dwóch różnych państw członkowskich;

Poprawka 47
Wniosek dotyczący dyrektywy
Artykuł 4 – akapit 1 – punkt 6 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	6a) „zdarzenie potencjalnie wypadkowe" oznacza zdarzenie, które mogło potencjalnie spowodować szkodę, ale którego pełnemu wystąpieniu udało się skutecznie zapobiec;

Poprawka 48
Wniosek dotyczący dyrektywy
Artykuł 4 – akapit 1 – punkt 15 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	15a) „usługi rejestracji nazw domen" oznaczają usługi świadczone przez rejestry nazw domen i rejestratorów, dostawców usług w zakresie rejestracji prywatności lub serwerów proxy, brokerów lub odsprzedawców domen oraz wszelkie inne usługi związane z rejestracją nazw domen;

Poprawka 49
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 1 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
1. Każde państwo członkowskie przyjmuje krajową strategię cyberbezpieczeństwa określającą cele strategiczne i odpowiednie środki polityczne i regulacyjne mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. Krajowa strategia cyberbezpieczeństwa obejmuje w szczególności:	1. Każde państwo członkowskie przyjmuje krajową strategię cyberbezpieczeństwa określającą cele strategiczne i odpowiednie środki polityczne i regulacyjne***, w tym odpowiednie zasoby ludzkie i finansowe,*** mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. Krajowa strategia cyberbezpieczeństwa obejmuje w szczególności:

Poprawka 50
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) ramy zarządzania służące realizacji tych celów i priorytetów, w tym polityki, o których mowa w ust. 2, a także role i obowiązki instytucji i podmiotów publicznych, jak również innych odpowiednich podmiotów;	b) ramy zarządzania służące realizacji tych celów i priorytetów, w tym polityki, o których mowa w ust. 2, a także role i obowiązki instytucji i podmiotów publicznych, jak również innych odpowiednich podmiotów***, w tym odpowiedzialnych za cyberwywiad i cyberobronę***;

Poprawka 51
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 1 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) ocenę służącą określeniu istotnych zasobów i ryzyk w cyberprzestrzeni w tym państwie członkowskim;	c) ocenę służącą określeniu istotnych zasobów i ryzyk w cyberprzestrzeni w tym państwie członkowskim***, w tym potencjalnych niedoborów, które mogą negatywnie wpłynąć na jednolity rynek***;

Poprawka 52
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 1 – litera e

Tekst proponowany przez Komisję	*Poprawka*
e) wykaz poszczególnych organów i podmiotów zaangażowanych we wdrażanie krajowej strategii cyberbezpieczeństwa;	e) wykaz poszczególnych organów i podmiotów zaangażowanych we wdrażanie krajowej strategii cyberbezpieczeństwa***, w tym punkt kompleksowej obsługi dla MŚP***;

Poprawka 53
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) wytyczne dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów i usług ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień;	b) wytyczne dotyczące uwzględniania w zamówieniach publicznych wymogów związanych z cyberbezpieczeństwem w odniesieniu do produktów i usług ICT oraz specyfikacji tych wymogów na potrzeby takich zamówień***, w tym wykorzystywania produktów z zakresu cyberbezpieczeństwa opartych na otwartym oprogramowaniu***;

Poprawka 54
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) politykę mającą na celu promowanie i ułatwianie skoordynowanego ujawniania podatności w rozumieniu art. 6;	c) politykę mającą na celu promowanie i ułatwianie skoordynowanego ujawniania podatności w rozumieniu art. 6***, w tym przez wprowadzenie wytycznych i najlepszych praktyk opartych na już uznanych międzynarodowo standardach dotyczących postępowania w przypadku wykrycia podatności i ujawniania podatności***;

Poprawka 55
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera e

Tekst proponowany przez Komisję	*Poprawka*
e) politykę dotyczącą promowania ***i rozwoju*** umiejętności z zakresu cyberbezpieczeństwa, ***zwiększania świadomości oraz*** inicjatyw badawczo-rozwojowych;	e) politykę dotyczącą promowania ***cyberbezpieczeństwa wśród konsumentów, podnoszenia ich świadomości na temat cyberzagrożeń, zwiększania umiejętności informatycznych, zaufania użytkowników, neutralnych technologicznie*** umiejętności z zakresu cyberbezpieczeństwa ***i edukacji***, ***a także promowania*** inicjatyw badawczo-rozwojowych ***oraz cyberbezpieczeństwa produktów połączonych***;

Poprawka 56
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera e a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ea) politykę promującą stosowanie kryptografii i szyfrowania, zwłaszcza przez MŚP;

Poprawka 57
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera h

Tekst proponowany przez Komisję	*Poprawka*
h) politykę uwzględniającą konkretne potrzeby małych i średnich przedsiębiorstw, w ***szczególności tych*** wyłączonych z zakresu stosowania ***niniejszej*** dyrektywy**,** związane z wytycznymi i wsparciem na rzecz poprawy ich odporności na zagrożenia dla cyberbezpieczeństwa**.**	h) politykę ***promowania cyberbezpieczeństwa*** uwzględniającą konkretne potrzeby małych i średnich przedsiębiorstw, ***przy jednoczesnym wywiązywaniu się z obowiązków określonych*** w ***dyrektywie, oraz szczególne potrzeby podmiotów*** wyłączonych z zakresu stosowania dyrektywy związane z wytycznymi i wsparciem na rzecz poprawy ich odporności na zagrożenia dla cyberbezpieczeństwa***, w tym na przykład fundusze i edukacja na rzecz wdrażania środków w dziedzinie cyberbezpieczeństwa;***

Poprawka 58
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera h a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ha) polityka ta obejmuje utworzenie krajowego pojedynczego punktu kontaktowego dla MŚP oraz zasady ramowe pozwalające jak najefektywniej wykorzystywać centra innowacji cyfrowych i dostępne środki finansowe do realizacji celów polityki;

Poprawka 59
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 2 – litera h b (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	hb) polityka promująca spójne i synergiczne wykorzystanie dostępnych funduszy;

Poprawka 60
Wniosek dotyczący dyrektywy
Artykuł 5 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Państwa członkowskie przeprowadzają ocenę swoich krajowych strategii cyberbezpieczeństwa co najmniej co cztery lata na podstawie kluczowych wskaźników skuteczności i w razie potrzeby wprowadzają do nich zmiany. Na wniosek państw członkowskich Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) udziela im wsparcia w opracowaniu strategii krajowej oraz kluczowych wskaźników skuteczności wykorzystywanych na potrzeby oceny strategii.	4. Państwa członkowskie przeprowadzają ocenę swoich krajowych strategii cyberbezpieczeństwa co najmniej co cztery lata na podstawie kluczowych wskaźników skuteczności i w razie potrzeby wprowadzają do nich zmiany. Na wniosek państw członkowskich Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) udziela im wsparcia w opracowaniu strategii krajowej oraz kluczowych wskaźników skuteczności wykorzystywanych na potrzeby oceny strategii. ***ENISA kieruje również do państw członkowskich zalecenia dotyczące opracowania kluczowych wskaźników skuteczności na potrzeby oceny strategii***

krajowej, porównywalnych na poziomie Unii.

Poprawka 61
Wniosek dotyczący dyrektywy
Artykuł 6 – tytuł

Tekst proponowany przez Komisję	*Poprawka*
Skoordynowane ujawnianie podatności i ***europejski rejestr*** podatności	Skoordynowane ujawnianie podatności i ***europejska baza danych dotyczących*** podatności

Poprawka 62
Wniosek dotyczący dyrektywy
Artykuł 6 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. ENISA opracowuje i prowadzi ***europejski rejestr*** podatności. W tym celu ENISA ustanawia i utrzymuje odpowiednie systemy informatyczne, polityki i procedury, w szczególności aby umożliwić podmiotom istotnym i niezbędnym oraz ich dostawcom sieci i systemów informatycznych ujawnianie i rejestrowanie podatności występujących w produktach lub usługach ICT, a także aby zapewnić wszystkim zainteresowanym stronom dostęp do informacji na temat podatności wykazanych w rejestrze. ***Rejestr*** zawiera w szczególności informacje na temat podatności, produktu lub usług ICT, których ta podatność dotyczy, oraz dotkliwości podatności pod względem okoliczności, w jakich może ona zostać wykorzystana, dostępności powiązanych łat oraz, w przypadku braku dostępnych łat, wytyczne skierowane do użytkowników produktów i usług, których dotyczy podatność, na temat sposobów ograniczania ryzyka wynikającego z ujawnionych podatności.	2. ENISA opracowuje i prowadzi ***europejską bazę danych dotyczących*** podatności. W tym celu ENISA ustanawia i utrzymuje odpowiednie systemy informatyczne, polityki i procedury, ***a także odpowiednie polityki ujawniania podatności,*** w szczególności aby umożliwić podmiotom istotnym i niezbędnym oraz ich dostawcom sieci i systemów informatycznych ujawnianie i ***łatwe*** rejestrowanie podatności występujących w produktach lub usługach ICT, a także aby zapewnić wszystkim zainteresowanym stronom dostęp do ***istotnych*** informacji na temat podatności wykazanych w rejestrze***, pod warunkiem że takie działania nie są sprzeczne z ochroną poufności i tajemnicy handlowej***. ***Baza danych dotyczących podatności*** zawiera w szczególności informacje na temat podatności, produktu lub usług ICT, których ta podatność dotyczy, oraz dotkliwości podatności pod względem okoliczności, w jakich może ona zostać wykorzystana, dostępności powiązanych łat oraz, w przypadku braku dostępnych łat, wytyczne skierowane do

użytkowników produktów i usług, których dotyczy podatność, na temat sposobów ograniczania ryzyka wynikającego z ujawnionych podatności. ***Aby uniknąć powielania wysiłków, ENISA zawiera umowę o wymianie informacji i umowę o współpracy strukturalnej z rejestrem Wspólnych Podatności i Ekspozycji na Ryzyko (CVE) oraz, w stosownych przypadkach, z innymi bazami danych na całym świecie i prowadzonymi przez zaufanych partnerów.***

Poprawka 63
Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	1a. Jeżeli państwo członkowskie wyznaczy więcej niż jeden właściwy organ, o którym mowa w ust. 1, wówczas wyraźnie wskazuje, który z tych właściwych organów będzie służyć jako główny punkt kontaktowy podczas incydentu lub kryzysu na dużą skalę.

Poprawka 64
Wniosek dotyczący dyrektywy
Artykuł 7 – ustęp 3 – litera f

Tekst proponowany przez Komisję	*Poprawka*
f) krajowe procedury i ***ustalenia*** między odpowiednimi organami i instytucjami krajowymi mające na celu zapewnienie skutecznego uczestnictwa danego państwa członkowskiego w skoordynowanym zarządzaniu cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę na szczeblu Unii oraz skutecznego wsparcia ze strony danego państwa członkowskiego dla tego rodzaju skoordynowanego zarządzania.	f) krajowe procedury i ***koordynacja*** między odpowiednimi organami i instytucjami krajowymi***, w tym odpowiedzialnymi za cyberwywiad i cyberobronę,*** mające na celu zapewnienie skutecznego uczestnictwa danego państwa członkowskiego w skoordynowanym zarządzaniu cyberincydentami i kryzysami cyberbezpieczeństwa na dużą skalę na szczeblu Unii oraz skutecznego wsparcia ze strony danego państwa członkowskiego dla tego rodzaju skoordynowanego zarządzania.

Poprawka 65
Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 2 – litera d

Tekst proponowany przez Komisję	*Poprawka*
d) zapewnianie dynamicznej analizy ryzyka i incydentów oraz orientacji sytuacyjnej w zakresie cyberbezpieczeństwa;	d) zapewnianie dynamicznej analizy ryzyka i incydentów oraz orientacji sytuacyjnej w zakresie cyberbezpieczeństwa***, w tym analiza wczesnych ostrzeżeń oraz zgłoszeń, o których mowa w art. 20***;

Poprawka 66
Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 2 – litera e

Tekst proponowany przez Komisję	*Poprawka*
e) przeprowadzanie, na wniosek podmiotu, ***aktywnego*** skanowania sieci i systemów informatycznych wykorzystywanych przez dany podmiot do świadczenia usług;	e) przeprowadzanie, na wniosek podmiotu, skanowania sieci i systemów informatycznych wykorzystywanych przez dany podmiot do świadczenia usług***, aby wykryć i ograniczyć konkretne zagrożenia lub im zapobiegać***;

Poprawka 67
Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 2 – litera f

Tekst proponowany przez Komisję	*Poprawka*
f) ***uczestnictwo*** w sieci CSIRT oraz udzielanie wzajemnej pomocy innym członkom sieci na ich wniosek.	f) ***aktywne uczestnictwo*** w sieci CSIRT oraz udzielanie wzajemnej pomocy innym członkom sieci na ich wniosek;

Poprawka 68
Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 2 – litera f a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	fa) pomoc operacyjna i wytyczne dla

podmiotom, o których mowa w załącznikach I i II, w szczególności MŚP;

Poprawka 69
Wniosek dotyczący dyrektywy
Artykuł 10 – ustęp 2 – litera f b (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	fb) udział we wspólnych ćwiczeniach w dziedzinie cyberbezpieczeństwa na szczeblu Unii.

Poprawka 70
Wniosek dotyczący dyrektywy
Artykuł 11 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Państwa członkowskie zapewniają, aby ich właściwe organy albo ich CSIRT odbierały zgłoszenia incydentów, istotnych cyberzagrożeń i zdarzeń potencjalnie wypadkowych dokonywane na podstawie niniejszej dyrektywy. W przypadku gdy państwo członkowskie postanowi, że jego CSIRT nie będą odbierać takich zgłoszeń, CSIRT otrzymają, w stopniu koniecznym do wykonywania swoich zadań, dostęp do danych dotyczących incydentów zgłaszanych przez podmioty niezbędne lub istotne na podstawie art. 20.	2. Państwa członkowskie zapewniają, aby ich właściwe organy albo ich CSIRT odbierały zgłoszenia incydentów, istotnych cyberzagrożeń i zdarzeń potencjalnie wypadkowych dokonywane na podstawie niniejszej dyrektywy. W przypadku gdy państwo członkowskie postanowi, że jego CSIRT nie będą odbierać takich zgłoszeń, CSIRT otrzymają, w stopniu koniecznym do ***skutecznego*** wykonywania swoich zadań, ***odpowiedni*** dostęp do danych dotyczących incydentów zgłaszanych przez podmioty niezbędne lub istotne na podstawie art. 20.

Poprawka 71
Wniosek dotyczący dyrektywy
Artykuł 11 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. W zakresie niezbędnym do skutecznej realizacji zadań i obowiązków przewidzianych w niniejszej dyrektywie państwa członkowskie zapewniają odpowiednią współpracę między	4. W zakresie niezbędnym do skutecznej realizacji zadań i obowiązków przewidzianych w niniejszej dyrektywie państwa członkowskie zapewniają odpowiednią współpracę między

właściwymi organami i pojedynczymi punktami kontaktowymi a organami ścigania, organami ochrony danych i organami odpowiedzialnymi za infrastrukturę krytyczną na mocy dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych] ***oraz*** krajowymi organami finansowymi wyznaczonymi na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) XXXX/XXXX [rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego][39] w danym państwie członkowskim.	właściwymi organami i pojedynczymi punktami kontaktowymi a organami ścigania, organami ochrony danych i organami odpowiedzialnymi za infrastrukturę krytyczną na mocy dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych]**,** krajowymi organami finansowymi wyznaczonymi na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) XXXX/XXXX [rozporządzenie w sprawie operacyjnej odporności cyfrowej sektora finansowego][39] w danym państwie członkowskim ***oraz organami cyberobrony i cyberwywiadu***.
[39] [wstawić pełny tytuł i odniesienie do publikacji w Dzienniku Urzędowym, kiedy już będą znane]	[39] [wstawić pełny tytuł i odniesienie do publikacji w Dzienniku Urzędowym, kiedy już będą znane]

Poprawka 72
Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Grupa Współpracy wykonuje swoje zadania na podstawie dwuletnich programów prac, o których mowa w ust. 6.	2. Grupa Współpracy ***regularnie się zbiera i*** wykonuje swoje zadania na podstawie dwuletnich programów prac, o których mowa w ust. 6.

Poprawka 73
Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 3 – akapit 2

Tekst proponowany przez Komisję	*Poprawka*
W stosownych przypadkach Grupa Współpracy może zapraszać przedstawicieli odpowiednich zainteresowanych stron do udziału w swoich pracach.	W stosownych przypadkach Grupa Współpracy może zapraszać przedstawicieli odpowiednich ***organów i agencji Unii oraz*** zainteresowanych stron do udziału w swoich pracach.

Poprawka 74
Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 4 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) udzielanie wskazówek właściwym organom w związku z transpozycją i wdrażaniem niniejszej dyrektywy;	a) udzielanie wskazówek właściwym organom w związku z transpozycją i wdrażaniem niniejszej dyrektywy ***oraz sprzyjanie jej jednolitemu wdrażaniu w państwach członkowskich***;

Poprawka 75
Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 4 – litera a a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	aa) wymiana informacji na temat priorytetów politycznych i kluczowych wyzwań w dziedzinie cyberbezpieczeństwa oraz określanie głównych celów cyberbezpieczeństwa;

Poprawka 76
Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 4 – litera a b (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ab) omawianie krajowych strategii państw członkowskich i ich gotowości;

Poprawka 77
Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 4 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) wymiana porad i współpraca z Komisją w zakresie nowych inicjatyw dotyczących polityki cyberbezpieczeństwa;	c) wymiana porad i współpraca z Komisją w zakresie nowych inicjatyw dotyczących polityki cyberbezpieczeństwa ***oraz z Europejską Służbą Działań Zewnętrznych w zakresie geopolitycznych aspektów cyberbezpieczeństwa w Unii***;

Poprawka 78
Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 4 – litera f

Tekst proponowany przez Komisję	*Poprawka*
f) omawianie sprawozdań z wzajemnej oceny, o których mowa w art. 16 ust. 7;	f) omawianie sprawozdań z wzajemnej oceny, o których mowa w art. 16 ust. 7***, ocena ich funkcjonowania oraz formułowanie wniosków i zaleceń***;

Poprawka 79
Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 4 – litera k a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ka) wspieranie ENISA w organizacji wspólnych szkoleń na szczeblu Unii dla właściwych organów krajowych.

Poprawka 80
Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. W terminie do dnia ...***[, 24 miesiące*** od daty wejścia w życie niniejszej dyrektywy] r., a następnie co dwa lata Grupa Współpracy opracowuje program prac obejmujący działania, które mają zostać podjęte w celu realizacji jej celów i zadań. Ramy czasowe pierwszego programu przyjętego na podstawie niniejszej dyrektywy muszą być zharmonizowane z ramami czasowymi ostatniego programu przyjętego na podstawie dyrektywy (UE) 2016/1148.	6. W terminie do dnia ... ***[12 miesięcy*** od daty wejścia w życie niniejszej dyrektywy] r., a następnie co dwa lata Grupa Współpracy opracowuje program prac obejmujący działania, które mają zostać podjęte w celu realizacji jej celów i zadań. Ramy czasowe pierwszego programu przyjętego na podstawie niniejszej dyrektywy muszą być zharmonizowane z ramami czasowymi ostatniego programu przyjętego na podstawie dyrektywy (UE) 2016/1148.

Poprawka 81
Wniosek dotyczący dyrektywy
Artykuł 12 – ustęp 8 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	8a. Grupa Współpracy regularnie publikuje sprawozdanie podsumowujące działania, nie naruszając poufności informacji wymienianych podczas jej posiedzeń.

Poprawka 82
Wniosek dotyczący dyrektywy
Artykuł 13 – ustęp 3 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) wymiana informacji na temat zdolności CSIRT;	a) wymiana informacji na temat zdolności ***i gotowości*** CSIRT;

Poprawka 83
Wniosek dotyczący dyrektywy
Artykuł 13 – ustęp 3 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) wymiana stosownych informacji na temat incydentów, zdarzeń potencjalnie wypadkowych, cyberzagrożeń, ryzyk i podatności;	b) wymiana stosownych informacji na temat incydentów, zdarzeń potencjalnie wypadkowych, cyberzagrożeń, ryzyk i podatności ***oraz wspieranie zdolności operacyjnych państw członkowskich***;

Poprawka 84
Wniosek dotyczący dyrektywy
Artykuł 13 – ustęp 3 – litera d a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	da) wymiana i omawianie informacji dotyczących incydentów o charakterze transgranicznym;

Poprawka 85
Wniosek dotyczący dyrektywy
Artykuł 13 – ustęp 3 – litera g – podpunkt i a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(ia) wymiana informacji;

Poprawka 86
Wniosek dotyczący dyrektywy
Artykuł 13 – ustęp 3 – litera j

Tekst proponowany przez Komisję	*Poprawka*
j) ***na wniosek danego CSIRT – omawianie*** zdolności i gotowości ***tego*** CSIRT;	j) ***omawianie*** zdolności i gotowości CSIRT;

Poprawka 87
Wniosek dotyczący dyrektywy
Artykuł 13 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Na potrzeby przeglądu, o którym mowa w art. 35, oraz w terminie do dnia **...** □24 miesiące od daty wejścia w życie niniejszej dyrektywy□ r., a następnie co ***dwa lata*** sieć CSIRT ocenia postępy we współpracy operacyjnej i sporządza sprawozdanie. Sprawozdanie to zawiera w szczególności wnioski dotyczące wyników wzajemnych ocen, o których mowa w art. 16, przeprowadzonych w odniesieniu do krajowych CSIRT, w tym wnioski i zalecenia sformułowane na podstawie tego artykułu. Sprawozdanie to przedkłada się także Grupie Współpracy.	4. Na potrzeby przeglądu, o którym mowa w art. 35, oraz w terminie do dnia □24 miesiące od daty wejścia w życie niniejszej dyrektywy□ r., a następnie co ***roku*** sieć CSIRT ocenia postępy we współpracy operacyjnej i sporządza sprawozdanie. Sprawozdanie to zawiera w szczególności wnioski dotyczące wyników wzajemnych ocen, o których mowa w art. 16, przeprowadzonych w odniesieniu do krajowych CSIRT, w tym wnioski i zalecenia sformułowane na podstawie tego artykułu. Sprawozdanie to przedkłada się także Grupie Współpracy.

Poprawka 88
Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 3 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) podnoszenie poziomu gotowości w zakresie zarządzania incydentami i kryzysami na dużą skalę;	a) podnoszenie poziomu gotowości w zakresie zarządzania incydentami i kryzysami na dużą skalę***, w tym***

	cyberzagrożeniami transgranicznymi;

Poprawka 89
Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. EU-CyCLONe regularnie składa Grupie Współpracy sprawozdania na temat cyberzagrożeń, incydentów i tendencji w dziedzinie cyberbezpieczeństwa, koncentrując się w szczególności na ich wpływie na podmioty niezbędne i istotne.	5. EU-CyCLONe regularnie składa Grupie Współpracy sprawozdania na temat cyberzagrożeń, incydentów i tendencji w dziedzinie cyberbezpieczeństwa, koncentrując się w szczególności na ich wpływie na podmioty niezbędne i istotne ***oraz na ich odporności***.

Poprawka 90
Wniosek dotyczący dyrektywy
Artykuł 14 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. EU-CyCLONe współpracuje z siecią CSIRT na podstawie uzgodnionych ustaleń proceduralnych.	6. EU-CyCLONe ***ściśle*** współpracuje z siecią CSIRT na podstawie uzgodnionych ustaleń proceduralnych.

Poprawka 91
Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 1 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
1. ENISA wydaje co dwa lata, we współpracy z Komisją, sprawozdanie o stanie cyberbezpieczeństwa w Unii. Sprawozdanie zawiera w szczególności ocenę następujących elementów:	1. ENISA wydaje co dwa lata, we współpracy z Komisją, sprawozdanie o stanie cyberbezpieczeństwa w Unii ***i przedstawia je Parlamentowi Europejskiemu***. Sprawozdanie zawiera w szczególności ocenę następujących elementów:

Poprawka 92
Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) rozwoju zdolności w zakresie cyberbezpieczeństwa w całej Unii;	a) rozwoju zdolności w zakresie cyberbezpieczeństwa w całej Unii***, w tym ogólnego poziomu umiejętności i kompetencji w dziedzinie cyberbezpieczeństwa, ogólnego poziomu odporności rynku wewnętrznego na cyberzagrożenia oraz zakresu wdrożenia dyrektywy w państwach członkowskich***;

Poprawka 93
Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 1 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) wskaźnika cyberbezpieczeństwa zapewniającego zbiorczą ocenę poziomu dojrzałości zdolności w zakresie cyberbezpieczeństwa**.**	c) wskaźnika cyberbezpieczeństwa zapewniającego zbiorczą ocenę poziomu dojrzałości zdolności w zakresie cyberbezpieczeństwa***, w tym ogólną ocenę cyberbezpieczeństwa konsumentów;***

Poprawka 94
Wniosek dotyczący dyrektywy
Artykuł 15 – ustęp 1 – litera c a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ca) aspektów geopolitycznych mających bezpośredni lub pośredni wpływ na stan cyberbezpieczeństwa w Unii.

Poprawka 95
Wniosek dotyczący dyrektywy
Artykuł 16 – ustęp 1 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
1. Komisja ustanawia, po konsultacji z Grupą Współpracy i ENISA i najpóźniej ***18*** miesięcy po wejściu w życie niniejszej dyrektywy, metodykę i zawartość systemu wzajemnej oceny służącego do oceny	1. Komisja ustanawia, po konsultacji z Grupą Współpracy i ENISA i najpóźniej ***12*** miesięcy po wejściu w życie niniejszej dyrektywy, metodykę i zawartość systemu wzajemnej oceny służącego do oceny

skuteczności polityki cyberbezpieczeństwa państw członkowskich. Oceny są przeprowadzane przez ekspertów technicznych ds. cyberbezpieczeństwa pochodzących z innych państw członkowskich niż państwo poddawane ocenie i obejmują co najmniej następujące kwestie:

skuteczności polityki cyberbezpieczeństwa państw członkowskich. Oceny są przeprowadzane przez ekspertów technicznych ds. cyberbezpieczeństwa pochodzących z ***co najmniej dwóch*** innych państw członkowskich niż państwo poddawane ocenie i ***ENISA i*** obejmują co najmniej następujące kwestie:

Poprawka 96
Wniosek dotyczący dyrektywy
Artykuł 16 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Metodyka ta obejmuje obiektywne, niedyskryminacyjne, sprawiedliwe i przejrzyste kryteria, na podstawie których państwa członkowskie wyznaczają ekspertów uprawnionych do przeprowadzania wzajemnych ocen. ENISA i Komisja wyznaczają ekspertów do udziału we wzajemnych ocenach w charakterze obserwatorów. Komisja, przy wsparciu ENISA, ustanawia w ramach metodyki, o której mowa w ust. 1, obiektywny, niedyskryminacyjny, sprawiedliwy i przejrzysty system wyboru i losowego przydzielania ekspertów do każdej wzajemnej oceny.	2. Metodyka ta obejmuje obiektywne, niedyskryminacyjne, ***neutralne pod względem technologicznym,*** sprawiedliwe i przejrzyste kryteria, na podstawie których państwa członkowskie wyznaczają ekspertów uprawnionych do przeprowadzania wzajemnych ocen. ENISA i Komisja wyznaczają ekspertów do udziału we wzajemnych ocenach w charakterze obserwatorów. Komisja, przy wsparciu ENISA, ustanawia w ramach metodyki, o której mowa w ust. 1, obiektywny, niedyskryminacyjny, sprawiedliwy i przejrzysty system wyboru i losowego przydzielania ekspertów do każdej wzajemnej oceny.

Poprawka 97
Wniosek dotyczący dyrektywy
Artykuł 18 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Państwa członkowskie zapewniają, aby podmioty niezbędne i istotne wprowadzały ***odpowiednie i proporcjonalne*** środki techniczne i organizacyjne w celu zarządzania ryzykami dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do	1. Państwa członkowskie zapewniają, aby podmioty niezbędne i istotne wprowadzały środki techniczne i organizacyjne w celu zarządzania ryzykami dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do świadczenia usług. ***Środki te są***

świadczenia usług. Uwzględniając najnowszy stan wiedzy, środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka.	***odpowiednie i proporcjonalne do poziomu krytyczności sektora lub rodzaju usługi oraz do poziomu zależności podmiotu od innych sektorów lub rodzajów usług. Środki te przyjmuje się po przeprowadzeniu oceny opartej na analizie ryzyka.*** Uwzględniając najnowszy stan wiedzy, środki te muszą zapewniać poziom bezpieczeństwa sieci i systemów informatycznych odpowiedni do istniejącego ryzyka. ***Podejmuje się zwłaszcza środki, które zapobiegają skutkom, jakie incydenty naruszające bezpieczeństwo mają dla odbiorców usług, a także w celu minimalizowania tych skutków.***

Poprawka 98
Wniosek dotyczący dyrektywy
Artykuł 18 – ustęp 2 – litera d

Tekst proponowany przez Komisję	*Poprawka*
d) ***bezpieczeństwo*** łańcucha dostaw, w tym ***aspekty związane*** z bezpieczeństwem ***dotyczące*** stosunków między każdym podmiotem a jego dostawcami lub usługodawcami, takimi jak dostawcy usług przechowywania i przetwarzania danych lub zarządzanych usług w zakresie bezpieczeństwa;	d) ***środki służące ocenie ryzyka dla bezpieczeństwa*** łańcucha dostaw, w tym ***aspektów związanych*** z bezpieczeństwem ***dotyczących*** stosunków między każdym podmiotem a jego dostawcami lub usługodawcami, takimi jak dostawcy usług przechowywania i przetwarzania danych lub zarządzanych usług w zakresie bezpieczeństwa;

Poprawka 99
Wniosek dotyczący dyrektywy
Artykuł 18 – ustęp 2 – litera f

Tekst proponowany przez Komisję	*Poprawka*
f) polityki i procedury (z zakresu testowania i audytu) służące ocenie skuteczności środków zarządzania ryzykiem w cyberprzestrzeni;	f) polityki i procedury (z zakresu testowania i audytu) ***oraz regularne ćwiczenia w dziedzinie cyberbezpieczeństwa*** służące ocenie skuteczności środków zarządzania ryzykiem w cyberprzestrzeni;

Poprawka 100
Wniosek dotyczący dyrektywy
Artykuł 18 – ustęp 2 – litera g

Tekst proponowany przez Komisję	*Poprawka*
g) stosowanie kryptografii ***i*** szyfrowania***.***	g) stosowanie kryptografii***,*** szyfrowania***, a w szczególności szyfrowania end-to-end;***

Poprawka 101
Wniosek dotyczący dyrektywy
Artykuł 18 – ustęp 2 – litera g a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ga) strategie gwarantujące odpowiednie szkolenia i świadomość w dziedzinie cyberbezpieczeństwa.

Poprawka 102
Wniosek dotyczący dyrektywy
Artykuł 18 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Państwa członkowskie zapewniają, aby w przypadku rozważania odpowiednich środków, o których mowa w ust. 2 lit. d), podmioty uwzględniały podatności charakterystyczne dla każdego dostawcy i usługodawcy oraz ogólną jakość produktów i praktyk w zakresie cyberbezpieczeństwa swoich dostawców produktów i usług, w tym ich procedury bezpiecznego opracowywania.	3. Państwa członkowskie zapewniają, aby w przypadku rozważania odpowiednich środków, o których mowa w ust. 2 lit. d), podmioty***, jeżeli mają dostęp do istotnych informacji,*** uwzględniały podatności charakterystyczne dla każdego dostawcy i usługodawcy oraz ogólną jakość produktów i praktyk w zakresie cyberbezpieczeństwa swoich dostawców produktów i usług, w tym ich procedury bezpiecznego opracowywania.

Poprawka 103
Wniosek dotyczący dyrektywy
Artykuł 18 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. Komisja ***może przyjąć akty***	5. Komisja ***jest uprawniona do***

wykonawcze w celu określenia specyfikacji technicznych i metodycznych elementów, o których mowa w ust. 2***. Przygotowując te akty, Komisja postępuje zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2***, i w jak najszerszym zakresie stosuje się do norm międzynarodowych i europejskich, a także odpowiednich specyfikacji technicznych.

przyjmowania aktów delegowanych w celu określenia specyfikacji technicznych i metodycznych elementów, o których mowa w ust. 2, i w jak najszerszym zakresie stosuje się do norm międzynarodowych i europejskich, a także odpowiednich specyfikacji technicznych. ***Opracowując akty delegowane, Komisja konsultuje się również ze wszystkimi odpowiednimi zainteresowanymi stronami.***

Poprawka 104
Wniosek dotyczący dyrektywy
Artykuł 18 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. Komisja ***jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 36, aby uzupełnić elementy określone*** w ust. 2 w ***celu uwzględnienia nowych cyberzagrożeń, rozwoju technologicznego lub specyfiki sektora***.	6. Komisja ***wraz z Grupą Współpracy i ENISA wydaje wytyczne i określa najlepsze praktyki dotyczące przestrzegania przepisów przez podmioty,*** w ***proporcjonalny sposób, zgodnie z wymogami określonymi w*** ust. 2***, a*** w ***szczególności wymogiem określonym w lit. d) tego ustępu***.

Poprawka 105
Wniosek dotyczący dyrektywy
Artykuł 19 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. ***Grupa Współpracy***, ***we*** współpracy z Komisją i ENISA, może przeprowadzać skoordynowane oceny ryzyka dotyczące bezpieczeństwa w odniesieniu do określonych krytycznych łańcuchów dostaw usług, systemów lub produktów ICT, z uwzględnieniem technicznych i, w stosownych przypadkach, pozatechnicznych czynników ryzyka.	1. ***Aby zwiększyć ogólny poziom cyberbezpieczeństwa***, ***Grupa*** Współpracy***, wraz*** z Komisją i ENISA, może przeprowadzać skoordynowane oceny ryzyka dotyczące bezpieczeństwa w odniesieniu do określonych krytycznych łańcuchów dostaw usług, systemów lub produktów ICT, z uwzględnieniem technicznych i, w stosownych przypadkach, pozatechnicznych czynników ryzyka***, takich jak zagrożenia geopolityczne***.

Poprawka 106
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Państwa członkowskie zapewniają, aby podmioty niezbędne i istotne bez zbędnej zwłoki zgłaszały właściwym organom lub CSIRT, zgodnie z ust. 3 i 4, każdy incydent mający istotny wpływ na świadczenie przez nich usług. W stosownych przypadkach podmioty te bez zbędnej zwłoki powiadamiają odbiorców swoich usług o incydentach, które mogą mieć niekorzystny wpływ na świadczenie danej usługi. Państwa członkowskie zapewniają, aby wspomniane podmioty zgłaszały m.in. wszelkie informacje umożliwiające właściwym organom lub CSIRT ustalenie transgranicznego wpływu incydentu.	1. Państwa członkowskie zapewniają, aby podmioty niezbędne i istotne bez zbędnej zwłoki zgłaszały właściwym organom lub CSIRT, zgodnie z ust. 3 i 4, każdy incydent mający istotny wpływ na świadczenie przez nich usług ***i każde zdarzenie potencjalnie wypadkowe***. W stosownych przypadkach podmioty te bez zbędnej zwłoki powiadamiają odbiorców swoich usług o incydentach, które mogą mieć niekorzystny wpływ na świadczenie danej usługi. Państwa członkowskie zapewniają, aby wspomniane podmioty zgłaszały m.in. wszelkie informacje umożliwiające właściwym organom lub CSIRT ustalenie transgranicznego wpływu incydentu ***lub zdarzenia potencjalnie wypadkowego***.

Poprawka 107
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 1 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	1a. W celu uproszczenia obowiązków dotyczących zgłaszania państwa członkowskie ustanawiają pojedynczy punkt kontaktowy na potrzeby wszystkich zgłoszeń wymaganych na podstawie dyrektywy, a także na podstawie innych przepisów unijnych, takich jak rozporządzenie (UE) 2016/679 i dyrektywa 2002/58/WE.

Poprawka 108
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 1 b (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	1b. ENISA, wraz z Grupą Współpracy, opracowuje wspólne wzory zgłoszeń w formie wytycznych, które ułatwią i usprawnią zgłaszanie informacji wymaganych zgodnie z prawem Unii oraz zmniejszą obciążenie regulacyjne przedsiębiorstw.

Poprawka 109
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 2 – akapit 1

Tekst proponowany przez Komisję	*Poprawka*
2. ***Państwa członkowskie zapewniają, aby podmioty niezbędne i istotne bez zbędnej zwłoki zgłaszały właściwym organom lub CSIRT wszelkie istotne cyberzagrożenia, które zidentyfikują jako zagrożenia mogące doprowadzić do wystąpienia znaczącego incydentu.***	***skreśla się***

Poprawka 110
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 2 – akapit 2

Tekst proponowany przez Komisję	*Poprawka*
W stosownych przypadkach podmioty te bez zbędnej zwłoki powiadamiają odbiorców swoich usług, których potencjalnie dotyczy znaczące cyberzagrożenie, o wszelkich środkach zaradczych lub innych środkach, które ci odbiorcy mogą zastosować w odpowiedzi na to zagrożenie. W stosownych przypadkach podmioty powiadamiają również tych odbiorców o samym zagrożeniu. Zgłoszenie nie może narażać podmiotu zgłaszającego na zwiększoną odpowiedzialność.	***skreśla się***

Poprawka 111
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 3 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) incydent spowodował ***lub może spowodować*** istotne zakłócenia operacyjne lub straty finansowe dla danego podmiotu;	a) incydent spowodował istotne zakłócenia operacyjne lub straty finansowe dla danego podmiotu;

Poprawka 112
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 3 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) incydent wpłynął ***lub może wpłynąć*** na inne osoby fizyczne lub prawne, powodując znaczne straty materialne lub niematerialne.	b) incydent wpłynął na inne osoby fizyczne lub prawne, powodując znaczne straty materialne lub niematerialne.

Poprawka 113
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 3 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	3a. Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 36, w celu uzupełnienia niniejszej dyrektywy przez wskazanie rodzaju informacji przekazywanych na podstawie ust. 1 niniejszego artykułu oraz przez dalsze doprecyzowanie sytuacji, w których incydent uznaje się za poważny, jak określono w ust. 3 niniejszego artykułu.

Poprawka 114
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 4 – litera -a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	-a) wczesne ostrzeżenie w ciągu

	pierwszych 24 godzin od momentu, w którym zainteresowany podmiot dowiedział się o incydencie, bez obowiązku ujawniania dodatkowych informacji o incydencie;

Poprawka 115
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 4 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) bez zbędnej zwłoki, a w każdym razie w ciągu ***24*** godzin od powzięcia wiedzy o incydencie – zgłoszenie wstępne, w którym, w stosownych przypadkach, wskazuje się, czy incydent został wywołany, jak przypuszcza się, działaniem bezprawnym lub działaniem w złym zamiarze;	a) bez zbędnej zwłoki, a w każdym razie w ciągu ***72*** godzin od powzięcia wiedzy o incydencie – zgłoszenie wstępne, w którym, w stosownych przypadkach, wskazuje się, czy incydent został wywołany, jak przypuszcza się, działaniem bezprawnym lub działaniem w złym zamiarze;

Poprawka 116
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 4 – litera c – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
c) ***sprawozdanie końcowe*** nie później niż ***miesiąc*** po dokonaniu zgłoszenia, o którym mowa w lit. a), zawierające co najmniej następujące elementy:	c) ***wyczerpujące sprawozdanie*** nie później niż ***trzy miesiące*** po dokonaniu zgłoszenia, o którym mowa w lit. a), zawierające co najmniej następujące elementy:

Poprawka 117
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 4 – litera c – podpunkt i

Tekst proponowany przez Komisję	*Poprawka*
(i) ***szczegółowy*** opis incydentu, jego dotkliwości i skutków;	(i) ***bardziej szczegółowy*** opis incydentu, jego dotkliwości i skutków;

Poprawka 118
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 4 – litera c a (nowa)

Tekst proponowany przez Komisję	*Poprawka*
	ca) jeżeli incydent jeszcze trwa w momencie złożenia wyczerpującego raportu zgodnie z lit. c) sprawozdanie końcowe przedstawia się miesiąc po ograniczeniu incydentu;

Poprawka 119
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 7

Tekst proponowany przez Komisję	*Poprawka*
7. W przypadku gdy świadomość społeczeństwa jest niezbędna, żeby zapobiec wystąpieniu incydentu lub poradzić sobie z trwającym incydentem, lub w przypadku gdy ujawnienie incydentu z innych względów leży w interesie publicznym, właściwy organ lub CSIRT oraz, w stosownych przypadkach, organy lub CSIRT innych zainteresowanych państw członkowskich ***mogą,*** po konsultacji z zainteresowanym podmiotem***,*** ***poinformować*** społeczeństwo o incydencie lub ***zobowiązać*** do tego ten podmiot.	7. W przypadku gdy świadomość społeczeństwa jest niezbędna, żeby zapobiec wystąpieniu incydentu lub poradzić sobie z trwającym incydentem, lub w przypadku gdy ujawnienie incydentu z innych względów leży w interesie publicznym, właściwy organ lub CSIRT oraz, w stosownych przypadkach, organy lub CSIRT innych zainteresowanych państw członkowskich po konsultacji z zainteresowanym podmiotem ***informują*** społeczeństwo o incydencie lub ***zobowiązują*** do tego ten podmiot.

Poprawka 120
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 8

Tekst proponowany przez Komisję	*Poprawka*
8. Na wniosek właściwego organu lub CSIRT pojedynczy punkt kontaktowy przekazuje zgłoszenia, otrzymane zgodnie z ust. 1 ***i 2***, pojedynczym punktom kontaktowym w innych państwach członkowskich, których dotyczy incydent.	8. Na wniosek właściwego organu lub CSIRT pojedynczy punkt kontaktowy przekazuje zgłoszenia, otrzymane zgodnie z ust. 1, pojedynczym punktom kontaktowym w innych państwach członkowskich, których dotyczy incydent.

Poprawka 121
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 9

Tekst proponowany przez Komisję	*Poprawka*
9. Pojedynczy punkt kontaktowy co miesiąc przedkłada ENISA sprawozdanie podsumowujące zawierające zanonimizowane i zagregowane dane dotyczące incydentów, znaczących cyberzagrożeń i zdarzeń potencjalnie wypadkowych zgłoszonych zgodnie z ust. 1 ***i 2*** oraz zgodnie z art. 27. Aby przyczynić się do dostarczania porównywalnych informacji, ENISA może wydawać wytyczne techniczne dotyczące parametrów informacji zawartych w sprawozdaniu podsumowującym.	9. Pojedynczy punkt kontaktowy co miesiąc przedkłada ENISA sprawozdanie podsumowujące zawierające zanonimizowane i zagregowane dane dotyczące incydentów, znaczących cyberzagrożeń i zdarzeń potencjalnie wypadkowych zgłoszonych zgodnie z ust. 1 oraz zgodnie z art. 27. Aby przyczynić się do dostarczania porównywalnych informacji, ENISA może wydawać wytyczne techniczne dotyczące parametrów informacji zawartych w sprawozdaniu podsumowującym.

Poprawka 122
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 10

Tekst proponowany przez Komisję	*Poprawka*
10. Właściwe organy przekazują właściwym organom wyznaczonym na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych] informacje na temat incydentów i cyberzagrożeń zgłaszanych zgodnie z ust. 1 ***i 2*** przez podmioty niezbędne uznane za podmioty krytyczne lub za podmioty równoważne z podmiotami krytycznymi na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych].	10. Właściwe organy przekazują właściwym organom wyznaczonym na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych] informacje na temat incydentów i cyberzagrożeń zgłaszanych zgodnie z ust. 1 przez podmioty niezbędne uznane za podmioty krytyczne lub za podmioty równoważne z podmiotami krytycznymi na podstawie dyrektywy (UE) XXXX/XXXX [dyrektywa w sprawie odporności podmiotów krytycznych].

Poprawka 123
Wniosek dotyczący dyrektywy
Artykuł 20 – ustęp 11

Tekst proponowany przez Komisję	*Poprawka*
11. Komisja może przyjąć akty wykonawcze doprecyzowujące rodzaj informacji, format i procedurę zgłoszenia dokonywanego zgodnie z ust. 1 ***i 2***. Komisja może również przyjąć akty wykonawcze w celu doprecyzowania przypadków, w których incydent uznaje się za znaczący, o czym mowa w ust. 3. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2.	11. Komisja może przyjąć akty wykonawcze doprecyzowujące rodzaj informacji, format i procedurę zgłoszenia dokonywanego zgodnie z ust. 1. Komisja może również przyjąć akty wykonawcze w celu doprecyzowania przypadków, w których incydent uznaje się za znaczący, o czym mowa w ust. 3. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 37 ust. 2.

Poprawka 124
Wniosek dotyczący dyrektywy
Artykuł 21 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Aby wykazać zgodność z niektórymi wymogami określonymi w art. 18, państwa członkowskie ***mogą wymagać od podmiotów niezbędnych*** i ***istotnych*** certyfikacji niektórych produktów, usług i procesów ICT w oparciu o ***określone*** europejskie programy ***certyfikacji*** cyberbezpieczeństwa przyjęte na podstawie art. 49 rozporządzenia (UE) 2019/881**.** ***Produkty, usługi i procesy podlegające*** certyfikacji ***mogą być opracowywane przez podmiot niezbędny lub istotny lub mogą być zamawiane u osób trzecich***.	1. Aby wykazać zgodność z niektórymi wymogami określonymi w art. 18 ***i podnieść poziom cyberbezpieczeństwa***, państwa członkowskie***, po konsultacji z Grupą Współpracy i ENISA, zachęcają niezbędne*** i ***istotne podmioty do*** certyfikacji niektórych produktów, usług i procesów ICT***, które albo zostały opracowane przez niezbędny lub istotny podmiot lub zamówione u osób trzecich,*** w oparciu o europejskie programy cyberbezpieczeństwa przyjęte na podstawie art. 49 rozporządzenia (UE) 2019/881 ***lub podobne programy*** certyfikacji ***uznawane na całym świecie. W miarę możliwości państwa członkowskie zachęcają do stosowania przyjętych systemów certyfikacji w sposób zharmonizowany***.

Poprawka 125
Wniosek dotyczący dyrektywy
Artykuł 21 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Komisja ***jest uprawniona do przyjęcia aktów delegowanych określających***, które kategorie podmiotów niezbędnych ***mają obowiązek na podstawie ust. 1 uzyskać certyfikację*** i na podstawie których konkretnych europejskich programów certyfikacji cyberbezpieczeństwa ***mają ją uzyskać***. ***Akty delegowane przyjmuje się zgodnie z art. 36.***	2. Komisja ***regularnie ocenia skuteczność i wykorzystanie przyjętych europejskich systemów certyfikacji cyberbezpieczeństwa zgodnie z art. 49 rozporządzenia (UE) 2019/881 i określa***, które kategorie podmiotów niezbędnych ***należy zachęcać do uzyskania certyfikacji*** i na podstawie których konkretnych europejskich programów certyfikacji cyberbezpieczeństwa ***na podstawie ust. 1***.

Poprawka 126
Wniosek dotyczący dyrektywy
Artykuł 22 – ustęp -1 (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	-1. Komisja we współpracy z ENISA wspiera i promuje opracowywanie i wdrażanie norm ustanowionych przez właściwe unijne i międzynarodowe organy normalizacyjne w celu spójnego wdrażania art. 18 ust. 1 i 2. Komisja wspiera aktualizację norm w świetle rozwoju technologicznego.

Poprawka 127
Wniosek dotyczący dyrektywy
Artykuł 22 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Aby wspierać spójne wdrażanie art. 18 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 istotnych z punktu widzenia bezpieczeństwa sieci i systemów informatycznych.	1. Aby wspierać spójne wdrażanie art. 18 ust. 1 i 2, państwa członkowskie, nie narzucając ani nie faworyzując wykorzystywania określonego rodzaju technologii, ***a także zgodnie z wytycznymi Agencji Unii Europejskiej ds. Cyberbezpieczeństwa i Grupy Współpracy,*** zachęcają do stosowania europejskich lub uznanych międzynarodowo norm i specyfikacji istotnych z punktu widzenia bezpieczeństwa sieci i systemów

informatycznych.

Poprawka 128
Wniosek dotyczący dyrektywy
Artykuł 23 – tytuł

Tekst proponowany przez Komisję	*Poprawka*
Bazy danych ***zawierające nazwy*** domen i ***dane rejestracyjne***	***Infrastruktura baz*** danych ***nazw*** domen i ***danych rejestracyjnych***

Poprawka 129
Wniosek dotyczący dyrektywy
Artykuł 23 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. W celu wzmocnienia bezpieczeństwa, stabilności i odporności DNS państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD z należytą starannością gromadziły i zachowywały w specjalnej bazie danych dokładne i kompletne dane dotyczące rejestracji nazw domen, z zastrzeżeniem unijnych przepisów o ochronie danych w odniesieniu do danych będących danymi osobowymi.	1. W celu wzmocnienia bezpieczeństwa, stabilności i odporności DNS państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen dla TLD z należytą starannością gromadziły***, weryfikowały*** i zachowywały w specjalnej bazie danych dokładne i kompletne dane dotyczące rejestracji nazw domen ***niezbędnych im do świadczenia usług***, z zastrzeżeniem unijnych przepisów o ochronie danych w odniesieniu do danych będących danymi osobowymi.

Poprawka 130
Wniosek dotyczący dyrektywy
Artykuł 23 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Państwa członkowskie zapewniają, aby w ***bazach*** danych ***zawierających dane dotyczące*** rejestracji nazw domen, o ***których*** mowa w ust. 1, znajdowały się informacje niezbędne do zidentyfikowania posiadaczy nazw domen i punktów kontaktowych zarządzających nazwami domen w ramach TLD i do skontaktowania	2. Państwa członkowskie zapewniają, aby w ***infrastrukturze baz*** danych ***dotyczących*** rejestracji nazw domen, o ***której*** mowa w ust. 1, znajdowały się informacje***, które zawierają co najmniej nazwy podmiotów rejestrujących, ich adresy fizyczne i adresy poczty elektronicznej, jak również numery***

się z ***nimi***.	***telefonów,*** niezbędne do zidentyfikowania posiadaczy nazw domen i punktów kontaktowych zarządzających nazwami domen w ramach TLD i do skontaktowania się z ***nimi, w tym co najmniej nazwy podmiotów rejestrujących, ich adresy fizyczne i adresy poczty elektronicznej, jak również numer telefonu***.

Poprawka 131
Wniosek dotyczący dyrektywy
Artykuł 23 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen ***dla TLD*** wdrożyły polityki i procedury służące zapewnieniu, by ***bazy*** danych ***zawierały*** dokładne i ***kompletne*** dane. Państwa członkowskie zapewniają, aby takie polityki i procedury podawano do wiadomości publicznej.	3. Państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen wdrożyły polityki i procedury służące zapewnieniu, by ***infrastruktura baz*** danych ***zawierała*** dokładne***, sprawdzone*** i ***kompletne informacje oraz aby podmiot rejestrujący bezzwłocznie korygował lub usuwał niedokładne lub niepełne*** dane. Państwa członkowskie zapewniają, aby takie polityki i procedury podawano do wiadomości publicznej.

Poprawka 132
Wniosek dotyczący dyrektywy
Artykuł 23 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Państwa członkowskie zapewniają, aby po rejestracji nazwy domeny rejestry TLD i podmioty świadczące usługi rejestracji nazw domen ***dla TLD*** bez zbędnej zwłoki publikowały dane dotyczące rejestracji domeny, które nie są danymi ***osobowymi***.	4. Państwa członkowskie zapewniają, aby po rejestracji nazwy domeny rejestry TLD i podmioty świadczące usługi rejestracji nazw domen bez zbędnej zwłoki***, a w każdym razie w ciągu 24 godzin*** publikowały ***wszystkie*** dane dotyczące rejestracji domeny, które nie są danymi ***osób prawnych jako podmiotów rejestrujących***.

Poprawka 133
Wniosek dotyczący dyrektywy
Artykuł 23 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. Państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen ***dla TLD***, na ***zgodny z prawem i*** należycie uzasadniony wniosek złożony przez wnioskodawców ubiegających się o prawnie uzasadniony dostęp, ***udzielały*** dostępu do konkretnych danych dotyczących rejestracji nazw domen zgodnie z unijnym prawem ochrony danych. Państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen ***dla TLD*** bez zbędnej zwłoki udzielały odpowiedzi na wszystkie wnioski o dostęp. Państwa członkowskie zapewniają, aby polityki i procedury regulujące ujawnianie takich danych podawano do wiadomości publicznej.	5. Państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen, na należycie uzasadniony wniosek złożony przez wnioskodawców ubiegających się o prawnie uzasadniony dostęp, ***były zobowiązane do udzielania*** dostępu do konkretnych danych dotyczących rejestracji nazw domen zgodnie z unijnym prawem ochrony danych. Państwa członkowskie zapewniają, aby rejestry TLD i podmioty świadczące usługi rejestracji nazw domen bez zbędnej zwłoki***, a w każdym przypadku w ciągu 72 godzin,*** udzielały odpowiedzi na wszystkie ***zgodne z prawem i należycie uzasadnione*** wnioski o dostęp. Państwa członkowskie zapewniają, aby polityki i procedury regulujące ujawnianie takich danych podawano do wiadomości publicznej.

Poprawka 134
Wniosek dotyczący dyrektywy
Artykuł 24 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Do celów niniejszej dyrektywy uznaje się, że podmioty, o których mowa w ust. 1, posiadają swoją główną jednostkę organizacyjną w Unii w tym państwie członkowskim, w którym podejmowane są decyzje związane ze środkami zarządzania ryzykiem w cyberprzestrzeni. Jeżeli takich decyzji nie podejmuje się w jednostce organizacyjnej położonej w Unii, uznaje się, że główna jednostka organizacyjna znajduje się w państwie członkowskim, w którym podmioty mają jednostkę organizacyjną o największej liczbie pracowników w Unii.	2. Do celów niniejszej dyrektywy uznaje się, że podmioty, o których mowa w ust. 1, posiadają swoją główną jednostkę organizacyjną w Unii w tym państwie członkowskim, w którym podejmowane są decyzje związane ze środkami zarządzania ryzykiem w cyberprzestrzeni. Jeżeli takich decyzji nie podejmuje się w jednostce organizacyjnej położonej w Unii, uznaje się, że główna jednostka organizacyjna znajduje się w państwie członkowskim, w którym podmioty mają jednostkę organizacyjną o największej liczbie pracowników w Unii. ***Odbywa się to w sposób gwarantujący, że krajowe organy***

	regulacyjne nie będą miały do czynienia z nieproporcjonalnym obciążeniem.

Poprawka 135
Wniosek dotyczący dyrektywy
Artykuł 25 – ustęp 1 – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
1. ENISA tworzy i prowadzi rejestr podmiotów niezbędnych i istotnych, o których mowa w art. 24 ust. 1. Do dnia [12 miesięcy po wejściu w życie niniejszej dyrektywy] r. podmioty te przekazują ENISA następujące informacje:	1. ENISA tworzy i prowadzi rejestr podmiotów niezbędnych i istotnych, o których mowa w art. 24 ust. 1. ***W tym celu*** do dnia [12 miesięcy po wejściu w życie niniejszej dyrektywy] r. podmioty te przekazują ENISA następujące informacje:

Poprawka 136
Wniosek dotyczący dyrektywy
Artykuł 26 – ustęp 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) zwiększa poziom cyberbezpieczeństwa, w szczególności poprzez podnoszenie świadomości w odniesieniu do cyberzagrożeń, ograniczanie lub utrudnianie rozprzestrzeniania się tych cyberzagrożeń, wspieranie różnorodnego potencjału obronnego, eliminowanie i ujawnianie podatności, techniki wykrywania zagrożeń, strategie ich minimalizowania lub etapy reagowania i przywracania gotowości do pracy.	b) zwiększa poziom cyberbezpieczeństwa, w szczególności poprzez podnoszenie świadomości w odniesieniu do cyberzagrożeń, ograniczanie lub utrudnianie rozprzestrzeniania się tych cyberzagrożeń, wspieranie różnorodnego potencjału obronnego, eliminowanie i ujawnianie podatności, techniki wykrywania zagrożeń ***i zapobiegania im***, strategie ich minimalizowania lub etapy reagowania i przywracania gotowości do pracy.

Poprawka 137
Wniosek dotyczący dyrektywy
Artykuł 26 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Państwa członkowskie ustanawiają ***przepisy*** określające procedurę, elementy operacyjne (w tym korzystanie ze specjalnych platform ICT), treść i warunki	3. Państwa członkowskie ustanawiają ***wytyczne*** określające procedurę, elementy operacyjne (w tym korzystanie ze specjalnych platform ICT), treść i warunki

funkcjonowania mechanizmów wymiany informacji, o których mowa w ust. 2. ***Przepisy*** takie ***określają*** również szczegóły zaangażowania organów publicznych we wspomniane mechanizmy, a także elementy operacyjne, w tym wykorzystanie specjalnych platform informatycznych. Państwa członkowskie oferują wsparcie w stosowaniu takich mechanizmów zgodnie ze swoją polityką, o której mowa w art. 5 ust. 2 lit. g).	funkcjonowania mechanizmów wymiany informacji, o których mowa w ust. 2. ***Wytyczne*** takie ***obejmują*** również ***w stosownych przypadkach*** szczegóły zaangażowania organów publicznych ***i niezależnych ekspertów*** we wspomniane mechanizmy, a także elementy operacyjne, w tym wykorzystanie specjalnych platform informatycznych. Państwa członkowskie oferują wsparcie w stosowaniu takich mechanizmów zgodnie ze swoją polityką, o której mowa w art. 5 ust. 2 lit. g).

Poprawka 138
Wniosek dotyczący dyrektywy
Artykuł 26 – ustęp 5

Tekst proponowany przez Komisję	*Poprawka*
5. Zgodnie z prawem Unii ENISA pomaga w ustanowieniu mechanizmów wymiany informacji na temat cyberbezpieczeństwa, o których mowa w ust. 2, ***zapewniając*** najlepsze praktyki i wytyczne.	5. Zgodnie z prawem Unii ENISA pomaga w ustanowieniu mechanizmów wymiany informacji na temat cyberbezpieczeństwa, o których mowa w ust. 2, ***zapewnia*** najlepsze praktyki i wytyczne***, a także ułatwia wymianę informacji na szczeblu Unii, dbając o ochronę informacji biznesowych***. ***Na wniosek podmiotów niezbędnych i istotnych Grupę Współpracy prosi się o przedstawienie najlepszych praktyk i wytycznych.***

Poprawka 139
Wniosek dotyczący dyrektywy
Artykuł 27 – akapit -1 (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	-1. Państwa członkowskie dopilnowują, by podmioty niezbędne i istotne mogły dobrowolnie zgłaszać zidentyfikowane przez nie cyberzagrożenia, które mogły doprowadzić do poważnego incydentu. Państwa członkowskie dopilnowują, by zgłaszając takie incydenty, podmioty te postępowały

według procedury określonej w art. 20. Dobrowolne zgłoszenia nie mogą skutkować nałożeniem na jednostkę zgłaszającą żadnych dodatkowych obowiązków.

Poprawka 140
Wniosek dotyczący dyrektywy
Artykuł 27 – akapit 1

Tekst proponowany przez Komisję	*Poprawka*
Nie naruszając przepisów art. 3, państwa członkowskie zapewniają, aby podmioty nieobjęte zakresem niniejszej dyrektywy mogły na zasadzie dobrowolności dokonywać zgłoszeń znaczących incydentów, cyberzagrożeń lub zdarzeń potencjalnie wypadkowych. Przy rozpatrywaniu zgłoszeń państwa członkowskie postępują zgodnie z procedurą określoną w art. 20. Państwa członkowskie ***mogą rozpatrywać*** zgłoszenia obowiązkowe priorytetowo względem zgłoszeń dobrowolnych. Zgłaszanie dobrowolne nie może skutkować nałożeniem na podmiot zgłaszający żadnych dodatkowych obowiązków, którym by nie podlegał, gdyby nie dokonał tego zgłoszenia.	***1.*** ***Nie*** naruszając przepisów art. 3, państwa członkowskie zapewniają, aby podmioty nieobjęte zakresem niniejszej dyrektywy mogły na zasadzie dobrowolności dokonywać zgłoszeń znaczących incydentów, cyberzagrożeń lub zdarzeń potencjalnie wypadkowych. Przy rozpatrywaniu zgłoszeń państwa członkowskie postępują zgodnie z procedurą określoną w art. 20. Państwa członkowskie ***rozpatrują*** zgłoszenia obowiązkowe priorytetowo względem zgłoszeń dobrowolnych. Zgłaszanie dobrowolne nie może skutkować nałożeniem na podmiot zgłaszający żadnych dodatkowych obowiązków, którym by nie podlegał, gdyby nie dokonał tego zgłoszenia***, ale państwo członkowskie może zaoferować mu pomoc zespołów CSIRT***.

Poprawka 141
Wniosek dotyczący dyrektywy
Artykuł 28 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Państwa członkowskie zapewniają, aby właściwe organy skutecznie monitorowały zgodność z niniejszą dyrektywą, w szczególności z obowiązkami przewidzianymi w art. 18 i 20, i stosowały środki niezbędne do zagwarantowania takiej zgodności.	1. Państwa członkowskie zapewniają, aby właściwe organy skutecznie monitorowały zgodność z niniejszą dyrektywą, w szczególności z obowiązkami przewidzianymi w art. 18 i 20, i stosowały środki niezbędne do zagwarantowania takiej zgodności ***oraz aby dysponowały odpowiednimi środkami***

gwarantującymi pełnienie ich roli.

Poprawka 142
Wniosek dotyczący dyrektywy
Artykuł 28 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Podejmując działania w odpowiedzi na incydenty, które doprowadziły do naruszeń danych osobowych, właściwy organ działa w ścisłej współpracy z organami ochrony danych.	2. Podejmując działania w odpowiedzi na incydenty, które doprowadziły do naruszeń danych osobowych, właściwy organ działa w ścisłej współpracy z organami ochrony danych***, w tym również, w stosownych przypadkach, z organami ochrony danych z innych państw członkowskich***.

Poprawka 143
Wniosek dotyczący dyrektywy
Artykuł 29 – ustęp 2 – litera c

Tekst proponowany przez Komisję	*Poprawka*
c) ukierunkowanymi audytami bezpieczeństwa w oparciu o oceny ryzyka lub dostępne informacje dotyczące ryzyka;	c) ukierunkowanymi audytami bezpieczeństwa w oparciu o oceny ryzyka lub dostępne informacje dotyczące ryzyka***, prowadzonymi przez wykwalifikowany niezależny organ lub właściwy urząd***;

Poprawka 144
Wniosek dotyczący dyrektywy
Artykuł 29 – ustęp 2 – litera f

Tekst proponowany przez Komisję	*Poprawka*
f) żądaniami udzielenia dostępu do danych, dokumentów lub ***wszelkich*** informacji koniecznych do wykonywania ***ich*** zadań nadzorczych;	f) żądaniami udzielenia dostępu do ***istotnych*** danych, dokumentów lub informacji koniecznych do wykonywania zadań nadzorczych;

Poprawka 145
Wniosek dotyczący dyrektywy
Artykuł 29 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Wykonując swoje uprawnienia zgodnie z ust. 2 lit. e)–g), właściwe organy podają cel żądania ***i*** określają żądane informacje.	3. Wykonując swoje uprawnienia zgodnie z ust. 2 lit. e)–g), właściwe organy podają cel żądania***,*** określają żądane informacje ***i ograniczają żądanie do zakresu incydentu lub problemu będącego przedmiotem zainteresowania***.

Poprawka 146
Wniosek dotyczący dyrektywy
Artykuł 29 – ustęp 5 – akapit 1 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) zawieszenia lub zwrócenia się do organu, który dokonał certyfikacji lub udzielił zezwolenia, o zawieszenie certyfikacji lub zezwolenia w odniesieniu do ***części lub wszystkich*** usług świadczonych bądź ***części lub całości*** działalności prowadzonej przez podmiot niezbędny;	a) zawieszenia lub zwrócenia się do organu, który dokonał certyfikacji lub udzielił zezwolenia, o zawieszenie certyfikacji lub zezwolenia w odniesieniu do ***odnośnych*** usług świadczonych bądź ***odnośnej*** działalności prowadzonej przez podmiot niezbędny;

Poprawka 147
Wniosek dotyczący dyrektywy
Artykuł 29 – ustęp 5 – akapit 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) nałożenia lub zwrócenia się o nałożenie przez właściwe organy lub sądy zgodnie z przepisami krajowymi tymczasowego zakazu pełnienia funkcji zarządczych w takim podmiocie niezbędnym na każdą osobę wykonującą obowiązki zarządcze na poziomie dyrektora generalnego lub przedstawiciela prawnego w tym podmiocie oraz na każdą inną osobę fizyczną uznaną za odpowiedzialną za naruszenie.	***skreśla się***

Poprawka 148
Wniosek dotyczący dyrektywy
Artykuł 30 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. W przypadku otrzymania dowodu lub wskazania, że podmiot istotny nie spełnia obowiązków przewidzianych w niniejszej dyrektywie, w szczególności w art. 18 i 20, państwa członkowskie zapewniają, aby właściwe organy podejmowały działania, w razie konieczności**,** w drodze środków nadzoru ex post.	1. W przypadku otrzymania dowodu lub wskazania, że podmiot istotny nie spełnia obowiązków przewidzianych w niniejszej dyrektywie, w szczególności w art. 18 i 20, państwa członkowskie zapewniają, aby właściwe organy podejmowały działania, w razie konieczności ***i z uwzględnieniem podejścia opartego na analizie ryzyka*** **–** w drodze środków nadzoru ex post.

Poprawka 149
Wniosek dotyczący dyrektywy
Artykuł 30 – ustęp 2 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) ukierunkowanymi audytami bezpieczeństwa w oparciu o oceny ryzyka lub dostępne informacje dotyczące ryzyka;	b) ukierunkowanymi audytami bezpieczeństwa w oparciu o oceny ryzyka lub dostępne informacje dotyczące ryzyka**,** ***prowadzonymi przez wykwalifikowany niezależny organ lub właściwy urząd***;

Poprawka 150
Wniosek dotyczący dyrektywy
Artykuł 30 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Wykonując swoje uprawnienia zgodnie z ust. 2 lit. d) lub e), właściwe organy podają cel żądania ***i*** określają żądane informacje.	3. Wykonując swoje uprawnienia zgodnie z ust. 2 lit. d) lub e), właściwe organy podają cel żądania**,** określają żądane informacje ***i ograniczają żądania do zakresu incydentu lub problemu będącego przedmiotem zainteresowania***.

Poprawka 151
Wniosek dotyczący dyrektywy
Artykuł 31 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
4. Państwa członkowskie zapewniają, aby naruszenia obowiązków przewidzianych w art. 18 lub 20 podlegały na mocy ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości ***co najmniej*** 10 000 000 EUR lub 2 % całkowitego rocznego światowego obrotu przedsiębiorstwa, do którego należy podmiot niezbędny lub istotny, z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.	4. Państwa członkowskie zapewniają, aby naruszenia obowiązków przewidzianych w art. 18 lub 20 podlegały na mocy ust. 2 i 3 niniejszego artykułu administracyjnym karom pieniężnym w maksymalnej wysokości 10 000 000 EUR lub 2 % całkowitego rocznego światowego obrotu przedsiębiorstwa, do którego należy podmiot niezbędny lub istotny, z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Poprawka 152
Wniosek dotyczący dyrektywy
Artykuł 32 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Jeżeli właściwe organy mają przesłanki wskazujące na to, że naruszenie przez podmiot niezbędny lub istotny obowiązków przewidzianych w art. 18 i 20 pociąga za sobą naruszenie ochrony danych osobowych, zdefiniowane w art. 4 pkt 12 rozporządzenia (UE) 2016/679, które podlega zgłoszeniu na podstawie art. 33 tego rozporządzenia, informują one o tym ***w rozsądnym terminie*** organy nadzorcze właściwe na mocy art. 55 i 56 tego rozporządzenia.	1. Jeżeli właściwe organy mają przesłanki wskazujące na to, że naruszenie przez podmiot niezbędny lub istotny obowiązków przewidzianych w art. 18 i 20 pociąga za sobą naruszenie ochrony danych osobowych, zdefiniowane w art. 4 pkt 12 rozporządzenia (UE) 2016/679, które podlega zgłoszeniu na podstawie art. 33 tego rozporządzenia, informują one o tym organy nadzorcze właściwe na mocy art. 55 i 56 tego rozporządzenia ***bez zbędnej zwłoki i nie później niż przed upływem 72 godzin***.

Poprawka 153
Wniosek dotyczący dyrektywy
Artykuł 32 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. Jeżeli organ nadzorczy właściwy na mocy rozporządzenia (UE) 2016/679 jest ustanowiony w innym państwie członkowskim niż właściwy organ,	3. Jeżeli organ nadzorczy właściwy na mocy rozporządzenia (UE) 2016/679 jest ustanowiony w innym państwie członkowskim niż właściwy organ,

właściwy organ ***może poinformować*** organ nadzorczy ustanowiony w tym samym państwie członkowskim.	właściwy organ ***informuje również*** organ nadzorczy ustanowiony w tym samym państwie członkowskim.

Poprawka 154
Wniosek dotyczący dyrektywy
Artykuł 36 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Uprawnienia do ***przyjęcia*** aktów delegowanych, o których mowa w art. 18 ust. ***6*** i art. ***21*** ust. ***2***, powierza się Komisji na okres pięciu lat od dnia [...] r.	2. Uprawnienia do ***przyjmowania*** aktów delegowanych, o których mowa w art. 18 ust. ***5*** i art. ***20*** ust. ***3***, powierza się Komisji na okres pięciu lat od dnia [...] r.

Poprawka 155
Wniosek dotyczący dyrektywy
Artykuł 36 – ustęp 3

Tekst proponowany przez Komisję	*Poprawka*
3. ***Przekazanie uprawnień, o którym mowa w*** art. 18 ust. ***6*** i art. ***21*** ust. ***2, może zostać*** w ***dowolnym momencie odwołane przez*** Parlament Europejski ***lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych*** w ***niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie w określonym w tej decyzji. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych***.	3. ***Akt delegowany przyjęty na podstawie*** art. 18 ust. ***5*** i art. ***20*** ust. ***3 wchodzi*** w ***życie tylko wówczas, gdy ani*** Parlament Europejski***, ani Rada nie wyraziły sprzeciwu*** w ***terminie trzech miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o trzy miesiące z inicjatywy Parlamentu Europejskiego lub Rady***.

Poprawka 156
Wniosek dotyczący dyrektywy
Artykuł 36 – ustęp 6

Tekst proponowany przez Komisję	*Poprawka*
6. Akt delegowany przyjęty na podstawie art. 18 ust. ***6*** i art. ***21*** ust. ***2*** wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie	6. Akt delegowany przyjęty na podstawie art. 18 ust. ***5*** i art. ***20*** ust. ***3*** wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie

wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.	wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie**,** lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

ZAŁĄCZNIK: WYKAZ PODMIOTÓW LUB OSÓB, OD KTÓRYCH SPRAWOZDAWCA OTRZYMAŁ INFORMACJE.

Poniższy wykaz opracowano na zasadzie zupełnej dobrowolności, na wyłączną odpowiedzialność sprawozdawcy. Przy sporządzaniu sprawozdania, do czasu przyjęcia go w komisji, sprawozdawca otrzymał informacje od następujących podmiotów lub osób:

Osoba	Podmiot
	BSA (The Software Alliance)
	BusinessEurope
	Confederation of Danish Industries
	Danish Permanent Representation
	Deutsche Telekom
	Digital Europe
	DOT Europe
	ETNO (European Telecommunications Network Operators)
	French Permanent Representation
	German Permanent Representation
	HUAWEI
	IFPI
	INTEL
	ITI (The Information Technology Industry Council)
	Kaspersky
	MÆRSK
	Microsoft
	ICANN
	MOTION PICTURE ASSOCIATION
	Orgalim
	Palo Alto Networks

	Rettighedsalliancen

PROCEDURA W KOMISJI OPINIODAWCZEJ

Tytuł	Środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylenie dyrektywy (UE) 2016/1148
Odsyłacze	COM(2020)0823 – C9-0422/2020 – 2020/0359(COD)
Komisja przedmiotowo właściwa Data ogłoszenia na posiedzeniu	ITRE 21.1.2021
Opinia wydana przez Data ogłoszenia na posiedzeniu	IMCO 21.1.2021
Sprawozdawca komisji opiniodawczej: Data powołania	Morten Løkkegaard 9.2.2021
Rozpatrzenie w komisji	26.5.2021 21.6.2021
Data przyjęcia	12.7.2021
Wynik głosowania końcowego	+: 42 –: 1 0: 2
Posłowie obecni podczas głosowania końcowego	Alex Agius Saliba, Andrus Ansip, Pablo Arias Echeverría, Alessandra Basso, Brando Benifei, Adam Bielan, Hynek Blaško, Biljana Borzan, Vlad-Marius Botoş, Markus Buchheit, Andrea Caroppo, Anna Cavazzini, Dita Charanzová, Deirdre Clune, David Cormand, Carlo Fidanza, Evelyne Gebhardt, Alexandra Geese, Sandro Gozi, Maria Grapini, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Marcel Kolaja, Kateřina Konečná, Andrey Kovatchev, Jean-Lin Lacapelle, Maria-Manuel Leitão-Marques, Morten Løkkegaard, Antonius Manders, Leszek Miller, Anne-Sophie Pelletier, Miroslav Radačovský, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Marco Zullo
Zastępcy obecni podczas głosowania końcowego	Clara Aguilera, Maria da Graça Carvalho, Christian Doleschal, Claude Gruffat, Jiří Pospíšil, Kosma Złotowski

GŁOSOWANIE KOŃCOWE W FORMIE GŁOSOWANIA IMIENNEGO W KOMISJI OPINIODAWCZEJ

42	+
ECR	Adam Bielan, Carlo Fidanza, Kosma Złotowski
ID	Alessandra Basso, Hynek Blaško, Markus Buchheit, Virginie Joron, Jean-Lin Lacapelle
PPE	Pablo Arias Echeverría, Andrea Caroppo, Maria da Graça Carvalho, Deirdre Clune, Christian Doleschal, Andrey Kovatchev, Antonius Manders, Jiří Pospíšil, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein
Renew	Andrus Ansip, Vlad-Marius Botoş, Dita Charanzová, Sandro Gozi, Morten Løkkegaard, Marco Zullo
S&D	Alex Agius Saliba, Clara Aguilera, Brando Benifei, Biljana Borzan, Evelyne Gebhardt, Maria Grapini, Maria-Manuel Leitão-Marques, Leszek Miller, Christel Schaldemose
The Left	Kateřina Konečná, Anne-Sophie Pelletier
Verts/ALE	Anna Cavazzini, David Cormand, Alexandra Geese, Claude Gruffat, Marcel Kolaja

1	-
NI	Miroslav Radačovský

2	0
ECR	Eugen Jurzyca
Renew	Svenja Hahn

Objaśnienie używanych znaków:
+ : za
- : przeciw
0 : wstrzymało się