Parlament Europejski
2019-2024

Komisja Przemysłu, Badań Naukowych i Energii

2023/0108(COD)

21.9.2023

POPRAWKI
17 - 52

Projekt sprawozdania
Josianne Cutajar
(PE752.802v01-00)

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa

Wniosek dotyczący rozporządzenia
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Poprawka 17
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Motyw 2

Tekst proponowany przez Komisję	*Poprawka*
(2) ***Coraz większą rolę w zapobieganiu cyberincydentom i ograniczaniu ich skutków odgrywają usługi zarządzane*** w zakresie bezpieczeństwa***, czyli*** usługi ***polegające*** na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, na jakie narażeni są klienci dostawców tych usług. W związku z tym dostawców ***takich usług*** uznaje się za podmioty kluczowe lub ważne należące do sektora kluczowego na podstawie ***dyrektywy Parlamentu Europejskiego*** i ***Rady*** (UE) 2022/2555[8]. Zgodnie z motywem 86 tej dyrektywy szczególnie ważną rolę w pomaganiu podmiotom w działaniach mających na celu zapobieganie incydentom, wykrywanie ich, reagowanie na nie lub przywracanie normalnego działania po ich wystąpieniu odgrywają dostawcy usług zarządzanych w zakresie bezpieczeństwa zajmujący się obszarami takimi jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo. Dostawcy usług zarządzanych w zakresie bezpieczeństwa również sami padają jednak ofiarą cyberataków, a ponieważ ich działalność jest ściśle zintegrowana z operacjami ich klientów, stanowią oni szczególne ryzyko. W związku z tym przy wyborze dostawcy usług zarządzanych w zakresie bezpieczeństwa podmioty kluczowe i ważne w rozumieniu przepisów dyrektywy (UE) 2022/2555 powinny dochować szczególnej staranności.	(2) ***Usługi zarządzane w zakresie bezpieczeństwa to usługi świadczone przez dostawców usług zarządzanych*** w zakresie bezpieczeństwa ***zgodnie z art. 6 pkt 40 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555.*** Usługi ***te polegają*** na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, na jakie narażeni są klienci dostawców tych usług***, i odgrywają coraz większą rolę w zapobieganiu cyberincydentom i ograniczaniu ich skutków***. W związku z tym dostawców ***usług zarządzanych w zakresie bezpieczeństwa*** uznaje się za podmioty kluczowe lub ważne należące do sektora kluczowego na podstawie ***pkt 10 załącznika*** I ***do dyrektywy*** (UE) 2022/2555. Zgodnie z motywem 86 tej dyrektywy szczególnie ważną rolę w pomaganiu podmiotom w działaniach mających na celu zapobieganie incydentom, wykrywanie ich, reagowanie na nie lub przywracanie normalnego działania po ich wystąpieniu odgrywają dostawcy usług zarządzanych w zakresie bezpieczeństwa zajmujący się obszarami takimi jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo. Dostawcy usług zarządzanych w zakresie bezpieczeństwa również sami padają jednak ofiarą cyberataków, a ponieważ ich działalność jest ściśle zintegrowana z operacjami ich klientów, stanowią oni szczególne ryzyko. W związku z tym przy wyborze dostawcy usług zarządzanych w zakresie bezpieczeństwa podmioty kluczowe i ważne w rozumieniu przepisów dyrektywy (UE) 2022/2555 powinny

dochować szczególnej staranności.

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

Or. en

Poprawka 18
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 2

Tekst proponowany przez Komisję	*Poprawka*
(2) Coraz większą rolę w zapobieganiu cyberincydentom i ograniczaniu ich skutków odgrywają usługi zarządzane w zakresie bezpieczeństwa, czyli usługi polegające na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, na jakie narażeni są klienci dostawców tych usług. W związku z tym dostawców takich usług uznaje się za podmioty kluczowe lub ważne należące do sektora kluczowego na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555[8]. Zgodnie z motywem 86 tej dyrektywy szczególnie ważną rolę w pomaganiu podmiotom w działaniach mających na celu zapobieganie incydentom, wykrywanie ich, reagowanie na nie lub przywracanie normalnego działania po ich wystąpieniu odgrywają dostawcy usług zarządzanych w zakresie bezpieczeństwa zajmujący się	(2) Coraz większą rolę w zapobieganiu cyberincydentom i ograniczaniu ich skutków odgrywają usługi zarządzane w zakresie bezpieczeństwa, czyli usługi polegające na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, na jakie narażeni są klienci dostawców tych usług***, m.in. w zakresie zapobiegania incydentom, ich wykrywania, reagowania na nie i usuwania ich skutków***. W związku z tym dostawców takich usług uznaje się za podmioty kluczowe lub ważne należące do sektora kluczowego na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555[8]. Zgodnie z motywem 86 tej dyrektywy szczególnie ważną rolę w pomaganiu podmiotom w działaniach mających na celu zapobieganie incydentom, wykrywanie ich, reagowanie na nie lub przywracanie

obszarami takimi jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo. Dostawcy usług zarządzanych w zakresie bezpieczeństwa również sami padają jednak ofiarą cyberataków, a ponieważ ich działalność jest ściśle zintegrowana z operacjami ich klientów, stanowią oni szczególne ryzyko. W związku z tym przy wyborze dostawcy usług zarządzanych w zakresie bezpieczeństwa podmioty kluczowe i ważne w rozumieniu przepisów dyrektywy (UE) 2022/2555 powinny dochować szczególnej staranności.

normalnego działania po ich wystąpieniu odgrywają dostawcy usług zarządzanych w zakresie bezpieczeństwa zajmujący się obszarami takimi jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo. Dostawcy usług zarządzanych w zakresie bezpieczeństwa również sami padają jednak ofiarą cyberataków, a ponieważ ich działalność jest ściśle zintegrowana z operacjami ich klientów, stanowią oni szczególne ryzyko. W związku z tym przy wyborze dostawcy usług zarządzanych w zakresie bezpieczeństwa podmioty kluczowe i ważne w rozumieniu przepisów dyrektywy (UE) 2022/2555 powinny dochować szczególnej staranności.

_____

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

[8] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

Or. en

Poprawka 19
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Motyw 3

Tekst proponowany przez Komisję	*Poprawka*
(3) Dostawcy usług zarządzanych w zakresie bezpieczeństwa odgrywają również ważną rolę w unijnej rezerwie cyberbezpieczeństwa, której stopniowe tworzenie wspierają przepisy rozporządzenia (UE) …/…**.** [rozporządzenie ustanawiające środki	(3) Dostawcy usług zarządzanych w zakresie bezpieczeństwa odgrywają również ważną rolę w unijnej rezerwie cyberbezpieczeństwa, której stopniowe tworzenie wspierają przepisy rozporządzenia (UE) …/… [rozporządzenie ustanawiające środki

mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty]. Unijna rezerwa cyberbezpieczeństwa ma być wykorzystywana do wspierania działań w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego przywracania normalnego działania po wystąpieniu tych incydentów. W rozporządzeniu (UE) …/… [rozporządzenie ustanawiające środki mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty] określono proces wyboru dostawców tworzących unijną rezerwę cyberbezpieczeństwa, w którym należy uwzględnić między innymi, czy dany dostawca uzyskał europejski lub krajowy certyfikat cyberbezpieczeństwa. ***Odpowiednie usługi świadczone przez „zaufanych dostawców" zgodnie z rozporządzeniem (UE) …./….. [rozporządzenie ustanawiające środki mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty] odpowiadają „usługom zarządzanym*** w zakresie ***bezpieczeństwa" określonym w niniejszym rozporządzeniu***.	mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty]. Unijna rezerwa cyberbezpieczeństwa ma być wykorzystywana do wspierania działań w zakresie reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz natychmiastowego przywracania normalnego działania po wystąpieniu tych incydentów. W rozporządzeniu (UE) …/… [rozporządzenie ustanawiające środki mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty] określono proces wyboru ***zaufanych*** dostawców ***usług zarządzanych w zakresie bezpieczeństwa*** tworzących unijną rezerwę cyberbezpieczeństwa, w którym należy uwzględnić między innymi, czy dany dostawca uzyskał europejski lub krajowy certyfikat cyberbezpieczeństwa. ***Ponadto po wprowadzeniu europejskiego systemu certyfikacji cyberbezpieczeństwa dla usług zarządzanych w zakresie bezpieczeństwa, który zastąpiłby również wszystkie odnośne krajowe systemy certyfikacji cyberbezpieczeństwa, należy zastosować obowiązkową certyfikację zgodnie z tym systemem certyfikacji, aby włączyć zaufanych dostawców usług zarządzanych*** w zakresie ***bezpieczeństwa do unijnej rezerwy cyberbezpieczeństwa***.

Or. en

Poprawka 20
Johan Nissinen

Wniosek dotyczący rozporządzenia
Motyw 4

Tekst proponowany przez Komisję	*Poprawka*
(4) Certyfikacja usług zarządzanych w zakresie bezpieczeństwa jest istotna nie tylko z punktu widzenia procesu wyboru dostawców do unijnej rezerwy cyberbezpieczeństwa, ale stanowi również podstawowy wyznacznik jakości dla podmiotów prywatnych i publicznych, które zamierzają nabyć takie usługi. W kontekście kluczowego znaczenia usług zarządzanych w zakresie bezpieczeństwa oraz wrażliwości danych przetwarzanych w ramach tych usług certyfikacja mogłaby zapewnić potencjalnym klientom istotne wskazówki i pewność co do wiarygodności tych usług. Europejskie programy certyfikacji dotyczące usług zarządzanych w zakresie bezpieczeństwa przyczyniają się do uniknięcia rozdrobnienia jednolitego rynku. Niniejsze rozporządzenie ma zatem na celu usprawnienie funkcjonowania rynku wewnętrznego.	(4) Certyfikacja usług zarządzanych w zakresie bezpieczeństwa jest istotna nie tylko z punktu widzenia procesu wyboru dostawców do unijnej rezerwy cyberbezpieczeństwa, ale stanowi również podstawowy wyznacznik jakości dla podmiotów prywatnych i publicznych, które zamierzają nabyć takie usługi. W kontekście kluczowego znaczenia usług zarządzanych w zakresie bezpieczeństwa oraz wrażliwości danych przetwarzanych w ramach tych usług certyfikacja mogłaby zapewnić potencjalnym klientom istotne wskazówki i pewność co do wiarygodności tych usług. Europejskie programy certyfikacji dotyczące usług zarządzanych w zakresie bezpieczeństwa przyczyniają się do uniknięcia rozdrobnienia jednolitego rynku. Niniejsze rozporządzenie ma zatem na celu usprawnienie funkcjonowania rynku wewnętrznego. ***Jednocześnie należy zapewnić równowagę między tymi wielorakimi celami rozporządzenia a możliwymi obciążeniami regulacyjnymi i kosztami związanymi z certyfikacją, biorąc pod uwagę, że przestrzeganie wymogów certyfikacyjnych będzie wiązało się z dodatkowymi wydatkami i wysiłkami administracyjnymi, co może stanowić problem dla mniejszych podmiotów.***

Or. en

Poprawka 21
Ville Niinistö
w imieniu grupy Verts/ALE

Wniosek dotyczący rozporządzenia
Motyw 4 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4a) Rynek i systemy edukacyjne oferują różnorodne zasoby edukacyjne i szkolenia formalne, dlatego należy podkreślić, że wiedzę uzyskuje się również w sposób pozaformalny, a umiejętności można wykazać nie tylko za pomocą dyplomów i świadectw. W szczególności w obecnym szybko ewoluującym krajobrazie zagrożeń państwa członkowskie i beneficjenci zarządzanych usług w zakresie bezpieczeństwa powinni liczyć się z wysoko wykwalifikowanymi naukowcami zajmującymi się kwestią podatności. Podmioty oraz osoby fizyczne i prawne wyszukujące podatności mogą w niektórych państwach członkowskich być narażone na odpowiedzialność karną i cywilną, zachęca się zatem państwa członkowskie do wydania wytycznych dotyczących nieścigania badań nad bezpieczeństwem informacji oraz zwolnienia z odpowiedzialności cywilnej za te działania.

Or. en

Uzasadnienie

Środowisko osób zajmujących się zawodowo bezpieczeństwem różni się częściowo ze względu na różne niestandardowe ścieżki kariery, dostęp do kształcenia formalnego i zasoby służących uzyskaniu certyfikatu. W związku z tym musimy zachęcać do zatrudniania wykwalifikowanych osób i zapewnić pozytywne ramy działań skutkujących poprawą cyberbezpieczeństwa.

Poprawka 22
Josianne Cutajar

Wniosek dotyczący rozporządzenia
Motyw 4 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4a) Unijny system certyfikacji usług zarządzanych w zakresie bezpieczeństwa powinien zapewniać dostępność

bezpiecznych i wysokiej jakości usług, które gwarantują bezpieczną transformację cyfrową i przyczyniają się do osiągnięcia celów określonych w programie polityki „Droga ku cyfrowej dekadzie”[8a], w szczególności w odniesieniu do celu, by 75 % przedsiębiorstw unijnych zaczęło korzystać z chmury obliczeniowej / AI / dużych zbiorów danych, by ponad 90 % MŚP osiągnęło co najmniej podstawowy poziom intensywności wykorzystania technologii cyfrowych oraz by kluczowe usługi publiczne były oferowane online.

[8a] Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie” do 2030 r.

Or. en

Poprawka 23
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 4 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(4a) Europejskie systemy certyfikacji usług zarządzanych w zakresie bezpieczeństwa powinny ułatwiać korzystanie z tych usług, zwłaszcza przez mniejsze podmioty, w tym organy lokalne i regionalne lub MŚP, które często nie mają zdolności finansowych ani kadrowych, by świadczyć te usługi samodzielnie, ale są narażone na cyberataki o potencjalnie dalekosiężnych skutkach.

Or. en

Poprawka 24
Josianne Cutajar

Wniosek dotyczący rozporządzenia
Motyw 5

Tekst proponowany przez Komisję	*Poprawka*
(5) Poza wdrażaniem produktów ICT, usług ICT lub procesów ICT usługi zarządzane w zakresie bezpieczeństwa często zapewniają dodatkowe funkcje usługowe, które opierają się na kompetencjach, wiedzy fachowej i doświadczeniu personelu. Bardzo wysoki poziom kompetencji, wiedzy fachowej i doświadczenia, a także odpowiednie procedury wewnętrzne powinny wchodzić w zakres celów bezpieczeństwa, aby zapewnić bardzo wysoką jakość świadczonych usług zarządzanych w zakresie bezpieczeństwa. W celu zapewnienia, aby wszystkie aspekty usług zarządzanych w zakresie bezpieczeństwa mogły być objęte programem certyfikacji, konieczna jest zatem zmiana rozporządzenia (UE) 2019/881. Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu [DD/MM/RRRR] r.	(5) Poza wdrażaniem produktów ICT, usług ICT lub procesów ICT usługi zarządzane w zakresie bezpieczeństwa często zapewniają dodatkowe funkcje usługowe, które opierają się na kompetencjach, wiedzy fachowej i doświadczeniu personelu. Bardzo wysoki poziom kompetencji, wiedzy fachowej i doświadczenia, a także odpowiednie procedury wewnętrzne powinny wchodzić w zakres celów bezpieczeństwa, aby zapewnić bardzo wysoką jakość świadczonych usług zarządzanych w zakresie bezpieczeństwa. W celu zapewnienia, aby wszystkie aspekty usług zarządzanych w zakresie bezpieczeństwa mogły być objęte programem certyfikacji, konieczna jest zatem zmiana rozporządzenia (UE) 2019/881. ***System certyfikacji ustanowiony na mocy niniejszego rozporządzenia powinien również uwzględniać wyniki i zalecenia oceny i przeglądu przewidzianych w jego art. 67.*** Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu [DD/MM/RRRR] r.

Or. en

Poprawka 25
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 5

Tekst proponowany przez Komisję	*Poprawka*
(5) Poza wdrażaniem produktów ICT, usług ICT lub procesów ICT usługi zarządzane w zakresie bezpieczeństwa często zapewniają dodatkowe funkcje usługowe, które opierają się na kompetencjach, wiedzy fachowej i doświadczeniu personelu. Bardzo wysoki poziom kompetencji, wiedzy fachowej i doświadczenia, a także odpowiednie procedury wewnętrzne powinny wchodzić w zakres celów bezpieczeństwa, aby zapewnić bardzo wysoką jakość świadczonych usług zarządzanych w zakresie bezpieczeństwa. W celu zapewnienia, aby wszystkie aspekty usług zarządzanych w zakresie bezpieczeństwa mogły być objęte programem certyfikacji, konieczna jest zatem zmiana rozporządzenia (UE) 2019/881. Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu [DD/MM/RRRR] r.	(5) Poza wdrażaniem produktów ICT, usług ICT lub procesów ICT usługi zarządzane w zakresie bezpieczeństwa często zapewniają dodatkowe funkcje usługowe, które opierają się na kompetencjach, wiedzy fachowej i doświadczeniu personelu. Bardzo wysoki poziom kompetencji, wiedzy fachowej i doświadczenia, a także odpowiednie procedury wewnętrzne powinny wchodzić w zakres celów bezpieczeństwa, aby zapewnić bardzo wysoką jakość ***i niezawodności*** świadczonych usług zarządzanych w zakresie bezpieczeństwa. W celu zapewnienia, aby wszystkie aspekty usług zarządzanych w zakresie bezpieczeństwa mogły być objęte programem certyfikacji, konieczna jest zatem zmiana rozporządzenia (UE) 2019/881. Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu [DD/MM/RRRR] r.

Or. en

Poprawka 26
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Motyw 5

Tekst proponowany przez Komisję	*Poprawka*
(5) Poza wdrażaniem produktów ICT, usług ICT lub procesów ICT usługi zarządzane w zakresie bezpieczeństwa często zapewniają dodatkowe funkcje usługowe, które opierają się na kompetencjach, wiedzy fachowej i doświadczeniu personelu. Bardzo wysoki poziom kompetencji, wiedzy fachowej	(5) Poza wdrażaniem produktów ICT, usług ICT lub procesów ICT usługi zarządzane w zakresie bezpieczeństwa często zapewniają dodatkowe funkcje usługowe, które opierają się na kompetencjach, wiedzy fachowej i doświadczeniu personelu. Bardzo wysoki poziom kompetencji, wiedzy fachowej

i doświadczenia, a także odpowiednie procedury wewnętrzne powinny wchodzić w zakres celów bezpieczeństwa, aby zapewnić bardzo wysoką jakość świadczonych usług zarządzanych w zakresie bezpieczeństwa. W celu zapewnienia, aby wszystkie aspekty usług zarządzanych w zakresie bezpieczeństwa mogły być objęte programem certyfikacji, konieczna jest zatem zmiana rozporządzenia (UE) 2019/881. Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu [DD/MM/RRRR] r.	i doświadczenia, a także odpowiednie procedury wewnętrzne powinny wchodzić w zakres celów bezpieczeństwa, aby zapewnić bardzo wysoką jakość świadczonych usług zarządzanych w zakresie bezpieczeństwa. W celu zapewnienia, aby wszystkie aspekty usług zarządzanych w zakresie bezpieczeństwa mogły być objęte ***specjalnym*** programem certyfikacji, konieczna jest zatem zmiana rozporządzenia (UE) 2019/881. Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu [DD/MM/RRRR] r.

Or. en

Poprawka 27
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Motyw 5 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(5a) Biorąc pod uwagę, że europejskie programy cyberbezpieczeństwa powinny potwierdzać, że usługi zarządzane w zakresie bezpieczeństwa są świadczone przez wysoko wykwalifikowany personel, który jest w stanie rzetelnie świadczyć te usługi zgodnie z najwyższymi standardami cyberbezpieczeństwa, należy zapewnić w Unii wystarczającą dostępność wysoko wykwalifikowanych pracowników. Unia stoi jednak w obliczu niedoboru talentów, charakteryzującego się brakiem wykwalifikowanych specjalistów, a jednocześnie musi stawić czoła szybko zmieniającemu się krajobrazowi zagrożeń, co potwierdzono w komunikacie Komisji z 18 kwietnia 2023 r. w sprawie Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa. Ważne jest, aby

zlikwidować ten niedobór dzięki zacieśnieniu współpracy i koordynacji między poszczególnymi zainteresowanymi stronami, w tym sektorem prywatnym, środowiskiem akademickim, państwami członkowskimi, Komisją i ENISA, aby zwiększyć skalę i stworzyć synergie na potrzeby inwestycji w kształcenie i szkolenie, rozwój partnerstw publiczno-prywatnych, wspieranie inicjatyw w zakresie badań naukowych i innowacji, opracowywanie i wzajemne uznawanie wspólnych norm oraz certyfikację umiejętności w dziedzinie cyberbezpieczeństwa, w tym za pośrednictwem europejskich ram umiejętności w dziedzinie cyberbezpieczeństwa. Powinno to również ułatwić mobilność specjalistów w dziedzinie cyberbezpieczeństwa w Unii.

Or. en

Poprawka 28
Johan Nissinen

Wniosek dotyczący rozporządzenia
Motyw 5 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(5a) Biorąc pod uwagę, że systemy certyfikacji zwiększą złożoność i tak już kompleksowego otoczenia regulacyjnego, niezwykle ważne jest, by zapobiegać ewentualnemu pokrywaniu się istniejących przepisów i norm w dziedzinie cyberbezpieczeństwa lub sprzecznościom między nimi. Podkreśla ponadto potrzebę starannej analizy i proporcjonalności podczas wdrażania rozporządzenia, aby ograniczyć negatywne skutki dla wolności rynkowej i innowacji.

Or. en

Poprawka 29
Josianne Cutajar

Wniosek dotyczący rozporządzenia
Motyw 5 a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	(5a) Należy rozważyć odpowiednie finansowanie i zasoby, aby umożliwić ENISA wykonywanie dodatkowych zadań powierzonych agencji na mocy niniejszego aktu.

Or. en

Poprawka 30
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 2 – litera a – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
a) pkt 9, 10 i 11 otrzymują brzmienie:	a) pkt ***7,*** 9, 10 i 11 otrzymują brzmienie:

Or. en

Poprawka 31
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 2 – litera a
Rozporządzenie (UE) 2019/881
Article 2 – punkt 7

Tekst proponowany przez Komisję	*Poprawka*
	7) „postępowanie w przypadku incydentu" oznacza postępowanie w przypadku incydentu zgodne z definicją w art. 6 pkt 8 dyrektywy (UE) 2022/2555;

Or. en

Poprawka 32
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 2 – litera b – wprowadzenie

Tekst proponowany przez Komisję	*Poprawka*
b) dodaje się ***punkt*** w brzmieniu:	b) dodaje się ***punkty*** w brzmieniu:

Or. en

Poprawka 33
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 2 – litera b
Rozporządzenie (UE) 2019/881
Article 2 – punkt 7a

Tekst proponowany przez Komisję	*Poprawka*
	7a) „ryzyko” oznacza ryzyko zdefiniowane w art. 6 pkt 9 dyrektywy (UE) 2022/2555.

Or. en

Poprawka 34
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 2 – litera b
Rozporządzenie (UE) 2019/881
Article 2 – punkt 14a

Tekst proponowany przez Komisję	*Poprawka*
14a) „usługa zarządzana w zakresie bezpieczeństwa” oznacza usługę ***polegającą na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem***	14a) „usługa zarządzana w zakresie bezpieczeństwa” oznacza usługę ***zarządzaną*** w ***zakresie bezpieczeństwa w rozumieniu art. 6 pkt 40 dyrektywy (UE) 2022/2555***;

w ***cyberprzestrzeni, takich jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo***;

Or. en

Poprawka 35
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 2 – litera b
Rozporządzenie (UE) 2019/881
Article 2 – punkt 14a

Tekst proponowany przez Komisję	*Poprawka*
14a) „usługa zarządzana w zakresie bezpieczeństwa" oznacza usługę polegającą na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, takich jak ***reagowanie na incydenty***, ***testy penetracyjne***, ***audyty bezpieczeństwa i doradztwo***;	14a) „usługa zarządzana w zakresie bezpieczeństwa" oznacza usługę ***zarządzaną*** polegającą na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, takich jak ***zapobieganie incydentom***, ***ich wykrywanie***, ***reagowanie na nie lub usuwanie ich skutków***;

Or. en

Poprawka 36
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 2 – litera b
Rozporządzenie (UE) 2019/881
Article 2 – punkt 14aa

Tekst proponowany przez Komisję	*Poprawka*
	14aa) „dostawca usług zarządzanych w zakresie bezpieczeństwa" oznacza dostawcę usług zarządzanych w zakresie bezpieczeństwa zdefiniowanego w art. 6 pkt 40 dyrektywy (UE) 2022/2555;

Or. en

Poprawka 37
Ville Niinistö
w imieniu grupy Verts/ALE

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 6
Rozporządzenie (UE) 2019/881
Article 47 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Unijny kroczący program prac zawiera w szczególności wykaz produktów ICT, usług ICT i procesów ICT lub ich kategorii oraz usług zarządzanych w zakresie bezpieczeństwa, które mają możliwość korzystania z włączenia w zakres stosowania danego europejskiego programu certyfikacji cyberbezpieczeństwa.	2. Unijny kroczący program prac zawiera w szczególności wykaz produktów ICT, usług ICT i procesów ICT lub ich kategorii oraz usług zarządzanych w zakresie bezpieczeństwa, które mają możliwość korzystania z włączenia w zakres stosowania danego europejskiego programu certyfikacji cyberbezpieczeństwa. ***Należy uwzględnić środki wsparcia służące ocenie zapotrzebowania na wykwalifikowanych pracowników, rodzajów umiejętności i istniejących ścieżek szkoleniowych, a także środki służące usunięciu wszelkich stwierdzonych braków.***

Or. en

Uzasadnienie

Procesowi identyfikacji produktów, usług i procesów ICT lub ich kategorii oraz usług zarządzanych w zakresie bezpieczeństwa musi towarzyszyć ocena umiejętności i środki służące usunięciu braków.

Poprawka 38
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 6
Rozporządzenie (UE) 2019/881
Article 47 – ustęp 3 – litera a

Tekst proponowany przez Komisję	*Poprawka*
a) obecność i rozwój krajowych programów certyfikacji cyberbezpieczeństwa obejmujących określoną kategorię produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, w szczególności w odniesieniu do ryzyka rozdrobnienia;	a) obecność i rozwój krajowych programów certyfikacji cyberbezpieczeństwa ***oraz norm międzynarodowych i branżowych*** obejmujących określoną kategorię produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, w szczególności w odniesieniu do ryzyka rozdrobnienia;

Or. en

Uzasadnienie

W unijnym kroczącym programie prac należy ocenić nie tylko rozwój systemów krajowych, lecz również normy branżowe i międzynarodowe.

Poprawka 39
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 7
Rozporządzenie (UE) 2019/881
Article 49 – ustęp 7

Tekst proponowany przez Komisję	*Poprawka*
7) art. 49 ust. 7 otrzymuje brzmienie:	***skreślony***
7. Komisja, w oparciu o propozycję programu przygotowaną przez ENISA, może przyjmować akty wykonawcze ustanawiające europejski program certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa spełniający wymogi określone w art. 51, 52 i 54. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 66 ust. 2.;	

Or. en

Poprawka 40
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 7
Rozporządzenie (UE) 2019/881
Article 49 – ustęp 7

Tekst proponowany przez Komisję	*Poprawka*
7. Komisja, w oparciu o propozycję programu przygotowaną przez ENISA, może przyjmować akty ***wykonawcze*** ustanawiające europejski program certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa spełniający wymogi określone w art. 51, 52 i 54. ***Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 66 ust. 2.;***	7. Komisja, w oparciu o propozycję programu przygotowaną przez ENISA, może przyjmować akty ***delegowane*** ustanawiające europejski program certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa spełniający wymogi określone w art. 51, 52 i 54. *(Zmiana dotyczy całości tekstu. Jej przyjęcie będzie wymagać zmian technicznych w całym tekście.)*

Or. en

Poprawka 41
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 7
Rozporządzenie (UE) 2019/881
Article 49 – ustęp 7a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	7a. Przed przyjęciem takich aktów delegowanych Komisja, we współpracy z ENISA, przeprowadza i publikuje ocenę skutków proponowanego europejskiego programu certyfikacji

cyberbezpieczeństwa. Przygotowując ocenę skutków, Komisja przeprowadza konsultacje publiczne oraz konsultuje się z Grupą Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa i Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa.

Or. en

Poprawka 42
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 7 a (nowy)
Rozporządzenie (UE) 2019/881
Article 49 – ustęp 7a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	7a) dodaje się ustęp w brzmieniu:
	„7a. Komisja, w oparciu o propozycję programu przygotowaną przez ENISA, może przyjmować akty delegowane ustanawiające europejski program certyfikacji cyberbezpieczeństwa usług zarządzanych w zakresie bezpieczeństwa spełniający wymogi określone w art. 51, 52 i 54. Te akty delegowane przyjmuje się zgodnie z procedurą, o której mowa w art. 66a.";

Or. en

Poprawka 43
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 9
Rozporządzenie (UE) 2019/881
Article 51a – ustęp 1 – litera b

Tekst proponowany przez Komisję	*Poprawka*
b) zapewniać, aby dostawca stosował odpowiednie procedury wewnętrzne w celu zagwarantowania, że usługi zarządzane w zakresie bezpieczeństwa są zawsze świadczone przy zachowaniu bardzo wysokiego poziomu jakości;	b) zapewniać, aby dostawca stosował odpowiednie procedury wewnętrzne w celu zagwarantowania, że usługi zarządzane w zakresie bezpieczeństwa są zawsze świadczone przy zachowaniu bardzo wysokiego poziomu jakości ***i niezawodności***;

Or. en

Poprawka 44
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 9
Rozporządzenie (UE) 2019/881
Article 51a – ustęp 1 – litera g

Tekst proponowany przez Komisję	*Poprawka*
g) zapewniać, aby produkty ICT, usługi ICT i procesy ICT [oraz sprzęt komputerowy] wdrażane w ramach świadczenia usług zarządzanych w zakresie bezpieczeństwa były bezpieczne zgodnie z zasadą, która stanowi, że kwestie bezpieczeństwa uwzględnia się domyślnie i już na etapie projektowania, oraz aby te produkty, usługi i procesy [oraz sprzęt komputerowy] nie zawierały znanych podatności i obejmowały najnowsze aktualizacje zabezpieczeń.;	g) zapewniać, aby produkty ICT, usługi ICT i procesy ICT [oraz sprzęt komputerowy] wdrażane w ramach świadczenia usług zarządzanych w zakresie bezpieczeństwa były bezpieczne zgodnie z zasadą, która stanowi, że kwestie bezpieczeństwa uwzględnia się domyślnie i już na etapie projektowania, ***aby były oferowane wraz z aktualnym oprogramowaniem i sprzętem*** oraz aby te produkty, usługi i procesy [oraz sprzęt komputerowy] nie zawierały znanych podatności i obejmowały najnowsze aktualizacje zabezpieczeń.***"***;

Or. en

Poprawka 45
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 9
Rozporządzenie (UE) 2019/881
Article 51a – ustęp 1 – litera g

Tekst proponowany przez Komisję	*Poprawka*
g) zapewniać, aby produkty ICT, usługi ICT i procesy ICT ***[oraz sprzęt komputerowy]*** wdrażane w ramach świadczenia usług zarządzanych w zakresie bezpieczeństwa były bezpieczne zgodnie z zasadą, która stanowi, że kwestie bezpieczeństwa uwzględnia się domyślnie i już na etapie projektowania, oraz aby te produkty, usługi i procesy [oraz sprzęt komputerowy] nie zawierały znanych podatności i obejmowały najnowsze aktualizacje zabezpieczeń.;	g) zapewniać, aby produkty ICT, usługi ICT i procesy ICT wdrażane w ramach świadczenia usług zarządzanych w zakresie bezpieczeństwa były bezpieczne zgodnie z zasadą, która stanowi, że kwestie bezpieczeństwa uwzględnia się domyślnie i już na etapie projektowania, oraz aby te produkty, usługi i procesy [oraz sprzęt komputerowy] nie zawierały znanych podatności i obejmowały najnowsze aktualizacje zabezpieczeń.***”***;

Or. en

Poprawka 46
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 13 – litera b – podpunkt ii – litera aa
Rozporządzenie (UE) 2019/881
Article 56 – ustęp 3 – akapit trzeci– litera a

Tekst proponowany przez Komisję	*Poprawka*
a) bierze pod uwagę wpływ danych środków na wytwórców lub dostawców takich produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa oraz na użytkowników pod względem kosztów tych środków oraz korzyści społecznych lub gospodarczych wynikających z przewidywanego zwiększonego poziomu bezpieczeństwa wskazanych produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa;	a) bierze pod uwagę wpływ danych środków na wytwórców lub dostawców takich produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa oraz na użytkowników pod względem kosztów tych środków oraz korzyści społecznych lub gospodarczych wynikających z przewidywanego zwiększonego poziomu bezpieczeństwa wskazanych produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa***, w tym na MŚP; Komisja zapewnia MŚP***

dostęp do odpowiedniego wsparcia finansowego w związku z wdrażaniem tych środków za pośrednictwem już istniejących programów unijnych;

Or. en

Poprawka 47
Bart Groothuis, Alin Mituța, Ivars Ijabs, Andrus Ansip, Morten Løkkegaard, Nicola Danti

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 14
Rozporządzenie (UE) 2019/881
Article 57 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
1. Bez uszczerbku dla ust. 3 niniejszego artykułu krajowe programy certyfikacji cyberbezpieczeństwa i powiązane z nimi procedury dotyczące produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa, które są objęte europejskim programem certyfikacji cyberbezpieczeństwa przestają być skuteczne z dniem określonym w akcie ***wykonawczym przyjętym na podstawie art. 49 ust. 7***. Krajowe programy certyfikacji cyberbezpieczeństwa i powiązane z nimi procedury dotyczące produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa, które nie są objęte europejskim programem certyfikacji cyberbezpieczeństwa, funkcjonują nadal.	1. Bez uszczerbku dla ust. 3 niniejszego artykułu krajowe programy certyfikacji cyberbezpieczeństwa i powiązane z nimi procedury dotyczące produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa, które są objęte europejskim programem certyfikacji cyberbezpieczeństwa przestają być skuteczne z dniem określonym w akcie ***delegowanym***. Krajowe programy certyfikacji cyberbezpieczeństwa i powiązane z nimi procedury dotyczące produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa, które nie są objęte europejskim programem certyfikacji cyberbezpieczeństwa, funkcjonują nadal. *(Zmiana dotyczy całości tekstu. Jej przyjęcie będzie wymagać zmian technicznych w całym tekście.)*

Or. en

Uzasadnienie

Zmiana odzwierciedla poprawkę do art. 49.

Poprawka 48
Angelika Niebler, Pilar del Castillo Vera, Tomas Tobé, Maria da Graça Carvalho, Sara Skyttedal, Ivan Štefanec, Cristian-Silviu Buşoi, Ioan-Rareş Bogdan

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 16 a (nowy)
Rozporządzenie (UE) 2019/881
Article 66a (nowy)

Tekst proponowany przez Komisję	*Poprawka*
	16a) dodaje się artykuł w brzmieniu:
	Article 66a (nowy)
	Wykonywanie przekazanych uprawnień
	1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.
	2. Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 49 ust. 7a, powierza się Komisji na okres pięciu lat od dnia … [data wejścia w życie podstawowego aktu ustawodawczego lub każda inna data ustalona przez współprawodawców]. Komisja sporządza sprawozdanie dotyczące przekazania uprawnień nie później niż dziewięć miesięcy przed końcem okresu pięciu lat. Przekazanie uprawnień zostaje automatycznie przedłużone na takie same okresy, chyba że Parlament Europejski lub Rada sprzeciwią się takiemu przedłużeniu nie później niż trzy miesiące przed końcem każdego okresu.
	3. Przekazanie uprawnień, o którym mowa w art. 49 ust. 7a, 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 następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność

jakichkolwiek już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 49 ust. 7a 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.

Or. en

Poprawka 49
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 17 – wprowadzenie
Rozporządzenie (UE) 2019/881
Article 67

Tekst proponowany przez Komisję	*Poprawka*
17) art. 67 ust. 2 ***i*** 3 otrzymują brzmienie:	17) art. 67 ust. ***1,*** 2***,*** 3 ***i 4*** otrzymuje brzmienie:

Or. en

Poprawka 50
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 17
Rozporządzenie (UE) 2019/881
Article 67 – ustęp 1

Tekst proponowany przez Komisję	*Poprawka*
	1 Do 28 czerwca 2024 r., a następnie co cztery lata, Komisja ocenia wpływ, skuteczność i efektywność ENISA oraz jej metod pracy, ewentualną potrzebę zmiany mandatu ENISA oraz skutki finansowe wszelkich takich zmian. W ocenie tej uwzględnia się wszelkie informacje zwrotne przekazane ENISA w odpowiedzi na jej działalność. Jeżeli Komisja uzna, że dalsze działanie ENISA w kontekście powierzonych jej celów, mandatu i zadań nie jest już uzasadnione, może wystąpić z wnioskiem o zmianę niniejszego rozporządzenia w zakresie przepisów dotyczących ENISA.

Or. en

Poprawka 51
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 17
Rozporządzenie (UE) 2019/881
Article 67 – ustęp 2

Tekst proponowany przez Komisję	*Poprawka*
2. Ocena dotyczy również wpływu, skuteczności i efektywności przepisów tytułu III niniejszego rozporządzenia w odniesieniu do celów, którymi są zapewnienie odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa w Unii oraz poprawa funkcjonowania	2. Ocena dotyczy również wpływu, skuteczności i efektywności przepisów tytułu III niniejszego rozporządzenia w odniesieniu do celów, którymi są zapewnienie odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa w Unii oraz poprawa funkcjonowania

rynku wewnętrznego.	rynku wewnętrznego***, i obejmuje również ocenę procedury i harmonogramów prowadzących do przygotowania i przyjęcia pierwszych europejskich systemów certyfikacji cyberbezpieczeństwa oraz sposobów usprawnienia i przyspieszenia tej procedury w odniesieniu do kolejnych systemów certyfikacji***.

Or. en

Poprawka 52
Evžen Tošenovský

Wniosek dotyczący rozporządzenia
Artykuł 1 – akapit 1 – punkt 17
Rozporządzenie (UE) 2019/881
Article 67 – ustęp 4

Tekst proponowany przez Komisję	*Poprawka*
	4. Do 28 czerwca 2024 r., a następnie co cztery lata, Komisja przekazuje sprawozdanie z oceny wraz z wnioskami Parlamentowi Europejskiemu, Radzie i Zarządowi. Ustalenia zawarte w tym sprawozdaniu podaje się do wiadomości publicznej. Sprawozdaniu towarzyszy w razie potrzeby wniosek ustawodawczy.

Or. en