Parlament Europejski
2019-2024

Dokument z posiedzenia

A9-0307/2023

26.10.2023

***I
SPRAWOZDANIE

w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Komisja Przemysłu, Badań Naukowych i Energii

Sprawozdawczyni: Josianne Cutajar

Objaśnienie używanych znaków

*	Procedura konsultacji
***	Procedura zgody
***I	Zwykła procedura ustawodawcza (pierwsze czytanie)
***II	Zwykła procedura ustawodawcza (drugie czytanie)
***III	Zwykła procedura ustawodawcza (trzecie czytanie)

(Wskazana procedura opiera się na podstawie prawnej zaproponowanej w projekcie aktu)

Poprawki do projektu aktu

Poprawki Parlamentu w postaci dwóch kolumn

Skreślenia zaznacza się ***wytłuszczonym drukiem i kursywą*** w lewej kolumnie. Zmianę brzmienia zaznacza się ***wytłuszczonym drukiem i kursywą*** w obu kolumnach. Nowy tekst zaznacza się ***wytłuszczonym drukiem i kursywą*** w prawej kolumnie.

Pierwszy i drugi wiersz nagłówka każdej poprawki wskazuje element rozpatrywanego projektu aktu, którego dotyczy poprawka. Jeżeli poprawka odnosi się do obowiązującego aktu, do którego zmiany zmierza projekt aktu, nagłówek zawiera dodatkowo trzeci wiersz wskazujący obowiązujący akt i czwarty wiersz wskazujący przepis tego aktu, którego dotyczy poprawka.

Poprawki Parlamentu w postaci tekstu skonsolidowanego

Nowe fragmenty tekstu zaznacza się ***wytłuszczonym drukiem i kursywą***. Fragmenty tekstu, które zostały skreślone, zaznacza się za pomocą symbolu ▌ lub przekreśla. Zmianę brzmienia zaznacza się przez wyróżnienie nowego tekstu ***wytłuszczonym drukiem i kursywą*** i usunięcie lub przekreślenie zastąpionego tekstu.
Tytułem wyjątku nie zaznacza się zmian o charakterze ściśle technicznym wprowadzonych przez służby w celu opracowania końcowej wersji tekstu.

SPIS TREŚCI

Strona

PROJEKT REZOLUCJI USTAWODAWCZEJ PARLAMENTU EUROPEJSKIEGO

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

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

(Zwykła procedura ustawodawcza: pierwsze czytanie)

Parlament Europejski,

– uwzględniając wniosek Komisji przedstawiony Parlamentowi Europejskiemu i Radzie (COM(2023)0208),

– uwzględniając art. 294 ust. 2 i art. 114 Traktatu o funkcjonowaniu Unii Europejskiej, zgodnie z którymi wniosek został przedstawiony Parlamentowi przez Komisję (C9-0137/2023),

– uwzględniając art. 294 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej,

– uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego z 13 lipca 2023 r.[1],

– uwzględniając art. 59 Regulaminu,

– uwzględniając pismo przesłane przez Komisję Rynku Wewnętrznego i Ochrony Konsumentów,

– uwzględniając sprawozdanie Komisji Przemysłu, Badań Naukowych i Energii (A9-0307/2023),

1. przyjmuje poniższe stanowisko w pierwszym czytaniu;

2. zwraca się do Komisji o ponowne przekazanie mu sprawy, jeśli zastąpi ona pierwotny wniosek, wprowadzi w nim istotne zmiany lub planuje ich wprowadzenie;

3. zobowiązuje swoją przewodniczącą do przekazania stanowiska Parlamentu Radzie i Komisji oraz parlamentom narodowym.

[1] Dz.U. C 349 z 29.9.2023, s. 167.

Poprawka 1

POPRAWKI PARLAMENTU EUROPEJSKIEGO*

do wniosku Komisji

2023/0108 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

zmieniające rozporządzenie (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[1],

uwzględniając opinię Komitetu Regionów,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą[2],

---

* Poprawki: tekst nowy lub zmieniony został zaznaczony wytłuszczonym drukiem i kursywą; symbol ▌ sygnalizuje skreślenia.

1 ***Dz.U. C 349 z 29.9.2023, s. 167.***

2 ***Stanowisko Parlamentu Europejskiego z dnia … (dotychczas nieopublikowane w Dzienniku Urzędowym) i decyzja Rady z dnia …***

a także mając na uwadze, co następuje:

(1) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881[3] utworzono ramy ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa produktów ***z zakresu technologii informacyjno-komunikacyjnych (***ICT***)***, usług ICT i procesów ICT w Unii oraz w celu uniknięcia rozdrobnienia rynku wewnętrznego w zakresie programów certyfikacji cyberbezpieczeństwa w Unii.

(1a) Aby zapewnić odporność Unii na cyberataki i zapobiec wszelkim lukom na rynku unijnym, niniejsze rozporządzenie ma za zadanie uzupełnić horyzontalne ramy regulacyjne ustanawiające kompleksowe wymogi cyberbezpieczeństwa dla wszystkich produktów z elementami cyfrowymi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) .../...[4] (2022/0272(COD)), określając zasadnicze wymogi dotyczące usług zarządzanych w zakresie cyberbezpieczeństwa, ich stosowania i wiarygodności.

(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 wykrywania incydentów, reagowania na nie i usuwania ich skutków***. ***Działalność dostawców usług zarządzanych w zakresie bezpieczeństwa obejmuje usługi związane z prewencją, identyfikacją, ochroną, wykrywaniem, analizą, powstrzymywaniem, reagowaniem i przywracaniem gotowości do pracy, w tym m.in. analizę cyberzagrożeń, monitorowanie zagrożeń w czasie rzeczywistym za pomocą proaktywnych technik, w tym uwzględnianie bezpieczeństwa już w fazie projektowania, ocenę ryzyka, rozszerzone wykrywanie, remediację i reagowanie.*** W związku z tym dostawców takich usług uznaje się za podmioty kluczowe lub

---

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

[4] Rozporządzenie (UE) .../... Parlamentu Europejskiego i Rady z dnia ... w sprawie ... (Dz.U. ..., ELI: …).

ważne należące do sektora kluczowego na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555[5]. 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.

(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,

[5] 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).

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.

(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.

(4a) Europejskie systemy certyfikacji usług zarządzanych w zakresie bezpieczeństwa powinny prowadzić do upowszechnienia tych usług i zwiększenia konkurencji w tej dziedzinie, z uwzględnieniem szczególnych potrzeb zarówno dostawców, jak i beneficjentów. Systemy te powinny zatem zapewniać równowagę między ich celem a potencjalnym obciążeniem regulacyjnym, administracyjnym i finansowym, jakie mogą napotkać dostawcy, zwłaszcza mikroprzedsiębiorstwa lub małe i średnie przedsiębiorstwa (MŚP). Ponadto systemy te powinny zachęcać do korzystania z certyfikowanych usług zarządzanych w zakresie bezpieczeństwa, przyczyniając się do ich dostępności, zwłaszcza dla mniejszych podmiotów, takich jak mikroprzedsiębiorstwa i MŚP, a także organów lokalnych i regionalnych, które mają ograniczone zdolności i zasoby, ale które są bardziej narażone na naruszenia cyberbezpieczeństwa mające skutki finansowe, prawne, wizerunkowe i operacyjne.

(4b) 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", w szczególności w odniesieniu do celu, by 75 % przedsiębiorstw unijnych zaczęło korzystać z chmury obliczeniowej, sztucznej inteligencji i dużych zbiorów danych, by ponad 90 % mikroprzedsiębiorstw i MŚP osiągnęło co najmniej podstawowy poziom wykorzystania technologii cyfrowych oraz by kluczowe usługi publiczne były oferowane online.

(4c) W obecnym szybko zmieniającym się otoczeniu cyfrowym i technologicznym oferta zasobów edukacyjnych i formalnych szkoleń jest różna, a wiedzę można zdobywać na różne sposoby, zarówno formalnie, na przykład za pośrednictwem uniwersytetów lub kursów, jak i nieformalnie, na przykład poprzez szkolenia w miejscu pracy lub wieloletnie doświadczenie zawodowe w danej dziedzinie.

(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 ***specjalnym*** programem certyfikacji, konieczna jest zatem zmiana rozporządzenia (UE) 2019/881. ***Przy tworzeniu systemów certyfikacji ustanowionych na mocy niniejszego rozporządzenia należy uwzględniać wyniki ocen i przeglądów przewidzianych w niniejszym rozporządzeniu oraz zawarte w nich zalecenia.***

(5a) Aby ułatwić rozwój wiarygodnego rynku unijnego, a zarazem tworzenie partnerstw z państwami trzecimi o podobnych poglądach, w tym w świetle przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) .../...[6] (2023/0109(COD)) w odniesieniu do dostępu do unijnej rezerwy cyberbezpieczeństwa, należy usprawnić proces certyfikacji ustanowiony na mocy przepisów niniejszego rozporządzenia, tak

---

6 Rozporządzenie (UE) .../... Parlamentu Europejskiego i Rady z dnia ... w sprawie ... (Dz.U. ..., ELI: …).

by zapewnić międzynarodowe uznawanie i dostosowanie do norm międzynarodowych.

(5b) ***Aby zapewnić rozwój wiarygodnego unijnego rynku usług zarządzanych w zakresie bezpieczeństwa, dostawcy tych usług i państwa członkowskie powinny współpracować i przyczyniać się do gromadzenia danych na temat stanu i rozwoju rynku pracy w dziedzinie cyberbezpieczeństwa.***

(5c) ***Ogólnounijne skoordynowane podejście do wzmacniania odporności infrastruktury krytycznej opiera się na budowaniu zdolności państw członkowskich. Unia zmaga się jednak z niedoborem talentów, przejawiającym się brakiem wykwalifikowanych specjalistów, a jednocześnie musi stawić czoła szybko zmieniającemu się krajobrazowi zagrożeń, jak stwierdzono w komunikacie Komisji z 18 kwietnia 2023 r. w sprawie Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa. Dlatego aby ułatwić powstawanie wysokiej jakości podstawowych usług zarządzanych w zakresie bezpieczeństwa oraz lepiej zrozumieć, jakiego typu pracownicy zajmują się cyberbezpieczeństwem, należy wzmocnić współpracę między państwami członkowskimi, Komisją, ENISA i zainteresowanymi stronami, w tym sektorem prywatnym i środowiskiem akademickim, poprzez rozwój partnerstw publiczno-prywatnych, wspieranie inicjatyw w zakresie badań naukowych i innowacji, opracowywanie i wzajemne uznawanie wspólnych norm oraz certyfikację umiejętności w zakresie cyberbezpieczeństwa, w tym za pośrednictwem europejskich ram umiejętności w zakresie cyberbezpieczeństwa. Powinno to również ułatwić mobilność specjalistów z dziedziny cyberbezpieczeństwa w Unii oraz włączenie wiedzy i szkoleń na temat cyberbezpieczeństwa do programów nauczania, kształcenia i szkolenia, a także zapewnić dostępność praktyk i staży dla młodych ludzi, zwłaszcza osób mieszkających w regionach defaworyzowanych, takich jak wyspy, obszary słabo zaludnione, obszary wiejskie i obszary oddalone. Działania te powinny również mieć na celu przyciągnięcie większej liczby kobiet i dziewcząt do tej dziedziny oraz przyczynienie się do rozwiązania problemu różnic w traktowaniu kobiet i mężczyzn w dziedzinie nauk przyrodniczych, technologii, inżynierii i matematyki. Sektor prywatny powinien również zapewniać szkolenia w miejscu pracy w zakresie***

najbardziej potrzebnych umiejętności, przy udziale administracji publicznej i przedsiębiorstw typu start-up, a także mikroprzedsiębiorstw i MŚP.

(5d) Należy zapewnić odpowiednie finansowanie i zasoby na potrzeby dodatkowych zadań powierzonych ENISA na mocy zmian do rozporządzenia (UE) 2019/881 wprowadzonych niniejszym rozporządzeniem.

(5e) W celu uzupełnienia niektórych innych niż istotne elementów niniejszego rozporządzenia należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w celu opracowania europejskiego systemu certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa. 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[7]. W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach 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.

(5e) 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][8],

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

---

7 Dz.U. L 123 z 12.5.2016, s. 1.

8 ***Dz.U. C .../…***

Artykuł 1

Zmiany w rozporządzeniu (UE) 2019/881

W rozporządzeniu (UE) 2019/881 wprowadza się następujące zmiany:

1) art. 1 ust. 1 akapit pierwszy lit. b) otrzymuje brzmienie:

„b) ramy ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa w Unii oraz w celu uniknięcia rozdrobnienia rynku wewnętrznego w zakresie programów certyfikacji cyberbezpieczeństwa w Unii.”;

2) w art. 2 wprowadza się następujące zmiany:

a) pkt 9, 10 i 11 otrzymują brzmienie:

„9) »europejski program certyfikacji cyberbezpieczeństwa« oznacza kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur ustanowionych na poziomie unijnym i mających zastosowanie do certyfikacji lub oceny zgodności określonych produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa;

„10) »krajowy program certyfikacji cyberbezpieczeństwa« oznacza kompleksowy zbiór przepisów, wymogów technicznych, norm i procedur określonych i przyjętych przez krajowy organ publiczny, i mających zastosowanie do certyfikacji lub oceny zgodności objętych zakresem danego programu produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa;

11) »europejski certyfikat cyberbezpieczeństwa« oznacza wydany przez odpowiedni organ dokument poświadczający, że dany produkt ICT, daną usługa ICT, dany proces ICT lub daną usługę zarządzaną w zakresie bezpieczeństwa oceniono pod względem zgodności ze szczegółowymi wymogami bezpieczeństwa określonymi w europejskim programie certyfikacji cyberbezpieczeństwa;”;

b) dodaje się punkt w brzmieniu:

„14a) »usługa zarządzana w zakresie bezpieczeństwa« oznacza usługę ***świadczoną osobie trzeciej,*** polegającą na prowadzeniu***,*** wspomaganiu ***lub wspieraniu radą*** działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, takich jak ***postępowanie w przypadku incydentu***, testy penetracyjne, audyty bezpieczeństwa i doradztwo;";

c) pkt 20, 21 i 22 otrzymują brzmienie:

„20) »specyfikacja techniczna« oznacza dokument określający wymogi techniczne, które mają być spełnione przez produkt ICT, usługę ICT, proces ICT lub usługę zarządzaną w zakresie bezpieczeństwa lub procedury oceny zgodności w odniesieniu do produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa;

21) »poziom uzasadnienia zaufania« oznacza podstawę dla pewności, że dany produkt ICT, dana usługa ICT, dany proces ICT lub dana usługa zarządzana w zakresie bezpieczeństwa spełniają wymogi bezpieczeństwa określonego europejskiego programu certyfikacji cyberbezpieczeństwa, oraz wskazuje on poziom, na jakim została dokonana ocena danego produktu ICT, danej usługi ICT, danego procesu ICT lub danej usługi zarządzanej w zakresie bezpieczeństwa, ale sam nie mierzy bezpieczeństwa danego produktu ICT, danej usługi ICT, danego procesu ICT lub danej usługi zarządzanej w zakresie bezpieczeństwa;

22) »ocena zgodności przez stronę pierwszą« oznacza przeprowadzone przez wytwórcę lub dostawcę produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa czynności oceniające, czy te produkty ICT, usługi ICT, procesy ICT lub usługi zarządzane w zakresie bezpieczeństwa spełniają wymogi określonego europejskiego programu certyfikacji cyberbezpieczeństwa.";

3) art. 4 ust. 6 otrzymuje brzmienie:

„6. ENISA propaguje korzystanie z europejskiej certyfikacji cyberbezpieczeństwa z myślą o unikaniu rozdrobnienia rynku wewnętrznego. ENISA przyczynia się do utworzenia i utrzymywania europejskich ram certyfikacji cyberbezpieczeństwa zgodnie z tytułem III niniejszego rozporządzenia,

z myślą o zwiększeniu przejrzystości cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa, zwiększając w ten sposób zaufanie do wewnętrznego rynku cyfrowego i jego konkurencyjność.”;

4) w art. 8 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. ENISA wspiera i propaguje opracowywanie i realizację ustanowionej w tytule III niniejszego rozporządzenia polityki Unii w zakresie certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa poprzez:

a) monitorowanie na bieżąco zmian w powiązanych dziedzinach normalizacji i zalecanie odpowiednich specyfikacji technicznych do zastosowania przy tworzeniu europejskich programów certyfikacji cyberbezpieczeństwa zgodnie z art. 54 ust. 1 lit. c), w przypadkach gdy nie istnieją normy w danym zakresie;

b) przygotowywanie propozycji dotyczących europejskich programów certyfikacji cyberbezpieczeństwa (zwanych dalej »propozycjami programów«) dla produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa zgodnie z art. 49;

c) ocenianie przyjętych europejskich programów certyfikacji cyberbezpieczeństwa zgodnie z art. 49 ust. 8;

d) uczestniczenie we wzajemnych przeglądach na podstawie art. 59 ust. 4;

e) udzielanie pomocy Komisji przy zapewnianiu obsługi sekretariatu dla ECCG zgodnie z art. 62 ust. 5.”;

b) ust. 3 otrzymuje brzmienie:

„3. ENISA sporządza i publikuje wytyczne oraz opracowuje dobre praktyki dotyczące wymogów cyberbezpieczeństwa dotyczących produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa we współpracy z krajowymi organami ds. certyfikacji

cyberbezpieczeństwa oraz z przemysłem prowadzonej w formalny, ustrukturyzowany i przejrzysty sposób.”;

c) ust. 5 otrzymuje brzmienie:

„5. ENISA ułatwia ustanowienie i upowszechnianie europejskich i międzynarodowych norm dotyczących zarządzania ryzykiem oraz dotyczących bezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa.”;

5) art. 46 ust. 1 i 2 otrzymują brzmienie:

„1. Ustanawia się europejskie ramy certyfikacji cyberbezpieczeństwa w celu poprawy warunków funkcjonowania rynku wewnętrznego poprzez zwiększenie poziomu cyberbezpieczeństwa w Unii oraz umożliwienia zharmonizowanego podejścia na poziomie unijnym do europejskich programów certyfikacji cyberbezpieczeństwa z myślą o stworzeniu jednolitego rynku cyfrowego w zakresie produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa.

2. Europejskie ramy certyfikacji cyberbezpieczeństwa określają mechanizm ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa. Zapewniają poświadczenie, że produkty ICT, usługi ICT i procesy ICT, które oceniono zgodnie z tymi programami, spełniają określone wymogi bezpieczeństwa w celu ochrony dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych bądź funkcji lub usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia. Zapewniają ponadto poświadczenie, że usługi zarządzane w zakresie bezpieczeństwa, które oceniono zgodnie z tymi programami, spełniają określone wymogi bezpieczeństwa w celu ochrony dostępności, autentyczności, integralności i poufności danych, do których uzyskuje się dostęp i które są przetwarzane, przechowywane lub przekazywane w związku ze świadczeniem tych usług, oraz że usługi te są świadczone w sposób ciągły z zachowaniem wymaganych kompetencji, wiedzy specjalistycznej i doświadczenia przez personel o bardzo wysokim poziomie odpowiedniej wiedzy technicznej i uczciwości

zawodowej.”;

6) art. 47 ust. 2 i 3 otrzymują brzmienie:

„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. ***W tym kontekście Komisja może dołączyć dogłębną ocenę istniejących ścieżek szkolenia w celu zniwelowania stwierdzonych niedoborów kwalifikacji oraz listę propozycji dotyczących zaspokojenia zapotrzebowania na wykwalifikowanych pracowników i określone rodzaje umiejętności.***

3. Objęcie określonych produktów ICT, usług ICT i procesów ICT lub ich kategorii lub usług zarządzanych w zakresie bezpieczeństwa unijnym kroczącym programem prac musi być uzasadnione jedną z poniższych przesłanek:

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;

b) odpowiednie przepisy lub polityki Unii lub państwa członkowskiego;

c) popyt na rynku;

ca) zmiany technologiczne oraz dostępność i rozwój międzynarodowych programów certyfikacji cyberbezpieczeństwa oraz norm międzynarodowych i przemysłowych.

d) zmiany w zakresie profilu cyberzagrożeń;

e) wniosek ECCG o przygotowanie konkretnej propozycji programu.”;

7) ***w*** art. 49 ***wprowadza się następujące zmiany***:

a) ust. 7 otrzymuje brzmienie:

„7. Komisja, w oparciu o propozycję programu przygotowaną przez ENISA,

jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 65a, uzupełniających niniejsze rozporządzenie poprzez ustanowienie europejskiego programu certyfikacji cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa***, spełniającego*** wymogi określone w art. 51, 52 i 54.***";***

b) dodaje się ustęp w brzmieniu:

„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.";

8) w art. 51 wprowadza się następujące zmiany:

a) tytuł otrzymuje brzmienie:

„Cele bezpieczeństwa europejskich programów certyfikacji cyberbezpieczeństwa dotyczących produktów ICT, usług ICT i procesów ICT"

b) formuła wprowadzająca otrzymuje brzmienie:

„Europejski program certyfikacji cyberbezpieczeństwa dotyczący produktów ICT, usług ICT lub procesów ICT musi być zaprojektowany tak, aby – w stosownych przypadkach – osiągać co najmniej następujące cele bezpieczeństwa:";

9) dodaje się artykuł w brzmieniu:

„Artykuł 51a Cele bezpieczeństwa europejskich programów certyfikacji cyberbezpieczeństwa dotyczących usług zarządzanych w zakresie bezpieczeństwa

Europejski program certyfikacji cyberbezpieczeństwa dotyczący usług zarządzanych w zakresie bezpieczeństwa musi być zaprojektowany tak, aby – w stosownych przypadkach – osiągać co najmniej następujące cele bezpieczeństwa:

a) zapewniać, aby usługi zarządzane w zakresie bezpieczeństwa były świadczone z zachowaniem wymaganych kompetencji, wiedzy specjalistycznej i doświadczenia, w tym aby personel odpowiedzialny za świadczenie tych usług posiadał bardzo wysoki poziom wiedzy technicznej i kompetencji w danej dziedzinie oraz wystarczające i odpowiednie doświadczenie, a także wykazywał najwyższy poziom uczciwości zawodowej;

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;

c) chronić dane, do których uzyskano dostęp i które są przechowywane, przekazywane lub w inny sposób przetwarzane w związku ze świadczeniem usług zarządzanych w zakresie bezpieczeństwa, przed przypadkowym lub nieuprawnionym dostępem, przechowywaniem, ujawnieniem, zniszczeniem, innym rodzajem przetwarzania, utratą, zmianą lub brakiem dostępności;

d) zapewniać, aby dostępność danych, usług i funkcji oraz dostęp do nich przywracano w odpowiednio krótkim czasie w przypadku incydentu fizycznego lub technicznego;

e) zapewniać, aby uprawnione osoby, programy lub maszyny miały dostęp tylko do tych danych, usług lub funkcji, do których odnoszą się ich prawa dostępu;

f) rejestrować i umożliwiać ocenę, do których danych, usług lub funkcji uzyskano dostęp, które dane, usługi lub funkcje wykorzystano lub przetwarzano w inny sposób, kiedy to miało miejsce i kto tego dokonał;

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, ***aby były oferowane wraz z aktualnym oprogramowaniem i sprzętem*** oraz aby te produkty, usługi i procesy nie zawierały znanych podatności i obejmowały najnowsze aktualizacje zabezpieczeń.”;

10) w art. 52 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Europejski program certyfikacji cyberbezpieczeństwa może przewidywać co najmniej jeden z następujących poziomów uzasadnienia zaufania produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa: »podstawowy«, »istotny« lub »wysoki«. Poziom uzasadnienia zaufania musi być proporcjonalny do poziomu ryzyka związanego z przewidzianym stosowaniem produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa pod względem prawdopodobieństwa wystąpienia i skutków incydentu.”;

b) ust. 3 otrzymuje brzmienie:

„3. Wymogi bezpieczeństwa, które odpowiadają poszczególnym poziomom uzasadnienia zaufania, muszą być określone w odpowiednich europejskich programach certyfikacji cyberbezpieczeństwa, w tym odpowiadające im funkcjonalności bezpieczeństwa oraz odpowiadająca im rygorystyczność i wnikliwość oceny, której ma zostać poddany produkt ICT, usługa ICT, proces ICT lub usługa zarządzana w zakresie bezpieczeństwa.”;

c) ust. 5, 6 i 7 otrzymują brzmienie:

„5. Europejski certyfikat cyberbezpieczeństwa lub unijna deklaracja zgodności, które odnoszą się do poziomu uzasadnienia zaufania »podstawowy«, dają uzasadnione zaufanie, że produkty ICT, usługi ICT, procesy ICT i usługi zarządzane w zakresie bezpieczeństwa, dla których wydany został ten certyfikat lub wydana została ta unijna deklaracji zgodności, spełniają odpowiadające im wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych podstawowych ryzyk w zakresie incydentów i cyberataków. Działania w zakresie oceny, jakie mają zostać podjęte, obejmują przynajmniej przegląd dokumentacji technicznej. W przypadku gdy taki przegląd nie jest odpowiedni, podejmuje się alternatywne działania w zakresie oceny, które mają równoważny skutek.

6. Europejski certyfikat cyberbezpieczeństwa, który odnosi się do poziomu uzasadnienia zaufania »istotny«, daje uzasadnione zaufanie, że produkty ICT, usługi ICT, procesy ICT i usługi zarządzane w zakresie bezpieczeństwa, dla których wydany został ten certyfikat, spełniają odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie znanych ryzyk w cyberprzestrzeni oraz ryzyka wystąpienia incydentów i cyberataków przeprowadzanych przez osoby o ograniczonych umiejętnościach i dysponujących niewielkimi zasobami. Działania w zakresie oceny, jakie mają zostać podjęte, obejmują co najmniej: sprawdzenie w celu wykazania, że nie występują powszechnie znane podatności, oraz testowanie w celu wykazania, że w produktach ICT, usługach ICT, procesach ICT lub usługach zarządzanych w zakresie bezpieczeństwa prawidłowo zaimplementowane zostały niezbędne funkcjonalności bezpieczeństwa. W przypadku gdy takie działania w zakresie oceny nie są odpowiednie podejmuje się alternatywne działania w zakresie oceny, które mają równoważny skutek.

7. Europejski certyfikat cyberbezpieczeństwa, który odnosi się do poziomu uzasadnienia zaufania »wysoki«, daje uzasadnione zaufanie, że produkty ICT, usługi ICT, procesy ICT i usługi zarządzane w zakresie bezpieczeństwa, dla których wydany został ten certyfikat, spełniają odpowiadające mu wymogi bezpieczeństwa, w tym funkcjonalności bezpieczeństwa, oraz zostały ocenione na poziomie, który ma na celu zminimalizowanie ryzyka wystąpienia zaawansowanych cyberataków przeprowadzanych przez osoby o znacznych umiejętnościach i dysponujących znaczącymi zasobami. Działania w zakresie oceny, jakie mają zostać podjęte, obejmują co najmniej: sprawdzenie w celu wykazania, że nie występują powszechnie znane podatności, testowanie w celu wykazania, że w produktach ICT, usługach ICT, procesach ICT lub usługach zarządzanych w zakresie bezpieczeństwa prawidłowo zaimplementowane zostały niezbędne funkcjonalności bezpieczeństwa według najnowszego stanu wiedzy, oraz ocenę sprawdzającą za pomocą

testów penetracyjnych ich odporność na zaawansowane ataki.
W przypadku gdy takie działania w zakresie oceny nie są odpowiednie, podejmuje się alternatywne działania w zakresie oceny, które mają równoważny skutek.”;

11) art. 53 ust. 1, 2 i 3 otrzymują brzmienie:

„1. Europejski program certyfikacji cyberbezpieczeństwa może zezwalać na ocenę zgodności przez stronę pierwszą przeprowadzaną na wyłączną odpowiedzialność wytwórcy lub dostawcy produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa. Na ocenę zgodności przez stronę pierwszą zezwala się jedynie w przypadku produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa, które stwarzają niewielkie ryzyko odpowiadające poziomowi uzasadnienia zaufania »podstawowy«.

2. Wytwórca lub dostawca produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa może wydać unijną deklarację zgodności stwierdzającą, że wykazano spełnienie wymogów określonych w programie. Wydając taką deklarację, wytwórca lub dostawca produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa przyjmuje na siebie odpowiedzialność za zgodność produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa z wymogami określonymi w tym programie.

3. Wytwórca lub dostawca produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa udostępnia – przez okres przewidziany w odpowiednim europejskim programie certyfikacji cyberbezpieczeństwa – krajowemu organowi ds. certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58, unijną deklarację zgodności, dokumentację techniczną oraz wszelkie inne istotne informacje związane ze zgodnością produktów ICT, usług ICT lub usług zarządzanych w zakresie bezpieczeństwa z programem. Kopię unijnej deklaracji zgodności przedkłada się krajowemu organowi ds. certyfikacji cyberbezpieczeństwa i ENISA.”;

12) w art. 54 ust. 1 wprowadza się następujące zmiany:

a) lit. a) otrzymuje brzmienie:

„a) przedmiot i zakres programu certyfikacji, w tym rodzaj lub kategorie objętych danym programem produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa;”;

b) lit. j) otrzymuje brzmienie:

„j) zasady monitorowania zgodności produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa z wymogami europejskich certyfikatów cyberbezpieczeństwa lub unijnymi deklaracjami zgodności, w tym mechanizmy służące wykazaniu ciągłej zgodności z określonymi wymogami cyberbezpieczeństwa;”;

c) lit. l) otrzymuje brzmienie:

„l) zasady dotyczące skutków dla produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa, które uzyskały certyfikację lub w przypadku których wydana została unijna deklaracja zgodności, które jednak nie spełniają wymogów programu;”;

d) lit. o) otrzymuje brzmienie:

„o) identyfikacja krajowych lub międzynarodowych programów certyfikacji cyberbezpieczeństwa, obejmujących ten sam rodzaj lub te same kategorie produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa, wymogów bezpieczeństwa, kryteriów i metod oceny oraz poziomów uzasadnienia zaufania;”;

e) lit. q) otrzymuje brzmienie:

„q) okres dostępności unijnej deklaracji zgodności, dokumentacji technicznej oraz wszelkich innych istotnych informacji, przez jaki mają je udostępniać wytwórcy lub dostawcy produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa;”;

13) w art. 56 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Przyjmuje się, że produkty ICT, usługi ICT, procesy ICT i usługi

zarządzane w zakresie bezpieczeństwa, które uzyskały certyfikację w ramach przyjętego na podstawie art. 49 europejskiego programu certyfikacji cyberbezpieczeństwa, są zgodne z wymogami takiego programu.”;

b) w ust. 3 wprowadza się następujące zmiany:

(i) akapit pierwszy otrzymuje brzmienie:

„Komisja ocenia regularnie wydajność i użyteczność przyjętych europejskich programów certyfikacji cyberbezpieczeństwa oraz to, czy określony europejski program certyfikacji cyberbezpieczeństwa należy uczynić obowiązkowym za pomocą odpowiedniego prawa Unii w celu zapewnienia w Unii odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa oraz w celu poprawy funkcjonowania rynku wewnętrznego. Pierwszą taką ocenę przeprowadza się nie później niż 31 grudnia 2023 r., a kolejne oceny przeprowadza się co najmniej raz na 2 lata. W oparciu o wynik tych ocen Komisja zidentyfikuje te produkty ICT, usługi ICT, procesy ICT i usługi zarządzane w zakresie bezpieczeństwa objęte jednym z istniejących programów certyfikacji, które należy objąć obowiązkowym programem certyfikacji.”;

(ii) w akapicie trzecim wprowadza się następujące zmiany:

aa) lit. a) otrzymuje brzmienie:

„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;”;

bb) lit. d) otrzymuje brzmienie:

„d) bierze pod uwagę terminy wdrożenia, środki i okresy przejściowe, w szczególności pod względem ewentualnego wpływu danego środka na wytwórców lub dostawców produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, w tym ***szczególne interesy i potrzeby mikroprzedsiębiorstw oraz MŚP***;”;

(iii) dodaje się akapit w brzmieniu:

„W odniesieniu do akapitu trzeciego lit. d) niniejszego artykułu Komisja zapewnia odpowiednie wsparcie finansowe w ramach istniejących programów unijnych, w szczególności w celu zmniejszenia obciążenia finansowego mikroprzedsiębiorstw i MŚP, w tym przedsiębiorstw typu start-up działających w dziedzinie usług zarządzanych w zakresie bezpieczeństwa.”;

c) ust. 7 i 8 otrzymują brzmienie:

„7. Osoba fizyczna lub prawna, która poddaje produkty ICT, usługi ICT, procesy ICT lub usługi zarządzane w zakresie bezpieczeństwa certyfikacji, udostępnia krajowemu organowi ds. certyfikacji cyberbezpieczeństwa, o którym mowa w art. 58 – w przypadku gdy organ ten jest podmiotem wydającym europejski certyfikat cyberbezpieczeństwa – lub jednostce oceniającej zgodność, o której mowa w art. 60, wszelkie informacje niezbędne to przeprowadzenia certyfikacji.

8. Posiadacz europejskiego certyfikatu cyberbezpieczeństwa informuje organ lub jednostkę, o których mowa w ust. 7, o wszelkich wykrytych następnie podatnościach lub nieprawidłowościach związanych z bezpieczeństwem certyfikowanych produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, które mogą mieć wpływ na zgodność z wymogami z zakresu certyfikacji. Organ lub jednostka przekazuje bez zbędnej zwłoki te informacje zainteresowanemu krajowemu organowi ds. certyfikacji cyberbezpieczeństwa.”;

14) art. 57 ust. 1 i 2 otrzymują brzmienie:

„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*** 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.

2. Państwa członkowskie nie mogą wprowadzać nowych krajowych programów certyfikacji cyberbezpieczeństwa dotyczących produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa, które są już objęte obowiązującym europejskim programem certyfikacji cyberbezpieczeństwa.”;

15) w art. 58 wprowadza się następujące zmiany:

a) w ust. 7 wprowadza się następujące zmiany:

(i) lit. a) i b) otrzymują brzmienie:

„a) nadzorują i egzekwują stosowanie zawartych w europejskich programach certyfikacji cyberbezpieczeństwa na podstawie art. 54 ust. 1 lit. j) zasad monitorowania zgodności produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa z wymogami europejskich certyfikatów cyberbezpieczeństwa wydanych na ich terytoriach, we współpracy z innymi odpowiednimi organami nadzoru rynku;

b) monitorują wykonywanie obowiązków wytwórców lub dostawców produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, którzy mają siedzibę na ich terytorium i którzy przeprowadzają ocenę zgodności przez stronę pierwszą, oraz egzekwują takie obowiązki, w szczególności monitorują

wykonywanie obowiązków takich wytwórców lub dostawców, które określono w art. 53 ust. 2 i 3 i w odpowiednich europejskich programach certyfikacji cyberbezpieczeństwa, oraz egzekwują takie obowiązki;";

(ii) lit. h) otrzymuje brzmienie:

„h) współpracują z innymi krajowymi organami ds. certyfikacji cyberbezpieczeństwa lub innymi organami publicznymi, w tym poprzez wymianę informacji na temat ewentualnej niezgodności produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa z wymogami niniejszego rozporządzenia lub z wymogami określonych europejskich programów certyfikacji cyberbezpieczeństwa; oraz";

b) ust. 9 otrzymuje brzmienie:

„9. Krajowe organy ds. certyfikacji cyberbezpieczeństwa współpracują ze sobą i z Komisją, w szczególności wymieniając informacje, doświadczenie i dobre praktyki odnoszące się do certyfikacji cyberbezpieczeństwa i kwestii technicznych dotyczących cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa.";

16) art. 59 ust. 3 lit. b) i c) otrzymują brzmienie:

„b) procedury nadzorowania i egzekwowania zasad monitorowania zgodności produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa z europejskimi certyfikatami cyberbezpieczeństwa na podstawie art. 58 ust. 7 lit. a);

c) procedury nadzorowania i egzekwowania obowiązków wytwórców lub dostawców produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa na podstawie art. 58 ust. 7 lit. b);"

16a) dodaje się artykuł w brzmieniu:

„Artykuł 65a

Wykonywanie przekazanych uprawnień

1. Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 49 ust. 7, powierza się Komisji na okres pięciu lat od dnia ... [data wejścia w życie niniejszego rozporządzenia zmieniającego]. 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. 7, 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 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. 7 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.;"

17) art. 67 otrzymuje brzmienie:

„Artykuł 67

Ocena i przegląd

1. *Do 28 czerwca 2024 r., a następnie co trzy 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.*

2. *Ocena dotyczy 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.*

3. *Ocena obejmuje również:*

   a) *ocenę efektywności i skuteczności procedur prowadzących do konsultacji, przygotowania i przyjęcia europejskich programów certyfikacji cyberbezpieczeństwa, a także sposobów poprawy i przyspieszenia tych procedur;*

   b) *ustalenie, czy w celu zapobieżenia wprowadzaniu na rynek unijny produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa niespełniających podstawowych wymogów cyberbezpieczeństwa konieczne są zasadnicze wymogi cyberbezpieczeństwa dotyczące dostępu do rynku wewnętrznego.*

4. *Do 28 czerwca 2024 r., a następnie co trzy lata, Komisja przekazuje sprawozdanie z oceny wraz z wnioskami Parlamentowi Europejskiemu, Radzie i Zarządowi. Ustalenia zawarte w tym sprawozdaniu podaje się do wiadomości publicznej.*”

Artykuł 2

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w Dzienniku Urzędowym Unii Europejskiej.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w ...

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*

UZASADNIENIE

Sprawozdawczyni popiera wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2019/8811 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa, rozumiejąc konieczność aktualizacji i wzmocnienia europejskiego programu certyfikacji cyberbezpieczeństwa, tak aby obejmował on ważne i rozwijające się usługi w tym sektorze. Biorąc pod uwagę, w jaki sposób poszczególne państwa członkowskie rozpoczęły już przyjmowanie programów certyfikacji dla usług zarządzanych w zakresie bezpieczeństwa, sprawozdawczyni jest zdania, że zmiany w akcie o cyberbezpieczeństwie mają kluczowe znaczenie dla zapobieżenia poważnym rozbieżnościom między programami krajowymi, które doprowadziłyby do fragmentacji rynku, co stoi w sprzeczności nie tylko z interesami gospodarczymi Unii, ale także z jej interesami strategicznymi.

W związku z tym sprawozdawczyni docenia sposób, w jaki omawiany wniosek ma uzupełniać akt w sprawie cybersolidarności, w szczególności rozszerzenie o europejski program certyfikacji cyberbezpieczeństwa, co umożliwi usługom zarządzanym w zakresie bezpieczeństwa – analogicznie do „zaufanych dostawców", o których mowa w akcie w sprawie cybersolidarności – odegrać ważną rolę w przyszłej unijnej rezerwie cyberbezpieczeństwa. Dlatego omawiany wniosek ma również ogromne znaczenie dla wspierania szerszych zdolności Unii w zakresie cyberbezpieczeństwa, które są kluczowe dla przeciwdziałania potencjalnym zagrożeniom w stale zmieniających się realiach geopolitycznych.

W granicach określonych we wniosku Komisji celem sprawozdawczyni jest skonsolidowanie tej ukierunkowanej zmiany aktu o cyberbezpieczeństwie i dalsze zwiększenie jasności przepisów. Ilustrują to zmiany wprowadzone przez sprawozdawczynię w definicji usług zarządzanych w zakresie bezpieczeństwa, wyjaśniające, że są one „zlecane usługodawcy zewnętrznemu", i doprecyzowujące zakres definicji. Zgłoszone poprawki dotyczące uznawania międzynarodowych norm cyberbezpieczeństwa mają na celu zwiększenie zaufania, a zarazem opracowanie kompleksowych przepisów UE.

W niniejszym projekcie sprawozdania położono większy nacisk na rozwiązanie problemu niedoboru kwalifikacji oraz na wspieranie mikroprzedsiębiorstw oraz małych i średnich

przedsiębiorstw. W pierwszym przypadku poprawki opierają się na już istniejącym założeniu konieczności posiadania umiejętności w programie certyfikacji cyberbezpieczeństwa w odniesieniu do „pracowników o bardzo wysokim poziomie odpowiedniej wiedzy technicznej i uczciwości zawodowej, posiadających wymagane kompetencje, wiedzę fachową i doświadczenie”. Zdaniem sprawozdawczyni europejski system certyfikacji, przy wsparciu współpracy między wszystkimi zaangażowanymi podmiotami, a także między państwami członkowskimi, sektorem prywatnym, środowiskiem akademickim i instytucjami badawczymi, musi stanowić czynnik umożliwiający opracowanie nowego planu działania na rzecz szkolenia i wzmocnienia pozycji pracowników, gromadząc więcej danych na temat potrzebnych umiejętności i przyczyniając się do rozwiązania problemu różnic w traktowaniu kobiet i mężczyzn w dziedzinie nauk ścisłych, technologii, inżynierii i matematyki.

Jednocześnie mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa, które stanowią trzon gospodarki europejskiej i z pewnością mogą odegrać pozytywną rolę w sektorze cyberbezpieczeństwa, powinny korzystać z odpowiedniego wsparcia finansowego w ramach istniejących programów unijnych, aby zmniejszyć wszelkie ciążące na nich nieproporcjonalne obciążenia finansowe.

21.9.2023

PISMO KOMISJI RYNKU WEWNĘTRZNEGO I OCHRONY KONSUMENTÓW

Sz.P. Cristian-Silviu Buşoi
Przewodniczący
Komisja Przemysłu, Badań Naukowych i Energii
BRUKSELA

Przedmiot: Opinia w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa (COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Szanowny Panie Przewodniczący!

W ramach procedury podanej w przedmiocie zwrócono się do Komisji Rynku Wewnętrznego i Ochrony Konsumentów o wydanie opinii. Na posiedzeniu 23 maja 2023 r. komisja postanowiła, że opinia ta będzie mieć formę pisma. Na posiedzeniu 19 września 2023 r. komisja rozpatrzyła sprawę i przyjęła opinię.

Na posiedzeniu tym[1] komisja postanowiła zwrócić się do Komisji Przemysłu, Badań Naukowych i Energii (ITRE), jako komisji przedmiotowo właściwej, aby uwzględniła w sprawozdaniu ustawodawczym następujące wskazówki.

Z wyrazami szacunku

Anna Cavazzini

WSKAZÓWKI

Komisja Rynku Wewnętrznego i Ochrony Konsumentów zwraca się do Komisji Przemysłu, Badań Naukowych i Energii, jako komisji przedmiotowo właściwej, aby wzięła pod uwagę następujące wskazówki:

A. mając na uwadze, że 18 kwietnia 2023 r. Komisja opublikowała wniosek ustawodawczy w sprawie usług zarządzanych w zakresie bezpieczeństwa, który obejmuje

[1] Na głosowaniu końcowym obecni byli: Anna Cavazzini (przewodnicząca), Andrus Ansip (wiceprzewodniczący), Krzysztof Hetman (wiceprzewodniczący), Alex Agius Saliba, João Albuquerque, Pablo Arias Echeverría, Laura Ballarín Cereza, Alessandra Basso, Brando Benifei, Biljana Borzan, Vlad Marius Botoş, Deirdre Clune, Dita Charanzová, David Cormand, Carlo Fidanza, Malte Gallée, Sandro Gozi, Svenja Hahn, Virginie Joron, Eugen Jurzyca, Arba Kokalari, Marcel Kolaja, Andrey Kovatchev, Jean-Lin Lacapelle, Morten Løkkegaard, Beata Mazurek, Leszek Miller, Anne Sophie Pelletier, Christel Schaldemose, Andreas Schwab, Tomislav Sokol, Ivan Štefanec, Róża Thun und Hohenstein, Tom Vandenkendelaere, Kim Van Sparrentak.

ukierunkowane zmiany w unijnym akcie o cyberbezpieczeństwie[2];

B. mając na uwadze, że w sprawie wniosku ustawodawczego dotyczącego unijnego aktu o cyberbezpieczeństwie (2017/0225(COD))[3] Komisja Rynku Wewnętrznego i Ochrony Konsumentów (IMCO) wydała na podstawie dawnego art. 54 Regulaminu opinię dla Komisji Przemysłu, Badań Naukowych i Energii (ITRE) – komisji przedmiotowo właściwej posiadającej kompetencje dzielone w zakresie ram certyfikacji cyberbezpieczeństwa, ponieważ komisja IMCO ma wyraźne kompetencje w dziedzinie systemów certyfikacji i ogólnie normalizacji, nadzoru rynku i tworzenia jednolitego rynku cyfrowego;

C. mając na uwadze, że unijny akt o cyberbezpieczeństwie[4] ma zapewnić 1) wysoki poziom cyberbezpieczeństwa, cyberodporności i zaufania do UE dzięki określeniu celów, zadań i kwestii organizacyjnych wzmocnionej i przemianowanej Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), która będzie mieć nowy i stały mandat, oraz 2) ramy dobrowolnych europejskich systemów certyfikacji cyberbezpieczeństwa produktów, usług i procesów w dziedzinie technologii informacyjno-komunikacyjnych (ICT);

D. mając na uwadze zaproponowane ukierunkowane zmiany, aby włączyć usług zarządzanych w zakresie bezpieczeństwa do zakresu unijnego aktu o cyberbezpieczeństwie oraz dodać definicję tych usług, która będzie ściśle dostosowana do definicji zawartej w dyrektywie NIS 2[5]; mając na uwadze, że dzięki zmianie Komisja mogłaby przyjmować w drodze aktów wykonawczych europejskie systemy certyfikacji cyberbezpieczeństwa w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa oprócz produktów, usług i procesów w dziedzinie ICT, które są już objęte unijnym aktem o cyberbezpieczeństwie;

E. mając na uwadze, że usługi zarządzane w zakresie bezpieczeństwa odgrywają coraz większą rolę w zapobieganiu cyberincydentom i ograniczaniu ich skutków;

1. przyznaje, że 23 maja 2022 r.[6] Rada wezwała, aby zwiększyć ogólny poziom cyberbezpieczeństwa w UE i aby w tym celu ułatwić powstawanie i rozwój zaufanych dostawców usług w zakresie cyberbezpieczeństwa; uważa, że m.in. wojna w Ukrainie, obecny kontekst geopolityczny, ciągłe zagrożenia ze strony reżimów państw trzecich, stale rosnący rynek technologii cyfrowych i ogólnie cyfrowa transformacja procesów powodują, że potrzebny jest wyższy poziom cyberbezpieczeństwa w UE i państwach członkowskich; zaleca, aby Komisja proaktywnie wspierała rozwój zaufanych dostawców usług w zakresie cyberbezpieczeństwa, np. poprzez finansowanie badań i rozwoju, programy szkoleniowe służące budowaniu umiejętności w zakresie cyberbezpieczeństwa oraz zachęty dla przedsiębiorstw do inwestowania w cyberbezpieczeństwo; sugeruje, że UE powinna zacieśnić współpracę z NATO i innymi partnerami międzynarodowymi, aby reagować na zagrożenia cybernetyczne ze strony reżimów państw trzecich, np. poprzez wymianę informacji wywiadowczych o

[2] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52023PC0208
[3] https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2017/0225(OLP)
[4] Dz.U. L 151 z 7.6.2019, s. 15.
[5] Dz.U. L 333/810 z 27.12.2022 r.
[6] 9364/22

zagrożeniach, wspólne ćwiczenia i skoordynowane reakcje na cyberataki;

2. podkreśla, że certyfikacja usług zarządzanych w zakresie bezpieczeństwa, oparta na niedyskryminacyjnych zasadach i odzwierciedlająca normy europejskie i międzynarodowe, ma zasadnicze znaczenie dla budowania i gwarantowania zaufania do jakości tych usług, w szczególności w celu osiągnięcia wysokiego poziomu ochrony konsumentów; zauważa, że niektóre państwa członkowskie przyjęły już systemy certyfikacji usług zarządzanych w zakresie bezpieczeństwa, oraz że w związku z tym należy nie tylko unikać fragmentacji rynku wewnętrznego i niespójności, które mogą mieć wpływ na branżę cyberbezpieczeństwa i działające w niej przedsiębiorstwa, ale i umożliwić zharmonizowane podejście przez utworzenie europejskiego systemu certyfikacji cyberbezpieczeństwa takich usług; domaga się, aby ramy certyfikacji cyberbezpieczeństwa uwzględniały najlepsze praktyki z istniejących krajowych systemów certyfikacji i były opracowywane w porozumieniu z kluczowymi zainteresowanymi stronami w branży cyberbezpieczeństwa;

3. podkreśla, że dostawcy usług zarządzanych w zakresie bezpieczeństwa zajmujący się obszarami takimi jak reagowanie na incydenty, testy penetracyjne, audyty bezpieczeństwa i doradztwo odgrywają ważną rolę w pomaganiu podmiotom w działaniach mających na celu zapobieganie incydentom, wykrywanie ich, reagowanie na nie lub przywracanie normalnego działania po ich wystąpieniu; uważa, że ponieważ coraz więcej przedsiębiorstw ma trudności z utrzymaniem różnych złożonych systemów oprogramowania i wzajemnie połączonych sieci korporacyjnych, muszą one korzystać z usług dostawców usług zarządzanych w zakresie bezpieczeństwa, dlatego takich dostawców należy uznać za kluczowy element unijnego systemu cyberbezpieczeństwa; zauważa jednak, że dostawcy usług zarządzanych w zakresie bezpieczeństwa również sami padają ofiarą cyberataków, a ponieważ ich działalność jest ściśle zintegrowana z operacjami ich klientów, mogą stanowić szczególne ryzyko;

4. przypomina, jak ważna dla wyższego poziomu cyberodporności w całej Unii jest przyjęta niedawno dyrektywa NIS 2; wzywa do szybkiego przyjęcia i wdrożenia aktów wykonawczych na mocy tej dyrektywy w celu dopilnowania, aby dostawcy usług zarządzanych w zakresie bezpieczeństwa przestrzegali wymogów dyrektywy dotyczących środków zarządzania ryzykiem w dziedzinie cyberbezpieczeństwa;

5. zaleca, aby dostawcy usług zarządzanych w zakresie bezpieczeństwa musieli przestrzegać odpowiednich norm cyberbezpieczeństwa i poddawać się regularnej ocenie w celu zapewnienia, by ich systemy były na tyle bezpieczne, by chronić nie tylko ich samych, ale i podmioty, które obsługują; uważa, że w takich ocenach należy sprawdzać, czy dostawcy stosują się do ogólnounijnych ram certyfikacji cyberbezpieczeństwa i czy są w stanie chronić zarówno swoje systemy, jak i systemy swoich klientów przed cyberzagrożeniami;

6. z zadowoleniem przyjmuje wniosek ustawodawczy w sprawie usług zarządzanych w zakresie bezpieczeństwa, którego celem jest poprawa jakości usług zarządzanych w zakresie bezpieczeństwa i zwiększenie ich porównywalności z korzyścią dla właściwego funkcjonowania rynku wewnętrznego i wdrożenia jednolitego rynku cyfrowego; podkreśla, że certyfikacja usług zarządzanych w zakresie bezpieczeństwa nie tylko jest istotna z punktu widzenia procesu wyboru dostawców do unijnej rezerwy

cyberbezpieczeństwa, ale stanowi też ważny wskaźnik jakości i zaufania dla podmiotów prywatnych i publicznych, które zamierzają nabyć takie usługi.

7. zauważa, że we wniosku wzmacnia się rolę ENISA, która powinna wspierać i promować rozwój i wdrażanie polityki Unii w zakresie certyfikacji cyberbezpieczeństwa produktów, usług i procesów w dziedzinie ICT oraz usług zarządzanych w zakresie bezpieczeństwa przez regularne monitorowanie zmian w powiązanych obszarach normalizacji i zalecanie specyfikacji technicznych, kiedy normy nie są dostępne; sugeruje, aby przekazać ENISA dodatkowe zasoby i uprawnienia, by mogła wywiązać się z rozszerzonej roli, w tym finansowania badań i rozwoju, a także jasny mandat do koordynowania działań z krajowymi agencjami ds. cyberbezpieczeństwa i zainteresowanymi stronami z branży; podkreśla zasadniczą rolę zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) w tworzeniu przewidywalnej i bezpiecznej przestrzeni cyfrowej dla przedsiębiorstw i obywateli;

8. wzywa Komisję i ENISA, aby wspierały i zapewniały spójne wdrażanie europejskiego systemu certyfikacji cyberbezpieczeństwa opartego na niedyskryminacyjnych zasadach i odzwierciedlającego europejskie i międzynarodowe normy dotyczące samooceny zgodności dokonywanej przez wytwórcę lub dostawcę produktów, usług i procesów w dziedzinie ICT czy usług zarządzanych w zakresie bezpieczeństwa, zgodnie z unijnym aktem o cyberbezpieczeństwie; uważa, że wdrożenie tego systemu powinno pomóc zrównoważyć koszty akredytacji i zachęcić większą liczbę producentów lub dostawców do udziału w nim;

9. podkreśla, że każdy system certyfikacji należy zaprojektować tak, aby pobudzał i zachęcał wszystkie podmioty z tego sektora do opracowywania i przyjmowania regularnie aktualizowanych standardów bezpieczeństwa, norm technicznych oraz zasad uwzględniania bezpieczeństwa i ochrony prywatności już w fazie projektowania na wszystkich etapach istnienia produktu lub usługi; podkreśla, że przy opracowywaniu takich zasad należy bardziej systematycznie uwzględniać wkład społeczeństwa obywatelskiego, niezależnych badaczy ds. bezpieczeństwa i odpowiednich zainteresowanych stron; uważa, że systemy certyfikacji powinny być spójne z innymi europejskimi systemami certyfikacji cyberbezpieczeństwa przyjętymi zgodnie z unijnym aktem o cyberbezpieczeństwie i nie powinny powodować nieproporcjonalnych obciążeń dla dostawców; zaleca, aby systemy certyfikacji obejmowały jasne i szczegółowe wytyczne dotyczące sposobu wdrażania zasad uwzględniania bezpieczeństwa i ochrony prywatności już w fazie projektowania, jeśli takie wytyczne są zgodne z przepisami określającymi ramy europejskich systemów cyberbezpieczeństwa w unijnym akcie o cyberbezpieczeństwie; sugeruje, aby tam, gdzie jest to konieczne i proporcjonalne, systemy certyfikacji składały się z mechanizmu ciągłego doskonalenia, takiego jak regularne przeglądy i aktualizacje standardów bezpieczeństwa i norm technicznych; uważa, że mechanizm ten powinien uwzględniać najnowsze zmiany w zakresie zagrożeń i technologii cyberbezpieczeństwa; nalega, aby każdy system certyfikacji obejmował środki promujące przejrzystość i rozliczalność, takie jak publiczne ujawnianie wyników certyfikacji i kar za nieprzestrzeganie przepisów;

10. apeluje, aby wprowadzić dobrowolny unijny znak zaufania dla certyfikowanych produktów, usług, procesów w dziedzinie ICT oraz usług zarządzanych w zakresie bezpieczeństwa; podkreśla w związku z tym, że znak ten mógłby pomóc podnieść

świadomość na temat cyberbezpieczeństwa na całym rynku wewnętrznym i zapewnić przedsiębiorstwom posiadającym dobre referencje w zakresie cyberbezpieczeństwa przewagę konkurencyjną; sugeruje, aby tak zaprojektować unijny znak zaufania, aby był łatwo rozpoznawalny i zrozumiały dla konsumentów i przedsiębiorstw;

11. zaleca, aby Komisja i ENISA ustanowiły specjalny program badawczo-rozwojowy na rzecz cyberbezpieczeństwa; zaleca, aby Komisja i ENISA ustanowiły ramy oceny ryzyka dla przedsiębiorstw w cyberprzestrzeni, które obejmowałyby wytyczne dotyczące sposobu identyfikowania, oceny i ograniczania ryzyka w cyberprzestrzeni i mogłyby być dostosowane do różnych sektorów i rozmiarów przedsiębiorstw; sugeruje, aby Komisja i ENISA oferowały państwom członkowskim pomoc w ustanowieniu mechanizmu zgłaszania cyberincydentów dla konsumentów i przedsiębiorstw, aby ułatwić gromadzenie danych o cyberincydentach, które można by wykorzystać do poprawy polityki i praktyk w zakresie cyberbezpieczeństwa.

PROCEDURA W KOMISJI PRZEDMIOTOWO WŁAŚCIWEJ

Tytuł	Zmiana rozporządzenia (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa
Odsyłacze	COM(2023)0208 – C9-0137/2023 – 2023/0108(COD)
Data przedstawienia Parlamentowi	19.4.2023
Komisja przedmiotowo właściwa Data ogłoszenia na posiedzeniu	ITRE 1.6.2023
Komisje opiniodawcze Data ogłoszenia na posiedzeniu	IMCO LIBE 1.6.2023 1.6.2023
Rezygnacja z wydania opinii Data decyzji	LIBE 30.5.2023
Sprawozdawcy Data powołania	Josianne Cutajar 2.5.2023
Rozpatrzenie w komisji	19.7.2023 19.9.2023
Data przyjęcia	25.10.2023
Wynik głosowania końcowego	+: 57 –: 0 0: 2
Posłowie obecni podczas głosowania końcowego	Matteo Adinolfi, Nicola Beer, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Michael Bloss, Paolo Borchia, Marc Botenga, Markus Buchheit, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Beatrice Covassi, Ciarán Cuffe, Josianne Cutajar, Nicola Danti, Marie Dauchy, Pilar del Castillo Vera, Christian Ehler, Lina Gálvez Muñoz, Jens Geier, Bart Groothuis, Christophe Grudler, Henrike Hahn, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Thierry Mariani, Marina Mesure, Dan Nica, Niklas Nienass, Ville Niinistö, Johan Nissinen, Mauri Pekkarinen, Tsvetelina Penkova, Morten Petersen, Markus Pieper, Clara Ponsatí Obiols, Manuela Ripa, Sara Skyttedal, Riho Terras, Patrizia Toia, Henna Virkkunen, Pernille Weiss, Carlos Zorrinho
Zastępcy obecni podczas głosowania końcowego	Pascal Arimont, Tiziana Beghin, Franc Bogovič, Damien Carême, Martina Dlabajová, Francesca Donato, Matthias Ecke, Nicolás González Casares, Ladislav Ilčić, Luděk Niedermayer, Emma Wiesner
Zastępcy (art. 209 ust. 7) obecni podczas głosowania końcowego	Asim Ademov, Aušra Maldeikienė, Irène Tolleret
Data złożenia	26.10.2023

GŁOSOWANIE KOŃCOWE W FORMIE GŁOSOWANIA IMIENNEGO W KOMISJI PRZEDMIOTOWO WŁAŚCIWEJ

57	+
ECR	Ladislav Ilčić
ID	Matteo Adinolfi, Paolo Borchia, Marie Dauchy, Thierry Mariani
NI	Tiziana Beghin, Francesca Donato, Clara Ponsatí Obiols
PPE	Asim Ademov, Pascal Arimont, François-Xavier Bellamy, Hildegard Bentele, Tom Berendsen, Franc Bogovič, Cristian-Silviu Buşoi, Jerzy Buzek, Maria da Graça Carvalho, Pilar del Castillo Vera, Christian Ehler, Aušra Maldeikienė, Luděk Niedermayer, Markus Pieper, Sara Skyttedal, Riho Terras, Henna Virkkunen, Pernille Weiss
Renew	Nicola Beer, Nicola Danti, Martina Dlabajová, Bart Groothuis, Christophe Grudler, Mauri Pekkarinen, Morten Petersen, Irène Tolleret, Emma Wiesner
S&D	Beatrice Covassi, Josianne Cutajar, Matthias Ecke, Lina Gálvez Muñoz, Jens Geier, Nicolás González Casares, Ivo Hristov, Romana Jerković, Miapetra Kumpula-Natri, Dan Nica, Tsvetelina Penkova, Patrizia Toia, Carlos Zorrinho
The Left	Marc Botenga, Marina Mesure
Verts/ALE	Michael Bloss, Damien Carême, Ciarán Cuffe, Henrike Hahn, Niklas Nienass, Ville Niinistö, Manuela Ripa

0	-

2	0
ECR	Johan Nissinen
ID	Markus Buchheit

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