UNIA EUROPEJSKA

PARLAMENT EUROPEJSKI **RADA**

Bruksela, 20 listopada 2024 r.
(OR. en)

2023/0108(COD) **PE-CONS 93/24**

CYBER 207
JAI 1083
TELECOM 217
DATAPROTECT 246
MI 632
IND 327
CODEC 1587

AKTY USTAWODAWCZE I INNE INSTRUMENTY

Dotyczy:	ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY w sprawie zmiany rozporządzenia (UE) 2019/881 w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa

ROZPORZĄDZENIE
PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2024/...

z dnia ...

w sprawie zmiany rozporządzenia (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],

po konsultacji z Komitetem Regionów,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą[2],

---

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

2 Stanowisko Parlamentu Europejskiego z dnia 24 kwietnia 2024 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz 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, a także w celu uniknięcia rozdrobnienia rynku wewnętrznego w zakresie programów certyfikacji cyberbezpieczeństwa w Unii.

[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).

(2) Aby zapewnić odporność Unii na cyberataki oraz zapobiec wszelkim lukom na rynku wewnętrznym, niniejsze rozporządzenie ma uzupełnić horyzontalne ramy regulacyjne ustanawiające kompleksowe wymagania w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/...[4+] poprzez ustanowienie celów bezpieczeństwa dotyczących usług zarządzanych w zakresie bezpieczeństwa, a także stosowania i wiarygodności tych usług.

---

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/... z dnia... w sprawie horyzontalnych wymagań w zakresie cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi oraz w sprawie zmiany rozporządzeń (UE) nr 168/2013 i (UE) 2019/1020 i dyrektywy (UE) 2020/1828 (akt o cyberodporności) (Dz.U. …, ELI: …).

[+] Dz.U.: proszę wstawić w tekście numer rozporządzenia zawartego w dokumencie PE-CONS 100/23 (2022/0272(COD)), a w przypisie jego numer, datę, odniesienie do publikacji w Dz.U. i odniesienie ELI.

(3) Usługi zarządzane w zakresie bezpieczeństwa są świadczone przez dostawców usług zarządzanych w zakresie bezpieczeństwa zdefiniowanych w art. 6 pkt 40 dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555[5]. Zawarta w niniejszym rozporządzeniu definicja usług zarządzanych w zakresie bezpieczeństwa powinna zatem być spójna z definicją dostawców usług zarządzanych w zakresie bezpieczeństwa zawartą w dyrektywie (UE) 2022/2555. Usługi te polegają na prowadzeniu lub zapewnianiu pomocy dla działań związanych z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa, na jakie narażeni są klienci dostawców tych usług, oraz odgrywają coraz większą rolę w zapobieganiu incydentom i ograniczaniu ich skutków. W związku z tym dostawców tych usług uznaje się za podmioty kluczowe lub ważne należące do sektora kluczowego zgodnie z dyrektywą (UE) 2022/2555. Jak wskazano w motywie 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. Jednak również sami dostawcy usług zarządzanych w zakresie bezpieczeństwa padają ofiarą cyberataków, a ponieważ ich działalność jest ściśle zintegrowana z operacjami ich klientów, wiąże się to ze szczególnym ryzykiem. Istotne jest zatem, aby przy wyborze dostawcy usług zarządzanych w zakresie bezpieczeństwa podmioty kluczowe i ważne w rozumieniu dyrektywy (UE) 2022/2555 dochowywały szczególnej staranności.

---

[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).

(4) Definicja usług zarządzanych w zakresie bezpieczeństwa zawarta w niniejszym rozporządzeniu obejmuje niewyczerpujący wykaz usług zarządzanych w zakresie bezpieczeństwa, które mogłyby kwalifikować się do europejskich programów certyfikacji cyberbezpieczeństwa, takich jak postępowanie w przypadku incydentów, testy penetracyjne, audyty bezpieczeństwa i doradztwo w ramach wsparcia technicznego. Usługi zarządzane w zakresie bezpieczeństwa mogą obejmować usługi w zakresie cyberbezpieczeństwa, które wspierają gotowość na incydenty, zapobieganie im, ich wykrywanie, analizę i łagodzenie ich skutków, reagowanie na nie oraz przywracanie normalnego działania po ich wystąpieniu. Analiza cyberzagrożeń i ocena ryzyka w ramach wsparcia technicznego również mogłyby kwalifikować się jako usługi zarządzane w zakresie bezpieczeństwa. Mogą istnieć osobne europejskie programy certyfikacji cyberbezpieczeństwa dotyczące różnych usług zarządzanych w zakresie bezpieczeństwa. Europejskie certyfikaty cyberbezpieczeństwa wydawane zgodnie z takimi programami powinny odnosić się do konkretnych usług zarządzanych w zakresie bezpieczeństwa świadczonych przez konkretnego dostawcę tych usług.

(5) Dostawcy usług zarządzanych w zakresie bezpieczeństwa mogą również odgrywać ważną rolę w unijnych działaniach wspierających reagowanie na istotne incydenty i cyberincydenty na dużą skalę oraz wstępne przywracanie normalnego działania po ich wystąpieniu, polegając na usługach świadczonych przez zaufanych dostawców prywatnych oraz na testowaniu podmiotów krytycznych pod kątem potencjalnych podatności w oparciu o skoordynowane na poziomie Unii szacowanie ryzyka. Certyfikacja usług zarządzanych w zakresie bezpieczeństwa może odgrywać rolę w wyborze zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa zdefiniowanych w rozporządzeniu Parlamentu Europejskiego i Rady (UE) .../...[6+].

(6) Certyfikacja usług zarządzanych w zakresie bezpieczeństwa jest istotna nie tylko z punktu widzenia procesu wyboru dostawców do rezerwy cyberbezpieczeństwa UE ustanowionej rozporządzeniem (UE) …/…[++], 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 wrażliwego charakteru przetwarzanych danych certyfikacja mogłaby zapewnić potencjalnym klientom ważne wskazówki oraz pewność co do wiarygodności tych usług. Europejskie programy certyfikacji cyberbezpieczeństwa dotyczące usług zarządzanych w zakresie bezpieczeństwa mają przyczyniać się do uniknięcia rozdrobnienia rynku wewnętrznego. Niniejsze rozporządzenie ma zatem na celu usprawnienie funkcjonowania rynku wewnętrznego.

---

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) .../... z dnia... w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowywania się i reagowania na takie cyberzagrożenia i incydenty oraz w sprawie zmiany rozporządzenia (UE) 2021/694 (akt w sprawie cybersolidarności) (Dz.U. …, ELI: …).

[+] Dz.U.: proszę wstawić w tekście numer rozporządzenia zawartego w dokumencie PE-CONS 94/24 (2023/0109(COD)), a w przypisie jego numer, datę, odniesienie do publikacji w Dz.U. i odniesienie ELI.

[++] Dz.U.: proszę wstawić w tekście numer rozporządzenia zawartego w dokumencie PE-CONS 94/24 (2023/0109(COD)).

(7) Europejskie programy certyfikacji cyberbezpieczeństwa dotyczące usług zarządzanych w zakresie bezpieczeństwa powinny prowadzić do upowszechnienia tych usług i zwiększenia konkurencji między dostawcami usług zarządzanych w zakresie bezpieczeństwa. Bez uszczerbku dla celu, jakim jest zapewnienie wystarczającego i odpowiedniego poziomu danej wiedzy technicznej i uczciwości zawodowej takich dostawców, takie programy certyfikacji powinny zatem ułatwiać wejście na rynek i oferowanie usług zarządzanych w zakresie bezpieczeństwa poprzez uproszczenie, w miarę możliwości, potencjalnych obciążeń regulacyjnych, administracyjnych i finansowych, które dostawcy, w szczególności małe i średnie przedsiębiorstwa (MŚP), w tym mikroprzedsiębiorstwa, mogą napotkać przy oferowaniu usług zarządzanych w zakresie bezpieczeństwa. Ponadto aby zachęcać do korzystania z usług zarządzanych w zakresie bezpieczeństwa i stymulować popyt na nie, europejskie programy certyfikacji cyberbezpieczeństwa powinny przyczyniać się do zwiększenia dostępności tych usług, w szczególności dla mniejszych podmiotów, takich jak MŚP, w tym mikroprzedsiębiorstwa, a także dla władz lokalnych i regionalnych, które mają ograniczone zdolności i zasoby, a są bardziej narażone na naruszenia cyberbezpieczeństwa mające skutki finansowe, prawne, wizerunkowe i operacyjne.

(8) Ważne jest wsparcie MŚP, w tym mikroprzedsiębiorstw, w wykonywaniu niniejszego rozporządzenia oraz w pozyskiwaniu specjalistycznych umiejętności i wiedzy fachowej w zakresie cyberbezpieczeństwa niezbędnych do świadczenia usług zarządzanych w zakresie bezpieczeństwa zgodnie z wymogami określonymi w niniejszym rozporządzeniu. Program „Cyfrowa Europa" ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/694[7] i inne odpowiednie programy unijne przewidują, że Komisja ma zapewnić wsparcie finansowe i techniczne, które pozwoli tym przedsiębiorstwom przyczynić się do wzrostu gospodarki unijnej oraz wzmocnienia wspólnego poziomu cyberbezpieczeństwa w Unii, w tym poprzez usprawnienie wsparcia finansowego z programu „Cyfrowa Europa" i innych odpowiednich programów unijnych oraz poprzez wspieranie MŚP, w tym mikroprzedsiębiorstw.

(9) Europejskie programy certyfikacji cyberbezpieczeństwa dotyczące usług zarządzanych w zakresie bezpieczeństwa powinny przyczyniać się do dostępności bezpiecznych i wysokiej jakości usług, które gwarantują bezpieczną transformację cyfrową, oraz do osiągnięcia celów programu polityki „Droga ku cyfrowej dekadzie" do 2030 r. ustanowionego decyzją Parlamentu Europejskiego i Rady (UE) 2022/2481[8], w szczególności w odniesieniu do celu, aby 75 % przedsiębiorstw unijnych zaczęło korzystać z usług przetwarzanych w chmurze, dużych zbiorów danych lub sztucznej inteligencji, aby ponad 90 % MŚP, w tym mikroprzedsiębiorstw, osiągnęło co najmniej podstawowy poziom wskaźnika wykorzystania technologii cyfrowych oraz by kluczowe usługi publiczne były dostępne online.

---

7 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa" oraz uchylające decyzję (UE) 2015/2240 (Dz.U. L 166 z 11.5.2021, s. 1).

8 Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie" do 2030 r. (Dz.U. L 323 z 19.12.2022, s. 4).

(10) 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 dostawców takich usług. Bardzo wysoki poziom tych 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 specjalnymi europejskimi programami certyfikacji cyberbezpieczeństwa, konieczna jest zmiana rozporządzenia (UE) 2019/881. Należy uwzględnić wyniki i zalecenia z ocen i przeglądów przewidzianych w rozporządzeniu (UE) 2019/881.

(11) Aby ułatwić rozwój wiarygodnego rynku wewnętrznego, przy jednoczesnym tworzeniu partnerstw z państwami trzecimi o podobnych poglądach, proces certyfikacji ustanowiony w europejskich ramach certyfikacji cyberbezpieczeństwa przewidzianych w rozporządzeniu (UE) 2019/881należy wdrażać w taki sposób, aby ułatwić międzynarodowe uznawanie i dostosowanie do norm międzynarodowych.

(12) Unia zmaga się z niedoborem talentów, przejawiającym się brakiem wykwalifikowanych specjalistów, a jednocześnie musi stawić czoła szybko zmieniającemu się krajobrazowi zagrożeń, co stwierdzono w komunikacie Komisji z dnia 18 kwietnia 2023 r. zatytułowanym „Wyeliminowanie niedoboru talentów w dziedzinie cyberbezpieczeństwa w celu zwiększenia konkurencyjności, wzrostu gospodarczego i odporności UE (»Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa«)". Oferta zasobów edukacyjnych i różnych postaci formalnych szkoleń jest różnorodna, a wiedzę można zdobywać na różne sposoby: formalnie, na przykład za pośrednictwem uniwersytetów lub kursów, lub nieformalnie, na przykład poprzez szkolenia w miejscu pracy lub doświadczenie zawodowe w danej dziedzinie. Dlatego aby ułatwić powstawanie wysokiej jakości usług zarządzanych w zakresie bezpieczeństwa oraz aby uzyskać lepszy ogląd struktury siły roboczej zajmującej się w Unii cyberbezpieczeństwem, ważne jest, aby wzmocnić współpracę między państwami członkowskimi, Komisją, Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), ustanowioną rozporządzeniem (UE) 2019/881, oraz zainteresowanymi stronami, w tym z sektora prywatnego i środowiska akademickiego, 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. Taka współpraca ułatwiłaby również mobilność specjalistów z dziedziny cyberbezpieczeństwa w Unii, a także włączenie wiedzy i szkoleń na temat cyberbezpieczeństwa do programów kształcenia, przy jednoczesnym zapewnieniu odstępności praktyk i staży dla młodych ludzi, w tym osób mieszkających w regionach w niekorzystnym położeniu, takich jak wyspy, obszary słabo zaludnione, obszary wiejskie i obszary oddalone. Ważne jest, aby taka współpraca miała na celu przyciągnięcie większej liczby kobiet i dziewcząt do tej dziedziny oraz przyczyniła się do rozwiązania problemu różnic w traktowaniu kobiet i mężczyzn w dziedzinie nauk przyrodniczych, technologii, inżynierii i matematyki, a sektor prywatny dążył do oferowania szkoleń w miejscu pracy, które koncentrują się na najbardziej potrzebnych umiejętnościach, przy udziale administracji publicznej i przedsiębiorstw typu start-up, a także MŚP, w tym mikroprzedsiębiorstw. Ważne jest również, aby dostawcy i państwa członkowskie współpracowali ze sobą oraz przyczyniali się do zbierania danych na temat stanu i rozwoju rynku pracy w dziedzinie cyberbezpieczeństwa.

(13) ENISA odgrywa ważną rolę w przygotowywaniu propozycji dotyczących europejskich programów certyfikacji cyberbezpieczeństwa. Przygotowując projekt budżetu ogólnego Unii, Komisja powinna ocenić, jakie są niezbędne zasoby budżetowe na potrzeby planu zatrudnienia ENISA, zgodnie z procedurą określoną w art. 29 rozporządzenia (UE) 2019/881.

(14) Niniejsze rozporządzenie przewiduje punktowe zmiany w rozporządzeniu (UE) 2019/881 mające na celu umożliwienie ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa dotyczących usług zarządzanych w zakresie bezpieczeństwa. W ten sposób doprecyzowuje i wyjaśnia ono również niektóre przepisy tego rozporządzenia dotyczące przygotowania i funkcjonowania wszystkich europejskich programów certyfikacji cyberbezpieczeństwa z myślą o zapewnieniu ich przejrzystości i otwartości. Te ostatnie zmiany, które ograniczają się do uszczegółowienia lub doprecyzowania rozporządzenia (UE) 2019/881, w szczególności zmiany dotyczące informacji, które ENISA ma przekazywać przekazując propozycję programu, grup roboczych ad hoc ustanawianych dla każdej propozycji programu oraz informacji i konsultacji w odniesieniu do europejskich programów certyfikacji cyberbezpieczeństwa, nie powinny w żaden sposób wpływać na szerszą ocenę i przegląd tego rozporządzenia, wymagane na podstawie art. 67 tego rozporządzenia, w szczególności ocenę wpływu, skuteczności i efektywności przepisów tytułu tego rozporządzenia odnoszącego się do ram certyfikacji cyberbezpieczeństwa. Ocena i przegląd dotyczące tego tytułu powinny opierać się na szerokich konsultacjach z zainteresowanymi stronami oraz na pełnej i dogłębnej analizie odnośnych procedur.

(15) Ponieważ cel niniejszego rozporządzenia, a mianowicie umożliwienie ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa dotyczących usług zarządzanych w zakresie bezpieczeństwa, nie może zostać osiągnięty w sposób wystarczający przez państwa członkowskie, natomiast ze względu na jego rozmiary i skutki możliwe jest lepsze jego osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu.

(16) Zgodnie z art. 42 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725[9] skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 10 stycznia 2024 r.,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.U. L 295 z 21.11.2018, s. 39).

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, a także 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 lub usług zarządzanych w zakresie bezpieczeństwa;

11) »europejski certyfikat cyberbezpieczeństwa« oznacza wydany przez odpowiedni organ dokument poświadczający, że dany produkt ICT, dana usługa ICT, dany proces ICT lub dana usługa zarządzana w zakresie bezpieczeństwa zostały ocenione 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 lub zapewnianiu pomocy dla działań związanych z zarządzaniem ryzykiem w zakresie cyberbezpieczeństwa, takich jak postępowanie w przypadku incydentu, testy penetracyjne, audyty bezpieczeństwa i doradztwo w ramach wsparcia technicznego, w tym doradztwo fachowe;”;

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 spełnia wymogi bezpieczeństwa określonego europejskiego programu certyfikacji cyberbezpieczeństwa; 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 jako taki nie dokonuje on pomiaru 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) w ust. 1 wprowadza się następujące zmiany:

(i) wyrażenie wprowadzające 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:”;

(ii) lit. b) otrzymuje brzmienie:

„b) przygotowywanie propozycji 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;”;

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 otrzymuje brzmienie:

„*Artykuł 46*

Europejskie ramy certyfikacji cyberbezpieczeństwa

1. Ustanawia się europejskie ramy certyfikacji cyberbezpieczeństwa w celu poprawy warunków funkcjonowania rynku wewnętrznego poprzez zwiększenie poziomu cyberbezpieczeństwa w Unii oraz umożliwienie 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 przewidują mechanizm ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa potwierdzania, że produkty ICT, usługi ICT i procesy ICT, które oceniono zgodnie z tymi programami, są zgodne z określonymi wymogami bezpieczeństwa mającymi na celu zabezpieczenie dostępności, autentyczności, integralności lub poufności przechowywanych, przekazywanych lub przetwarzanych danych, lub funkcji lub usług oferowanych lub dostępnych za pośrednictwem tych produktów, usług i procesów w trakcie ich całego cyklu życia. Potwierdza on ponadto, że usługi zarządzane w zakresie bezpieczeństwa, które oceniono zgodnie z tymi programami, są zgodne z określonymi wymogami bezpieczeństwa mającymi na celu zabezpieczenie dostępności, autentyczności, integralności i poufności danych, do których uzyskuje się dostęp, lub 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 fachowej i doświadczenia przez personel o wystarczającym i odpowiednim poziomie odpowiedniej wiedzy technicznej i uczciwości zawodowej.”;

6) w art. 47 wprowadza się następujące zmiany:

a) ust. 2 otrzymuje brzmienie:

„2. Unijny kroczący program prac zawiera w szczególności wykaz produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa lub ich kategorii, które mają możliwość korzystania z włączenia w zakres stosowania danego europejskiego programu certyfikacji cyberbezpieczeństwa.”;

b) ust. 3 otrzymuje brzmienie:

(i) wyrażenie wprowadzające otrzymuje brzmienie:

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

(ii) lit. a) otrzymuje brzmienie:

„a) dostępność 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;”;

(iii) dodaje się literę w brzmieniu:

„ca) zmiany technologiczne oraz dostępność i rozwój międzynarodowych programów certyfikacji cyberbezpieczeństwa oraz norm międzynarodowych i norm stosowanych przez przemysł;”;

7) w art. 49 wprowadza się następujące zmiany:

a) ust. 1– 4 otrzymują brzmienie:

„1. Po otrzymaniu wniosku Komisji na podstawie art. 48 ENISA przygotowuje propozycję programu spełniającego mające zastosowanie wymogi określone w art. 51, 51a, 52 i 54.

2. Po otrzymaniu wniosku ECCG na podstawie art. 48 ust. 2 ENISA może przygotować propozycję programu spełniającego mające zastosowanie wymogi określone w art. 51, 51a, 52 i 54. Jeżeli ENISA odmawia uwzględnienia takiego wniosku, uzasadnia swoją odmowę. Każdą decyzję o odmowie uwzględnienia wniosku podejmuje Zarząd.

3. Przygotowując propozycję programu, ENISA konsultuje się w odpowiednim czasie ze wszystkimi odpowiednimi interesariuszami w drodze formalnego, otwartego, przejrzystego i integracyjnego procesu konsultacji. Przekazując Komisji propozycję programu zgodnie z ust. 6, ENISA przekazuje informacje na temat sposobu, w jaki wypełniła obowiązki przewidziane w niniejszym ustępie.

4. Dla każdej propozycji programu ENISA ustanawia grupę roboczą ad hoc zgodnie z art. 20 ust. 4, której celem jest służenie ENISA doradztwem i wiedzą fachową. Grupy robocze ad hoc, w stosownych przypadkach oraz bez uszczerbku dla procedur i uprawnień dyskrecjonalnych przewidzianych w art. 20 ust. 4, obejmują ekspertów z administracji publicznej państw członkowskich, instytucji, organów i jednostek organizacyjnych Unii oraz sektora prywatnego.”;

b) ust. 7 otrzymuje brzmienie:

„7. Komisja, w oparciu o propozycję programu przygotowaną przez ENISA, może przyjmować akty wykonawcze ustanawiające europejski program certyfikacji cyberbezpieczeństwa dotyczący produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa spełniający odpowiednie wymogi określone w art. 51, 51a, 52 i 54. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 66 ust. 2.”;

8) dodaje się artykuł w brzmieniu:

„*Artykuł 49a*
Informacje i konsultacje dotyczące europejskich programów certyfikacji cyberbezpieczeństwa

1. Komisja podaje do wiadomości publicznej informacje dotyczące swoich wniosków do ENISA o przygotowanie propozycji programu lub o przegląd istniejącego europejskiego programu certyfikacji cyberbezpieczeństwa, o których mowa w art. 48.

2. Podczas przygotowywania przez ENISA propozycji programu zgodnie z art. 49 Parlament Europejski lub Rada mogą zwrócić się do Komisji – jako organu przewodniczącego ECCG – oraz do ENISA o przedstawianie co kwartał odpowiednich informacji dotyczących projektu propozycji programu. Na wniosek Parlamentu Europejskiego lub Rady ENISA, w porozumieniu z Komisją oraz bez uszczerbku dla art. 27, może udostępnić Parlamentowi Europejskiemu i Radzie odpowiednie części projektu propozycji programu w sposób adekwatny do wymaganego poziomu poufności, a w stosownych przypadkach w ograniczonym zakresie.

3. Aby wzmocnić dialog między instytucjami Unii oraz wnieść wkład w formalny, otwarty, przejrzysty i inkluzywny proces konsultacji, Parlament Europejski lub Rada mogą zaprosić Komisję i ENISA do przedyskutowania kwestii dotyczących funkcjonowania europejskich programów certyfikacji cyberbezpieczeństwa dotyczących produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa.

4. Oceniając niniejsze rozporządzenie zgodnie z art. 67, Komisja uwzględnia w stosownych przypadkach elementy wynikające z opinii wyrażonych przez Parlament Europejski i przez Radę na temat kwestii, o których mowa w ust. 3 niniejszego artykułu.”;

9) 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) wyrażenie wprowadzające otrzymuje brzmienie:

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

10) 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 osiągać – w stosownych przypadkach – co najmniej następujące cele bezpieczeństwa:

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

b) aby dostawca stosował odpowiednie procedury wewnętrzne w celu zapewnienia, aby usługi zarządzane w zakresie bezpieczeństwa były zawsze świadczone przy zachowaniu wystarczającego i odpowiedniego poziomu jakości;

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

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

e) aby uprawnione osoby, programy lub maszyny miały możliwość dostępu tylko do tych danych, usług lub funkcji, do których mają prawa dostępu;

f) aby prowadzono rejestr danych, usług lub funkcji, do których uzyskano dostęp, które wykorzystano lub przetwarzano w inny sposób, kiedy to miało miejsce i kto tego dokonał, oraz aby rejestr ten był dostępny do oceny;

g) aby produkty ICT, usługi ICT i procesy ICT wdrażane w ramach świadczenia usług zarządzanych w zakresie bezpieczeństwa były bezpieczne zgodnie z zasadą bezpieczeństwa w fazie projektowania i bezpieczeństwa domyślnego oraz aby w stosownych przypadkach obejmowały najnowsze aktualizacje zabezpieczeń i nie zawierały powszechnie znanych podatności.”;

11) w art. 52 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Europejski program certyfikacji cyberbezpieczeństwa może przewidywać jeden lub większą liczbę 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«, muszą zapewniać uzasadnione zaufanie, że produkty ICT, usługi ICT, procesy ICT lub 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«, musi zapewniać uzasadnione zaufanie, że produkty ICT, usługi ICT, procesy ICT lub 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«, musi zapewniać uzasadnione zaufanie, że produkty ICT, usługi ICT, procesy ICT lub 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 znacznymi 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, nowoczesne funkcjonalności bezpieczeństwa; 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.”;

12) 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 lub 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 wyznaczonemu zgodnie z art. 58, unijną deklarację zgodności, dokumentację techniczną oraz wszelkie inne istotne informacje związane ze zgodnością produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa z programem. Kopię unijnej deklaracji zgodności przedkłada się krajowemu organowi ds. certyfikacji cyberbezpieczeństwa i ENISA.”;

13) 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 lub usług zarządzanych w zakresie bezpieczeństwa;”;

b) lit. g) otrzymuje brzmienie:

„g) szczegółowe kryteria oceny i metody, w tym rodzaje oceny, stosowane w celu wykazania, że zostały osiągnięte mające zastosowanie cele w zakresie bezpieczeństwa, o których mowa w art. 51 i 51a;”;

c) lit. j) otrzymuje brzmienie:

„j) zasady monitorowania zgodności produktów ICT, usług ICT, procesów ICT lub 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;”;

d) lit. l) otrzymuje brzmienie:

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

e) 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 lub usług zarządzanych w zakresie bezpieczeństwa, wymogów bezpieczeństwa, kryteriów i metod oceny oraz poziomów uzasadnienia zaufania;”;

f) 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;”;

14) w art. 56 wprowadza się następujące zmiany:

a) ust. 1 otrzymuje brzmienie:

„1. Domniemywa 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 regularnie ocenia skuteczność i użyteczność przyjętych europejskich programów certyfikacji cyberbezpieczeństwa oraz to, czy określony europejski program certyfikacji cyberbezpieczeństwa należy uczynić obowiązkowym za pomocą odpowiednich przepisów prawa Unii w celu zapewnienia w Unii odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT, procesów ICT oraz – od dnia... [data wejścia w życie niniejszego rozporządzenia zmieniającego] – usług zarządzanych w zakresie bezpieczeństwa, a także w celu poprawy funkcjonowania rynku wewnętrznego. Pierwszą taką ocenę przeprowadza się do dnia 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:

– 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;”;

– 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 na szczególne interesy i potrzeby MŚP, w tym mikroprzedsiębiorstw;”;

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 wyznaczonemu zgodnie z 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. Ten organ lub ta jednostka przekazuje bez zbędnej zwłoki te informacje zainteresowanemu krajowemu organowi ds. certyfikacji cyberbezpieczeństwa.”;

15) 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 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, będą nadal istnieć.

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.”;

16) 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 dotyczących ewentualnej niezgodności produktów ICT, usług ICT, procesów ICT lub 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 oraz 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.”;

17) 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 monitorowania 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);”;

18) art. 67 ust. 2 i 3 otrzymują brzmienie:

„2. Ocena dotyczy również wpływu, skuteczności i efektywności przepisów tytułu III niniejszego rozporządzenia, w tym procedur prowadzących do przyjęcia europejskich programów certyfikacji cyberbezpieczeństwa i ich bazy dowodowej, 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 ustalenie, czy w celu zapobieżenia wprowadzaniu na rynek wewnętrzny 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.”;

19) w załączniku wprowadza się zmiany określone w załączniku do niniejszego rozporządzenia.

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 / Przewodnicząca*

ZAŁĄCZNIK

W załączniku do rozporządzenia (UE) 2019/881 wprowadza się następujące zmiany:

1) pkt 2 do 5 otrzymują brzmienie:

„2. Jednostka oceniająca zgodność musi być stroną trzecią, niezależną od ocenianych przez nią organizacji lub produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa.

3. Za jednostkę oceniającą zgodność można uważać jednostkę należącą do organizacji przedsiębiorców lub zrzeszenia zawodowego reprezentujących przedsiębiorstwa zaangażowane w projektowanie, wytwarzanie, dostarczanie, montowanie, użytkowanie lub utrzymywanie ocenianych przez nią produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, pod warunkiem że wykazano jej niezależność i brak konfliktu interesów.

4. Jednostki oceniające zgodność, ich ścisłe kierownictwo oraz pracownicy odpowiedzialni za realizację zadań z zakresu oceny zgodności nie mogą być projektantami, wytwórcami, dostawcami, instalatorami, nabywcami, właścicielami, użytkownikami ani osobami odpowiedzialnymi za utrzymanie produktu ICT, usługi ICT, procesu ICT lub usługi zarządzanej w zakresie bezpieczeństwa będących przedmiotem oceny, ani upoważnionymi przedstawicielami którejkolwiek z wymienionych stron. Zakaz ten nie wyklucza wykorzystywania ocenianych produktów ICT, które są niezbędne do prowadzenia działalności przez jednostkę oceniającą zgodność, lub wykorzystywania takich produktów ICT do celów osobistych.

5. Jednostki oceniające zgodność, ich ścisłe kierownictwo oraz pracownicy odpowiedzialni za wykonywanie zadań z zakresu oceny zgodności nie mogą być bezpośrednio zaangażowani w projektowanie, wytwarzanie ani konstruowanie, świadczenie, wprowadzanie do obrotu, instalację lub użytkowanie ani być osobami odpowiedzialnymi za utrzymanie produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa będących przedmiotem oceny, ani reprezentować stron zaangażowanych w taką działalność. Jednostki oceniające zgodność, ich ścisłe kierownictwo oraz pracownicy odpowiedzialni za realizację zadań z zakresu oceny zgodności nie mogą angażować się w jakąkolwiek działalność, która może zagrozić niezależności ich osądów lub uczciwości w odniesieniu do podejmowanych przez nich czynności z zakresu oceny zgodności. Zakaz ten ma w szczególności zastosowanie do usług konsultingowych.”;

2) w pkt 10 wprowadza się następujące zmiany:

a) wyrażenie wprowadzające otrzymuje brzmienie:

„10. Przez cały czas i w odniesieniu do każdej procedury oceny zgodności oraz do każdego rodzaju, każdej kategorii lub podkategorii produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa, jednostka oceniająca zgodność musi dysponować niezbędnymi:”;

b) lit. c) otrzymuje brzmienie:

„c) procedurami dotyczącymi prowadzenia działalności, które w należytym stopniu uwzględniają wielkość przedsiębiorstwa, sektor, w którym ono działa, strukturę przedsiębiorstwa, stopień złożoności technologii danego produktu ICT, danej usługi ICT, danego procesu ICT lub danej usługi zarządzanej w zakresie bezpieczeństwa oraz masowy lub seryjny charakter procesu produkcyjnego.”;

3) pkt 19 i 20 otrzymują brzmienie:

„19. Jednostki oceniające zgodność muszą spełniać wymogi odpowiedniej normy zharmonizowanej, zdefiniowanej w art. 2 pkt 9 rozporządzenia (WE) nr 765/2008, dotyczącej akredytacji jednostek oceniających zgodność dokonujących certyfikacji produktów ICT, usług ICT, procesów ICT lub usług zarządzanych w zakresie bezpieczeństwa.

20. Jednostki oceniające zgodność zapewniają, aby wykorzystywane do celów oceny zgodności laboratoria przeprowadzające testy spełniały wymogi odpowiedniej normy zharmonizowanej, zdefiniowanej w art. 2 pkt 9 rozporządzenia (WE) nr 765/2008, dotyczącej akredytacji laboratoriów przeprowadzających testy.”.

W odniesieniu do niniejszego aktu wydane zostało oświadczenie, które zostało opublikowane w ... [Dz.U.: proszę podać Dz.U. C XXX, XX.XX.2024, s. XX] oraz pod następującym adresem internetowym:... [Dz.U.: proszę wstawić link do oświadczenia].