KOMISJA
EUROPEJSKA

Strasburg, dnia 18.4.2023 r.
COM(2023) 208 final

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)

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Niniejsze uzasadnienie towarzyszy wnioskowi dotyczącemu rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (UE) 2019/881[1] w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa

Proponowana ukierunkowana zmiana ma na celu umożliwienie, w drodze aktów wykonawczych Komisji, przyjmowania europejskich programów certyfikacji cyberbezpieczeństwa w odniesieniu do „usług zarządzanych w zakresie bezpieczeństwa", oprócz produktów opartych na technologiach informacyjno-komunikacyjnych (ICT), usług ICT i procesów ICT, które są już objęte aktem o cyberbezpieczeństwie. Usługi zarządzane w zakresie bezpieczeństwa odgrywają coraz większą rolę w zapobieganiu cyberincydentom i ograniczaniu ich skutków.

W konkluzjach z dnia 23 maja 2022 r.[2] o rozwijaniu pozycji Unii Europejskiej w kwestiach cyberprzestrzeni Rada wezwała Unię i jej państwa członkowskie do zintensyfikowania starań na rzecz zwiększenia ogólnego poziomu cyberbezpieczeństwa, na przykład poprzez ułatwianie powstawania zaufanych dostawców usług w zakresie cyberbezpieczeństwa, oraz podkreśliła, że wspieranie rozwoju takich dostawców powinno stanowić priorytet polityki przemysłowej Unii w dziedzinie cyberbezpieczeństwa. Rada zwróciła się również do Komisji o przedstawienie możliwości wspierania powstawania branży zaufanych usług w zakresie cyberbezpieczeństwa. Certyfikacja usług zarządzanych w zakresie bezpieczeństwa jest skutecznym sposobem budowania zaufania do jakości tych usług, a tym samym sprzyja powstaniu europejskiej branży zaufanych usług w zakresie cyberbezpieczeństwa.

We wspólnym komunikacie „Polityka UE w zakresie cyberobrony", przyjętym przez Komisję i wysokiego przedstawiciela w dniu 10 listopada 2022 r.[3], zapowiedziano, że Komisja zbada możliwości tworzenia na szczeblu UE programów certyfikacji cyberbezpieczeństwa dla branży cyberbezpieczeństwa oraz prywatnych przedsiębiorstw. Dostawcy usług zarządzanych w zakresie bezpieczeństwa będą również odgrywać ważną rolę w unijnej rezerwie cyberbezpieczeństwa, której stopniowe tworzenie jest wspierane w ramach aktu w sprawie cybersolidarności, zaproponowanego wraz z niniejszym rozporządzeniem. 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 przywracania normalnego działania po wystąpieniu takich incydentów. Odpowiednie usługi w zakresie cyberbezpieczeństwa świadczone przez „zaufanych dostawców", o których mowa w akcie w sprawie cybersolidarności, odpowiadają „usługom zarządzanym w zakresie bezpieczeństwa", o których mowa w niniejszym wniosku.

Niektóre państwa członkowskie zaczęły już przyjmować programy certyfikacji dotyczące usług zarządzanych w zakresie bezpieczeństwa. W związku z tym rośnie ryzyko rozdrobnienia rynku wewnętrznego usług zarządzanych w zakresie bezpieczeństwa z powodu braku spójności programów certyfikacji cyberbezpieczeństwa w całej Unii. Niniejszy wniosek

---

[1] 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] 9364/22.

[3] JOIN(2022) 49 final.

umożliwia tworzenie europejskich programów certyfikacji cyberbezpieczeństwa w odniesieniu do wspomnianych usług, aby zapobiec takiemu rozdrobnieniu.

- **Spójność z przepisami obowiązującymi w tej dziedzinie polityki**

Niniejszy wniosek jest spójny z aktem o cyberbezpieczeństwie, który zmienia. .Opiera się on na przepisach tego rozporządzenia i dostosowuje je w taki sposób, aby obejmowały również usługi zarządzane w zakresie bezpieczeństwa. Proponowane zmiany są ograniczone do tego, co jest absolutnie konieczne, i nie powodują zmiany charakterystyki ani funkcjonowania aktu o cyberbezpieczeństwie.

Niniejszy wniosek jest ponadto zgodny z dyrektywą 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, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2)[4]. Zgodnie z dyrektywą (UE) 2022/2555 dostawcy usług zarządzanych w zakresie bezpieczeństwa są uznawani za kluczowe lub ważne podmioty należące do sektora kluczowego. Motyw 86 tej dyrektywy stanowi, że 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.

Niniejszy wniosek ma na celu poprawę jakości usług zarządzanych w zakresie bezpieczeństwa oraz zwiększenie ich porównywalności. Tym samym umożliwia on podmiotom kluczowym i ważnym dochowanie szczególnej staranności przy wyborze dostawcy usług zarządzanych w zakresie bezpieczeństwa zgodnie z wymogami dyrektywy (UE) 2022/2555. Co więcej, definicja „usług zarządzanych w zakresie bezpieczeństwa" przedstawiona w niniejszym wniosku opiera się na definicji „dostawców usług zarządzanych w zakresie bezpieczeństwa" zawartej w dyrektywie (UE) 2022/2555 i jest do niej bardzo podobna. Z tych powodów niniejszy wniosek jest w dużym stopniu komplementarny wobec dyrektywy NIS 2.

Jest on ponadto komplementarny wobec proponowanego aktu w sprawie cybersolidarności. W proponowanym akcie w sprawie cybersolidarności przewiduje się proces wyboru dostawców w celu utworzenia unijnej rezerwy cyberbezpieczeństwa, który to proces powinien między innymi uwzględniać, czy dostawcy ci uzyskali europejski lub krajowy certyfikat cyberbezpieczeństwa. Przyszłe programy certyfikacji usług zarządzanych w zakresie bezpieczeństwa będą więc odgrywały istotną rolę we wdrażaniu aktu w sprawie cybersolidarności.

- **Spójność z innymi politykami Unii**

Niniejszy wniosek nie ma wpływu na zgodność aktu o cyberbezpieczeństwie z rozporządzeniem (UE) 2016/679 (ogólne rozporządzenie o ochronie danych, „RODO")[5] i jego przepisami dotyczącymi ustanawiania mechanizmów certyfikacji oraz znaków jakości

[4] Dz.U. L 333 z 27.12.2022, s. 810.
[5] Dz.U. L 119 z 4.5.2016, s. 1.

i oznaczeń w zakresie ochrony danych osobowych mających świadczyć o zgodności z niniejszym rozporządzeniem operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające. Przepisy aktu o cyberbezpieczeństwie pozostają bez uszczerbku dla certyfikacji operacji przetwarzania danych, także wówczas, gdy takie operacje są wbudowane w produkty i usługi, zgodnie z RODO.

Niniejszy wniosek nie ma ponadto wpływu na zgodność aktu o cyberbezpieczeństwie z rozporządzeniem (WE) nr 765/2008 w sprawie wymagań w zakresie akredytacji i nadzoru rynku[6], w szczególności w odniesieniu do ram dotyczących krajowych jednostek akredytujących i jednostek oceniających zgodność oraz krajowych organów nadzorczych ds. certyfikacji.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

• Podstawa prawna

Niniejszy wniosek zmienia akt o cyberbezpieczeństwie, którego podstawę stanowi art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Podobnie jak w przypadku aktu o cyberbezpieczeństwie niniejszy wniosek ma na celu uniknięcie rozdrobnienia rynku wewnętrznego, mianowicie poprzez zapewnienie możliwości przyjmowania europejskich programów certyfikacji cyberbezpieczeństwa dotyczących usług zarządzanych w zakresie bezpieczeństwa. Państwa członkowskie zaczęły już przyjmować krajowe programy certyfikacji usług zarządzanych w zakresie bezpieczeństwa. W związku z tym istnieje konkretne ryzyko rozdrobnienia rynku wewnętrznego tych usług, które to ryzyko niniejszy wniosek ma na celu wyeliminować. W związku z tym odpowiednią podstawą prawną tej inicjatywy jest art. 114 TFUE.

• Pomocniczość (w przypadku kompetencji niewyłącznych)

Celu, jakim jest zapewnienie możliwości przyjmowania europejskich programów certyfikacji cyberbezpieczeństwa dotyczących usług zarządzanych w zakresie bezpieczeństwa oraz uniknięcie rozdrobnienia rynku wewnętrznego, nie można osiągnąć na poziomie krajowym, lecz wyłącznie na poziomie Unii. Co więcej, usługi zarządzane w zakresie bezpieczeństwa, które są przedmiotem proponowanej nowelizacji, oferują dostawcy działający w całej Unii, gdzie również znajdują się ich najwięksi potencjalni klienci. W związku z tym działanie na poziomie Unii jest jednocześnie konieczne i bardziej skuteczne niż działanie na poziomie krajowym.

• Proporcjonalność

Niniejszy wniosek ma na celu ukierunkowaną zmianę aktu o cyberbezpieczeństwie. Jest on ograniczony do tego, co jest bezwzględnie konieczne do osiągnięcia jego celu, jakim jest umożliwienie przyjmowania europejskich programów certyfikacji cyberbezpieczeństwa dotyczących usług zarządzanych w zakresie bezpieczeństwa, obok tego rodzaju programów dotyczących produktów ICT, usług ICT i procesów ICT. Proponowane zmiany polegają w szczególności na dostosowaniu zakresu europejskich ram certyfikacji cyberbezpieczeństwa w celu uwzględnienia „usług zarządzanych w zakresie bezpieczeństwa”, wprowadzeniu definicji tych usług zgodnie z dyrektywą NIS 2 oraz zmianie celów bezpieczeństwa europejskich programów certyfikacji cyberbezpieczeństwa, aby uwzględnić w nich „usługi zarządzane w zakresie bezpieczeństwa”. Pozostałe zmiany mają charakter techniczny i mają na celu zapewnienie, aby odpowiednie artykuły miały zastosowanie również do „usług

[6] Dz.U. L 218 z 13.8.2008, s. 30.

zarządzanych w zakresie bezpieczeństwa”. Proponowana inicjatywa jest zatem proporcjonalna do zamierzonego celu.

- **Wybór instrumentu**

Ponieważ niniejszy wniosek zmienia rozporządzenie (UE) 2019/881, właściwym instrumentem prawnym jest rozporządzenie.

3. WYNIKI OCEN *EX POST,* KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

- **Oceny *ex post*/oceny adekwatności obowiązującego prawodawstwa**

Nie dotyczy.

- **Konsultacje z zainteresowanymi stronami**

Przeprowadzono ukierunkowane konsultacje z państwami członkowskimi i ENISA. W ramach tych konsultacji państwa członkowskie przedstawiły swoje obecne działania i opinie dotyczące certyfikacji usług zarządzanych w zakresie bezpieczeństwa. ENISA przedstawiła swoje poglądy i ustalenia z dyskusji z państwami członkowskimi i zainteresowanymi stronami. Uwagi i informacje otrzymane od państw członkowskich i ENISA uwzględniono w niniejszym wniosku.

- **Gromadzenie i wykorzystanie wiedzy specjalistycznej**

Nie dotyczy.

- **Ocena skutków**

Zwrócono się o zwolnienie z konieczności przeprowadzenia oceny skutków, ponieważ wniosek stanowi bardzo ograniczoną i ukierunkowaną zmianę aktu o cyberbezpieczeństwie. Na podstawie tej zmiany Komisja byłaby upoważniona do przyjmowania, w drodze aktów wykonawczych, programów certyfikacji dotyczących „usług zarządzanych w zakresie bezpieczeństwa”, obok tego rodzaju programów dotyczących produktów ICT, usług ICT i procesów ICT, które są już objęte wspomnianym aktem. Zmiana ta wywoła jednak skutki dopiero wówczas, gdy takie programy certyfikacji zostaną przyjęte w późniejszym czasie. Co więcej, przedmiotowa zmiana nie będzie mieć wpływu na dobrowolny charakter programów certyfikacji.

- **Sprawność regulacyjna i uproszczenie**

Nie dotyczy.

- **Prawa podstawowe**

Wniosek nie ma żadnych przewidywalnych skutków dla ochrony praw podstawowych.

4. WPŁYW NA BUDŻET

Brak.

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Przepisy, które mają zostać zmienione wnioskiem, zostaną ocenione w ramach okresowej oceny aktu o cyberbezpieczeństwie, którą Komisja przeprowadzi zgodnie z jego art. 67. Ocena dotyczy m.in. wpływu, skuteczności i efektywności przepisów ram certyfikacji cyberbezpieczeństwa w odniesieniu do celów, którymi są zapewnienie odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT w Unii oraz poprawa funkcjonowania rynku wewnętrznego. Niniejszy wniosek przewiduje zmianę, dzięki której ocena obejmie również usługi zarządzane w zakresie bezpieczeństwa. Komisja przesyła również sprawozdanie z oceny i wnioski z oceny Parlamentowi Europejskiemu, Radzie oraz Zarządowi ENISA oraz podaje do wiadomości publicznej ustalenia zawarte w sprawozdaniu.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

Wniosek zawiera dwa artykuły. W art. 1 przedstawiono zmiany w rozporządzeniu (UE) 2019/881, natomiast art. 2 dotyczy wejścia w życie. Art. 1 zawiera ukierunkowane zmiany służące dostosowaniu zakresu europejskich ram certyfikacji cyberbezpieczeństwa w celu uwzględnienia „usług zarządzanych w zakresie bezpieczeństwa” w akcie o cyberbezpieczeństwie (art. 1 i 46 aktu o cyberbezpieczeństwie). Wprowadza się w nim definicję tych usług, która jest bardzo zbliżona do definicji „dostawców usług zarządzanych w zakresie bezpieczeństwa” zawartej w dyrektywie NIS 2 (art. 2 aktu o cyberbezpieczeństwie). Dodaje się również nowy art. 51a dotyczący celów bezpieczeństwa europejskich programów certyfikacji cyberbezpieczeństwa uwzględniających „usługi zarządzane w zakresie bezpieczeństwa”. Pozostałe zmiany mają charakter techniczny i mają na celu zapewnienie, aby odpowiednie artykuły miały zastosowanie również do „usług zarządzanych w zakresie bezpieczeństwa”.

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,

uwzględniając opinię Komitetu Regionów,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881[7] utworzono ramy ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa produktów ICT, usług ICT i procesów ICT w Unii oraz w celu uniknięcia rozdrobnienia rynku wewnętrznego w zakresie programów certyfikacji cyberbezpieczeństwa w Unii.

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

[7] 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).

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

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, 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.

(5) Poza wdrażaniem produktów ICT, usług ICT lub procesów ICT usługi zarządzane w zakresie bezpieczeństwa często zapewniają dodatkowe funkcje usługowe, które opierają się na kompetencjach, wiedzy fachowej i doświadczeniu personelu. Bardzo wysoki poziom kompetencji, wiedzy fachowej i doświadczenia, a także odpowiednie procedury wewnętrzne powinny wchodzić w zakres celów bezpieczeństwa, aby zapewnić bardzo wysoką jakość świadczonych usług zarządzanych w zakresie bezpieczeństwa. W celu zapewnienia, aby wszystkie aspekty usług zarządzanych w zakresie bezpieczeństwa mogły być objęte programem certyfikacji, konieczna jest zatem zmiana rozporządzenia (UE) 2019/881.

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

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

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 polegającą na prowadzeniu lub wspomaganiu działań związanych z zarządzaniem ryzykiem w cyberprzestrzeni, takich jak reagowanie na incydenty, 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.

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;

d) zmiany w zakresie profilu cyberzagrożeń;

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

7) art. 49 ust. 7 otrzymuje brzmienie:

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

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 [oraz sprzęt komputerowy] wdrażane w ramach świadczenia usług zarządzanych w zakresie bezpieczeństwa były bezpieczne zgodnie z zasadą, która stanowi, że kwestie bezpieczeństwa uwzględnia się domyślnie i już na etapie projektowania, oraz aby te produkty, usługi i procesy [oraz sprzęt komputerowy] nie zawierały znanych podatności i obejmowały najnowsze aktualizacje zabezpieczeń.";

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 na MŚP;”;

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 wykonawczym przyjętym na podstawie art. 49 ust. 7. Krajowe programy certyfikacji cyberbezpieczeństwa i powiązane z nimi procedury dotyczące produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa, które nie są objęte europejskim programem certyfikacji cyberbezpieczeństwa, funkcjonują nadal.

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 obwiązki;”;

(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);”;

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

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

3. Ocena obejmuje również 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.”.

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 Strasburgu dnia r.

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