



2024/3143

19.12.2024

**ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2024/3143**

**z dnia 18 grudnia 2024 r.**

**ustanawiające okoliczności, formaty i procedury dotyczące notyfikacji zgodnie z art. 61 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych**

**(Tekst mający znaczenie dla EOG)**

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając 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 uchylecia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) <sup>(1)</sup>, w szczególności jego art. 61 ust. 5,

a także mając na uwadze, co następuje:

- (1) Zgodnie z art. 61 ust. 1 rozporządzenia (UE) 2019/881 (akt o cyberbezpieczeństwie) krajowe organy ds. certyfikacji cyberbezpieczeństwa notyfikują Komisji jednostki oceniające zgodność, które zostały akredytowane i którym, w stosownych przypadkach, udzielono zezwolenia na wydawanie europejskich certyfikatów cyberbezpieczeństwa na określonych poziomach uzasadnienia zaufania, przy czym notyfikacja ta powinna być aktualizowana. Ponadto zgodnie z art. 61 ust. 2 rozporządzenia (UE) 2019/881 Komisja jest zobowiązana opublikować w *Dzienniku Urzędowym Unii Europejskiej* wykaz jednostek oceniających zgodność notyfikowanych w ramach europejskiego programu certyfikacji cyberbezpieczeństwa rok po jego wejściu w życie. Aby zapewnić zharmonizowane podejście do notyfikacji i ułatwić krajowym organom ds. certyfikacji cyberbezpieczeństwa ten proces, w niniejszym rozporządzeniu należy doprecyzować okoliczności, formaty i procedury dotyczące notyfikacji. Aspekty te należy wyjaśnić z myślą o stosowaniu pierwszego europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC), ustanowionego rozporządzeniem wykonawczym Komisji (UE) 2024/482 <sup>(2)</sup>.
- (2) Niniejsze rozporządzenie uznaje synergii między rozporządzeniem (UE) 2019/881 a odpowiednim unijnym prawodawstwem harmonizacyjnym, w tym rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2024/2847 (akt dotyczący cyberodporności) <sup>(3)</sup>. Proponuje się zatem, aby krajowe organy ds. certyfikacji cyberbezpieczeństwa notyfikowały Komisję za pośrednictwem elektronicznego narzędzia notyfikacji, opracowanego i zarządzanego przez Komisję, o którym mowa w decyzji Parlamentu Europejskiego i Rady nr 768/2008/WE <sup>(4)</sup>. Nie naruszając spoczywającego na Komisji obowiązku publikowania wykazu notyfikowanych jednostek oceniających zgodność w *Dzienniku Urzędowym Unii Europejskiej*, wykaz ten powinien być również publicznie dostępny w elektronicznym narzędziu notyfikacji opracowanym i zarządzanym przez Komisję.

<sup>(1)</sup> Dz.U. L 151 z 7.6.2019, s. 15, ELI: <http://data.europa.eu/eli/reg/2019/881/oj>.

<sup>(2)</sup> Rozporządzenie wykonawcze Komisji (UE) 2024/482 z dnia 31 stycznia 2024 r. ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do przyjęcia europejskiego programu certyfikacji cyberbezpieczeństwa opartego na wspólnych kryteriach (EUCC) (Dz.U. L, 2024/482, 7.2.2024, ELI: [http://data.europa.eu/eli/reg\\_impl/2024/482/oj](http://data.europa.eu/eli/reg_impl/2024/482/oj)).

<sup>(3)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/2847 z dnia 23 października 2024 r. 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. L, 2024/2847, 20.11.2024, ELI: <http://data.europa.eu/eli/reg/2024/2847/oj>).

<sup>(4)</sup> Decyzja Parlamentu Europejskiego i Rady nr 768/2008/WE z dnia 9 lipca 2008 r. w sprawie wspólnych ram dotyczących wprowadzania produktów do obrotu, uchylająca decyzję Rady 93/465/EWG (Dz.U. L 218 z 13.8.2008, s. 82, ELI: [http://data.europa.eu/eli/dec/2008/768\(1\)/oj](http://data.europa.eu/eli/dec/2008/768(1)/oj)).

- (3) Notyfikacja jednostek oceniających zgodność, które zostały akredytowane i którym, w stosownych przypadkach, udzielono zezwolenia, oznacza, że jednostkom tym można zaufać w odniesieniu do prowadzenia działań w zakresie oceny i certyfikacji zgodnie z rozporządzeniem (UE) 2019/881, co przyczynia się do ogólnej reputacji europejskich programów certyfikacji cyberbezpieczeństwa. Zasadnicze znaczenie ma zatem zapewnienie, aby notyfikowane jednostki oceniające zgodność spełniały wymagania i wypełniały swoje obowiązki z biegiem czasu. Opublikowany wykaz notyfikowanych jednostek oceniających zgodność powinien być dokładny i aktualny, i odzwierciedlać ich zgodność z wymogami określonymi w rozporządzeniu (UE) 2019/881 oraz, w stosownych przypadkach, ze szczegółowymi lub dodatkowymi wymogami w ramach europejskiego programu certyfikacji cyberbezpieczeństwa. W tym celu konieczne jest, aby krajowe organy ds. certyfikacji cyberbezpieczeństwa bez zbędnej zwłoki powiadamiały Komisję o wszelkich zmianach w notyfikacji, zgodnie z art. 61 ust. 1 rozporządzenia (UE) 2019/881.
- (4) Krajowe organy ds. certyfikacji cyberbezpieczeństwa są odpowiedzialne za zapewnienie zgodności jednostek oceniających zgodność z rozporządzeniem (UE) 2019/881 i europejskimi programami certyfikacji cyberbezpieczeństwa oraz za zapewnienie w tym kontekście dokładności notyfikacji. Działania te podlegają wzajemnym przeglądom, których wynik powinien pomóc w określeniu wszelkich niezbędnych zmian w celu zwiększenia ich skuteczności. W wyniku zgłoszenia obaw w różnych okolicznościach krajowe organy ds. certyfikacji cyberbezpieczeństwa mogą stwierdzić, że jednostka oceniająca zgodność przestała spełniać odpowiednie wymagania. W stosownych przypadkach ustalenia wynikające z mechanizmów wzajemnego przeglądu powinny pomagać krajowym organom ds. certyfikacji cyberbezpieczeństwa w monitorowaniu ciągłości kompetencji notyfikowanych jednostek oceniających zgodność. Ponadto inne krajowe organy ds. certyfikacji cyberbezpieczeństwa, Komisja lub zainteresowane strony mogą zgłaszać do notyfikującego krajowego organu ds. certyfikacji cyberbezpieczeństwa obawy dotyczące ciągłości kompetencji notyfikowanych jednostek oceniających zgodność.
- (5) Podejmując decyzję o zawieszeniu, ograniczeniu lub wycofaniu notyfikacji jednostki oceniającej zgodność, notyfikujący krajowy organ ds. certyfikacji cyberbezpieczeństwa ma współpracować z krajową jednostką akredytującą wyznaczoną na podstawie rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008<sup>(3)</sup>. Jest to zgodne z rozporządzeniem (UE) 2019/881, które stanowi, że krajowe organy ds. certyfikacji cyberbezpieczeństwa powinny aktywnie pomagać krajowym jednostkom akredytującym, wspierać je i współpracować z nimi w swoich działaniach monitorujących i nadzorczych. Ograniczenie notyfikacji powinno odnosić się do przypadku, w którym zakres akredytacji lub, w stosownych przypadkach, zakres zezwolenia i w związku z tym – notyfikacji – został zmniejszony.
- (6) Zgodnie z art. 54 ust. 1 lit. n) rozporządzenia (UE) 2019/881 każdy europejski program certyfikacji cyberbezpieczeństwa musi zawierać, w stosownych przypadkach, zasady dotyczące przechowywania dokumentów przez jednostki oceniające zgodność. Konieczne jest zatem, aby w przypadku ograniczenia, zawieszenia lub wycofania notyfikacji, lub w przypadku zaprzestania działalności przez notyfikowaną jednostkę oceniającą zgodność notyfikujący krajowy organ ds. certyfikacji cyberbezpieczeństwa zapewnił, aby dokumentacja tej jednostki oceniającej zgodność była przechowywana w sposób bezpieczny i przez niezbędny okres, zgodnie z wymogami europejskiego programu certyfikacji cyberbezpieczeństwa.
- (7) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na mocy art. 66 rozporządzenia (UE) 2019/881,

<sup>(3)</sup> Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30, ELI: <http://data.europa.eu/eli/reg/2008/765/oj>).

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

#### Artykuł 1

##### **Przedmiot**

W niniejszym rozporządzeniu ustanawia się okoliczności, formaty i procedury dotyczące notyfikacji jednostek oceniających zgodność przez krajowe organy ds. certyfikacji cyberbezpieczeństwa zgodnie z art. 61 ust. 1 rozporządzenia (UE) 2019/881.

#### Artykuł 2

##### **Procedury dotyczące notyfikacji**

1. Zgodnie z art. 61 ust. 1 rozporządzenia (UE) 2019/881 krajowe organy ds. certyfikacji cyberbezpieczeństwa notyfikują Komisji jednostki oceniające zgodność, które spełniły wymogi określone w rozporządzeniu (UE) 2019/881 oraz, w stosownych przypadkach, szczegółowe lub dodatkowe wymogi w ramach europejskiego programu certyfikacji cyberbezpieczeństwa.
2. Krajowy organ ds. certyfikacji cyberbezpieczeństwa notyfikuje Komisję za pomocą elektronicznego narzędzia notyfikacji opracowanego i zarządzanego przez Komisję, o którym mowa w decyzji nr 768/2008/WE.
3. Notyfikacja zawiera informacje wymienione w załączniku.

#### Artykuł 3

##### **Numery identyfikacyjne i wykaz jednostek oceniających zgodność**

1. Komisja przydziela notyfikowanej jednostce oceniającej zgodność numer identyfikacyjny. Przydziela ona jeden taki numer, nawet jeśli dana jednostka jest notyfikowana na podstawie kilku europejskich programów certyfikacji cyberbezpieczeństwa lub aktów Unii.
2. Udostępniając wykaz notyfikowanych jednostek oceniających zgodność za pomocą elektronicznego narzędzia notyfikacji opracowanego i zarządzanego przez Komisję, Komisja uwzględnia numery identyfikacyjne, które zostały przydzielone notyfikowanym jednostkom oceniającym zgodność, oraz rodzaje działalności, w związku z którymi zostały one notyfikowane.
3. ENISA udostępnia informacje dotyczące notyfikowanych jednostek oceniających zgodność na swojej specjalnej stronie internetowej poświęconej europejskim programom certyfikacji cyberbezpieczeństwa, o której mowa w art. 50 ust. 1 rozporządzenia (UE) 2019/881.

#### Artykuł 4

##### **Zmiany w notyfikacjach**

1. Krajowe organy ds. certyfikacji cyberbezpieczeństwa bez zbędnej zwłoki powiadamiają Komisję o wszelkich późniejszych zmianach w notyfikacji, o której mowa w art. 2, za pośrednictwem elektronicznego narzędzia notyfikacji opracowanego i zarządzanego przez Komisję, zgodnie z art. 61 ust. 1 rozporządzenia (UE) 2019/881.
2. W przypadku gdy krajowy organ ds. certyfikacji cyberbezpieczeństwa stwierdzi, że współpraca z krajową jednostką akredytującą, jak przewidziano w rozporządzeniu (UE) 2019/881, że notyfikowana jednostka oceniająca zgodność przestała spełniać wymagania lub obowiązki, którym podlega, krajowy organ ds. certyfikacji cyberbezpieczeństwa ogranicza, zawiesza lub cofa notyfikację, stosownie do sytuacji, w zależności od wagi niespełnienia tych wymagań lub niewypełnienia tych obowiązków. Powiadamia on o tym Komisję bez zbędnej zwłoki za pośrednictwem elektronicznego narzędzia notyfikacji opracowanego i zarządzanego przez Komisję.
3. W przypadku ograniczenia, zawieszenia lub wycofania notyfikacji lub w przypadku zaprzestania działalności przez notyfikowaną jednostkę oceniającą zgodność notyfikujący krajowy organ ds. certyfikacji cyberbezpieczeństwa podejmuje stosowne działania w celu zapewnienia, aby dokumentacja tej jednostki oceniającej zgodność była przechowywana w sposób bezpieczny i przez niezbędny okres, zgodnie z wymogami europejskiego programu certyfikacji cyberbezpieczeństwa.

*Artykuł 5***Wejście w życie**

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 Brukseli dnia 18 grudnia 2024 r.

W imieniu Komisji  
Przewodnicząca  
Ursula VON DER LEYEN

## ZAŁĄCZNIK

**Informacje, które należy uwzględnić w notyfikacji jednostki oceniającej zgodność w ramach europejskiego programu certyfikacji cyberbezpieczeństwa na podstawie art. 61 ust. 1 rozporządzenia (UE) 2019/881, o których mowa w art. 2 ust. 3 niniejszego rozporządzenia**

1. Informacje ogólne:
  - 1) Tytuł programu certyfikacji cyberbezpieczeństwa
  - 2) Poziom lub poziomy uzasadnienia zaufania, w stosownych przypadkach, oraz związane z nimi procedury oceny zgodności (np. podstawowy, istotny, wysoki)
  - 3) Zakres (np. zakres akredytacji, kategorie lub rodzaje produktów, usług, procesów)
2. Informacje na temat notyfikującego krajowego organu ds. certyfikacji cyberbezpieczeństwa:
  - 1) Nazwa
  - 2) Państwo
  - 3) Adres pocztowy
  - 4) Adres(-y) e-mail
  - 5) Numer(-y) telefonu
  - 6) Strona internetowa
3. Informacje dotyczące notyfikowanej jednostki oceniającej zgodność:
  - 1) Nazwa
  - 2) Państwo
  - 3) Adres pocztowy
  - 4) Adres(-y) e-mail
  - 5) Numer(-y) telefonu
  - 6) Strona internetowa
4. Informacje na temat akredytacji:
  - 1) Akredytacja:
    - a) Data akredytacji
    - b) Numer referencyjny akredytacji
    - c) Zakres akredytacji
    - d) Okres ważności akredytacji
  - 2) Krajowa jednostka akredytująca
    - a) Nazwa
    - b) Państwo
    - c) Adres pocztowy
    - d) Adres(-y) e-mail
    - e) Numer(-y) telefonu
    - f) Strona internetowa
5. Informacje dotyczące zezwolenia (w stosownych przypadkach):
  - 1) Zezwolenie:
    - a) Data udzielenia zezwolenia
    - b) Numer referencyjny zezwolenia
    - c) Zakres zezwolenia

- d) Okres ważności zezwolenia
  - 2) Krajowy organ ds. cyberbezpieczeństwa udzielający zezwolenia (jeżeli jest inny niż notyfikujący krajowy organ ds. certyfikacji cyberbezpieczeństwa):
    - a) Nazwa
    - b) Państwo
    - c) Adres pocztowy
    - d) Adres(-y) e-mail
    - e) Numer(-y) telefonu
    - f) Strona internetowa
  - 6. Informacje dodatkowe:
    - 1) Wszelkie dodatkowe informacje wymagane w konkretnym europejskim programie certyfikacji cyberbezpieczeństwa
    - 2) Wszelkie dokumenty uzupełniające
-