European Commission

| ZAPROSZENIE DO ZGŁASZANIA UWAG<br>DOTYCZĄCYCH OCENY/OCENY ADEKWATNOŚCI | |
|---|---|
| | |
| **TYTUŁ OCENY** | Ocena ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) i europejskich ram certyfikacji cyberbezpieczeństwa |
| **WIODĄCA DG I ODPOWIEDZIALNY DZIAŁ** | Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii (CNECT) H.1 |
| **ORIENTACYJNY HARMONOGRAM (PLANOWANE TERMINY ROZPOCZĘCIA I ZAKOŃCZENIA)** | pierwszy kwartał 2023 – drugi kwartał 2024 |
| **INFORMACJE DODATKOWE** | https://www.enisa.europa.eu/about-enisa/about/pl |
| *Niniejszy dokument jest przeznaczony wyłącznie do celów informacyjnych. Nie przesądza on o ostatecznej decyzji Komisji co do tego, czy inicjatywa ta zostanie zrealizowana, ani o jej ostatecznej treści. Wszystkie opisane tu elementy inicjatywy, w tym jej harmonogram, mogą ulec zmianie.* | |

## A. Kontekst polityczny, cel i zakres oceny

### Kontekst polityczny

Agencja Unii Europejskiej ds. Cyberbezpieczeństwa, ENISA, została ustanowiona w 2004 r. [rozporządzenie (WE) nr 460/2004] jako Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji, aby przyczynić się do osiągnięcia ogólnego celu, jakim jest zapewnienie wysokiego poziomu bezpieczeństwa sieci i informacji w UE.

Obecny mandat Agencji określono w art. 3 ust. 1 rozporządzenia (UE) 2019/881 uchylającego rozporządzenie (UE) nr 526/2013, który stanowi, że ENISA przyczynia się do osiągnięcia „wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii", „działa jako punkt odniesienia w zakresie doradztwa i wiedzy fachowej z zakresu cyberbezpieczeństwa" oraz „przyczynia się do zmniejszenia rozdrobnienia rynku wewnętrznego".

Cele ENISA obejmują w szczególności pomoc w opracowywaniu i wdrażaniu polityk Unii związanych z cyberbezpieczeństwem, w tym polityk sektorowych; wspieranie budowania potencjału i gotowości w całej Unii; propagowanie współpracy, w tym wymiany informacji i koordynacji na poziomie unijnym; zwiększanie zdolności w zakresie cyberbezpieczeństwa na poziomie unijnym służących zapobieganiu cyberzagrożeniom i reagowaniu na nie; przyczynianie się do utworzenia i utrzymywania europejskiego programu certyfikacji cyberbezpieczeństwa oraz propagowanie wysokiego poziomu świadomości w dziedzinie cyberbezpieczeństwa.

Zgodnie z art. 67 rozporządzenia (UE) 2019/881 Komisja przeprowadza ocenę ENISA oraz przepisów europejskich ram certyfikacji cyberbezpieczeństwa do 28 czerwca 2024 r., a następnie co pięć lat. Ustalenia przekazuje się Parlamentowi Europejskiemu, Radzie i Zarządowi ENISA.

### Cel i zakres

Celem jest ocena wyników ENISA w zakresie realizacji jej mandatu, celu i zadań określonych w rozporządzeniu (UE) 2019/881, a także ewentualnej potrzeby zmiany mandatu oraz skutków finansowych wszelkich takich zmian.

Konsultacje powinny dotyczyć w szczególności:

- struktury organizacyjnej, metod pracy i wyników ENISA, w tym adekwatności zasobów i przydziału personelu oraz tego, w jakim stopniu ENISA stała się ośrodkiem wiedzy fachowej w społeczności zajmującej się cyberbezpieczeństwem;
- wpływu, skuteczności i efektywności przepisów europejskich ram certyfikacji cyberbezpieczeństwa (tytuł III rozporządzenia (UE) 2019/881) oraz roli ENISA we wspieraniu i promowaniu opracowywania i wdrażania europejskiego programu certyfikacji cyberbezpieczeństwa. W ocenie należy również wskazać wszelkie ewentualne luki i niedociągnięcia w tych ramach;
- stosunków roboczych ENISA z Komisją Europejską i odpowiednimi instytucjami i organami UE, a także z zainteresowanymi stronami;
- zmieniających się potrzeb zainteresowanych stron oraz elastyczności i gotowości ENISA do rozwiązywania nadchodzących problemów i podejmowania nowych zadań w odpowiedzi na zmieniające się zagrożenie cyberbezpieczeństwa i otoczenie regulacyjne.

W art. 67 rozporządzenia (UE) 2019/881 wezwano również Komisję do rozważenia, czy konieczne są zasadnicze wymogi cyberbezpieczeństwa dotyczące dostępu do rynku wewnętrznego, aby zapobiec wprowadzeniu na rynek unijny produktów ICT, usług ICT i procesów ICT niespełniających tych

wymogów. Kwestia ta została jednak w dużej mierze uwzględniona w niedawnym wniosku odnoszącym się do aktu dotyczącego cyberodporności[1] i nie będzie przedmiotem tej oceny.

W ocenie uwzględnione zostaną zmiany ram regulacyjnych i ram polityki UE (np. zmieniona dyrektywa w sprawie środków na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii (dyrektywa NIS 2[2]) oraz niedawne wnioski legislacyjne dotyczące aktu dotyczącego cyberodporności, aktu dotyczącego cybersolidarności[3] i Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa[4]), a ocenie zostanie poddana elastyczność ENISA w rozwiązywaniu nadchodzących problemów, która może być wymagana na mocy nowych przepisów na szczeblu UE.

Ustalenia z oceny zostaną podane do wiadomości publicznej, a Komisja przekaże sprawozdanie z oceny wraz z wnioskami Parlamentowi Europejskiemu, Radzie i Zarządowi ENISA do 28 czerwca 2024 r.

Ocena obejmie okres od wejścia w życie rozporządzenia (UE) 2019/881, z zastrzeżeniem dostępności danych.

Zakres oceny będzie ograniczony do państw członkowskich Unii Europejskiej, państw EOG będących obserwatorami oraz, w stosownych przypadkach, ich wymiany z państwami trzecimi.

## B. Lepsze stanowienie prawa

### Strategia konsultacji

Konsultacje pomogą Komisji w ocenie ENISA oraz przepisów rozporządzenia (UE) 2019/881 w sprawie europejskich ram certyfikacji cyberbezpieczeństwa. Celem konsultacji będzie zebranie opinii odpowiednich zainteresowanych stron, w szczególności własnych struktur zarządczych ENISA, struktur organizacyjnych agencji oraz jej struktur skupiających zainteresowane strony, w tym struktur certyfikacji, organów unijnych i krajowych zajmujących się cyberbezpieczeństwem i prywatnością cyfrową, a także organizacji przedstawicielskich branży w dziedzinie cyberbezpieczeństwa oraz niektórych sektorów, na które unijne ramy regulacyjne w dziedzinie cyberbezpieczeństwa mają największy wpływ.

Działania konsultacyjne obejmą czterotygodniowy okres konsultacji w III kwartale 2023 r., podczas którego wszystkie zainteresowane strony będą mogły przekazać informacje zwrotne w odpowiedzi na to zaproszenie do zgłaszania uwag. Ocena zostanie również poparta badaniem zewnętrznym, w ramach którego przeprowadzone zostaną, m. in. w drodze wywiadów i ankiet, bardziej ukierunkowane konsultacje z odpowiednimi zainteresowanymi stronami.

[1] Wniosek Komisji Europejskiej COM(2022) 454 final dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020.

[2] 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).

[3] Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego 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, COM(2023) 209 final.

[4] Komunikat Komisji do Parlamentu Europejskiego i Rady „Wyeliminowanie niedoboru talentów w dziedzinie cyberbezpieczeństwa w celu zwiększenia konkurencyjności, wzrostu gospodarczego i odporności UE (»Akademia Umiejętności w dziedzinie Cyberbezpieczeństwa«)”, COM(2023) 207 final.

**Powody prowadzenia konsultacji**

Celem tych konsultacji jest zebranie informacji od odpowiednich zainteresowanych stron działających w dziedzinie cyberbezpieczeństwa w całej Unii, na które działalność ENISA może mieć wpływ lub których uwagi mogą pomóc ENISA wypełnić jej mandat. Wszystkie zgromadzone informacje uzupełnią analizę badania zewnętrznego oraz ocenę jako całość.

**Grupa docelowa**

Zachęcamy wszystkich do przekazania informacji zwrotnych na temat tego zaproszenia do zgłaszania uwag.

Komisja planuje skonsultować się z głównymi zainteresowanymi stronami bezpośrednio zaangażowanymi w zarządzanie ENISA i z grupami konsultacyjnymi określonymi w jej akcie założycielskim: członkami Zarządu i Rady Wykonawczej, Dyrektorem Wykonawczym, Grupą Doradczą ENISA, grupami roboczymi ad hoc, Siecią Krajowych Urzędników Łącznikowych oraz personelem agencji.

W ramach konsultacji dotyczących europejskich ram certyfikacji cyberbezpieczeństwa o przekazanie uwag mogą zostać poproszone: Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, Grupa Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa, grupy robocze ad hoc (np.: zajmujące się europejskim programem certyfikacji cyberbezpieczeństwa, programem usług w chmurze, certyfikacją cyberbezpieczeństwa 5G (EU5G)), krajowe organy ds. certyfikacji cyberbezpieczeństwa oraz jednostki oceniające zgodność oraz organy normalizacyjne, unijne i krajowe organy zajmujące się cyberbezpieczeństwem oraz prywatnością w sieci, służby Komisji Europejskiej, Europejska Służba Działań Zewnętrznych, unijne organy i agencje, takie jak BEREC, Europol, Centrum ds. Cyberbezpieczeństwa instytucji, organów i agencji Unii (CERT-UE), krajowe organy właściwe w sprawach cyberbezpieczeństwa lub organy regulacyjne, krajowe zespoły CSIRT/międzyinstytucjonalne zespoły reagowania na incydenty komputerowe oraz Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC) i sieć krajowych ośrodków koordynacji.

Komisja pragnie ponadto wysłuchać głosu przedstawicieli sektora i MŚP, np. Europejskiej Organizacji ds. Cyberbezpieczeństwa (ECSO), a także organizacji sektorowych działających w sektorach, na które ramy regulacyjne w dziedzinie cyberbezpieczeństwa mają największy wpływ (np. w sektorze transportu, energii).

| Gromadzenie danych i metodyka |
| --- |
| Metodyka będzie opierać się na różnych metodach gromadzenia dowodów jakościowych i ilościowych w oparciu o przegląd dokumentacji, badanie źródeł wtórnych, wywiady i ankiety. Przeprowadzone zostanie badanie uzupełniające, w ramach którego zwróci się szczególną uwagę na wieloaspektowy charakter dziedziny cyberbezpieczeństwa, a we wnioskach z tego badania zestawione zostaną różne poglądy reprezentowane przez zainteresowane strony ENISA.<br><br>Następujące materiały będą miały kluczowe znaczenie dla oceny: akt ustanawiający ENISA; jednolity dokument programowy uwzględniający roczny program prac agencji, roczne sprawozdanie z działalności ENISA oraz DG CNECT (jako partnerskiej dyrekcji generalnej), protokoły ustaleń między ENISA i innymi podmiotami (organami UE i podmiotami zewnętrznymi); protokoły regularnych posiedzeń Zarządu/Rady Wykonawczej[5], decyzje Zarządu[6], protokoły i dokumenty związane z różnymi grupami roboczymi (w szczególności zajmującymi się programami certyfikacji), badania i publikacje ENISA[7].<br><br>Udostępnione zostaną również sprawozdania Europejskiego Trybunału Obrachunkowego[8] oraz wyniki ostatniej oceny ENISA[9]. |

[5] https://www.enisa.europa.eu/about-enisa/about/pl

[6] https://www.enisa.europa.eu/about-enisa/structure-organization/management-board/management-board-decisions

[7] https://www.enisa.europa.eu/about-enisa/about/pl

[8] https://www.eca.europa.eu/pl/publications/enisa_2019 & https://www.eca.europa.eu/pl/publications/sr22_05

[9] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017DC0478&qid=1687184329002 & https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017SC0502&rid=6