Dziennik Urzędowy
Unii Europejskiej

PL
Seria L

2025/2540

12.12.2025

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2025/2540

z dnia 9 grudnia 2025 r.

ustanawiające zasady stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 w odniesieniu do opracowania planu wzajemnego przeglądu

(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 uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) ([1]), w szczególności jego art. 59 ust. 5,

a także mając na uwadze, co następuje:

(1) Zgodnie z art. 59 ust. 4 rozporządzenia (UE) 2019/881 wzajemne przeglądy krajowych organów ds. certyfikacji cyberbezpieczeństwa muszą przeprowadzać dwa krajowe organy ds. certyfikacji cyberbezpieczeństwa z innych państw członkowskich i Komisja. W celu uzyskania równoważnych norm w odniesieniu do europejskich certyfikatów cyberbezpieczeństwa i unijnych deklaracji zgodności Komisja powinna monitorować kwestie związane ze zgodnością z niniejszym rozporządzeniem i zapewnić, aby wzajemne przeglądy przeprowadzano w sposób spójny w całej Unii. Aby pomóc w określeniu dobrych praktyk, wyzwań i wniosków wyciągniętych z wdrażania europejskich programów certyfikacji cyberbezpieczeństwa, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) powinna mieć możliwość uczestniczenia we wzajemnych przeglądach jako obserwator. Aby wspierać zharmonizowane wdrażanie przepisów niniejszego rozporządzenia, ENISA, we współpracy z Komisją i Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa (ECCG), również powinna mieć możliwość opracowywania wzorów.

(2) Aby zapewnić przewidywalne planowanie i efektywną alokację zasobów, wzajemne przeglądy każdego krajowego organu ds. certyfikacji cyberbezpieczeństwa należy przeprowadzać zgodnie z ustalonym harmonogramem. Krajowy organ ds. certyfikacji cyberbezpieczeństwa powinien mieć możliwość zwrócenia się z wnioskiem o odroczenie wzajemnego przeglądu w wyjątkowych okolicznościach, takich jak nieoczekiwane niedobory pracowników lub przypadki działania siły wyższej. W tym celu należy określić zasady oceny takiego wniosku oraz zapewnić utrzymanie nadrzędnego harmonogramu i realizację celów mechanizmu wzajemnego przeglądu.

(3) Aby zagwarantować, że wszystkie państwa członkowskie przyczyniają się do wdrażania mechanizmu wzajemnego przeglądu, a także aby umożliwić im korzystanie z partnerskiego uczenia się, krajowe organy ds. certyfikacji cyberbezpieczeństwa każdego państwa członkowskiego powinny przeprowadzać dwa wzajemne przeglądy w okresie pięciu lat. Należy zatem ustanowić system rotacji umożliwiający krajowym organom ds. certyfikacji cyberbezpieczeństwa wszystkich państw członkowskich zorganizowanie ich udziału. Należy również określić kryteria, które krajowe organy ds. certyfikacji cyberbezpieczeństwa powinny brać pod uwagę przy wyborze przedstawicieli do przeprowadzania wzajemnych przeglądów, aby zapewnić odpowiednią wiedzę fachową i kompetencje. Krajowe organy ds. certyfikacji cyberbezpieczeństwa powinny również móc brać udział we wzajemnych przeglądach w charakterze obserwatorów, by monitorować proces i uczyć się na jego podstawie. W takich przypadkach nie należy wymagać, aby ich przedstawiciele posiadali taką samą wiedzę fachową i kompetencje, jakich oczekuje się od przedstawicieli krajowych organów ds. certyfikacji cyberbezpieczeństwa, które przeprowadzają wzajemne przeglądy.

(4) W dążeniu do zapewnienia, aby krajowy organ ds. certyfikacji cyberbezpieczeństwa poddano wzajemnemu przeglądowi przeprowadzanemu przez co najmniej jeden krajowy organ ds. certyfikacji cyberbezpieczeństwa stosujący to samo podejście do wydawania certyfikatów o poziomie uzasadnienia zaufania „wysoki", ENISA powinna wskazać, zwracając się do krajowych organów ds. certyfikacji cyberbezpieczeństwa o wyrażenie zainteresowania statusem podmiotu przeprowadzającego wzajemny przegląd, czy poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa bezpośrednio wydaje certyfikaty o poziomie uzasadnienia zaufania „wysoki", korzysta z modelu uprzedniego zatwierdzenia, o którym mowa w art. 56 ust. 6 lit. a) rozporządzenia (UE) 2019/881, udziela ogólnego powierzenia zgodnie z lit. b) tego ustępu, czy też posiada kombinację tych cech.

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

(5) Aby zapewnić wspólne kryteria oceny i procedury przeprowadzania wzajemnych przeglądów w całej Unii, każdy wzajemny przegląd powinien zawsze obejmować kwestionariusz samooceny, przegląd dokumentacji i wizytę na miejscu wraz z rozmowami. Po wizycie na miejscu zespół ds. wzajemnego przeglądu powinien omówić ustalenia z poddanym wzajemnemu przeglądowi krajowym organem ds. certyfikacji cyberbezpieczeństwa, przygotować projekt sprawozdania i przedłożyć go poddanemu wzajemnemu przeglądowi krajowemu organowi ds. certyfikacji cyberbezpieczeństwa w celu otrzymania od niego uwag, aby osiągnąć konsensus, jeżeli jest on możliwy. Zespół ds. wzajemnego przeglądu powinien przedłożyć Europejskiej Grupie ds. Certyfikacji Cyberbezpieczeństwa sprawozdanie końcowe, które może zawierać wytyczne lub zalecenia umożliwiające poprawę funkcjonowania poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa. Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, na wniosek zespołu ds. wzajemnego przeglądu, powinna również zatwierdzić sprawozdanie podsumowujące, które zostanie podane do wiadomości publicznej.

(6) W dążeniu do zapewnienia bezpiecznego przetwarzania informacji uzyskanych w ramach procesu wzajemnego przeglądu zespół ds. wzajemnego przeglądu powinien zapewnić korzystanie z bezpiecznych kanałów komunikacji, takich jak bezpieczna platforma do przechowywania i udostępniania dokumentów, oraz stosowanie odpowiednich zabezpieczeń w odniesieniu do danych poufnych udostępnianych przez członków zespołu ds. wzajemnego przeglądu. Biorąc pod uwagę istniejące najlepsze praktyki krajowych organów ds. certyfikacji cyberbezpieczeństwa, ENISA powinna również mieć możliwość opracowania wytycznych dotyczących sposobu zapewnienia bezpiecznej komunikacji, w szczególności by sprawić, aby poziom bezpieczeństwa stosowany przez zespół ds. wzajemnego przeglądu przy gromadzeniu, udostępnianiu i przetwarzaniu informacji był dostosowany do potrzeb w zakresie bezpieczeństwa poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa.

(7) Aby ułatwić współpracę i skuteczną wymianę informacji między krajowymi organami ds. certyfikacji cyberbezpieczeństwa, Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa, w szczególności jej podgrupa ds. wzajemnego przeglądu, powinna wnosić wkład w opracowywanie wzorów, a także wspierać Komisję we wdrażaniu niniejszego rozporządzenia.

(8) Mechanizm wzajemnego przeglądu stanowi transeuropejską cyfrową usługę publiczną w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2024/903 ([2]). W drodze niniejszego rozporządzenia wprowadzono nowe wiążące wymogi mające wpływ na tę usługę i z tego względu podlega ono obowiązkowi oceny interoperacyjności na podstawie art. 3 rozporządzenia (UE) 2024/903. W związku z tym przeprowadzono ocenę interoperacyjności, a sprawozdanie z tej oceny ma zostać opublikowane w portalu Interoperacyjna Europa.

(9) Przy opracowywaniu niniejszego rozporządzenia Komisja wzięła pod uwagę opinie Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa, w tym jej podgrupy ds. wzajemnego przeglądu.

(10) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego w art. 66 rozporządzenia (UE) 2019/881,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Harmonogram, częstotliwość i koszty wzajemnych przeglądów

1. Wzajemne przeglądy krajowych organów ds. certyfikacji cyberbezpieczeństwa (NCCA) przeprowadza się zgodnie z harmonogramem określonym w załączniku I. Każdy wzajemny przegląd należy ukończyć w terminie wskazanym w tym harmonogramie; kolejne przeglądy przeprowadza się co pięć lat.

2. W wyjątkowych okolicznościach poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa może przedłożyć Komisji należycie uzasadniony wniosek o odroczenie wzajemnego przeglądu na termin późniejszy niż wskazany w harmonogramie określonym w załączniku I. Komisja, we współpracy z Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa (ECCG) ustanowioną na mocy art. 62 rozporządzenia (UE) 2019/881, ocenia taki wniosek i niezwłocznie informuje wszystkie zainteresowane strony o decyzji w sprawie odroczenia przeglądu.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/903 z dnia 13 marca 2024 r. w sprawie ustanowienia środków na rzecz wysokiego poziomu interoperacyjności sektora publicznego na terytorium Unii (akt w sprawie Interoperacyjnej Europy) (Dz.U. L, 2024/903, 22.3.2024, ELI: http://data.europa.eu/eli/reg/2024/903/oj).

3. W przypadku gdy państwo członkowskie, zgodnie z art. 58 ust. 1 rozporządzenia (UE) 2019/881, wyznaczyło:

a) więcej niż jeden krajowy organ ds. certyfikacji cyberbezpieczeństwa na swoim terytorium, wszystkie krajowe organy ds. certyfikacji cyberbezpieczeństwa tego państwa członkowskiego należy równocześnie poddać wzajemnemu przeglądowi;

b) krajowy organ lub organy ds. certyfikacji cyberbezpieczeństwa innego państwa członkowskiego, ten krajowy organ lub organy ds. certyfikacji cyberbezpieczeństwa można poddać wzajemnemu przeglądowi zgodnie z harmonogramem określonym dla wyznaczającego państwa członkowskiego albo dla państwa członkowskiego wyznaczonego krajowego organu lub organów ds. certyfikacji cyberbezpieczeństwa, w odniesieniu do zadań nadzorczych wykonywanych w wyznaczającym państwie członkowskim.

4. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) udostępnia publicznie na stronie internetowej poświęconej europejskim programom certyfikacji cyberbezpieczeństwa utworzonej na podstawie art. 50 rozporządzenia (UE) 2019/881 następujące informacje:

a) informacje dotyczące harmonogramu określonego w załączniku I;

b) prowadzony na podstawie art. 2 ust. 5 wykaz krajowych organów ds. certyfikacji cyberbezpieczeństwa przeprowadzających wzajemny przegląd.

5. Każdy krajowy organ ds. certyfikacji cyberbezpieczeństwa uczestniczący w procesie wzajemnego przeglądu pokrywa własne koszty uczestnictwa.

Artykuł 2

System rotacji dla przeprowadzających wzajemny przegląd krajowych organów ds. certyfikacji cyberbezpieczeństwa

1. Zgodnie z art. 59 ust. 4 rozporządzenia (UE) 2019/881 każdy wzajemny przegląd musi być przeprowadzony przez dwa krajowe organy ds. certyfikacji cyberbezpieczeństwa z innych państw członkowskich oraz Komisję. Krajowe organy ds. certyfikacji cyberbezpieczeństwa każdego państwa członkowskiego uczestniczą we wzajemnym przeglądzie co najmniej dwóch krajowych organów ds. certyfikacji cyberbezpieczeństwa w każdym okresie określonym w załączniku I.

2. Krajowe organy ds. certyfikacji cyberbezpieczeństwa innych państw członkowskich mogą uczestniczyć we wzajemnym przeglądzie w charakterze obserwatorów z udziałem co najmniej jednego przedstawiciela, za zgodą poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa, krajowych organów ds. certyfikacji cyberbezpieczeństwa przeprowadzających wzajemny przegląd i Komisji.

3. We wzajemnym przeglądzie może uczestniczyć jeden przedstawiciel ENISA w charakterze obserwatora. Za zgodą poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa, krajowego organu ds. certyfikacji cyberbezpieczeństwa, przeprowadzającego wzajemny przegląd i Komisji mogą również uczestniczyć dodatkowi przedstawiciele.

4. Obserwatorzy mają dostęp do tych samych informacji co inni członkowie zespołu ds. wzajemnego przeglądu, ale nie wykonują zadań związanych z jego przeprowadzaniem.

5. ENISA, we współpracy z Komisją oraz Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa, opracowuje i utrzymuje listę krajowych organów ds. certyfikacji cyberbezpieczeństwa wyznaczonych do przeprowadzenia wzajemnych przeglądów zgodnie z harmonogramem określonym w załączniku I. W danym roku ENISA, we współpracy z Komisją, zwraca się do krajowych organów ds. certyfikacji cyberbezpieczeństwa o zgłoszenie chęci przeprowadzenia wzajemnych przeglądów krajowych organów ds. certyfikacji cyberbezpieczeństwa lub uczestnictwa w nich w charakterze obserwatorów, które to przeglądy zaplanowano zgodnie z harmonogramem w załączniku I na następny rok.

6. Jeżeli więcej niż dwa krajowe organy ds. certyfikacji cyberbezpieczeństwa wyrażą zainteresowanie przeprowadzeniem wzajemnego przeglądu tego samego krajowego organu ds. certyfikacji cyberbezpieczeństwa, Komisja i ENISA konsultują się z zainteresowanymi krajowymi organami ds. certyfikacji cyberbezpieczeństwa i podejmują decyzję w sprawie uczestników wzajemnego przeglądu.

7. Jeżeli w danym roku nie ma wystarczającej liczby krajowych organów ds. certyfikacji cyberbezpieczeństwa wyrażających zainteresowanie przeprowadzaniem wzajemnych przeglądów, Komisja, po konsultacji z Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa, wybiera krajowe organy ds. certyfikacji cyberbezpieczeństwa, które przeprowadzą wzajemne przeglądy. Komisja, dokonując wyboru, bierze pod uwagę spoczywający na krajowych organach ds. certyfikacji cyberbezpieczeństwa każdego państwa członkowskiego obowiązek uczestnictwa we wzajemnym przeglądzie co najmniej dwóch krajowych organów ds. certyfikacji cyberbezpieczeństwa, o którym to obowiązku mowa w ust. 1.

Artykuł 3

Kryteria dotyczące składu zespołu ds. wzajemnego przeglądu

1. W odpowiednim terminie przed rozpoczęciem wzajemnego przeglądu każdy przeprowadzający wzajemny przegląd krajowy organ ds. certyfikacji cyberbezpieczeństwa wyznacza jednego przedstawiciela do przeprowadzenia wzajemnego przeglądu. Przeprowadzający wzajemny przegląd krajowy organ ds. certyfikacji cyberbezpieczeństwa może wyznaczyć więcej niż jednego przedstawiciela, jeżeli jest to konieczne do zapewnienia, aby zespół ds. wzajemnego przeglądu posiadał kompetencje niezbędne do przeprowadzenia wzajemnego przeglądu.

2. Przedstawiciel przeprowadzającego wzajemny przegląd krajowego organu ds. certyfikacji cyberbezpieczeństwa, z wyjątkiem przedstawicieli organów, które uczestniczą w przeglądzie w charakterze obserwatorów, musi spełniać następujące kryteria:

a) posiadać co najmniej dwuletnie doświadczenie w pracy dla przeprowadzającego wzajemny przegląd krajowego organu ds. certyfikacji cyberbezpieczeństwa lub uczestniczyć w co najmniej dwóch wzajemnych przeglądach w charakterze obserwatora;

b) posiadać wystarczającą wiedzę na temat ram certyfikacji cyberbezpieczeństwa określonych w rozporządzeniu (UE) 2019/881;

c) wykazywać się dobrą praktyczną znajomością języka angielskiego oraz, w miarę możliwości, co najmniej jednego z języków używanych w państwie członkowskim poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa;

d) działać niezależnie od poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa.

3. Przeprowadzające wzajemne przeglądy krajowe organy ds. certyfikacji cyberbezpieczeństwa zapewniają, aby ujawniono wszelkie ryzyko konfliktu interesów dotyczące wyznaczonych przedstawicieli pozostałym krajowym organom ds. certyfikacji cyberbezpieczeństwa, Komisji i ENISA przed rozpoczęciem procesu wzajemnego przeglądu. Poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa może sprzeciwić się wyznaczeniu konkretnych przedstawicieli zgodnie z ust. 5.

4. Przeprowadzające wzajemny przegląd krajowe organy ds. certyfikacji cyberbezpieczeństwa wybierają spośród siebie jednego przedstawiciela („szef zespołu"), który koordynuje wzajemny przegląd.

5. Przed rozpoczęciem procesu wzajemnego przeglądu Komisja przekazuje poddanemu wzajemnemu przeglądowi krajowemu organowi ds. certyfikacji cyberbezpieczeństwa nazwiska i dane kontaktowe przedstawicieli przeprowadzających wzajemny przegląd krajowych organów ds. certyfikacji cyberbezpieczeństwa. W przypadku gdy poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa chce sprzeciwić się powołaniu jednego lub większej liczby przedstawicieli, w terminie dwóch tygodni przedstawia on Komisji jasne uzasadnienie, informuje o tym ENISA i Europejską Grupę ds. Certyfikacji Cyberbezpieczeństwa, a także zwraca się do przeprowadzającego wzajemny przegląd krajowego organu ds. certyfikacji cyberbezpieczeństwa o wyznaczenie innego przedstawiciela.

6. W przypadku gdy procedura określona w ust. 5 powoduje nieuzasadnione opóźnienia w rozpoczęciu wzajemnego przeglądu ze względu na wyjątkowe okoliczności, Komisja, w porozumieniu z ENISA i Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa, podejmuje decyzję w przedmiocie składu zespołu ds. wzajemnego przeglądu.

Artykuł 4

Metodyka wzajemnego przeglądu

1. Wzajemny przegląd obejmuje ocenę aspektów wymienionych w załączniku II zgodnie z art. 59 ust. 3 rozporządzenia (UE) 2019/881.

2. ENISA, we współpracy z Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa i Komisją, może opracować wzory na potrzeby oceny procesów ustanowionych przez poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa.

3. Wzajemny przegląd obejmuje następujące elementy:

a) kwestionariusz samooceny;

b) ocenę odnośnej dokumentacji;

c) rozmowy bezpośrednie i online, lub oba te rodzaje rozmów;

d) wizytę na miejscu.

4. Czas trwania wzajemnego przeglądu można uprzednio uzgodnić między zespołem ds. wzajemnego przeglądu a poddanym wzajemnemu przeglądowi krajowym organem ds. certyfikacji cyberbezpieczeństwa, w zależności od wielkości i złożoności działań poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa. Wizyta na miejscu nie może trwać dłużej niż trzy dni robocze.

5. O ile zespół ds. wzajemnego przeglądu, poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa i Komisja nie uzgodnią inaczej, językiem współpracy jest język angielski. Sprawozdanie z wzajemnego przeglądu, o którym mowa w art. 5, sporządza się przynajmniej w języku angielskim.

6. Poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa współpracuje z zespołem ds. wzajemnego przeglądu i zapewnia mu dostęp do informacji i dokumentów niezbędnych do przeprowadzenia wzajemnego przeglądu. Poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa przedkłada kwestionariusz samooceny i najnowsze roczne sprawozdanie przyjęte zgodnie z art. 58 ust. 7 lit. g) rozporządzenia (UE) 2019/881 co najmniej 21 dni przed datą wizyty na miejscu. Dodatkowe dokumenty przedkłada się na wniosek zespołu ds. wzajemnego przeglądu w terminie 7 dni od otrzymania takich wniosków.

7. Dokumenty przekazuje się w języku angielskim, chyba że uzgodniono inaczej zgodnie z ust. 5. W przypadku gdy dokumentów nie przekazano w języku angielskim, zespół ds. wzajemnego przeglądu może zwrócić się o przetłumaczenie na język angielski dokumentów niezbędnych do przeprowadzenia wzajemnego przeglądu.

8. Przed sporządzeniem sprawozdania z wzajemnego przeglądu zgodnie z art. 5 zespół ds. wzajemnego przeglądu omawia wstępne ustalenia z poddanym wzajemnemu przeglądowi krajowym organem ds. certyfikacji cyberbezpieczeństwa.

Artykuł 5

Sprawozdanie z wzajemnego przeglądu

1. W ciągu 21 dni od przeprowadzenia wzajemnego przeglądu zespół ds. wzajemnego przeglądu sporządza projekt sprawozdania z wzajemnego przeglądu, który zawiera szczegółowe informacje na temat państwa członkowskiego poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa, krajowych organów ds. certyfikacji cyberbezpieczeństwa przeprowadzających wzajemny przegląd, Komisji i wszelkich obserwatorów, a także ustalenia i wnioski z wzajemnego przeglądu. W razie potrzeby sprawozdania te zawierają zalecenia umożliwiające poprawę w aspektach objętych wzajemnym przeglądem.

2. ENISA, we współpracy z Komisją i Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa, może opracować wzór sprawozdania z wzajemnego przeglądu.

3. Po sporządzeniu projektu sprawozdania z wzajemnego przeglądu zgodnie z ust. 1 zespół ds. wzajemnego przeglądu przekazuje go poddanemu wzajemnemu przeglądowi krajowemu organowi ds. certyfikacji cyberbezpieczeństwa w celu zgłoszenia uwag w terminie 14 dni. Zespół ds. wzajemnego przeglądu ocenia uwagi i, w miarę możliwości, włącza je do sprawozdania końcowego, aby osiągnąć konsensus. W przypadku braku porozumienia do sprawozdania końcowego załącza się odpowiedź poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa.

4. Sprawozdanie końcowe, w tym streszczenie do publikacji, przesyła się Europejskiej Grupie ds. Certyfikacji Cyberbezpieczeństwa w terminie dwóch miesięcy od zrealizowania wzajemnego przeglądu. Zgodnie z art. 59 ust. 6 rozporządzenia (UE) 2019/881 Europejska Grupa ds. Certyfikacji Cyberbezpieczeństwa analizuje sprawozdanie i zatwierdza jego streszczenie, które publikuje się na stronie internetowej poświęconej europejskim programom certyfikacji cyberbezpieczeństwa utworzonej na podstawie art. 50 rozporządzenia (UE) 2019/881. Podsumowanie zawiera również odpowiedź poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa lub jej części, w porozumieniu z poddanym wzajemnemu przeglądowi krajowym organem ds. certyfikacji cyberbezpieczeństwa.

5. Przed przekazaniem sprawozdania z wzajemnego przeglądu poza zespół ds. wzajemnego przeglądu zespół ds. wzajemnego przeglądu anonimizuje dane osobowe, które mógł zgromadzić podczas wzajemnego przeglądu.

Artykuł 6

Poufność

1. Wszystkie strony zaangażowane we wzajemne przeglądy przestrzegają zasady poufności informacji i danych uzyskanych podczas wykonywania swoich zadań i swojej działalności w taki sposób, aby chronić w szczególności:

a) prawa własności intelektualnej oraz poufne informacje handlowe lub tajemnice przedsiębiorstwa osoby fizycznej lub prawnej, w tym kod źródłowy, chyba że zastosowanie mają przypadki określone w art. 5 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/943 ([3]);

b) skuteczne wykonywanie niniejszego rozporządzenia;

c) interesy bezpieczeństwa publicznego i narodowego;

d) uczciwy przebieg postępowań karnych i administracyjnych.

2. Zespół ds. wzajemnego przeglądu zapewnia bezpieczne przetwarzanie wszelkich informacji uzyskanych w ramach procesu wzajemnego przeglądu. Po sporządzeniu sprawozdania końcowego i podsumowania, o których mowa w art. 5 ust. 4, zespół ds. wzajemnego przeglądu, w tym każdy obserwator, usuwa lub niszczy wszystkie dokumenty, inne niż sprawozdanie końcowe i streszczenie, które zebrano lub wygenerowano w ramach procesu wzajemnego przeglądu.

3. ENISA, uwzględniając istniejące najlepsze praktyki krajowych organów ds. certyfikacji cyberbezpieczeństwa, może, we współpracy z Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa, opracować wytyczne dotyczące bezpiecznej i poufnej komunikacji.

([3]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz.U. L 157 z 15.6.2016, s. 1, ELI: http://data.europa.eu/eli/dir/2016/943/oj).

Artykuł 7

Budowanie zdolności

ENISA analizuje zagregowane wyniki wzajemnych przeglądów i zwraca uwagę na zdobyte doświadczenia i najlepsze praktyki, aby przyczynić się do budowania zdolności krajowych organów ds. certyfikacji cyberbezpieczeństwa oraz do utrzymania europejskich programów certyfikacji cyberbezpieczeństwa. Analiza ta może obejmować, w stosownych przypadkach, szkolenia i dodatkowe wytyczne dla krajowych organów ds. certyfikacji cyberbezpieczeństwa, opracowane we współpracy z Europejską Grupą ds. Certyfikacji Cyberbezpieczeństwa.

Artykuł 8

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 9 grudnia 2025 r.

W imieniu Komisji
Przewodnicząca
Ursula VON DER LEYEN

ZAŁĄCZNIK I

Harmonogram krajowych organów ds. certyfikacji cyberbezpieczeństwa (NCCA), które podlegają wzajemnemu przeglądowi

Krajowe organy ds. certyfikacji cyberbezpieczeństwa następujących państw członkowskich podlegają wzajemnemu przeglądowi do dnia 31 grudnia 2026 r., a następnie co pięć lat:

Szwecja, Belgia, Słowacja, Niemcy, Malta, Czechy.

Krajowe organy ds. certyfikacji cyberbezpieczeństwa następujących państw członkowskich podlegają wzajemnemu przeglądowi do dnia 31 grudnia 2027 r., a następnie co pięć lat:

Węgry, Grecja, Estonia, Słowenia, Niderlandy, Włochy.

Krajowe organy ds. certyfikacji cyberbezpieczeństwa następujących państw członkowskich podlegają wzajemnemu przeglądowi do dnia 31 grudnia 2028 r., a następnie co pięć lat:

Chorwacja, Dania, Litwa, Hiszpania, Bułgaria, Irlandia.

Krajowe organy ds. certyfikacji cyberbezpieczeństwa następujących państw członkowskich podlegają wzajemnemu przeglądowi do dnia 31 grudnia 2029 r., a następnie co pięć lat:

Finlandia, Austria, Rumunia, Luksemburg, Łotwa, Polska.

Krajowe organy ds. certyfikacji cyberbezpieczeństwa następujących państw EOG–EFTA podlegają wzajemnemu przeglądowi do dnia 31 grudnia 2030 r., a następnie co pięć lat:

Cypr, Francja, Portugalia, Liechtenstein, Norwegia, Islandia.

ZAŁĄCZNIK II

Metodyka wzajemnego przeglądu

II.1. **Oddzielenie działalności związanej z certyfikacją od działalności związanej z nadzorem**

Przy ocenie oddzielenia działalności związanej z certyfikacją od działalności związanej z nadzorem prowadzonej przez poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa, o którym to oddzieleniu mowa w art. 59 ust. 3 lit. a) rozporządzenia (UE) 2019/881, wzajemny przegląd obejmuje co najmniej następujące kwestie:

a) szczegółowy opis funkcjonowania poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa, wyraźnie wskazujący poszczególne podmioty lub departamenty zaangażowane we wdrażanie rozporządzenia (UE) 2019/881;

b) przyporządkowanie działań poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa do działań wymienionych w art. 58 ust. 7 rozporządzenia (UE) 2019/881;

c) w przypadku gdy poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa wydaje certyfikaty – wyjaśnienie wykazujące, że jego działalność związana z certyfikacją nie koliduje z działalnością związaną z nadzorem, jak określono w lit. b).

II.2. **Nadzorowane i egzekwowanie zasad monitorowania zgodności z certyfikatami**

Przy ocenie procedur poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa dotyczących nadzorowania i egzekwowania zasad monitorowania zgodności produktów ICT, usług ICT, procesów ICT i usług zarządzanych w zakresie bezpieczeństwa z europejskimi certyfikatami cyberbezpieczeństwa, o których mowa w art. 59 ust. 3 lit. b) rozporządzenia (UE) 2019/881, wzajemny przegląd obejmuje co najmniej następujące kwestie:

a) jakość i poziom szczegółowości opisu takich procesów i procedur oraz zakres, w jakim je udokumentowano;

b) czy i w jakim zakresie takie procesy i procedury obejmują odpowiednie europejskie programy certyfikacji cyberbezpieczeństwa;

c) czy poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa jest faktycznie uprawniony do przeprowadzania kontroli jednostek oceniających zgodność, które wydają certyfikaty, oraz, w razie potrzeby, do egzekwowania wycofywania certyfikatów;

d) zakres współpracy między poddanym wzajemnemu przeglądowi krajowym organem ds. certyfikacji cyberbezpieczeństwa a odpowiednimi organami nadzoru rynku;

e) czy poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa stosuje mechanizm rozpatrywania skarg osób fizycznych lub prawnych wymagany na podstawie art. 58 ust. 7 lit. f) rozporządzenia (UE) 2019/881, w tym dowody potwierdzające, że osoby fizyczne i prawne mają prawo do wniesienia skargi i do skutecznego środka prawnego przed sądem zgodnie z, odpowiednio, art. 63 i 64 tego rozporządzenia.

II.3. **Monitorowanie i egzekwowanie obowiązków producentów lub dostawców**

Przy ocenie procedur poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa w zakresie monitorowania i egzekwowania obowiązków producentów lub dostawców dokonujących oceny zgodności przez stronę pierwszą, o której mowa w art. 59 ust. 3 lit. c) rozporządzenia (UE) 2019/881, wzajemny przegląd obejmuje co najmniej następujące kwestie:

a) czy poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa ustanowił takie procedury i w jakim stopniu są one udokumentowane, w szczególności czy ustanowiono mechanizm otrzymywania i przetwarzania informacji pochodzących ze źródeł zewnętrznych;

b) czy i w jakim zakresie takie procedury obejmują odpowiednie europejskie programy certyfikacji cyberbezpieczeństwa;

c) czy i w jakim zakresie poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa prowadzi własne dochodzenia oraz czy zakres dochodzeń obejmuje obowiązki producentów określone w art. 53 ust. 2 i 3 rozporządzenia (UE) 2019/881 oraz w odpowiednich europejskich programach certyfikacji cyberbezpieczeństwa;

d) czy istnieje procedura wymiany informacji między obszarami działalności związanej z certyfikacją i działalności związanej z nadzorem poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa, które to informacje są istotne dla monitorowania i egzekwowania obowiązków producentów lub dostawców.

II.4. **Monitorowanie, wydawanie zezwoleń na działalność i nadzorowanie jednostek oceniających zgodność**

Przy ocenie procedur poddanego wzajemnemu przeglądowi krajowego organu ds. certyfikacji cyberbezpieczeństwa w zakresie monitorowania, wydawania zezwoleń na działalność i nadzorowania jednostek oceniających zgodność, o których to procedurach mowa w art. 59 ust. 3 lit. d) rozporządzenia (UE) 2019/881, wzajemny przegląd obejmuje co najmniej następujące kwestie:

a) jakość i poziom szczegółowości opisu takich procedur oraz zakres, w jakim są one udokumentowane, w tym w odniesieniu do współpracy z krajową jednostką akredytującą;

b) kluczowe dane statystyczne dotyczące liczby udzielonych, zawieszonych lub cofniętych zezwoleń na działalność, całkowitej liczby działających jednostek oceniających zgodność, liczby wydanych certyfikatów oraz liczby działań naprawczych podjętych przez poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa;

c) w przypadku gdy poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa zezwala na wydawanie europejskich certyfikatów cyberbezpieczeństwa o poziomie uzasadnienia zaufania „wysoki" po uprzednim zatwierdzeniu lub na podstawie ogólnego powierzenia zadania jak określono w art. 56 ust. 6 rozporządzenia (UE) 2019/881, wiedzę fachową personelu oraz procedury, za pomocą których poddany wzajemnemu przeglądowi krajowy organ ds. certyfikacji cyberbezpieczeństwa monitoruje i nadzoruje działalność jednostek oceniających zgodność.