Rada
Unii Europejskiej

Bruksela, 22 marca 2022 r.
(OR. en)

7474/22

Międzyinstytucjonalny numer referencyjny:
2022/0085 (COD)

CYBER 93
TELECOM 116
JAI 383
INST 89
INF 32
CSC 119
CSCI 39
DATAPROTECT 81
FIN 353
BUDGET 2
CODEC 349
IA 30

WNIOSEK

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	22 marca 2022 r.
Do:	Jeppe TRANHOLM-MIKKELSEN, sekretarz generalny Rady Unii Europejskiej
Nr dok. Kom.:	COM(2022) 122 final
Dotyczy:	Wniosek ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY ustanawiające środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii

Delegacje otrzymują w załączeniu dokument COM(2022) 122 final.

Zał.: COM(2022) 122 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 22.3.2022 r.
COM(2022) 122 final

2022/0085 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

ustanawiające środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii

{SWD(2022) 67 final} - {SWD(2022) 68 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

W niniejszym wniosku ustanawia się ramy zapewniające wspólne przepisy i środki w zakresie cyberbezpieczeństwa dla instytucji, organów i agencji Unii. Jego celem jest dalsze wzmocnienie odporności wszystkich podmiotów i ich zdolności do reagowania na incydenty. Jest on zgodny z priorytetami Komisji dotyczącymi tworzenia Europy na miarę ery cyfrowej i zbudowania gospodarki gotowej na przyszłość, która będzie przynosić korzyści obywatelom. Ponadto zagwarantowanie bezpiecznej i odpornej administracji publicznej stanowi podstawę transformacji cyfrowej całego społeczeństwa.

Niniejszy wniosek opiera się na strategii UE w zakresie unii bezpieczeństwa (COM(2020) 605 final) oraz strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę (JOIN(2020) 18 final).

We wniosku uaktualniono istniejące ramy prawne dotyczące CERT-UE oraz uwzględniono zmieniony charakter i wyższy poziom cyfryzacji instytucji, organów i agencji Unii w ostatnich latach, jak również zmieniający się krajobraz zagrożeń cyberbezpieczeństwa. Skala obu tych zjawisk dodatkowo uległa zwiększeniu od początku kryzysu związanego z COVID-19, a liczba incydentów wciąż rośnie, przy czym pojawiają się coraz bardziej wyrafinowane ataki pochodzące z wielu różnych źródeł.

We wniosku zmieniono nazwę CERT-UE z „zespołu reagowania na incydenty komputerowe” na „Centrum ds. Cyberbezpieczeństwa” instytucji, organów i agencji Unii, aby odzwierciedlić zmiany zachodzące w państwach członkowskich i na świecie, gdzie wiele zespołów CERT przemianowano na centra ds. cyberbezpieczeństwa, ale zachowano nazwę skróconą „CERT-UE” ze względu na jej rozpoznawalność.

• Spójność z przepisami obowiązującymi w tej dziedzinie polityki

Niniejszy wniosek ma na celu zwiększenie odporności instytucji, organów i agencji Unii na cyberzagrożenia przy jednoczesnym zapewnieniu spójności z przepisami następujących obowiązujących aktów prawnych:

- dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Wniosek jest również zgodny z wnioskiem dotyczącym dyrektywy (UE) XXXX/XXXX w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 [wniosek dotyczący dyrektywy NIS 2];

- rozporządzenia (UE) 2019/881 w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych (akt o cyberbezpieczeństwie);

- wniosku dotyczącego rozporządzenia (UE) XXXX/XXXX w sprawie bezpieczeństwa informacji w instytucjach, organach, urzędach i agencjach Unii;

- zalecenia Komisji z dnia 23 czerwca 2021 r. w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni;

- zalecenia Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę.

W załączniku do zalecenia Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę określono Plan skoordynowanego reagowania na wypadek wystąpienia transgranicznych incydentów cybernetycznych na dużą skalę i kryzysów cybernetycznych.

W rezolucji z dnia 9 marca 2021 r. Rada Unii Europejskiej podkreśliła, że cyberbezpieczeństwo ma kluczowe znaczenie dla funkcjonowania administracji publicznej zarówno na szczeblu krajowym, jak i unijnym, a także dla całego społeczeństwa i gospodarki, zwracając uwagę na znaczenie solidnych i spójnych ram bezpieczeństwa dla ochrony całego personelu, danych, sieci komunikacyjnych, systemów informatycznych i procesów decyzyjnych Unii. Ma to zostać osiągnięte w szczególności dzięki zwiększeniu odporności oraz poprawie kultury bezpieczeństwa instytucji, organów i agencji Unii. Należy udostępnić wystarczające zasoby i zdolności, także w kontekście wzmocnienia mandatu CERT-UE.

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- **Podstawa prawna**

Podstawą prawną niniejszego rozporządzenia jest art. 298 Traktatu o funkcjonowaniu Unii Europejskiej („TFUE”), który przewiduje, że wykonując swoje zadania, instytucje, organy i jednostki organizacyjne Unii korzystają ze wsparcia otwartej, efektywnej i niezależnej administracji europejskiej. Z poszanowaniem regulaminu pracowniczego i warunków zatrudnienia przyjętych na podstawie art. 336 Parlament Europejski i Rada, stanowiąc w drodze rozporządzeń zgodnie ze zwykłą procedurą ustawodawczą, określają stosowne przepisy.

Technologia informacyjna otworzyła przed instytucjami, organami i agencjami Unii nowe możliwości pracy, interakcji z obywatelami i ogólnej poprawy funkcjonowania. Wraz z nieprzerwanym rozwojem technologii ewoluuje również krajobraz cyberzagrożeń. Instytucje, organy i agencje Unii stały się wysoce atrakcyjnym celem wyrafinowanych cyberataków. Wydaje się, że ustanowienie systemów i wymogów w celu zapewnienia cyberbezpieczeństwa przyczynia się do zwiększenia efektywności i niezależności administracji europejskiej, dzięki czemu instytucje, organy, urzędy i agencje Unii mogą skuteczniej funkcjonować w cyfrowym świecie, realizując swoje misje.

Ponadto występujące obecnie rozbieżności – omówione poniżej w sekcji 3 – w zakresie stanu cyberbezpieczeństwa i podejścia do cyberbezpieczeństwa pomiędzy instytucjami, organami i agencjami Unii stanowią kolejną przeszkodę dla otwartej, efektywnej i niezależnej administracji europejskiej. Bez wspólnego podejścia stan cyberbezpieczeństwa w poszczególnych instytucjach, organach i agencjach Unii będzie nadal ewoluować w rozbieżnych kierunkach. Jest to zatem właściwa podstawa prawna, biorąc pod uwagę, że rozporządzenie ma na celu utworzenie wspólnych ram prawnych dotyczących cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii.

- **Pomocniczość**

Rozporządzenie ustanawiające środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii wchodzi w zakres wyłącznych kompetencji Unii.

- **Proporcjonalność**

Przepisy proponowane w niniejszym rozporządzeniu nie wykraczają poza to, co jest konieczne do zadowalającego osiągnięcia szczegółowych celów. Przewidziane środki przyczynią się do zapewnienia wysokiego wspólnego poziomu cyberbezpieczeństwa, nie wykraczając poza to, co jest konieczne do osiągnięcia tego celu w świetle coraz większych zagrożeń.

- **Wybór instrumentu**

Rozporządzenie, które ma bezpośrednie zastosowanie, uznano za odpowiedni wybór instrumentu prawnego w celu określenia i optymalizacji obowiązków nakładanych na instytucje, organy i agencje Unii. Aby umożliwić wprowadzenie ukierunkowanych ulepszeń, najwłaściwszym instrumentem prawnym jest rozporządzenie.

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

- **Oceny *ex ante***

CERT-UE przeprowadził ocenę głównych cyberzagrożeń, na które instytucje, organy i agencje Unii są obecnie narażone lub na które mogą być narażone w przewidywalnej przyszłości.

W analizie wykorzystano trzy kategorie obserwacji:

- próby naruszenia infrastruktury informatycznej instytucji, organów i agencji Unii (jeśli się powiodły, są traktowane jako incydenty; w pozostałych przypadkach są również rejestrowane – jako wykryte próby);
- zagrożenia wykryte w bliskim otoczeniu instytucji, organów i agencji Unii (np. w powiązanych z nimi sektorach, społecznościach zainteresowanych stron lub w Europie);
- główne tendencje dotyczące zagrożeń obserwowane w skali globalnej.

Ponadto w analizie uwzględniono wpływ najważniejszych zachodzących obecnie zmian mających wpływ na sposoby zarządzania przez instytucje unijne swoją infrastrukturą i usługami IT oraz korzystania z nich. Do zmian tych zaliczają się:

- zwiększony zakres telepracy;
- migracje systemów do chmury;
- rosnący outsourcing usług IT.

W okresie od 2019 do 2021 r. liczba znaczących incydentów[1] mających wpływ na instytucje, organy i agencje Unii, za którymi to incydentami stali agresorzy stwarzający zaawansowane, trwałe zagrożenie, wzrosła w sposób dramatyczny. W pierwszej połowie 2021 r. odnotowano taką samą liczbę znaczących incydentów jak w całym 2020 r. Jest to również odzwierciedlone w liczbie kopii danych wykonanych na potrzeby informatyki śledczej (zrzutów zawartości systemów lub urządzeń dotkniętych incydentem), które CERT-UE analizował w 2020 r. – trzykrotnie wyższej w stosunku do 2019 r., podczas gdy liczba znaczących incydentów wzrosła od 2018 r. ponad dziesięciokrotnie.

W 2020 r. rada sterująca CERT-UE ustaliła nowy cel strategiczny, zgodnie z którym CERT-UE ma zapewnić wszystkim instytucjom, organom i agencjom kompleksowy poziom cyberobrony o odpowiednim zakresie i poziomie szczegółowości oraz stałą zdolność dostosowywania się do obecnych lub przyszłych zagrożeń, w tym ataków na urządzenia mobilne, środowiska chmury obliczeniowej i urządzenia internetu rzeczy.

W uzupełnieniu do analizy zagrożeń przeprowadzonej przez CERT-UE Komisja przeprowadziła ocenę funkcjonowania 20 instytucji, organów i agencji Unii pod względem cyberbezpieczeństwa. Umożliwiło to zapoznanie się z ustalonymi praktykami w zakresie cyberbezpieczeństwa i możliwościami zarządzania cyberbezpieczeństwem oraz przeprowadzenie zewnętrznych analiz porównawczych niektórych technicznych środków kontroli bezpieczeństwa.

Oceny tej dokonano w oparciu o kwestionariusze, na które odpowiedziały wspomniane instytucje, organy i agencje, oraz dane dostępne publicznie i dane dostarczone bezpośrednio przez same instytucje, organy i agencje Unii. Ocena zapewnia wystarczający ogląd bieżącej sytuacji, by można było stwierdzić, że:

- dojrzałość w zakresie cyberbezpieczeństwa, wielkość infrastruktury IT oraz poziom zdolności w ocenianych instytucjach, organach i agencjach Unii różnią się znacząco;

- podczas gdy wiele instytucji, organów i agencji Unii posiada ogólnie dojrzałe zdolności wykrywania i reagowania, ich zdolności w zakresie zarządzania cyberbezpieczeństwem różnią się pod względem poziomu zintegrowanego zarządzania ryzykiem;

- chociaż zasadniczo ramy dotyczące cyberbezpieczeństwa (strategia, polityka i zbiór przepisów) ocenianych instytucji, organów i agencji Unii są dobrze ugruntowane w kluczowych dziedzinach cyberbezpieczeństwa wymienionych w załączniku I do rozporządzenia, niektóre instytucje, organy i agencje Unii nie stosują dojrzałego zarządzania ciągłością działania, zapewniania zgodności, audytu i ciągłego doskonalenia;

- stwierdzono, że środki techniczne uznawane za najlepsze praktyki są stosowane w ocenianych instytucjach, organach i agencjach Unii w sposób nierównomierny.

Podsumowując, z analizy przeprowadzonej wśród 20 instytucji, organów i agencji Unii wynika, że ich system zarządzania, higiena cyberbezpieczeństwa, ogólna zdolność i dojrzałość różnią się w dużym stopniu. Zobowiązanie wszystkich instytucji, organów

[1] „Znaczący incydent” oznacza każdy incydent, chyba że ma on ograniczony wpływ i prawdopodobnie jest już dobrze poznany pod względem metod bądź technologii.

i agencji Unii do wdrożenia podstawowego poziomu środków w zakresie cyberbezpieczeństwa ma zasadnicze znaczenie dla zniwelowania tych różnic w dojrzałości i zapewnienia we wszystkich instytucjach, organach i agencjach Unii wysokiego wspólnego poziomu cyberbezpieczeństwa.

Żadne unijne przepisy nie koncentrowały się dotychczas na cyberbezpieczeństwie instytucji, organów i agencji Unii i nie uwzględniały w sposób kompleksowy sytuacji związanej z krajobrazem zagrożeń cyberbezpieczeństwa oraz pojawiającymi się zagrożeniami w obszarze IT wynikającymi z cyfryzacji.

- **Konsultacje z zainteresowanymi stronami**

Komisja przeprowadziła konsultacje z zainteresowanymi stronami ze wszystkich instytucji, organów i agencji Unii, jak również z przedstawicielami państw członkowskich w Radzie oraz zainteresowanymi stronami w Parlamencie Europejskim. W dniu 25 czerwca 2021 r. przedstawiciele państw członkowskich i właściwych zainteresowanych stron z instytucji, organów i agencji Unii wzięli udział w warsztatach organizowanych przez Komisję, aby przedyskutować treść przyszłego wniosku dotyczącego rozporządzenia.

- **Ocena skutków**

Skutki niniejszego wniosku będą dotyczyć instytucji, organów i agencji Unii. Oznacza to, że szczególna ocena skutków nie jest konieczna, ponieważ wniosek nie będzie miał zastosowania do państw członkowskich.

- **Prawa podstawowe**

Unia Europejska dąży do zapewnienia najwyższych standardów ochrony praw podstawowych. Wszelka wymiana informacji dokonywana na podstawie niniejszego rozporządzenia odbywałaby się z pełnym poszanowaniem prawa do ochrony danych osobowych określonego w art. 8 Karty praw podstawowych Unii Europejskiej oraz odpowiedniego prawodawstwa w zakresie ochronie danych, w szczególności rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725.

4. WPŁYW NA BUDŻET

Z rynkowych wskaźników referencyjnych i badań rynku[2] wynika, że bezpośrednie wydatki na cyberbezpieczeństwo wahają się od 4 do 7 % zagregowanych wydatków organizacji w obszarze IT. W analizie zagrożeń przeprowadzonej przez CERT-UE na poparcie niniejszego wniosku ustawodawczego wskazano jednak, że instytucje międzynarodowe i organizacje polityczne są narażone na podwyższone ryzyko, w związku z czym bardziej adekwatnym celem wydaje się ustalenie pułapu wydatków w obszarze IT na cyberbezpieczeństwo na poziomie 10 %. Nie można określić dokładnego kosztu takich

[2] Źródło: Gartner, „Identifying the Real Information Security Budget" [„Określenie rzeczywistego budżetu na bezpieczeństwo informacji"] (2016). Należy doliczyć do tego także wydatki pośrednie na bezpieczeństwo informatyczne, uwzględniając wydatki na bezpieczeństwo sieci, w tym na zapory sieciowe, programy antywirusowe oraz obowiązki właściciela systemu, takie jak ocena ryzyka i wdrażanie kontroli bezpieczeństwa. W artykule z 2020 r. wydatki na cyberbezpieczeństwo w instytucjach finansowych określono na poziomie 10–11 % wydatków na IT, źródło: DI_2020-FS-ISAC-Cybersecurity.pdf (deloitte.com).

działań ze względu na brak szczegółowych informacji na temat wydatków w obszarze IT ponoszonych przez instytucje, organy i agencje Unii oraz odnośnego udziału wydatków na cyberbezpieczeństwo.

Chociaż w związku z tym istnieje prawdopodobieństwo, że wiele instytucji, organów i agencji Unii wydaje mniej na cyberbezpieczeństwo niż powinny, niniejsze rozporządzenie jako takie nie spowoduje wzrostu tych bieżących wydatków. Nawet bez rozporządzenia każdy podmiot musiałby zapewnić odpowiedni poziom cyberbezpieczeństwa. Rozporządzenie stanowi kontynuację wcześniejszej współpracy w radzie sterującej CERT-UE i formalizuje częściowo już istniejący mechanizm wymiany informacji. Jak wyszczególniono w ocenie skutków finansowych regulacji, CERT-UE będzie potrzebował dodatkowych zasobów w celu wypełnienia swojej rozbudowanej roli, a zasoby te powinny zostać przesunięte z instytucji, organów i agencji Unii korzystających z usług CERT-UE.

5. ELEMENTY FAKULTATYWNE

- **Rozwiązania dotyczące wdrożenia, monitorowania, oceny i sprawozdawczości**

Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa (IICB), z pomocą CERT-UE, powinna dokonywać przeglądu funkcjonowania niniejszego rozporządzenia, przeprowadzać oceny i przedkładać Komisji sprawozdania zawierające jej ustalenia. Komisja powinna zapewnić, aby regularne sprawozdania przedkładano Parlamentowi Europejskiemu, Radzie, Europejskiemu Komitetowi Ekonomiczno-Społecznemu i Komitetowi Regionów.

CERT-UE może przygotować projekt wniosku w sprawie wytycznych lub zaleceń, a IICB może podjąć decyzję o jego przyjęciu. Wytyczne to dokument skierowany do wszystkich instytucji, organów i agencji Unii lub części z nich; zalecenie natomiast kieruje się do poszczególnych instytucji, organów i agencji Unii. Wezwanie do działania to wydawany przez CERT-UE dokument opisujący pilne środki w zakresie bezpieczeństwa, o których podjęcie w określonym terminie apeluje się do instytucji, organów i agencji Unii.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

Przepisy ogólne

W rozporządzeniu ustanowiono środki mające na celu zapewnienie wysokiego wspólnego poziomu cyberbezpieczeństwa i ma ono zastosowanie do instytucji, organów i agencji Unii, aby umożliwić im realizowanie powierzonych im zadań w sposób otwarty, efektywny i niezależny (art. 1–3, 23–25).

Środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa

Instytucje, organy i agencje Unii są zobowiązane do ustanowienia wewnętrznych ram zarządzania ryzykiem w cyberprzestrzeni, jego nadzoru i kontroli, które to ramy umożliwią skuteczne i ostrożne zarządzanie wszelkiego rodzaju ryzykiem w cyberprzestrzeni. Instytucje, organy i agencje wprowadzają ponadto podstawowy poziom cyberbezpieczeństwa, aby przeciwdziałać ryzyku stwierdzonemu na podstawie powyższych ram, przeprowadzają regularne oceny dojrzałości w zakresie cyberbezpieczeństwa oraz przyjmują plany dotyczące cyberbezpieczeństwa (art. 4–8).

Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa

Ustanawia się Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa, która jest odpowiedzialna za monitorowanie wdrażania niniejszego rozporządzenia przez instytucje, organy i agencje Unii, a także za nadzór nad realizacją ogólnych priorytetów i celów przez CERT-UE oraz zapewnianie mu strategicznego kierunku działania (art. 9–11).

CERT-UE

CERT-UE przyczynia się do bezpieczeństwa środowiska informatycznego wszystkich instytucji, organów i agencji Unii, pełniąc funkcję doradczą, pomagając w zapobieganiu incydentom, wykrywaniu ich, łagodzeniu ich skutków i reagowaniu na nie oraz działając dla tych instytucji, organów i agencji w charakterze punktu wymiany informacji na temat cyberbezpieczeństwa i koordynacji reakcji na incydenty (art. 12–17).

Obowiązki w zakresie współpracy i zgłaszania

Rozporządzenie zapewnia współpracę oraz wymianę informacji między CERT-UE oraz instytucjami, organami i agencjami Unii, aby budować zaufanie i pewność. W tym celu CERT-UE może zwrócić się do instytucji, organów i agencji Unii o udzielenie mu istotnych informacji, a także prowadzić z instytucjami, organami i agencjami Unii wymianę danych dotyczących konkretnych incydentów bez zgody zainteresowanego podmiotu dotkniętego incydentem, aby ułatwić wykrywanie podobnych cyberzagrożeń lub incydentów. CERT-UE może prowadzić wymianę informacji dotyczących konkretnych incydentów, które to informacje umożliwiają identyfikację celu, w który wymierzony jest cyberincydent, wyłącznie za zgodą zainteresowanego podmiotu dotkniętego incydentem.

W szczególności wszystkie instytucje, organy i agencje Unii powiadamiają CERT-UE o znaczących cyberzagrożeniach, znaczących podatnościach lub znaczących incydentach bez zbędnej zwłoki, jednak w żadnym wypadku nie później niż 24 godziny po powzięciu wiadomości o ich zaistnieniu (art. 18–22).

2022/0085 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

ustanawiające środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 298,

uwzględniając Traktat ustanawiający Europejską Wspólnotę Energii Atomowej, w szczególności jego art. 106a,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) W epoce cyfrowej technologie informacyjno-komunikacyjne stanowią podstawę otwartej, efektywnej i niezależnej administracji unijnej. Rozwój technologii, ich coraz większa złożoność i wzajemne powiązania systemów cyfrowych zwiększają ryzyko w cyberprzestrzeni, co sprawia, że administracja unijna jest bardziej podatna na cyberzagrożenia i incydenty, a to z kolei stanowi zagrożenie dla ciągłości działania administracji i jej zdolności do zabezpieczenia swoich danych. Mimo że coraz częstsze korzystanie z usług w chmurze, wszechobecne wykorzystanie technologii informacyjnych, wysoki poziom cyfryzacji, praca zdalna i rozwój technologii oraz możliwości połączenia z siecią stanowią obecnie trzon wszystkich działań podmiotów administracji Unii, to ich odporność cyfrowa nie rozwinęła się jeszcze w wystarczającym stopniu.

(2) Krajobraz cyberzagrożeń, z jakimi mierzą się instytucje, organy i agencje Unii, podlega ciągłym zmianom. Stosowane przez agresorów taktyki, techniki i sposoby działania ciągle ewoluują, natomiast główne motywy takich ataków zmieniają się w niewielkim stopniu – ich celem jest kradzież cennych, nieujawnionych informacji, osiągnięcie korzyści finansowych, manipulowanie opinią publiczną czy też osłabienie infrastruktury cyfrowej. Tempo przeprowadzania przez nich cyberataków stale rośnie, podczas gdy ich działania są coraz bardziej wyrafinowane i w coraz większym stopniu zautomatyzowane, ukierunkowane na eksponowane powierzchnie ataków, które stale powiększają się, i mają na celu szybkie wykorzystanie podatności na zagrożenia.

(3) Środowiska informatyczne instytucji, organów i agencji Unii są współzależne, występują w nich zintegrowane przepływy danych, a ich użytkownicy ściśle ze sobą

współpracują. Ta integracja oznacza, że wszelkie zakłócenia, nawet początkowo ograniczone do jednej instytucji, organu lub agencji Unii, mogą mieć szerszy efekt kaskadowy, potencjalnie powodując dalekosiężne i długotrwałe negatywne skutki dla pozostałych instytucji, organów i agencji. Ponadto środowiska informatyczne niektórych instytucji, organów i agencji są połączone ze środowiskami informatycznymi państw członkowskich, co powoduje, że incydent w jednym podmiocie unijnym może stanowić zagrożenie dla cyberbezpieczeństwa środowisk informatycznych państw członkowskich i odwrotnie.

(4) Instytucje, organy i agencje Unii stanowią atrakcyjne cele i muszą stawiać czoła wysoko wykwalifikowanym i dobrze zaopatrzonym agresorom, a także innym zagrożeniom. Jednocześnie poziom i dojrzałość w zakresie cyberodporności oraz zdolność do wykrywania szkodliwych działań w cyberprzestrzeni i reagowania na nie znacznie się w tych podmiotach różnią. Dla funkcjonowania administracji unijnej konieczne jest zatem, aby instytucje, organy i agencje Unii osiągnęły wysoki wspólny poziom cyberbezpieczeństwa dzięki podstawowemu poziomowi cyberbezpieczeństwa (minimalnemu zbiorowi przepisów dotyczących cyberbezpieczeństwa, z którymi muszą być zgodne sieci i systemy informatyczne oraz których muszą przestrzegać ich operatorzy i użytkownicy, aby zminimalizować ryzyko w cyberprzestrzeni) oraz dzięki wymianie informacji i współpracy.

(5) Dyrektywa [wniosek dotyczący dyrektywy NIS 2] w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii ma na celu dalszą poprawę odporności podmiotów publicznych i prywatnych, właściwych organów i instytucji krajowych, jak również całej Unii pod względem cyberbezpieczeństwa oraz dalsze zwiększenie ich zdolności reagowania na incydenty w zakresie cyberbezpieczeństwa. Należy zatem zadbać o to, by podobnymi środkami objęto instytucje, organy i agencje Unii, poprzez ustanowienie przepisów, które są zgodne z dyrektywą [wniosek dotyczący dyrektywy NIS 2] i odzwierciedlają przewidziany w niej poziom ambicji.

(6) Aby osiągnąć wysoki wspólny poziom cyberbezpieczeństwa, każda instytucja, każdy organ i każda agencja Unii musi ustanowić wewnętrzne ramy zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli, które to ramy umożliwią skuteczne i ostrożne zarządzanie wszelkiego rodzaju ryzykiem w cyberprzestrzeni, z uwzględnieniem ciągłości działania i zarządzania kryzysowego.

(7) Zróżnicowanie instytucji, organów i agencji Unii wymaga elastyczności w procesie wdrożenia, ponieważ w omawianym obszarze nie istnieje uniwersalne rozwiązanie. Środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa nie powinny obejmować żadnych obowiązków bezpośrednio kolidujących z wykonywaniem przez instytucje, organy i agencje Unii ich misji lub naruszających ich autonomię instytucjonalną. Te instytucje, organy i agencje powinny zatem ustanowić własne ramy zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli, a także przyjąć swój własny poziom podstawowy i plan dotyczący cyberbezpieczeństwa.

(8) Aby uniknąć nakładania nieproporcjonalnie dużych obciążeń finansowych i administracyjnych na instytucje, organy i agencje Unii, wymogi w zakresie zarządzania ryzykiem w cyberprzestrzeni powinny być proporcjonalne do ryzyka związanego z daną siecią oraz danym systemem informatycznym oraz powinny uwzględniać najnowszy stan wiedzy na temat takich środków. Wszystkie instytucje,

organy i agencje Unii powinny dążyć do przeznaczenia odpowiedniego odsetka swojego budżetu przewidzianego na technologie informatyczne na poprawę swojego poziomu cyberbezpieczeństwa; w dłuższej perspektywie należy dążyć do osiągnięcia celu w wysokości 10 %.

(9) Wysoki wspólny poziom cyberbezpieczeństwa wymaga objęcia cyberbezpieczeństwa nadzorem przez kierownictwo najwyższego szczebla każdej instytucji, każdego organu i każdej agencji Unii, a kierownictwo to powinno zatwierdzić podstawowy poziom cyberbezpieczeństwa, w którym należy uwzględnić czynniki ryzyka stwierdzone na podstawie ram, które mają zostać ustanowione przez każdą instytucję, każdy organ i każdą agencję. Uwzględnienie kultury cyberbezpieczeństwa, tj. codziennej praktyki w dziedzinie cyberbezpieczeństwa, jest nieodłączną częścią podstawowego poziomu cyberbezpieczeństwa we wszystkich instytucjach, organach i agencjach Unii.

(10) Instytucje, organy i agencje Unii powinny przeprowadzić ocenę ryzyka związanego z relacjami z dostawcami i usługodawcami, w tym dostawcami usług przechowywania i przetwarzania danych lub zarządzanych usług w zakresie bezpieczeństwa, oraz wprowadzić odpowiednie środki w celu wyeliminowania tego ryzyka. Środki te powinny stanowić część podstawowego poziomu cyberbezpieczeństwa i być szczegółowo określone w wytycznych lub zaleceniach wydanych przez CERT-UE. Przy określeniu środków i wytycznych należy należycie uwzględnić odpowiednie przepisy i strategie UE, w tym oceny ryzyka i zalecenia wydane przez grupę współpracy ds. bezpieczeństwa sieci i informacji, takie jak unijna skoordynowana ocena ryzyka i unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G. Ponadto można wprowadzić wymóg certyfikacji odpowiednich produktów, usług i procesów ICT zgodnie ze specjalnymi unijnymi programami certyfikacji cyberbezpieczeństwa przyjętymi na podstawie art. 49 rozporządzenia (UE) 2019/881.

(11) W maju 2011 r. sekretarze generalni instytucji i organów Unii postanowili utworzyć zespół ds. wstępnej konfiguracji zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach Unii (CERT-UE), pod nadzorem międzyinstytucjonalnej rady sterującej. W lipcu 2012 r. sekretarze generalni potwierdzili ustalenia praktyczne i zgodzili się co do utrzymania CERT-UE jako stałego podmiotu, tak aby dalej wspomagać poprawę ogólnego poziomu bezpieczeństwa technologii informacyjnej w instytucjach, organach i agencjach Unii jako przykład dostrzegalnej współpracy międzyinstytucjonalnej w dziedzinie cyberbezpieczeństwa. We wrześniu 2012 r. powołano CERT-UE jako grupę zadaniową Komisji Europejskiej z mandatem międzyinstytucjonalnym. W grudniu 2017 r. instytucje i organy Unii zawarły porozumienie międzyinstytucjonalne w sprawie organizacji i funkcjonowania CERT-UE[3]. Ustalenia te powinny nadal ewoluować, aby wspierać wdrażanie niniejszego rozporządzenia.

(12) Należy zmienić nazwę CERT-UE z „zespołu reagowania na incydenty komputerowe” na „Centrum ds. Cyberbezpieczeństwa” instytucji, organów i agencji Unii, aby odzwierciedlić rozwój sytuacji w państwach członkowskich i na świecie, gdzie wiele zespołów CERT przemianowano na centra ds. cyberbezpieczeństwa, natomiast należy zachować nazwę skróconą „CERT-UE” ze względu na jej rozpoznawalność.

[3] Dz.U. C 12 z 13.1.2018, s. 1.

(13) Wiele cyberataków jest częścią szerszych kampanii, których celem są grupy instytucji, organów i agencji Unii lub wspólnoty interesów, do których należą instytucje, organy i agencje Unii. Aby umożliwić aktywne wykrywanie incydentów, reagowanie na nie lub wprowadzanie środków ograniczających ryzyko, instytucje, organy i agencje Unii powinny powiadamiać CERT-UE o znaczących cyberzagrożeniach, znaczących podatnościach i znaczących incydentach oraz przekazywać odpowiednie szczegółowe informacje techniczne, które umożliwiają wykrywanie lub ograniczenie ryzyka wystąpienia podobnych cyberzagrożeń, podatności i incydentów w innych instytucjach, organach i agencjach Unii, a także reagowanie na nie. Kierując się podejściem przewidzianym w dyrektywie [wniosek dotyczący dyrektywy NIS 2], należy zobowiązać podmioty, które powzięły wiedzę o znaczącym incydencie, do dokonania wstępnego zgłoszenia do CERT-UE w ciągu 24 godzin. Taka wymiana informacji powinna umożliwić CERT-UE rozpowszechnianie informacji wśród innych instytucji, organów i agencji Unii, jak również wśród ich właściwych odpowiedników, aby pomóc w ochronie środowisk informatycznych Unii i jej partnerów przed podobnymi incydentami, zagrożeniami i podatnościami.

(14) Oprócz powierzenia CERT-UE większej liczby zadań i rozszerzonej roli należy ustanowić Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa (IICB), która powinna ułatwiać osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa przez instytucje, organy i agencje Unii w drodze monitorowania wdrażania niniejszego rozporządzenia przez instytucje, organy i agencje Unii oraz nadzoru nad realizacją ogólnych priorytetów i celów przez CERT-UE i zapewniania CERT-UE strategicznego kierunku działania. IICB powinna zapewnić, aby instytucje były należycie reprezentowane, a w jej skład powinni wchodzić przedstawiciele agencji i organów za pośrednictwem sieci agencji Unii Europejskiej.

(15) CERT-UE powinien wspierać realizację działań na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa, przedstawiając propozycje wytycznych i zaleceń dla IICB lub wydając wezwania do działania. Wspomniane wytyczne i zalecenia powinny być zatwierdzane przez IICB. W razie potrzeby CERT-UE powinien wydawać wezwania do działania opisujące pilne środki w zakresie bezpieczeństwa, o których wprowadzenie w określonym terminie apeluje się do instytucji, organów i agencji Unii.

(16) IICB powinna monitorować przestrzeganie niniejszego rozporządzenia, jak również działania następcze związane z wytycznymi i zaleceniami oraz wezwaniami do działania wydanymi przez CERT-UE. W kwestiach technicznych IICB powinny wspierać techniczne grupy doradcze działające w składzie, który IICB uzna za stosowny, i ściśle współpracujące z CERT-UE, instytucjami, organami i agencjami Unii oraz innymi zainteresowanymi stronami, jeżeli zajdzie taka potrzeba. W stosownych przypadkach IICB powinna wydawać niewiążące ostrzeżenia i zalecać audyty.

(17) CERT-UE należy powierzyć misję przyczyniania się do bezpieczeństwa środowiska informatycznego wszystkich instytucji, organów i agencji Unii. CERT-UE powinien działać w charakterze odpowiednika wyznaczonego koordynatora dla instytucji, organów i agencji Unii, którego zadaniem jest koordynacja ujawniania podatności w europejskim rejestrze podatności, o którym mowa w art. 6 dyrektywy [wniosek dotyczący dyrektywy NIS 2].

(18) W 2020 r. rada sterująca CERT-UE ustaliła nowy cel strategiczny, zgodnie z którym CERT-UE ma zapewnić wszystkim instytucjom, organom i agencjom Unii kompleksowy poziom cyberobrony o odpowiednim zakresie i poziomie szczegółowości oraz stałą zdolność dostosowywania się do obecnych lub przyszłych zagrożeń, w tym ataków na urządzenia mobilne, środowiska chmury obliczeniowej i urządzenia internetu rzeczy. Ten strategiczny cel zakłada również utworzenie centrów monitorowania bezpieczeństwa (SOC) o szerokim zakresie działania, których zadaniem jest monitorowanie sieci, oraz prowadzenie całodobowego monitoringu zagrożeń o potencjalnie poważnych skutkach. W przypadku większych instytucji, organów i agencji Unii CERT-UE powinien wspierać ich zespoły ds. bezpieczeństwa informatycznego, m.in. poprzez prowadzenie całodobowego monitorowania jako pierwszej linii obrony. W przypadku mniejszych i niektórych średniej wielkości instytucji, organów i agencji Unii CERT-UE powinien zapewniać wszystkie te usługi.

(19) CERT-UE powinien również wypełniać przewidzianą dla niego w dyrektywie [wniosek dotyczący dyrektywy NIS 2] rolę dotyczącą współpracy i wymiany informacji z siecią zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT). Ponadto, zgodnie z zaleceniem Komisji (UE) 2017/1584[4], CERT-UE powinien współpracować z odpowiednimi zainteresowanymi stronami przy prowadzeniu działań podejmowanych w reakcji na incydenty oraz koordynować te działania. Aby przyczyniać się do wysokiego poziomu cyberbezpieczeństwa w całej Unii, CERT-UE powinien prowadzić wymianę informacji dotyczących konkretnych incydentów ze swoimi odpowiednikami krajowymi. CERT-UE powinien również współpracować z innymi partnerami publicznymi i prywatnymi, w tym NATO, pod warunkiem uzyskania uprzedniej zgody IICB.

(20) Wspierając cyberbezpieczeństwo na poziomie operacyjnym, CERT-UE powinien korzystać z dostępnej wiedzy fachowej Agencji Unii Europejskiej ds. Cyberbezpieczeństwa w ramach współpracy strukturalnej przewidzianej w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/881[5]. W stosownych przypadkach należy poczynić specjalne ustalenia pomiędzy oboma podmiotami, aby określić sposób praktycznej realizacji takiej współpracy i uniknąć powielania działań. CERT-UE powinien współpracować z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa w obszarze analizy zagrożeń i regularnie udostępniać Agencji swoje sprawozdanie dotyczące krajobrazu zagrożeń.

(21) W ramach wspierania wspólnej jednostki ds. cyberprzestrzeni utworzonej zgodnie z zaleceniem Komisji z 23 czerwca 2021 r.[6] CERT-UE powinien współpracować i prowadzić wymianę informacji z zainteresowanymi stronami, aby wzmocnić współpracę operacyjną i umożliwić istniejącym sieciom wykorzystanie ich pełnego potencjału w zakresie ochrony Unii.

---

4 Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz.U. L 239 z 19.9.2017, s. 36).

5 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)

6 Zalecenie Komisji C(2021) 4520 z dnia 23 czerwca 2021 r. w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni.

(22) Wszelkie dane osobowe przetwarzane na podstawie niniejszego rozporządzenia należy przetwarzać zgodnie z przepisami o ochronie danych, w tym z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2018/1725[7].

(23) Postępowanie z informacjami przez CERT-UE oraz instytucje, organy i agencje Unii powinno być zgodne z przepisami określonymi w rozporządzeniu [rozporządzenie w sprawie bezpieczeństwa informacji będące przedmiotem wniosku]. W celu zapewnienia koordynacji w sprawach bezpieczeństwa o wszelkich kontaktach z CERT-UE, które inicjują lub do których dążą krajowe służby bezpieczeństwa i wywiadu, należy bezzwłocznie informować Dyrekcję Komisji ds. Bezpieczeństwa oraz przewodniczącego IICB.

(24) Ponieważ usługi i zadania CERT-UE leżą w interesie wszystkich instytucji, organów i agencji Unii, wszystkie instytucje, organy i agencje Unii, które ponoszą wydatki na technologię informatyczną, powinny wnosić odpowiedni wkład na poczet kosztów tych usług i zadań. Wkład ten pozostaje bez uszczerbku dla autonomii budżetowej instytucji, organów i agencji Unii.

(25) IICB, z pomocą CERT-UE, powinna dokonywać przeglądu i oceny wykonania niniejszego rozporządzenia oraz przedkładać Komisji sprawozdania zawierające jej ustalenia. Na tej podstawie Komisja powinna przedkładać regularne sprawozdania Parlamentowi Europejskiemu, Radzie, Europejskiemu Komitetowi Ekonomiczno-Społecznemu i Komitetowi Regionów,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

Rozdział I
PRZEPISY OGÓLNE

Artykuł 1
Przedmiot

Niniejszym rozporządzeniem ustanawia się:

a) spoczywający na instytucjach, organach i agencjach Unii obowiązek ustanowienia wewnętrznych ram zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli;

b) spoczywające na instytucjach, organach i agencjach Unii obowiązki w zakresie zarządzania ryzykiem w cyberprzestrzeni i obowiązki w zakresie zgłaszania incydentów;

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

c) przepisy dotyczące organizacji i funkcjonowania Centrum ds. Cyberbezpieczeństwa instytucji, organów i agencji Unii (CERT-UE) oraz organizacji i funkcjonowania Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa.

Artykuł 2
Zakres

Niniejsze rozporządzenie ma zastosowanie do zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontrolowania przez wszystkie instytucje, organy i agencje Unii oraz do organizacji i funkcjonowania CERT-UE i Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa.

Artykuł 3
Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „instytucje, organy i agencje Unii” oznaczają instytucje, organy i agencje Unii ustanowione Traktatem o Unii Europejskiej, Traktatem o funkcjonowaniu Unii Europejskiej lub Traktatem ustanawiającym Europejską Wspólnotę Energii Atomowej lub na podstawie wspomnianych traktatów;

2) „sieci i systemy informatyczne” oznaczają sieci i systemy informatyczne zgodnie z definicją w art. 4 pkt 1 dyrektywy [wniosek dotyczący dyrektywy NIS 2];

3) „bezpieczeństwo sieci i systemów informatycznych” oznacza bezpieczeństwo sieci i systemów informatycznych zgodnie z definicją w art. 4 pkt 2 dyrektywy [wniosek dotyczący dyrektywy NIS 2];

4) „cyberbezpieczeństwo” oznacza cyberbezpieczeństwo zgodnie z definicją w art. 4 pkt 3 dyrektywy [wniosek dotyczący dyrektywy NIS 2];

5) „kierownictwo najwyższego szczebla” oznacza kierownika, organ zarządzający lub organ ds. koordynacji i nadzoru na najwyższym szczeblu administracyjnym, z uwzględnieniem ustaleń dotyczących zarządzania na wysokim szczeblu w każdej instytucji, każdym organie lub każdej agencji Unii;

6) „incydent” oznacza incydent zgodnie z definicją w art. 4 pkt 5 dyrektywy [wniosek dotyczący dyrektywy NIS 2];

7) „znaczący incydent” oznacza każdy incydent, chyba że ma on ograniczony wpływ i prawdopodobnie jest już dobrze poznany pod względem metod bądź technologii;

8) „poważny atak” oznacza każdy incydent wymagający większych zasobów niż zasoby dostępne w instytucji, organie lub agencji Unii dotkniętych incydentem oraz w CERT-UE;

9) „postępowanie w przypadku incydentu” oznacza postępowanie w przypadku incydentu zgodnie z definicją w art. 4 pkt 6 dyrektywy [wniosek dotyczący dyrektywy NIS 2];

10) „cyberzagrożenie” oznacza cyberzagrożenie zgodnie z definicją w art. 2 pkt 8 rozporządzenia (UE) 2019/881;

11) „znaczące cyberzagrożenie” oznacza cyberzagrożenie, za którym stoi zamiar, możliwość i zdolność do spowodowania znaczącego incydentu;

12) „podatność” oznacza podatność zgodnie z definicją w art. 4 pkt 8 dyrektywy [wniosek dotyczący dyrektywy NIS 2];

13) „znacząca podatność” oznacza podatność, która, jeżeli zostanie wykorzystana, prawdopodobnie doprowadzi do znaczącego incydentu;

14) „ryzyko w cyberprzestrzeni” oznacza każdą dającą się racjonalnie określić okoliczność lub każde dające się racjonalnie określić zdarzenie o potencjalnym niekorzystnym wpływie na bezpieczeństwo sieci i systemów informatycznych;

15) „wspólna jednostka ds. cyberprzestrzeni” oznacza wirtualną i fizyczną platformę współpracy przeznaczoną dla poszczególnych społeczności zajmujących się cyberbezpieczeństwem w Unii, z naciskiem na koordynację operacyjną i techniczną w przypadku poważnych transgranicznych cyberzagrożeń i cyberincydentów w rozumieniu zalecenia Komisji z 23 czerwca 2021 r.;

16) „podstawowy poziom cyberbezpieczeństwa” oznacza minimalny zbiór przepisów dotyczących cyberbezpieczeństwa, z którymi muszą być zgodne sieci i systemy informatyczne oraz których muszą przestrzegać ich operatorzy i użytkownicy, aby zminimalizować ryzyko w cyberprzestrzeni.

Rozdział II
ŚRODKI NA RZECZ WYSOKIEGO WSPÓLNEGO POZIOMU CYBERBEZPIECZEŃSTWA

Artykuł 4
Zarządzanie ryzykiem, jego nadzorowanie i kontrola

1. Każda instytucja, każdy organ i każda agencja Unii ustanawiają swoje własne wewnętrzne ramy zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli („ramy”), które mają wspierać misję danego podmiotu i umożliwiać mu korzystania z jego autonomii instytucjonalnej. Nadzór nad tymi pracami sprawuje kierownictwo najwyższego szczebla danego podmiotu, aby zapewnić skuteczne i ostrożne zarządzanie wszystkimi rodzajami ryzyka w cyberprzestrzeni. Ramy te wdraża się najpóźniej do dnia .... [15 miesięcy po wejściu w życie niniejszego rozporządzenia] r.

2. Ramy obejmują swym zakresem całość środowiska informatycznego danej instytucji, danego organu lub danej agencji, w tym każde środowisko informatyczne znajdujące się w ich siedzibie, wszelkie aktywa i usługi, które przekazano w ramach outsourcingu do środowisk przetwarzania w chmurze lub których hosting prowadzą strony trzecie, a także urządzenia mobilne, sieci korporacyjne, sieci biznesowe niepodłączone do internetu oraz wszelkie urządzenia podłączone do środowiska

informatycznego. W ramach tych uwzględnia się ciągłość działania i zarządzanie kryzysowe oraz bezpieczeństwo łańcucha dostaw, a także zarządzanie ryzykiem związanym z czynnikiem ludzkim, które może mieć wpływ na cyberbezpieczeństwo danej instytucji, danego organu lub danej agencji Unii.

3. Kierownictwo najwyższego szczebla każdej instytucji, każdego organu i każdej agencji Unii zapewnia nadzór nad przestrzeganiem przez swoją organizację obowiązków związanych z zarządzaniem ryzykiem w cyberprzestrzeni, jego nadzorowaniem i kontrolą, bez uszczerbku dla formalnej odpowiedzialności innych szczebli zarządzania za zgodność z przepisami i zarządzanie ryzykiem w ich odpowiednich obszarach odpowiedzialności.

4. Każda instytucja, każdy organ i każda agencja Unii posiadają skuteczne mechanizmy gwarantujące, że odpowiedni odsetek budżetu przewidzianego na technologie informatyczne jest przeznaczany na cyberbezpieczeństwo.

5. Każda instytucja, każdy organ i każda agencja Unii wyznaczają lokalnego urzędnika ds. cyberbezpieczeństwa lub osobę pełniącą równoważną funkcję, która działa jako pojedynczy punkt kontaktowy w odniesieniu do wszystkich kwestii związanych z cyberbezpieczeństwem.

Artykuł 5
Podstawowy poziom cyberbezpieczeństwa

1. Kierownictwo najwyższego szczebla każdej instytucji, każdego organu i każdej agencji Unii zatwierdza podstawowy poziom cyberbezpieczeństwa swojego podmiotu w celu uwzględnienia zagrożeń zidentyfikowanych na podstawie ram, o których mowa w art. 4 ust. 1. Dokonuje tego, aby wspierać misję podmiotu i zapewnić mu możliwość korzystania z jego autonomii instytucjonalnej. Podstawowy poziom cyberbezpieczeństwa wdraża się najpóźniej do dnia .... [18 miesięcy po wejściu w życie niniejszego rozporządzenia] r. i uwzględnia się w nim dziedziny wymienione w załączniku I oraz środki wymienione w załączniku II.

2. Kadra kierownicza najwyższego szczebla każdej instytucji, każdego organu i każdej agencji Unii regularnie uczestniczy w specjalnych szkoleniach, aby zdobyć wystarczającą wiedzę i wystarczające umiejętności umożliwiające zrozumienie i ocenę ryzyka w cyberprzestrzeni i praktyk zarządzania nim oraz ich wpływu na działalność organizacji.

Artykuł 6
Oceny dojrzałości

Każda instytucja, każdy organ i każda agencja Unii co najmniej raz na trzy lata przeprowadza ocenę dojrzałości w zakresie cyberbezpieczeństwa, obejmującą wszystkie elementy ich środowiska informatycznego opisane w art. 4, z uwzględnieniem odpowiednich wytycznych i zaleceń przyjętych zgodnie z art. 13.

Artykuł 7
Plany dotyczące cyberbezpieczeństwa

1. Zgodnie z wnioskami wynikającymi z oceny dojrzałości oraz z uwzględnieniem aktywów i zagrożeń określonych zgodnie z art. 4 kierownictwo najwyższego szczebla każdej instytucji, każdego organu i każdej agencji Unii zatwierdza plan dotyczący cyberbezpieczeństwa bez zbędnej zwłoki po ustanowieniu ram zarządzania ryzykiem, jego nadzorowania i kontroli oraz podstawowego poziomu cyberbezpieczeństwa. Plan ten ma na celu zwiększenie ogólnego poziomu cyberbezpieczeństwa danego podmiotu, a tym samym przyczynia się do osiągnięcia lub wzmocnienia wysokiego wspólnego poziomu cyberbezpieczeństwa wszystkich instytucji, organów i agencji Unii. Z myślą o wsparciu misji podmiotu w oparciu o jego autonomię instytucjonalną w planie uwzględnia się co najmniej dziedziny wymienione w załączniku I, środki wymienione w załączniku II, jak również środki związane z gotowością na wypadek incydentów, reagowaniem na nie i usuwaniem ich skutków, takie jak monitorowanie bezpieczeństwa i rejestrowanie danych dotyczących bezpieczeństwa. Plan poddaje się przeglądowi co najmniej raz na trzy lata po przeprowadzeniu ocen dojrzałości zgodnie z art. 6.

2. W planie dotyczącym cyberbezpieczeństwa uwzględnia się role i obowiązki członków personelu związane z wykonaniem planu.

3. W planie dotyczącym cyberbezpieczeństwa uwzględnia się wszelkie mające zastosowanie wytyczne i zalecenia wydane przez CERT-UE.

Artykuł 8
Wykonanie

1. Po przeprowadzeniu ocen dojrzałości instytucje, organy i agencje Unii przedkładają je Międzyinstytucjonalnej Radzie ds. Cyberbezpieczeństwa. Po sporządzeniu planów dotyczących bezpieczeństwa instytucje, organy i agencje Unii powiadamiają Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa o tym fakcie. Na wniosek Rady składają one sprawozdanie na temat konkretnych aspektów niniejszego rozdziału.

2. Wykonanie przepisów ustanowionych w niniejszym rozdziale wspierają wytyczne i zalecenia wydawane zgodnie z art. 13.

Rozdział III
MIĘDZYINSTYTUCJONALNA RADA DS. CYBERBEZPIECZEŃSTWA

Artykuł 9
Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa

1. Ustanawia się Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa (IICB).

2. IICB jest odpowiedzialna za:

a) monitorowanie wdrażania niniejszego rozporządzenia przez instytucje, organy i agencje Unii.

b) nadzór nad realizacją ogólnych priorytetów i celów przez CERT-UE oraz zapewnianie mu strategicznego kierunku działania.

3. W skład IICB wchodzi trzech przedstawicieli wyznaczonych przez sieć agencji Unii Europejskiej (EUAN) na wniosek jej komitetu doradczego ds. ICT w celu reprezentowania interesów agencji i organów, które posiadają własne środowisko informatyczne, oraz po jednym przedstawicielu wyznaczonym przez każdy z następujących podmiotów:

a) Parlament Europejski;

b) Radę Unii Europejskiej;

c) Komisję Europejską;

d) Trybunał Sprawiedliwości Unii Europejskiej;

e) Europejski Bank Centralny;

f) Europejski Trybunał Obrachunkowy;

g) Europejską Służbę Działań Zewnętrznych;

h) Europejski Komitet Ekonomiczno-Społeczny,

i) Europejski Komitet Regionów;

j) Europejski Bank Inwestycyjny;

k) Agencję Unii Europejskiej ds. Cyberbezpieczeństwa.

Członkowie mogą być wspomagani przez zastępców. Przewodniczący może zaprosić innych przedstawicieli organizacji wymienionych powyżej lub innych instytucji, organów i agencji Unii do udziału w posiedzeniach IICB bez prawa głosu.

4. IICB uchwala swój regulamin wewnętrzny.

5. IICB wyznacza spośród swoich członków przewodniczącego, zgodnie z regulaminem wewnętrznym, na okres czterech lat. Zastępca przewodniczącego staje się pełnoprawnym członkiem IICB na ten sam okres.

6. IICB odbywa posiedzenia z inicjatywy swojego przewodniczącego, na wniosek CERT-UE lub na wniosek któregokolwiek z członków IICB.

7. Każdy członek IICB dysponuje jednym głosem. Decyzje IICB zapadają zwykłą większością głosów, chyba że niniejsze rozporządzenie stanowi inaczej. Przewodniczący nie bierze udziału w głosowaniach, z wyjątkiem sytuacji gdy oddano taką samą liczbę głosów za i przeciw, w którym to przypadku przewodniczący może oddać decydujący głos.

8. IICB może podejmować działania w drodze uproszczonej procedury pisemnej zainicjowanej zgodnie z regulaminem wewnętrznym IICB. W ramach tej procedury daną decyzję uznaje się za zatwierdzoną w terminie wyznaczonym przez przewodniczącego, z wyjątkiem sytuacji, gdy członek zgłosi sprzeciw.

9. W posiedzeniach IICB uczestniczy szef CERT-UE lub jego zastępca, chyba że IICB postanowi inaczej.

10. Komisja zapewnia sekretariat IICB.

11. Przedstawiciele wyznaczeni przez EUAN na wniosek komitetu doradczego ds. ICT przekazują decyzje IICB agencjom i wspólnym przedsięwzięciom Unii. Każda agencja lub organ Unii ma prawo zwracać się do przedstawicieli lub przewodniczącego IICB z każdą sprawą, o której zdaniem tej agencji lub organu należy poinformować IICB.

12. IICB może działać w drodze uproszczonej procedury pisemnej zainicjowanej przez przewodniczącego, w ramach której daną decyzję uznaje się za zatwierdzoną w terminie wyznaczonym przez przewodniczącego, z wyjątkiem sytuacji, gdy członek zgłosi sprzeciw.

13. IICB może powołać komitet wykonawczy, który będzie pomagał w jej pracach, i przekazać komitetowi wykonawczemu niektóre swoje zadania i uprawnienia. IICB ustanawia regulamin wewnętrzny komitetu wykonawczego, w tym jego zadania i uprawnienia, oraz określa kadencje jego członków.

Artykuł 10
Zadania IICB

Wykonując swoje obowiązki, IICB w szczególności:

a) dokonuje przeglądu wszelkich sprawozdań dotyczących stanu wdrożenia niniejszego rozporządzenia przez instytucje, organy i agencje Unii, o które IICB wystąpiła do CERT-UE;

b) zatwierdza, na podstawie wniosku szefa CERT-UE, roczny program prac CERT-UE i monitoruje jego wykonanie;

c) zatwierdza, na podstawie wniosku szefa CERT-UE, katalog usług CERT-UE;

d) zatwierdza, na podstawie wniosku szefa CERT-UE, roczne planowanie finansowe w zakresie przychodów i wydatków, w tym dotyczące personelu, na potrzeby działalności CERT-UE;

e) zatwierdza, na podstawie wniosku szefa CERT-UE, ustalenia dotyczące umów o gwarantowanym poziomie usług;

f) analizuje i zatwierdza sprawozdanie roczne sporządzone przez szefa CERT-UE dotyczące działalności CERT-UE i zarządzania środkami finansowymi przez CERT-UE;

g) zatwierdza i monitoruje kluczowe wskaźniki skuteczności w odniesieniu do CERT-UE, określone w oparciu o wniosek szefa CERT-UE;

h) zatwierdza porozumienia o współpracy, porozumienia o gwarantowanym poziomie usług lub umowy między CERT-UE a innymi podmiotami zawarte na podstawie art. 17;

i) ustanawia taką liczbę technicznych grup doradczych, jaka jest niezbędna, aby wspierać prace IICB, zatwierdza zakres ich uprawnień i zadań i wyznacza ich przewodniczących.

Artykuł 11
Zapewnianie zgodności

IICB monitoruje wdrażanie niniejszego rozporządzenia oraz przyjętych wytycznych, zaleceń i wezwań do działania przez instytucje, organy i agencje Unii. W przypadku gdy IICB stwierdzi, że instytucje, organy lub agencje Unii nie stosują lub nie wdrażają skutecznie niniejszego rozporządzenia lub wytycznych, zaleceń i wezwań do działania wydanych na podstawie niniejszego rozporządzenia, bez uszczerbku dla wewnętrznych procedur odpowiedniej instytucji, odpowiedniego organu lub odpowiedniej agencji Unii może:

a) wydać ostrzeżenie; w stosownych przypadkach ze względu na istotne ryzyko w cyberprzestrzeni grono adresatów ostrzeżenia ulega odpowiedniemu ograniczeniu;

b) zalecić stosownej służbie audytu przeprowadzenie audytu.

Rozdział IV
CERT-UE

Artykuł 12
Misja i zadania CERT-UE

1. Misją CERT-UE, autonomicznego międzyinstytucjonalnego Centrum ds. Cyberbezpieczeństwa wszystkich instytucji, organów i agencji Unii, jest przyczynianie się do bezpieczeństwa jawnego środowiska informatycznego wszystkich instytucji, organów i agencji Unii poprzez doradzanie im w zakresie cyberbezpieczeństwa, pomaganie im w zapobieganiu incydentom, wykrywaniu ich, łagodzeniu ich skutków i reagowaniu na nie oraz poprzez występowanie dla tych instytucji, organów i agencji w roli punktu wymiany informacji na temat cyberbezpieczeństwa i koordynacji reakcji na incydenty.

2. CERT-UE wykonuje następujące zadania dla instytucji, organów i agencji Unii:

   a) wspiera je we wdrażaniu niniejszego rozporządzenia oraz przyczynia się do koordynacji stosowania niniejszego rozporządzenia za pomocą środków wymienionych w art. 13 ust. 1 lub poprzez sporządzanie doraźnych sprawozdań, o które wystąpiła IICB;

b) wspiera je, świadcząc pakiet usług z zakresu cyberbezpieczeństwa opisanych w katalogu usług („usługi podstawowe”);

c) utrzymuje sieć równorzędnych podmiotów i partnerów w celu wspierania usług określonych w art. 16 i 17;

d) zwraca uwagę IICB na wszelkie problemy związane z wdrażaniem niniejszego rozporządzenia oraz wdrażaniem wytycznych, zaleceń i wezwań do działania;

e) przedkłada sprawozdania dotyczące cyberzagrożeń, z jakimi mierzą się instytucje, organy i agencje Unii, oraz przyczynia się do zapewnienia orientacji sytuacyjnej w zakresie cyberbezpieczeństwa UE.

3. CERT-UE wspiera wspólną jednostkę ds. cyberprzestrzeni utworzoną zgodnie z zaleceniem Komisji z dnia 23 czerwca 2021 r., w tym w następujących obszarach:

a) gotowość, koordynowanie reakcji na incydenty, wymiana informacji i reagowanie w sytuacjach kryzysowych na poziomie technicznym w sprawach związanych z instytucjami, organami i agencjami Unii;

b) współpraca operacyjna w ramach sieci zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), w tym w zakresie wzajemnej pomocy, a także w ramach szerszej społeczności zajmującej się cyberbezpieczeństwem;

c) analiza cyberzagrożeń, w tym orientacja sytuacyjna;

d) w każdym obszarze wymagającym fachowej wiedzy technicznej CERT-UE w dziedzinie cyberbezpieczeństwa.

4. CERT-UE prowadzi zorganizowaną współpracę z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa w zakresie budowania zdolności, współpracy operacyjnej i długoterminowych analiz strategicznych cyberzagrożeń zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881.

5. CERT-UE może świadczyć następujące usługi nie opisane w jego katalogu usług („usługi płatne”):

a) usługi wspierające cyberbezpieczeństwo środowiska informatycznego instytucji, organów i agencji Unii inne niż usługi określone w ust. 2, na podstawie umów o gwarantowanym poziomie usług i z zastrzeżeniem dostępnych zasobów;

b) usługi wspierające operacje lub projekty w zakresie cyberbezpieczeństwa instytucji, organów i agencji Unii inne niż usługi zapewniające ochronę ich środowiska informatycznego, na podstawie pisemnych umów i po uprzednim zatwierdzeniu przez IICB;

c) usługi świadczone na rzecz organizacji niebędących instytucjami, organami i agencjami Unii, które ściśle współpracują z instytucjami, organami i agencjami Unii, na przykład ze względu na przydzielone im zadania lub obowiązki na mocy prawa Unii, które to usługi wspierają bezpieczeństwo

środowiska informatycznego tych organizacji, na podstawie pisemnych umów i po uprzednim zatwierdzeniu przez IICB.

6. CERT-UE może organizować ćwiczenia w zakresie cyberbezpieczeństwa lub zalecać uczestnictwo w istniejących ćwiczeniach, w stosownych przypadkach w ścisłej współpracy z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa, w celu testowania poziomu cyberbezpieczeństwa instytucji, organów i agencji Unii.

7. CERT-UE może udzielać pomocy instytucjom, organom i agencjom Unii w zakresie incydentów w niejawnym środowisku informatycznym, o ile zainteresowany podmiot wyraźnie się o to zwróci.

Artykuł 13
Wytyczne, zalecenia i wezwania do działania

1. CERT-UE wspiera wdrażanie niniejszego rozporządzenia poprzez:

   a) wydawanie wezwań do działania opisujących pilne środki w zakresie bezpieczeństwa, o których zastosowanie w określonym terminie apeluje się do instytucji, organów i agencji Unii;

   b) przedstawianie IICB propozycji wytycznych skierowanych do wszystkich instytucji, organów i agencji Unii lub części z nich;

   c) przedstawianie IICB propozycji zaleceń skierowanych do poszczególnych instytucji, organów i agencji Unii.

2. Wytyczne i zalecenia mogą obejmować:

   a) sposoby zarządzania ryzykiem w cyberprzestrzeni i formułowania podstawowego poziomu cyberbezpieczeństwa lub usprawnienia tych procesów;

   b) sposoby przeprowadzania ocen dojrzałości i opracowywania planów dotyczących cyberbezpieczeństwa; oraz

   c) w stosownych przypadkach, wykorzystanie wspólnej technologii, architektury i powiązanych najlepszych praktyk w celu osiągnięcia interoperacyjności i wspólnych norm w rozumieniu art. 4 pkt 10 dyrektywy [wniosek dotyczący dyrektywy NIS 2].

3. IICB może przyjmować wytyczne lub zalecenia zgodnie z propozycją CERT-UE.

4. IICB może polecić CERT-UE wydanie, wycofanie lub zmianę proponowanych wytycznych lub zaleceń, lub wezwań do działania.

Artykuł 14
Szef CERT-UE

Szef CERT-UE regularnie przedkłada IICB i przewodniczącemu IICB sprawozdania dotyczące realizacji zadań CERT-UE, planowania finansowego, przychodów, wykonania

budżetu, realizacji zawartych umów o gwarantowanym poziomie usług i pisemnych umów, współpracy z jego odpowiednikami i partnerami, a także podróży służbowych realizowanych przez jego pracowników, w tym sprawozdania, o których mowa w art. 10 ust. 1.

Artykuł 15
Sprawy finansowe i kadrowe

1. Komisja, po uzyskaniu jednomyślnej zgody IICB, mianuje szefa CERT-UE. Na wszystkich etapach procedury poprzedzającej mianowanie szefa CERT-UE, w szczególności podczas przygotowywania ogłoszeń o naborze, rozpatrywania zgłoszeń oraz powoływania komisji selekcyjnych w odniesieniu do tego stanowiska, zasięga się opinii IICB.

2. W zakresie stosowania procedur administracyjnych i finansowych szef CERT-UE działa z upoważnienia Komisji.

3. Zadania i działania CERT-UE, w tym usługi świadczone przez CERT-UE zgodnie z art. 12 ust. 2, 3, 4 i 6 oraz art. 13 ust. 1 na rzecz instytucji, organów i agencji Unii finansowanych w ramach działu wieloletnich ram finansowych dotyczącego europejskiej administracji publicznej, są finansowane z odrębnej linii budżetowej budżetu Komisji. Stanowiska przeznaczone dla CERT-UE wyszczególnia się w przypisie do planu zatrudnienia Komisji.

4. Instytucje, organy i agencje Unii inne niż te wymienione w ust. 3 wnoszą roczny wkład finansowy na rzecz CERT-UE w celu pokrycia kosztów usług świadczonych przez CERT-UE na podstawie ust. 3. Odpowiednie wkłady opierają się na wskazówkach wydanych przez IICB i są przedmiotem uzgodnień zawartych między każdym podmiotem a CERT-UE w umowach o gwarantowanym poziomie usług. Wkłady odzwierciedlają sprawiedliwy i proporcjonalny udział w całkowitych kosztach świadczonych usług. Ujmuje się je w odrębnej linii budżetowej, o której mowa w ust. 3, jako dochody przeznaczone na określony cel, jak przewidziano w art. 21 ust. 3 lit. c) rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046[8].

5. Koszty realizacji zadań określonych w art. 12 ust. 5 odzyskuje się od instytucji, organów i agencji Unii korzystających z usług CERT-UE. Dochody przypisuje się do linii budżetowych przeznaczonych na pokrycie kosztów.

Artykuł 16
Współpraca CERT-UE z jego odpowiednikami w państwach członkowskich

1. CERT-UE współpracuje i prowadzi wymianę informacji ze swoimi odpowiednikami krajowymi w państwach członkowskich, w tym z zespołami CERT, Krajowymi Centrami ds. Cyberbezpieczeństwa, zespołami CSIRT oraz pojedynczymi punktami

[8] Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 z dnia 18 lipca 2018 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, zmieniające rozporządzenia (UE) nr 1296/2013, (UE) nr 1301/2013, (UE) nr 1303/2013, (UE) nr 1304/2013, (UE) nr 1309/2013, (UE) nr 1316/2013, (UE) nr 223/2014 i (UE) nr 283/2014 oraz decyzję nr 541/2014/UE, a także uchylające rozporządzenie (UE, Euratom) nr 966/2012 (Dz.U. L 193 z 30.7.2018, s. 1).

kontaktowymi, o których mowa w art. 8 dyrektywy [wniosek dotyczący dyrektywy NIS 2], w zakresie cyberzagrożeń, podatności i incydentów, możliwych środków przeciwdziałania oraz wszystkich kwestii istotnych dla poprawy ochrony środowiska informatycznego instytucji, organów i agencji Unii, w tym za pośrednictwem sieci CSIRT, o której mowa w art. 13 dyrektywy [wniosek dotyczący dyrektywy NIS 2].

2. CERT-UE może prowadzić wymianę informacji dotyczących konkretnych incydentów ze swoimi odpowiednikami krajowymi w państwach członkowskich, aby ułatwić wykrywanie podobnych cyberzagrożeń lub incydentów bez konieczności uzyskania zgody zainteresowanego podmiotu dotkniętego incydentem. CERT-UE może prowadzić wymianę informacji dotyczących konkretnych incydentów, które to informacje umożliwiają identyfikację celu, w który wymierzony jest cyberincydent, wyłącznie za zgodą zainteresowanego podmiotu dotkniętego incydentem.

Artykuł 17
Współpraca CERT-UE z jego odpowiednikami w państwach trzecich

1. CERT-UE może współpracować ze swoimi odpowiednikami w państwach trzecich, w tym z odpowiednikami działającymi w konkretnych sektorach, w zakresie narzędzi i metod, takich jak techniki, taktyka, procedury i najlepsze praktyki, a także w zakresie cyberzagrożeń i podatności. CERT-UE zwraca się do IICB o uprzednią zgodę na podjęcie wszelkiej współpracy z takimi odpowiednikami, w tym w kontekście współpracy odpowiedników spoza UE z odpowiednikami krajowymi w państwach członkowskich.

2. CERT-UE może współpracować z innymi partnerami, takimi jak podmioty handlowe, organizacje międzynarodowe, podmioty krajowe spoza Unii Europejskiej lub indywidualni eksperci, w celu gromadzenia informacji na temat ogólnych i szczególnych cyberzagrożeń, podatności i możliwych środków przeciwdziałania. CERT-UE zwraca się do IICB o uprzednią zgodę na podjęcie szerszej współpracy z takimi partnerami.

3. Po uzyskaniu zgody zainteresowanego podmiotu dotkniętego incydentem CERT-UE może przekazać informacje dotyczące tego incydentu partnerom, którzy mogą wnieść wkład w jego analizy.

Rozdział V
OBOWIĄZKI W ZAKRESIE WSPÓŁPRACY I ZGŁASZANIA

Artykuł 18
Postępowanie z informacjami

1. CERT-UE oraz instytucje, organy i agencje Unii przestrzegają obowiązku zachowania tajemnicy zawodowej zgodnie z art. 339 Traktatu o funkcjonowaniu Unii Europejskiej lub równoważnymi mającymi zastosowanie ramami.

2. Przepisy rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady[9] mają zastosowanie w odniesieniu do wniosków o udzielenie publicznego dostępu do dokumentów przechowywanych przez CERT-UE, w tym wynikającego z tego rozporządzenia obowiązku konsultowania się z innymi instytucjami, organami i agencjami Unii, jeśli przedmiotem wniosku są ich dokumenty.

3. Do przetwarzania danych osobowych na podstawie niniejszego rozporządzenia stosuje się rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725.

4. CERT-UE oraz korzystające z jego usług instytucje, organy i agencje Unii postępują z informacjami w sposób zgodny z przepisami określonymi w [wniosek dotyczący rozporządzenia w sprawie bezpieczeństwa informacji].

5. O wszelkich kontaktach z CERT-UE, które inicjują lub do których dążą krajowe służby bezpieczeństwa i wywiadu, bezzwłocznie informuje się Dyrekcję Komisji ds. Bezpieczeństwa oraz przewodniczącego IICB.

Artykuł 19
Obowiązki w zakresie wymiany informacji

1. Aby umożliwić CERT-UE koordynację zarządzania podatnościami oraz reagowania na incydenty, CERT-UE może zwracać się do instytucji, organów i agencji Unii o przekazanie mu informacji z ich odpowiednich rejestrów zasobów informatycznych, które to informacje są istotne z punktu widzenia wsparcia świadczonego przez CERT-UE. Instytucja, organ lub agencja, do których się zwrócono, bez zbędnej zwłoki przekazują przedmiotowe informacje oraz ich wszelkie późniejsze aktualizacje.

2. Instytucje, organy i agencje Unii, na wniosek CERT-UE i bez zbędnej zwłoki, przekazują mu informacje cyfrowe powstałe w wyniku korzystania z urządzeń elektronicznych uczestniczących w incydentach, które u nich wystąpiły. CERT-UE może dodatkowo sprecyzować, jakich rodzajów tych informacji cyfrowych potrzebuje do celów orientacji sytuacyjnej i reagowania na incydenty.

3. CERT-UE może prowadzić wymianę informacji dotyczących konkretnych incydentów, które to informacje umożliwiają identyfikację instytucji, organu lub agencji Unii dotkniętych incydentem, wyłącznie za zgodą tego podmiotu. CERT-UE może prowadzić wymianę informacji dotyczących konkretnych incydentów, które to informacje umożliwiają identyfikację celu, w który wymierzony jest cyberincydent, wyłącznie za zgodą podmiotu dotkniętego incydentem.

4. Obowiązki w zakresie wymiany informacji nie obejmują informacji niejawnych UE (EUCI) ani informacji, które służby bezpieczeństwa lub wywiadu lub organy ścigania państwa członkowskiego przekazały instytucji, organowi lub agencji Unii z wyraźnym zastrzeżeniem, że nie można ich udostępniać CERT-UE.

[9] Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. L 145 z 31.5.2001, s. 43).

Artykuł 20

Obowiązki w zakresie zgłaszania

1. Wszystkie instytucje, organy i agencje Unii przekazują CERT-UE wstępne zgłoszenie dotyczące znaczących cyberzagrożeń, znaczących podatności i znaczących incydentów bez zbędnej zwłoki, jednak w żadnym wypadku nie później niż 24 godziny po powzięciu wiedzy o ich zaistnieniu.

   W należycie uzasadnionych przypadkach i w porozumieniu z CERT-UE instytucja, organ lub agencja Unii, których to dotyczy, mogą odstąpić od terminu określonego w poprzednim ustępie.

2. Ponadto instytucje, organy i agencje Unii bez zbędnej zwłoki przekazują CERT-UE odpowiednie szczegółowe informacje techniczne dotyczące cyberzagrożeń, podatności i incydentów, które to informacje umożliwiają ich wykrywanie, reagowanie na incydenty lub wprowadzanie środków ograniczających ryzyko. Zgłoszenie zawiera następujące informacje, o ile są one dostępne:

   a) odpowiednie oznaki naruszenia integralności systemu;

   b) odpowiednie mechanizmy wykrywania;

   c) potencjalny wpływ;

   d) odpowiednie środki łagodzące skutki cyberzagrożeń, podatności lub incydentów.

3. CERT-UE co miesiąc przekazuje ENISA sprawozdanie podsumowujące zawierające zanonimizowane i zagregowane dane dotyczące znaczących cyberzagrożeń, znaczących podatności i znaczących incydentów zgłoszonych zgodnie z ust. 1.

4. IICB może wydawać wytyczne lub zalecenia dotyczące sposobu dokonywania zgłoszeń i ich treści. CERT-UE rozpowszechnia odpowiednie szczegółowe informacje techniczne w celu umożliwienia proaktywnego wykrywania incydentów, reagowania na nie lub wprowadzania środków łagodzących ich skutki przez instytucje, organy i agencje Unii.

5. Obowiązki w zakresie zgłaszania nie obejmują EUCI ani informacji, które służby bezpieczeństwa i wywiadu lub organy ścigania państwa członkowskiego przekazały instytucji, organowi lub agencji Unii z wyraźnym zastrzeżeniem, że nie można ich udostępniać CERT-UE.

Artykuł 21

Koordynacja reakcji na incydenty i współpraca w zakresie znaczących incydentów

1. Działając jako punkt wymiany informacji na temat cyberbezpieczeństwa i koordynacji reakcji na incydenty, CERT-UE ułatwia wymianę informacji dotyczących cyberzagrożeń, podatności i incydentów między:

   a) instytucjami, organami i agencjami Unii;

b) odpowiednikami, o których mowa w art. 16 i 17.

2. CERT-UE ułatwia koordynację między instytucjami, organami i agencjami Unii reakcji na incydenty, co obejmuje:

a) przyczynianie się do spójnej komunikacji zewnętrznej;

b) wzajemną pomoc;

c) optymalne wykorzystanie zasobów operacyjnych;

d) koordynację z innymi mechanizmami reagowania kryzysowego na szczeblu Unii.

3. CERT-UE wspiera instytucje, organy i agencje Unii w zakresie orientacji sytuacyjnej w odniesieniu do cyberzagrożeń, podatności i incydentów.

4. IICB wydaje wytyczne dotyczące koordynacji reakcji na incydenty i współpracy w tym zakresie w odniesieniu do znaczących incydentów. W przypadku podejrzenia, że incydent nosi znamiona przestępstwa, CERT-UE doradza, jak zgłaszać incydent organom ścigania.

Artykuł 22
Poważne ataki

1. CERT-UE koordynuje między instytucjami, organami i agencjami Unii reakcje na poważne ataki. Prowadzi wykaz fachowej wiedzy technicznej, która może być potrzebna, aby reagować na incydenty w przypadku takich ataków.

2. Instytucje, organy i agencje Unii wnoszą wkład w tworzenie wykazu fachowej wiedzy technicznej, udostępniając aktualizowany co roku wykaz ekspertów dostępnych w ich odpowiednich organizacjach, z wyszczególnieniem ich konkretnych umiejętności technicznych.

3. Za zgodą zainteresowanych instytucji, organów i agencji Unii CERT-UE może również zwrócić się do ekspertów wymienionych w wykazie, o którym mowa w ust. 2, o wniesienie wkładu w działania podejmowane w reakcji na poważny atak w państwie członkowskim, zgodnie z procedurami operacyjnymi wspólnej jednostki ds. cyberprzestrzeni.

Rozdział VI
PRZEPISY KOŃCOWE

Artykuł 23
Początkowa realokacja środków budżetowych

Komisja proponuje realokację zasobów ludzkich i finansowych z odpowiednich instytucji, organów i agencji Unii do budżetu Komisji. Realokacja ta staje się skuteczna w tym samym czasie co pierwszy budżet przyjęty po wejściu w życie niniejszego rozporządzenia.

Artykuł 24
Przegląd

1. IICB, z pomocą CERT-UE, składa Komisji okresowe sprawozdania z wykonania niniejszego rozporządzenia. IICB może również kierować do Komisji zalecenia, aby Komisja zaproponowała zmiany w niniejszym rozporządzeniu.

2. Komisja składa Parlamentowi Europejskiemu i Radzie sprawozdanie z wykonania niniejszego rozporządzenia najpóźniej 48 miesięcy po jego wejściu w życie, a następnie co trzy lata.

3. Komisja dokonuje oceny funkcjonowania niniejszego rozporządzenia i składa sprawozdanie Parlamentowi Europejskiemu, Radzie, Europejskiemu Komitetowi Ekonomiczno-Społecznemu i Komitetowi Regionów nie wcześniej niż pięć lat od daty jego wejścia w życie.

Artykuł 25
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 […] r.

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

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

1.2. Obszary polityki, których dotyczy wniosek/inicjatywa

1.3. Wniosek/inicjatywa dotyczy:

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

1.4.2. Cel(e) szczegółowy(e)

1.4.3. Oczekiwane wyniki i wpływ

1.4.4. Wskaźniki dotyczące realizacji celów

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii" należy rozumieć jako wartość wynikającą z unijnej interwencji, wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie

1.5.3. Główne wnioski wyciągnięte z podobnych działań

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym zakresu przegrupowania środków

1.6. Czas trwania i wpływ finansowy wniosku/inicjatywy

1.7. Planowane tryby zarządzania

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

2.2. System zarządzania i kontroli

2.2.1. Uzasadnienie dla systemu zarządzania, mechanizmów finansowania wykonania, warunków płatności i proponowanej strategii kontroli

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

2.2.3. Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu)

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

3.2. Szacunkowy wpływ finansowy wniosku na środki

3.2.1. Podsumowanie szacunkowego wpływu na środki operacyjne

3.2.2. Przewidywany produkt finansowany ze środków operacyjnych

3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

3.2.5. Udział osób trzecich w finansowaniu

3.3. Szacunkowy wpływ na dochody

OCENA SKUTKÓW FINANSOWYCH REGULACJI

1. STRUKTURA WNIOSKU/INICJATYWY

1.1. Tytuł wniosku/inicjatywy

Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach, urzędach i agencjach Unii

1.2. Obszary polityki, których dotyczy wniosek/inicjatywa

Europejska administracja publiczna.

Wniosek dotyczy środków zapewniających wysoki wspólny poziom cyberbezpieczeństwa w instytucjach, organach i agencjach Unii.

1.3. Wniosek/inicjatywa dotyczy:

☑nowego działania

☐ nowego działania, będącego następstwem projektu pilotażowego/działania przygotowawczego[10]

☐ przedłużenia bieżącego działania

☑ połączenia lub przekształcenia co najmniej jednego działania pod kątem innego/nowego działania

1.4. Cel(e)

1.4.1. Cel(e) ogólny(e)

– Ustanowienie ram zapewniających wysoki wspólny poziom cyberbezpieczeństwa w instytucjach, organach i agencjach Unii.

– Zapewnienie nowej podstawy prawnej dla CERT-UE w celu wzmocnienia jego mandatu i finansowania.

1.4.2. Cel(e) szczegółowy(e)

1) Określenie spoczywających na instytucjach, organach i agencjach Unii obowiązków w zakresie ustanowienia wewnętrznych ram zarządzania ryzykiem w cyberprzestrzeni, jego nadzoru i kontroli.

2) Określenie spoczywających na instytucjach, organach i agencjach Unii obowiązków w zakresie składania sprawozdań dotyczących ram zarządzania

[10] O którym mowa w art. 58 ust. 2 lit. a) lub b) rozporządzenia finansowego.

ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli oraz zgłaszania cyberincydentów.

3) Określenie przepisów dotyczących organizacji i funkcjonowania Centrum ds. Cyberbezpieczeństwa instytucji, organów i agencji Unii (CERT-UE) oraz organizacji i funkcjonowania Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa (IICB).

4) Wspieranie wspólnej jednostki ds. cyberprzestrzeni.

1.4.3. Oczekiwane wyniki i wpływ

Należy wskazać, jakie efekty przyniesie wniosek/inicjatywa beneficjentom/grupie docelowej.

– Wewnętrzne ramy zarządzania ryzykiem w cyberprzestrzeni, jego nadzoru i kontroli, podstawowy poziom cyberbezpieczeństwa, regularne oceny dojrzałości i plany dotyczące cyberbezpieczeństwa w instytucjach, organach i agencjach Unii. – Poprawa odporności pod względem cyberbezpieczeństwa i zdolności w zakresie reagowania na incydenty w instytucjach, organach i agencjach Unii. – Modernizacja CERT-UE. – Wspieranie wspólnej jednostki ds. cyberprzestrzeni.

1.4.4. Wskaźniki dotyczące realizacji celów

Należy wskazać wskaźniki stosowane do monitorowania postępów i osiągnięć.

– Istniejące ramy i poziomy podstawowe, regularne oceny dojrzałości i plany dotyczące cyberbezpieczeństwa przeprowadzane w instytucjach, organach i agencjach Unii. – Skuteczniejsze postępowanie w przypadku incydentu. – Zwiększenie świadomości w zakresie ryzyka w cyberprzestrzeni na poziomie kadry kierowniczej najwyższego szczebla w instytucjach, organach i agencjach Unii. – Wyrównanie wydatków na bezpieczeństwo ICT jako odsetka całkowitych wydatków na ICT. – Silne przywództwo IICB i CERT-UE. – Zwiększona wymiana informacji między instytucjami, organami i agencjami Unii oraz z odpowiednimi organami i zainteresowanymi stronami w UE. – Zacieśniona współpraca w zakresie cyberbezpieczeństwa z odpowiednimi organami i zainteresowanymi stronami w UE za pośrednictwem CERT-UE i ENISA.

1.5. Uzasadnienie wniosku/inicjatywy

1.5.1. Potrzeby, które należy zaspokoić w perspektywie krótko- lub długoterminowej, w tym szczegółowy terminarz przebiegu realizacji inicjatywy

Celem wniosku jest zwiększenie poziomu cyberodporności instytucji, organów i agencji Unii, zmniejszenie niespójności w odporności tych podmiotów oraz podniesienie poziomu wspólnej orientacji sytuacyjnej i wspólnej zdolności do przygotowania się i reagowania na incydenty.

Wniosek jest w pełni zgodny z innymi powiązanymi inicjatywami, w szczególności z wnioskiem dotyczącym dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 [wniosek dotyczący dyrektywy NIS 2].

Wniosek jest niezbędnym elementem strategii UE w zakresie unii bezpieczeństwa oraz strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę.

Wniosek dotyczący rozporządzenia ma zostać przedstawiony przez Komisję Europejską w październiku 2021 r., rozporządzenie ma zostać przyjęte przez Parlament Europejski i Radę w 2022 r., a jego przepisy zaczną obowiązywać z chwilą wejścia w życie rozporządzenia. Wpływ finansowy i wpływ na zasoby ludzkie przedstawione w niniejszej ocenie skutków finansowych regulacji mają rozpocząć się w 2023 r. Okres przygotowawczy rozpoczął się już w 2021 r., ale działania przygotowawcze podejmowane w latach 2021 i 2022 nie są uwzględnione w skutkach finansowych wniosku.

1.5.2. Wartość dodana z tytułu zaangażowania Unii Europejskiej (może wynikać z różnych czynników, na przykład korzyści koordynacyjnych, pewności prawa, większej efektywności lub komplementarności). Na potrzeby tego punktu „wartość dodaną z tytułu zaangażowania Unii" należy rozumieć jako wartość wynikającą z unijnej interwencji, wykraczającą poza wartość, która zostałaby wytworzona przez same państwa członkowskie.

Przyczyny działania na poziomie europejskim (*ex ante*)

W okresie od 2019 do 2021 r. liczba znaczących incydentów mających wpływ na instytucje, organy i agencje Unii, za którymi to incydentami stali agresorzy stwarzający zaawansowane, trwałe zagrożenie, wzrosła w sposób dramatyczny. W pierwszej połowie 2021 r. odnotowano taką samą liczbę znaczących incydentów jak w całym 2020 r. Jest to również odzwierciedlone w liczbie kopii danych wykonanych na potrzeby informatyki śledczej (zrzutów zawartości zainfekowanych systemów lub urządzeń), które CERT-UE analizowało w 2020 r., trzykrotnie wyższej w stosunku do 2019 r., podczas gdy liczba znaczących incydentów wzrosła ponad dziesięciokrotnie od 2018 r.

Poziomy dojrzałości w zakresie cyberbezpieczeństwa różnią się znacznie w zależności od podmiotu[11]. Niniejsze rozporządzenie zapewnia, aby wszystkie

[11] Odniesienie: [sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego w sprawie cyberbezpieczeństwa w instytucjach, organach i agencjach Unii].

instytucje, organy i agencje Unii wdrażały podstawowe środki bezpieczeństwa i współpracowały ze sobą w celu otwartego i skutecznego funkcjonowania administracji unijnej.

Systemy, które mają zostać zachowane, wchodzą w zakres autonomii instytucji, organów i agencji Unii i są przez nie obsługiwane; proponowane działania nie mogły zostać podjęte przez państwa członkowskie.

1.5.3. Główne wnioski wyciągnięte z podobnych działań

Dyrektywa NIS jest pierwszym horyzontalnym instrumentem rynku wewnętrznego mającym na celu zwiększenie odporności sieci i systemów w Unii na ryzyko w cyberprzestrzeni. Od czasu jej wejścia w życie w 2016 r. przyczyniła się ona w znacznym stopniu do podniesienia wspólnego poziomu cyberbezpieczeństwa wśród państw członkowskich. Wniosek dotyczący dyrektywy NIS2 ma na celu dalszą poprawę tych środków.

Celem rozporządzenia jest zapewnienie podobnych środków dla instytucji, organów i agencji Unii.

1.5.4. Spójność z wieloletnimi ramami finansowymi oraz możliwa synergia z innymi właściwymi instrumentami

Wniosek jest spójny z wieloletnimi ramami finansowymi i jest niezbędnym elementem strategii UE w zakresie unii bezpieczeństwa oraz strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę.

We wniosku przewidziano zastosowanie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w odniesieniu do instytucji, organów i agencji Unii. Wniosek jest zgodny z wnioskiem dotyczącym dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającej dyrektywę (UE) 2016/1148 [wniosek dotyczący dyrektywy NIS 2].

1.5.5. Ocena różnych dostępnych możliwości finansowania, w tym zakresu przegrupowania środków

Zarządzanie zadaniami przez CERT-UE wymaga szczególnych profili i dodatkowego obciążenia pracą, których nie można zaspokoić bez zwiększenia zasobów ludzkich i finansowych.

1.6. Czas trwania i wpływ finansowy wniosku/inicjatywy

☐ **ograniczony czas trwania**

– ☐ Okres trwania wniosku/inicjatywy: od [DD.MM]RRRR r. do [DD.MM]RRRR r.

– ☐ Okres trwania wpływu finansowego: od RRRR r. do RRRR r. w odniesieniu do środków na zobowiązania oraz od RRRR r. do RRRR r. w odniesieniu do środków na płatności.

☑ **nieograniczony czas trwania**

– Wpływ finansowy powinien rozpocząć się wraz z pierwszym budżetem przyjętym po wejściu w życie rozporządzenia. Realokacja zasobów z instytucji i głównych organów Unii na rzecz Komisji miałaby miejsce w pierwszym roku, uważanym za rok przejściowy; ta i inna (ponowna) alokacja zasobów odbędzie się w ramach budżetów rocznych. Jeżeli rozporządzenie zostanie przyjęte w 2022 r., rok budżetowy 2023 będzie okresem przejściowym, a rok 2024 będzie rokiem funkcjonowania na pełną skalę.

1.7. Planowane tryby zarządzania[12]

☑ **Bezpośrednie zarządzanie** przez Komisję i poszczególne instytucje, organy i agencje Unii

– ☑ w ramach jej służb, w tym za pośrednictwem jej pracowników w delegaturach Unii;

– ☐ przez agencje wykonawcze.

☐ **Zarządzanie dzielone** z państwami członkowskimi

☐ **Zarządzanie pośrednie** poprzez przekazanie zadań związanych z wykonaniem budżetu:

– ☐ państwom trzecim lub organom przez nie wyznaczonym;

– ☐ organizacjom międzynarodowym i ich agencjom (należy wyszczególnić);

– ☐ EBI oraz Europejskiemu Funduszowi Inwestycyjnemu;

– ☐ organom, o których mowa w art. 70 i 71 rozporządzenia finansowego;

– ☐ organom prawa publicznego;

– ☐ podmiotom podlegającym prawu prywatnemu, które świadczą usługi użyteczności publicznej, o ile zapewniają one odpowiednie gwarancje finansowe;

[12] Wyjaśnienia dotyczące trybów zarządzania oraz odniesienia do rozporządzenia finansowego znajdują się na następującej stronie: https://myintracomm.ec.europa.eu/budgweb/PL/man/budgmanag/Pages/budgmanag.aspx

– ☐ podmiotom podlegającym prawu prywatnemu państwa członkowskiego, którym powierzono realizację partnerstwa publiczno-prywatnego oraz które zapewniają odpowiednie gwarancje finansowe;

– ☐ osobom odpowiedzialnym za wykonanie określonych działań w dziedzinie wspólnej polityki zagranicznej i bezpieczeństwa na mocy tytułu V Traktatu o Unii Europejskiej oraz określonym we właściwym podstawowym akcie prawnym.

– *W przypadku wskazania więcej niż jednego trybu należy podać dodatkowe informacje w części „Uwagi”.*

Uwagi

W zakresie stosowania procedur administracyjnych i finansowych CERT-UE działa z upoważnienia Komisji.

Dodatkowe zasoby wynikające z projektu rozporządzenia:

Wdrożenie art. 12 i 13 projektu rozporządzenia prowadzi do rozszerzenia katalogu usług o dodatkowe usługi podstawowe. W przypadku funkcjonowania na pełną skalę konieczne będą następujące dodatkowe zasoby (do zakończenia obowiązywania WRF z końcem 2027 r.): 21 EPC i 14,05 mln EUR.

Podział dodatkowych zasobów budżetowych na poszczególne zadania przedstawia się następująco:

a) na wykonywanie zadań dla instytucji, organów i agencji Unii wyszczególnionych w art. 12 ust. 2 lit. a), b), c) i e): 13,75 EPC i 11,275 mln EUR;

b) na wykonywanie zadań wyszczególnionych w art. 12 ust. 3 (wspieranie wspólnej jednostki ds. cyberprzestrzeni): 2 EPC i 381 000 EUR;

c) na wykonywanie zadań wyszczególnionych w art. 12 ust. 4 (zorganizowana współpraca z ENISA): 0,25 EPC i 236 000 EUR;

d) na wykonywanie zadań wyszczególnionych w art. 12 ust. 6 (ćwiczenia w dziedzinie cyberbezpieczeństwa): 0,25 EPC i 79 000 EUR;

e) na wykonywanie zadań wyszczególnionych w art. 12 ust. 2 lit. d) i art. 13 (analiza i sprawozdawczość w zakresie wdrażania rozporządzenia, przygotowanie wytycznych, zaleceń i wezwań do działania): 3,75 EPC i 2,079 mln EUR;

f) na wykonywanie zadań w celu wsparcia sekretariatu Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa (IICB): 1 EPC.

Przegląd bieżących zasobów i przejście na funkcjonowanie na pełną skalę:

We wrześniu 2021 r. CERT-UE funkcjonował, mając do dyspozycji następujące zasoby:

– stanowiska stałe i oddelegowane: 14 EPC,

– pracownicy kontraktowi finansowani z przychodów z umów o gwarantowanym poziomie usług: 24 EPC,

– ogółem 38 EPC.

Budżet CERT-UE w 2020 r. wynosił: 250 000 EUR w ramach budżetu Komisji, 3,5 mln EUR z dochodów przeznaczonych na określony cel uzyskanych z tytułu umów o gwarantowanym poziomie usług. Ogółem: 3,75 mln EUR. Ta kwota stanowiła cały budżet CERT-UE obejmujący szkolenia, sprzęt, oprogramowanie, podróże służbowe, wsparcie, pracowników kontraktowych i konferencje.

Po wejściu w życie rozporządzenia przewiduje się, że przyszłe zasoby CERT-UE będą obejmowały:

– stanowiska stałe: 34 EPC,

– personel kontraktowy: 15 EPC,

– 49 EPC ogółem, co oznacza wzrost netto o 11 EPC.

Zmiana proporcji stanowisk stałych i pracowników kontraktowych stanowi odpowiedź na istotną przeszkodę w zatrudnianiu i zatrzymywaniu starszych specjalistów w dziedzinie cyberbezpieczeństwa ze względu na ich niedobór na rynku pracy.

Ponadto do wsparcia IICB (Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa) wymagany będzie 1 pracownik kontraktowy w przeliczeniu na EPC w Dyrekcji Generalnej Komisji Europejskiej ds. Informatyki.

W związku z tym w celu wdrożenia rozporządzenia wymaganych będzie łącznie 21 EPC (20 EPC dla CERT-UE i 1 dla Dyrekcji Generalnej Komisji ds. Informatyki). Zostanie to skompensowane równoległą redukcją o 9 pracowników kontraktowych w przeliczeniu na EPC w CERT-UE, które to stanowiska były wcześniej finansowane z dochodów przeznaczonych na określony cel uzyskiwanych z tytułu umów o gwarantowanym poziomie usług.

Budżet CERT-UE na zasoby inne niż ludzkie w 2024 r. po okresie przejściowym obejmie zadania wymienione powyżej w lit. a)–e) i przewiduje się, że zostanie on sfinansowany w następujący sposób:

– 8,921 mln EUR rocznie od instytucji Unii finansowanych w ramach działu 7 budżetu Unii,

– 2,459 mln EUR od instytucji, organów i agencji Unii finansowanych w ramach działów 1–6 budżetu Unii,

– 2,670 mln EUR od instytucji, organów i agencji Unii, które finansują się ze środków własnych.

– Całkowity budżet CERT-UE: 14,05 mln EUR.

Zadania wymienione w art. 12 ust. 5 nie są opisane w katalogu usług centrum – są to usługi płatne. Mają one charakter pomocniczy, generują stosunkowo niskie kwoty przychodów, mają w większości charakter tymczasowy, a koszty tych usług zostaną odzyskane od beneficjentów usług w drodze umów o gwarantowanym poziomie usług lub umów pisemnych.

W odniesieniu do wkładów na rzecz personelu CERT-UE: instytucje i główne organy Unii wnoszą sprawiedliwy wkład, który jest proporcjonalny do odpowiedniego udziału stałych stanowisk AD w danej organizacji. Należy zbadać, czy EBC i EBI mogą również wnieść sprawiedliwy wkład poprzez oddelegowanie stałych pracowników.

2. ŚRODKI ZARZĄDZANIA

2.1. Zasady nadzoru i sprawozdawczości

Należy określić częstotliwość i warunki.

Komisja, z pomocą IICB i CERT-UE, będzie dokonywać okresowego przeglądu funkcjonowania rozporządzenia i składać sprawozdania Parlamentowi Europejskiemu i Radzie, po raz pierwszy nie później niż 48 miesięcy od wejścia w życie niniejszego rozporządzenia, a następnie co trzy lata.

Źródła danych wykorzystywanych do przeglądów pochodziłyby głównie z IICB i CERT-UE. Ponadto w razie potrzeby można wykorzystać specjalne narzędzia gromadzenia danych, np. ankiety przeprowadzone przez instytucje, organy i agencje Unii, ENISA lub sieć CSIRT.

2.2. System zarządzania i kontroli

2.2.1. Uzasadnienie dla systemu zarządzania, mechanizmów finansowania wykonania, warunków płatności i proponowanej strategii kontroli

Działania wynikające z rozporządzenia będą zarządzane w ramach poszczególnych instytucji, organów i agencji Unii zgodnie z ich odpowiednimi mającymi zastosowanie regulaminami.

Zarządzanie administracyjne i finansowe działalnością CERT-UE stanowi element administracji Komisji i jest zgodne z mającymi zastosowanie mechanizmami zarządzania i wdrażania, warunkami płatności i środkami kontroli.

Audytor wewnętrzny Komisji ma te same uprawnienia wobec CERT-UE co wobec departamentów Komisji.

2.2.2. Informacje dotyczące zidentyfikowanego ryzyka i systemów kontroli wewnętrznej ustanowionych w celu jego ograniczenia

Bardzo niskie ryzyko, ponieważ CERT-UE jest już powiązany administracyjnie z Dyrektorem Generalnym DG ds. Informatyki jako grupa zadaniowa Komisji, a IICB jest wzorowana na obecnej radzie sterującej CERT-UE. W związku z tym istnieje już ekosystem zarządzania finansowego i kontroli wewnętrznej.

2.2.3. Oszacowanie i uzasadnienie efektywności kosztowej kontroli (relacja kosztów kontroli do wartości zarządzanych funduszy powiązanych) oraz ocena prawdopodobnego ryzyka błędu (przy płatności i przy zamykaniu)

Procedury udzielania zamówień, zarządzania finansami i kontroli są już wdrożone i dobrze przetestowane. Racjonalność mechanizmów kontroli pod względem kosztów i poziomy ryzyka błędu odpowiadają poziomom stosowanym w poszczególnych instytucjach, organach lub agencjach Unii oraz w Komisji w odniesieniu do działań CERT-UE.

2.3. Środki zapobiegania nadużyciom finansowym i nieprawidłowościom

Określić istniejące lub przewidywane środki zapobiegania i ochrony, np. ze strategii zwalczania nadużyć finansowych.

Systemy zarządzania finansami i kontroli wewnętrznej Komisji mają zastosowanie do działań CERT-UE.

W celu zwalczania nadużyć finansowych, korupcji i innych działań bezprawnych stosuje się bez ograniczeń przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. dotyczącego dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF).

3. SZACUNKOWY WPŁYW FINANSOWY WNIOSKU/INICJATYWY

3.1. Działy wieloletnich ram finansowych i linie budżetowe po stronie wydatków, na które wniosek/inicjatywa ma wpływ

- Istniejące linie budżetowe

Według działów wieloletnich ram finansowych i linii budżetowych.

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn./niezróżn.[13]	państw EFTA[14]	krajów kandydujących[15]	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
1 do 6	Linie budżetowe obejmujące wkłady Unii na rzecz agencji i organów zdecentralizowanych	Zróżn.	NIE	NIE	NIE	NIE
7	Linie budżetowe obejmujące wynagrodzenia pracowników, wydatki na IT i inne wydatki administracyjne w poszczególnych sekcjach budżetu UE	Niezróżn.	NIE	NIE	NIE	NIE

- Nowe linie budżetowe, o których utworzenie się wnioskuje

Według działów wieloletnich ram finansowych i linii budżetowych.

Dział wieloletnich ram finansowych	Linia budżetowa	Rodzaj środków	Wkład			
	Numer	Zróżn./niezróżn.	państw EFTA	krajów kandydujących	państw trzecich	w rozumieniu art. 21 ust. 2 lit. b) rozporządzenia finansowego
	Brak		TAK/NIE	TAK/NIE	TAK/NIE	TAK/NIE

[13] Środki zróżnicowane/środki niezróżnicowane

[14] EFTA: Europejskie Stowarzyszenie Wolnego Handlu

[15] Kraje kandydujące oraz w stosownych przypadkach potencjalne kraje kandydujące Bałkanów Zachodnich.

3.2. Szacunkowy wpływ finansowy wniosku na środki

3.2.1. Podsumowanie szacunkowego wpływu na środki operacyjne

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków operacyjnych

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków operacyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

Dział wieloletnich ram finansowych	1 do 6	Działy obejmujące wkłady na rzecz agencji i organów zdecentralizowanych

DG: kilka			Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	Rok **2027**	**OGÓŁEM**
○ Środki operacyjne								
Linie budżetowe obejmujące wkłady Unii na rzecz agencji zdecentralizowanych (xx 10 xx xx)[16]	Środki na zobowiązania	(1a)	2,459	2,459	2,459	2,459	2,459	12,293
	Środki na płatności	(2a)	2,459	2,459	2,459	2,459	2,459	12,293
Środki administracyjne finansowane ze środków przydzielonych na określone programy[17]								
Linia budżetowa		(3)						
OGÓŁEM środki dla DG: kilka	Środki na zobowiązania	=1a+1b +3	2,459	2,459	2,459	2,459	2,459	12,293
	Środki na	=2a+2b	2,459	2,459	2,459	2,459	2,459	12,293

[16] Zgodnie z oficjalną nomenklaturą budżetową.

[17] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie realizacji programów lub działań UE (dawne linie „BA”), pośrednie badania naukowe, bezpośrednie badania naukowe.

	płatności	+3						

○ OGÓŁEM środki operacyjne	Środki na zobowiązania	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Środki na płatności	(5)	2,459	2,459	2,459	2,459	2,459	12,293
○ OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy		(6)						
OGÓŁEM środki na DZIAŁY od 1 do 6 wieloletnich ram finansowych	Środki na zobowiązania	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Środki na płatności	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

Jeżeli wpływ wniosku/inicjatywy nie ogranicza się do jednego działu operacyjnego, należy powtórzyć powyższą część:

○ OGÓŁEM środki operacyjne (wszystkie działy operacyjne)	Środki na zobowiązania	(4)	2,459	2,459	2,459	2,459	2,459	12,293
	Środki na płatności	(5)	2,459	2,459	2,459	2,459	2,459	12,293
OGÓŁEM środki administracyjne finansowane ze środków przydzielonych na określone programy (wszystkie działy operacyjne)		(6)						
OGÓŁEM środki na DZIAŁY od 1 do 6 wieloletnich ram finansowych (kwota referencyjna)	Środki na zobowiązania	=4+6	2,459	2,459	2,459	2,459	2,459	12,293
	Środki na płatności	=5+ 6	2,459	2,459	2,459	2,459	2,459	12,293

Dział wieloletnich ram finansowych	7	„Wydatki administracyjne”

Niniejszą część uzupełnia się przy użyciu „danych budżetowych o charakterze administracyjnym”, które należy najpierw wprowadzić do załącznika do oceny skutków finansowych regulacji (załącznika V do zasad wewnętrznych), przesyłanego do DECIDE w celu konsultacji między służbami.

w mln EUR (do trzech miejsc po przecinku)

		Rok **2023**	Rok **2024**	Rok **2025**	Rok **2026**	**Rok 2027**	**OGÓŁEM**
DG: DIGIT (CERT-UE)							
○ Zasoby ludzkie		1,184	2,126	2,754	3,225	3,225	12,514
○ Pozostałe wydatki administracyjne		7,938	8,921	8,921	8,921	8,921	43,622
OGÓŁEM DG DIGIT (CERT-UE)	Środki	9,122	11,047	11,675	12,146	12,146	56,136

OGÓŁEM środki na DZIAŁ 7 wieloletnich ram finansowych	(Środki na zobowiązania ogółem = środki na płatności ogółem)	9,122	11,047	11,675	12,146	12,146	**56,136**

w mln EUR (do trzech miejsc po przecinku)

		Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	**OGÓŁEM**
OGÓŁEM środki na DZIAŁY od 1 do 7 wieloletnich ram finansowych (*)	Środki na zobowiązania	11,581	13,506	14,134	14,605	14,605	68,429
	Środki na płatności	11,581	13,506	14,134	14,605	14,605	68,429

(*) Wkłady pochodzące od instytucji, organów i agencji Unii, które finansują się ze środków własnych, szacuje się na 2,670 mln EUR rocznie (ogółem na pięć lat – 13,350 mln EUR). Wkłady te będą stanowiły dla CERT-UE dochody przeznaczone na określony cel. Powyższe tabele zawierają jedynie szacunkowy łączny wpływ na budżet Unii i nie obejmują tych wkładów.

3.2.2. Przewidywany produkt finansowany ze środków operacyjnych

Środki na zobowiązania w mln EUR (do trzech miejsc po przecinku)

Określić cele i produkty			Rok **N**		Rok **N+1**		Rok **N+2**		Rok **N+3**		Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)						**OGÓŁEM**	
	PRODUKT																	
⇩	Rodzaj[18]	Średni koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba	Koszt	Liczba ogółem	Koszt całkowity
CEL SZCZEGÓŁOWY nr 1[19]																		
– Produkt																		
– Produkt																		
– Produkt																		
Cel szczegółowy nr 1 – suma cząstkowa																		
CEL SZCZEGÓŁOWY nr 2																		
– Produkt																		
Cel szczegółowy nr 2 – suma cząstkowa																		

[18] Produkty odnoszą się do produktów i usług, które zostaną zapewnione (np. liczba sfinansowanych wymian studentów, liczba kilometrów zbudowanych dróg itp.).

[19] Zgodnie z opisem w pkt 1.4.2. „Cele szczegółowe …”.

OGÓŁEM																

3.2.3. Podsumowanie szacunkowego wpływu na środki administracyjne

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania środków administracyjnych

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania środków administracyjnych, jak określono poniżej:

w mln EUR (do trzech miejsc po przecinku)

	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027	**OGÓŁEM**
DZIAŁ 7 wieloletnich ram finansowych						
Zasoby ludzkie						
Personel stały (grupa funkcyjna AD)	1,099	2,041	2,669	3,14	3,14	12,089
Personel kontraktowy	0,085	0,085	0,085	0,085	0,085	0,425
Pozostałe wydatki administracyjne	7,938	8,921	8,921	8,921	8,921	43,622
Suma cząstkowa DZIAŁU 7 wieloletnich ram finansowych	9,122	11,047	11,675	12,146	12,146	56,136

Poza DZIAŁEM 7[20] wieloletnich ram finansowych						
Zasoby ludzkie						
Pozostałe wydatki o charakterze administracyjnym						
Suma cząstkowa poza DZIAŁEM 7 wieloletnich ram finansowych						

OGÓŁEM	9,122	11,047	11,675	12,146	12,146	56,136

Potrzeby w zakresie środków na zasoby ludzkie i inne wydatki o charakterze administracyjnym zostaną pokryte z zasobów DG już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych

[20] Wsparcie techniczne lub administracyjne oraz wydatki na wsparcie realizacji programów lub działań UE (dawne linie „BA"), pośrednie badania naukowe, bezpośrednie badania naukowe.

w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

3.2.3.1. Szacowane zapotrzebowanie na zasoby ludzkie

– ☐ Wniosek/inicjatywa nie wiąże się z koniecznością wykorzystania zasobów ludzkich.

– ☑ Wniosek/inicjatywa wiąże się z koniecznością wykorzystania zasobów ludzkich, jak określono poniżej:

Wartości szacunkowe należy wyrazić w ekwiwalentach pełnego czasu pracy

	Rok 2023	Rok 2024	Rok 2025	Rok 2026	Rok 2027
O Stanowiska przewidziane w planie zatrudnienia (stanowiska urzędników i pracowników zatrudnionych na czas określony)					
20 01 02 01 (w centrali i w biurach przedstawicielstw Komisji)	7	13	17	20	20
20 01 02 03 (w delegaturach)					
01 01 01 01 (pośrednie badania naukowe)					
01 01 01 11 (bezpośrednie badania naukowe)					
Inna linia budżetowa (określić)					
O Personel zewnętrzny (w ekwiwalentach pełnego czasu pracy: EPC)[21]					
20 02 01 (CA, SNE, INT z globalnej koperty finansowej)	1	1	1	1	1
20 02 03 (CA, LA, SNE, INT i JPD w delegaturach)					
XX 01 xx **yy zz** [22] – w centrali					
XX 01 xx **yy zz** [22] – w delegaturach					
01 01 01 02 (CA, SNE, INT – pośrednie badania naukowe)					
01 01 01 12 (CA, INT, SNE – bezpośrednie badania naukowe)					
Inna linia budżetowa (określić)					
OGÓŁEM	**8**	**14**	**18**	**21**	**21**

XX oznacza odpowiedni obszar polityki lub odpowiedni tytuł w budżecie.

Potrzeby w zakresie zasobów ludzkich zostaną pokryte z zasobów DG już przydzielonych na zarządzanie tym działaniem lub przesuniętych w ramach dyrekcji generalnej, uzupełnionych w razie potrzeby wszelkimi dodatkowymi zasobami, które mogą zostać przydzielone zarządzającej dyrekcji generalnej w ramach procedury rocznego przydziału środków oraz w świetle istniejących ograniczeń budżetowych.

Opis zadań do wykonania:

Urzędnicy i pracownicy zatrudnieni na czas określony	Urzędnicy będą realizować zadania i działania CERT-UE zgodnie z rozporządzeniem, w szczególności z rozdziałami IV i V.
Personel zewnętrzny	Pracownik kontraktowy będzie wspomagał obsługę sekretariatu Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa.

[21] CA = personel kontraktowy; LA = personel miejscowy; SNE = oddelegowany ekspert krajowy; INT = personel tymczasowy; JPD = młodszy specjalista w delegaturze.

[22] W ramach podpułapu na personel zewnętrzny ze środków operacyjnych (dawne linie „BA").

3.2.4. Zgodność z obowiązującymi wieloletnimi ramami finansowymi

Wniosek/inicjatywa:

– ☑ może zostać w pełni sfinansowany(a) przez przegrupowanie środków w ramach odpowiedniego działu wieloletnich ram finansowych (WRF).

Należy wyjaśnić, na czym ma polegać przeprogramowanie, określając linie budżetowe, których ma ono dotyczyć, oraz podając odpowiednie kwoty. W przypadku znacznego przeprogramowania należy załączyć arkusz kalkulacyjny.

– ☐ wymaga zastosowania nieprzydzielonego marginesu środków w ramach odpowiedniego działu WRF lub zastosowania specjalnych instrumentów zdefiniowanych w rozporządzeniu w sprawie WRF.

Należy wyjaśnić, który wariant jest konieczny, określając działy i linie budżetowe, których ma dotyczyć, odpowiadające im kwoty oraz proponowane instrumenty, które należy zastosować.

– ☐ wymaga rewizji WRF.

Należy wyjaśnić, który wariant jest konieczny, określając działy i linie budżetowe, których ma on dotyczyć, oraz podając odpowiednie kwoty.

3.2.5. Udział osób trzecich w finansowaniu

Wniosek/inicjatywa:

– ☑ nie przewiduje współfinansowania ze strony osób trzecich[23]

– ☐ przewiduje współfinansowanie ze strony osób trzecich szacowane zgodnie z poniższymi szacunkami:

Środki w mln EUR (do trzech miejsc po przecinku)

	Rok **N**[24]	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)			Łącznie
Określić organ współfinansujący								
OGÓŁEM środki objęte współfinansowaniem								

[23] Dochody przeznaczone na określony cel pochodzące ze sporadycznego świadczenia usług na rzecz organizacji zewnętrznych, o których to usługach mowa w art. 12 ust. 5 lit. c), nie zostały oszacowane, ponieważ powinny być marginalne.

[24] Rok N jest rokiem, w którym rozpoczyna się realizację wniosku/inicjatywy. „N" należy zastąpić oczekiwanym pierwszym rokiem realizacji (np.: 2021). Tak samo należy postąpić dla kolejnych lat.

3.3. Szacunkowy wpływ na dochody

– ☑ Wniosek/inicjatywa nie ma wpływu finansowego na dochody.

– ☐ Wniosek/inicjatywa ma wpływ finansowy określony poniżej:

  – ☐ wpływ na zasoby własne

  – ☐ wpływ na dochody inne

  – Wskazać, czy dochody są przypisane do linii budżetowej po stronie wydatków ☐

w mln EUR (do trzech miejsc po przecinku)

Linia budżetowa po stronie dochodów	Środki zapisane w budżecie na bieżący rok budżetowy	Wpływ wniosku/inicjatywy[25]						
		Rok **N**	Rok **N+1**	Rok **N+2**	Rok **N+3**	Wprowadzić taką liczbę kolumn dla poszczególnych lat, jaka jest niezbędna, by odzwierciedlić cały okres wpływu (por. pkt 1.6)		
Artykuł …								

W przypadku wpływu na dochody przeznaczone na określony cel należy wskazać linie budżetowe po stronie wydatków, które ten wpływ obejmie.

Pozostałe uwagi (np. metoda/wzór użyte do obliczenia wpływu na dochody albo inne informacje).

[25] W przypadku tradycyjnych zasobów własnych (opłaty celne, opłaty wyrównawcze od cukru) należy wskazać kwoty netto, tzn. kwoty brutto po odliczeniu 20 % na poczet kosztów poboru.