Środa, 17 kwietnia 2019 r.

P8_TA(2019)0419

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji ***I

Rezolucja ustawodawcza Parlamentu Europejskiego z dnia 17 kwietnia 2019 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji (COM(2018)0630 – C8-0404/2018 – 2018/0328(COD))

(Zwykła procedura ustawodawcza: pierwsze czytanie)

(2021/C 158/66)

Parlament Europejski,

— uwzględniając wniosek Komisji przedstawiony Parlamentowi Europejskiemu i Radzie (COM(2018)0630),

— uwzględniając art. 294 ust. 2, art. 173 ust. 3 i art. 188 akapit pierwszy Traktatu o funkcjonowaniu Unii Europejskiej, zgodnie z którymi wniosek został przedstawiony Parlamentowi przez Komisję (C8-0404/2018),

— uwzględniając art. 294 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej,

— uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego z 23 stycznia 2019 r. ([1]),

— uwzględniając art. 59 Regulaminu,

— uwzględniając sprawozdanie Komisji Przemysłu, Badań Naukowych i Energii oraz opinię przedstawioną przez Komisję Rynku Wewnętrznego i Ochrony Konsumentów (A8-0084/2019),

1. przyjmuje poniższe stanowisko w pierwszym czytaniu ([2]);

2. zwraca się do Komisji o ponowne przekazanie mu sprawy, jeśli zastąpi ona pierwotny wniosek, wprowadzi w nim istotne zmiany lub planuje ich wprowadzenie;

3. zobowiązuje swojego przewodniczącego do przekazania stanowiska Parlamentu Radzie i Komisji oraz parlamentom narodowym.

P8_TC1-COD(2018)0328

Stanowisko Parlamentu Europejskiego przyjęte w pierwszym czytaniu w dniu 17 kwietnia 2019 r. w celu przyjęcia rozporządzenia Parlamentu Europejskiego i Rady (UE) …/… ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 173 ust. 3 i art. 188 akapit pierwszy,

---

([1]) Dotychczas nieopublikowana w Dzienniku Urzędowym.
([2]) Niniejsze stanowisko odpowiada poprawkom przyjętym dnia 13 marca 2019 r. (Teksty przyjęte, P8_TA(2019)0189).

uwzględniając wniosek Komisji Europejskiej,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego ([1]),

uwzględniając opinię Komitetu Regionów ([2]),

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([3]),

a także mając na uwadze, co następuje:

(1) ~~Nasze~~ ***Ponad 80 % ludności Unii Europejskiej ma dostęp do internetu, a nasze*** życie codzienne i gospodarki stają się ***coraz*** bardziej zależne od technologii cyfrowych, ~~dlatego~~ obywatele ***są zatem*** w coraz większym stopniu narażeni są na poważne cyberincydenty. Przyszłe bezpieczeństwo zależy między innymi od ***zwiększenia ogólnej odporności, od*** poprawy zdolności technologicznych i przemysłowych ~~Unii~~ do ochrony ***Unii*** przed ***ciągle zmieniającymi się*** zagrożeniami dla cyberbezpieczeństwa, ponieważ zarówno infrastruktura ~~cywilna~~, jak i potencjał ~~wojskowy~~ ***w zakresie bezpieczeństwa*** opierają się na bezpiecznych systemach cyfrowych. ***Takie bezpieczeństwo można osiągnąć dzięki zwiększaniu świadomości zagrożeń dla cyberbezpieczeństwa oraz rozwojowi kompetencji, możliwości i zdolności w całej Unii, dogłębnie uwzględniając zależności między infrastrukturą sprzętu i oprogramowania, sieciami, produktami i procesami, a także konsekwencje i obawy społeczne oraz etyczne.*** **[Popr. 1]**

(1a) Cyberprzestępczość stanowi szybko rosnące zagrożenie dla Unii, jej obywateli i gospodarki. W 2017 r. 80 % przedsiębiorstw europejskich doświadczyło co najmniej jednego cyberincydentu. W maju 2017 r. atak za pomocą Wannacry objął ponad 150 państw i 230 000 systemów informatycznych i wywarł znaczący wpływ na infrastrukturę krytyczną, taką jak szpitale. Wskazuje to na konieczność wprowadzenia najwyższych norm cyberbezpieczeństwa i kompleksowych rozwiązań w tym zakresie, obejmujących ludzi, produkty, procesy i technologie w Unii, a także na konieczność wiodącej pozycji Unii w tej dziedzinie i autonomii cyfrowej. **[Popr. 2]**

(2) Unia stale intensyfikuje swoje działania w celu rozwiązania rosnących wyzwań w zakresie cyberbezpieczeństwa, realizując strategię bezpieczeństwa cybernetycznego z 2013 r. ([4]) służącą promowaniu niezawodnego, bezpiecznego i otwartego ekosystemu cybernetycznego. W 2016 r. Unia przyjęła pierwsze środki w dziedzinie cyberbezpieczeństwa w postaci dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 ([5]) w sprawie bezpieczeństwa sieci i systemów informatycznych.

(3) We wrześniu 2017 r. Komisja i Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa przedstawili wspólny komunikat ([6]) „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej", aby w dalszym ciągu wzmacniać odporność, prewencję i reakcję Unii w kwestii cyberataków.

(4) Podczas Tallińskiego Szczytu Cyfrowego we wrześniu 2017 r. szefowie państw i rządów wezwali Unię, aby stała się „do 2025 r. światowym liderem w dziedzinie cyberbezpieczeństwa w celu zapewnienia ~~zaufania, pewności i ochrony~~ naszym obywatelom, konsumentom i przedsiębiorstwom ***zaufania, pewności i ochrony*** online oraz umożliwienia istnienia wolnego***, bezpieczniejszego*** i podlegającego przepisom prawa internetu"***, a także zadeklarowali „szersze korzystanie z rozwiązań w zakresie otwartego oprogramowania i otwartych standardów przy (prze)budowie systemów i rozwiązań ICT (m.in. aby uniknąć zależności od jednego dostawcy), w tym tych opracowanych lub promowanych w ramach unijnych programów na rzecz interoperacyjności i standaryzacji, np. ISA²"***. **[Popr. 3]**

([1]) Dz.U. C z, s. .
([2]) Dz.U. C […] z […], s. […].
([3]) Stanowisko Parlamentu Europejskiego z dnia 17 kwietnia 2019 r.
([4]) Wspólny komunikat do Parlamentu Europejskiego i Rady „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: Otwarta, bezpieczna i chroniona cyberprzestrzeń", JOIN(2013)001 final.
([5]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).
([6]) Wspólny komunikat do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej", JOIN(2017)0450 final.

Środa, 17 kwietnia 2019 r.

(4a) ***Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych („Centrum Kompetencji") powinno przyczynić się do zwiększenia odporności i niezawodności infrastruktury sieci i systemów informatycznych, w tym internetu i innej infrastruktury krytycznej dla funkcjonowania społeczeństwa, takiej jak systemy transportowe, systemy opieki zdrowotnej i bankowość.*** **[Popr. 4]**

(4b) ***Centrum Kompetencji i jego działania powinny uwzględniać wdrażanie rozporządzenia (UE) 2019/XXX [wersja przekształcona rozporządzenia (WE) nr 428/2009 zgodnie z wnioskiem COM(2016)0616]*** [7]**. [Popr. 5]**

(5) Znaczne zakłócenie funkcjonowania sieci i systemów informatycznych może wpływać na poszczególne państwa członkowskie i na Unię jako całość. ~~Bezpieczeństwo~~ ***Najwyższy poziom bezpieczeństwa*** sieci i systemów informatycznych ***w całej Unii*** ma zatem zasadnicze znaczenie ***zarówno*** dla ~~sprawnego funkcjonowania rynku wewnętrznego~~ ***społeczeństwa, jak i gospodarki***. Obecnie Unia jest uzależniona od dostawców cyberbezpieczeństwa spoza Europy. W strategicznym interesie Unii leży jednak zapewnienie, aby utrzymała ***ona*** i rozwijała podstawowe zdolności ***i możliwości*** technologiczne w zakresie cyberbezpieczeństwa w celu ochrony ~~swojego jednolitego rynku cyfrowego, a w szczególności ochrony sieci i systemów informatycznych o znaczeniu krytycznym, oraz~~ ***danych oraz krytycznych sieci i systemów informatycznych europejskich obywateli i przedsiębiorstw***, w ***tym infrastruktury krytycznej dla funkcjonowania społeczeństwa, takiej jak systemy transportowe, systemy opieki zdrowotnej*** i ***bankowość, oraz jednolitego rynku cyfrowego***, ***a także w celu*** dostarczania kluczowych usług w zakresie cyberbezpieczeństwa. **[Popr. 6]**

(6) Chociaż w Unii istnieje bardzo wysoki poziom wiedzy fachowej i doświadczenia w zakresie badań naukowych, technologii i rozwoju przemysłu w dziedzinie cyberbezpieczeństwa, to wysiłki środowisk branżowych i naukowych są rozproszone, brakuje zbieżności działań i wspólnej misji, co stanowi przeszkodę dla konkurencyjności ***i skutecznej ochrony krytycznych danych, sieci i systemów*** w tej dziedzinie. Należy połączyć te wysiłki i wiedzę fachową, utworzyć sieć kontaktów i wykorzystać je w skuteczny sposób, aby wzmocnić i uzupełnić trwające badania naukowe, zdolności technologiczne i przemysłowe ***oraz umiejętności*** na szczeblu unijnym i na szczeblach krajowych. ***Choć sektor technologii informacyjno-komunikacyjnych (ICT) stoi w obliczu ważnych wyzwań, takich jak zaspokojenie popytu na wykwalifikowanych pracowników, może skorzystać na tym, że reprezentuje różnorodność całego społeczeństwa oraz charakteryzuje się zrównoważoną reprezentacją płci, różnorodnością etniczną i niedyskryminacją osób z niepełnosprawnościami, jak również na tym, że ułatwia dostęp do wiedzy i szkoleń przyszłym ekspertom w dziedzinie cyberbezpieczeństwa, w tym kształcenia w warunkach pozaformalnych, na przykład w ramach projektów dotyczących wolnego i otwartego oprogramowania, obywatelskich projektów technicznych, przedsiębiorstw typu start-up i mikroprzedsiębiorstw.*** **[Popr. 7]**

(6a) ***Małe i średnie przedsiębiorstwa (MŚP) są kluczowymi podmiotami w unijnym sektorze cyberbezpieczeństwa, które ze względu na swoją elastyczność mogą zapewnić najnowocześniejsze rozwiązania. Jednak MŚP, które nie są wyspecjalizowane w zakresie cyberbezpieczeństwa, są również bardziej podatne na cyberincydenty ze względu na wysokie inwestycje i zasoby wiedzy wymagane do wprowadzenia skutecznych rozwiązań w dziedzinie cyberbezpieczeństwa. W związku z tym konieczne jest, aby Centrum Kompetencji i sieć kompetencji w dziedzinie cyberbezpieczeństwa (zwana dalej „siecią") zapewniły MŚP specjalne wsparcie, ułatwiając im dostęp do wiedzy i szkoleń, tak aby umożliwić im wystarczające zabezpieczenie się, a tym, które działają w dziedzinie cyberbezpieczeństwa, umożliwić wkład w rozwój wiodącej pozycji Unii w tej dziedzinie.*** **[Popr. 8]**

(6b) ***Wiedza fachowa istnieje również poza kontekstem przemysłowym i badawczym. Niekomercyjne i przedkomercyjne projekty, nazywane „obywatelskimi projektami technicznymi", wykorzystują otwarte standardy, otwarte dane oraz wolne i otwarte oprogramowanie w interesie społeczeństwa i dobra publicznego. Przyczyniają się one do zwiększenia odporności i świadomości oraz rozwoju kompetencji w dziedzinie cyberbezpieczeństwa i odgrywają ważną rolę w budowaniu zdolności przemysłu i badań w tej dziedzinie.*** **[Popr. 9]**

---

(7) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/… z dnia … ustanawiające unijny system kontroli wywozu, transferu, pośrednictwa, pomocy technicznej i tranzytu w odniesieniu do produktów podwójnego zastosowania (Dz.U. L … z …, s. …).

(6c) W kontekście niniejszego rozporządzenia termin „zainteresowane strony" odnosi się między innymi do przemysłu, podmiotów publicznych i innych podmiotów zajmujących się kwestiami operacyjnymi i technicznymi w dziedzinie cyberbezpieczeństwa, a także do społeczeństwa obywatelskiego, między innymi związków zawodowych, stowarzyszeń konsumentów, społeczności wolnego i otwartego oprogramowania oraz środowiska akademickiego i naukowego. **[Popr. 10]**

(7) W swoich konkluzjach przyjętych w listopadzie 2017 r. Rada wezwała Komisję do szybkiego dostarczenia oceny skutków na temat możliwych wariantów stworzenia sieci centrów kompetencji w dziedzinie cyberbezpieczeństwa wraz z Europejskim Centrum Badań Naukowych i Kompetencji i do zaproponowania do połowy 2018 r. odpowiedniego instrumentu prawnego.

(8) Centrum Kompetencji powinno być głównym unijnym instrumentem służącym łączeniu inwestycji w badania naukowe w dziedzinie cyberbezpieczeństwa, technologię i rozwój przemysłowy oraz wdrażaniu odpowiednich projektów i inicjatyw razem z siecią ~~kompetencji w dziedzinie cyberbezpieczeństwa~~. Centrum to powinno zapewnić wsparcie finansowe związane z cyberbezpieczeństwem z programów „Horyzont Europa" i „Cyfrowa Europa"***, jak również z Europejskiego Funduszu Obronnego na działania i koszty administracyjne związane z obronnością,*** oraz, w stosownych przypadkach, powinno być otwarte na Europejski Fundusz Rozwoju Regionalnego i inne programy. Podejście to powinno przyczynić się do tworzenia synergii i koordynacji wsparcia finansowego związanego z ~~badaniami naukowymi, innowacjami, rozwojem technologiczno-przemysłowym~~ ***inicjatywami Unii na rzecz badań naukowych i rozwoju***, ***innowacji i rozwoju technologiczno-przemysłowego*** w dziedzinie cyberbezpieczeństwa oraz do unikania powielania działań. **[Popr. 11]**

(8a) „Uwzględnianie bezpieczeństwa na etapie projektowania" jako zasada ustanowiona we wspólnym komunikacie Komisji z 13 września 2017 r. pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej" obejmuje najnowocześniejsze metody zwiększania bezpieczeństwa na wszystkich etapach cyklu życia produktu lub usługi, począwszy od bezpiecznych metod projektowania i rozwoju, zmniejszania płaszczyzny ataku oraz wprowadzania odpowiednich testów i kontroli bezpieczeństwa. W okresie eksploatacji i konserwacji producenci lub dostawcy muszą bezzwłocznie udostępniać aktualizacje eliminujące nowe luki lub zagrożenia przez szacowany okres eksploatacji produktu i w dłuższej perspektywie czasowej. Można to osiągnąć także przez umożliwianie osobom trzecim tworzenia i dostarczania takich aktualizacji. Zapewnianie aktualizacji jest szczególnie konieczne w przypadku wspólnie używanych infrastruktur, produktów i procesów. **[Popr. 12]**

(8b) Z uwagi na zakres wyzwania związanego z cyberbezpieczeństwem oraz inwestycje w zdolności i możliwości w zakresie cyberbezpieczeństwa w innych częściach świata Unia i jej państwa członkowskie powinny zwiększyć wsparcie finansowe na badania, rozwój i działania wdrożeniowe w tej dziedzinie. Aby osiągnąć korzyści skali i porównywalny poziom ochrony w całej Unii, państwa członkowskie powinny skoncentrować wysiłki w ramach europejskich, dokonując, w stosownych przypadkach, inwestycji za pośrednictwem mechanizmu Centrum Kompetencji. **[Popr. 13]**

(8c) W celu wspierania konkurencyjności unijnej i najwyższych norm cyberbezpieczeństwa na arenie międzynarodowej Centrum Kompetencji i środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinny dążyć do wymiany ze społecznością międzynarodową produktów, standardów i norm technicznych w dziedzinie cyberbezpieczeństwa. Normy techniczne obejmują tworzenie wzorcowych implementacji publikowanych jako otwarte licencje. Bezpieczny projekt, szczególnie w przypadku wzorcowych implementacji, ma kluczowe znaczenie dla ogólnej niezawodności i odporności powszechnie używanej infrastruktury sieciowej i infrastruktury systemów informatycznych, na przykład internetu i infrastruktury krytycznej. **[Popr. 14]**

(9) Biorąc pod uwagę, że cele tej inicjatywy zostaną osiągnięte w najlepszy sposób, jeżeli ~~uczestniczyć~~ ***wkład*** w ~~nici będą~~ ***nią wniosą*** wszystkie państwa członkowskie lub jak najwięcej państw członkowskich, i aby zachęcić państwa członkowskie do uczestnictwa, wyłącznie państwa członkowskie, które wniosą wkład finansowy w koszty administracyjne i operacyjne Centrum Kompetencji, powinny dysponować prawem głosu.

(10) Finansowy udział uczestniczących państw członkowskich powinien być współmierny do finansowego wkładu Unii na rzecz tej inicjatywy.

Środa, 17 kwietnia 2019 r.

(11) Centrum Kompetencji powinno ułatwiać i wspierać koordynację pracy sieci kompetencji w dziedzinie cyberbezpieczeństwa („sieć"), składającej się z krajowych ośrodków koordynacji z każdego państwa członkowskiego. Krajowe ośrodki koordynacji powinny otrzymywać bezpośrednie wsparcie finansowe Unii, w tym dotacje przyznawane bez zaproszenia do składania wniosków, w celu przeprowadzania działań związanych z niniejszym rozporządzeniem.

(12) Krajowe ośrodki koordynacji powinny zostać wybrane przez państwa członkowskie. Poza niezbędnym potencjałem administracyjnym ośrodki powinny posiadać wiedzę techniczną w dziedzinie cyberbezpieczeństwa, zwłaszcza w obszarach takich jak kryptografia, usługi w zakresie bezpieczeństwa ICT, wykrywanie włamań, bezpieczeństwo systemu, bezpieczeństwo sieci, bezpieczeństwo oprogramowania i aplikacji lub ludzkie ~~i~~ ***, etyczne,*** społeczne ***i środowiskowe*** aspekty bezpieczeństwa i prywatności, albo mieć do takiej wiedzy bezpośredni dostęp. Powinny one mieć również zdolność do skutecznego angażowania i koordynowania wysiłków przemysłu, sektora publicznego, w tym organów wyznaczonych na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 ([8]), oraz środowiska naukowego***, aby nawiązać stały dialog publiczno-prywatny na temat cyberbezpieczeństwa. Należy ponadto podnosić świadomość ogółu społeczeństwa w zakresie cyberbezpieczeństwa za pomocą odpowiednich środków komunikacji***. **[Popr. 16]**

(13) Jeżeli krajowym ośrodkom koordynacji zostanie zapewnione wsparcie finansowe w celu wsparcia osób trzecich na szczeblu krajowym, należy przekazać je odpowiednim zainteresowanym stronom za pośrednictwem umów o udzielenie dotacji w systemie kaskadowym.

(14) Powstające technologie, np. sztuczna inteligencja, internet rzeczy, obliczenia wielkiej skali (HPC) i informatyka kwantowa, ~~łańcuch bloków oraz~~ ***a także*** koncepcje takie jak bezpieczna tożsamość cyfrowa, ~~jednocześnie~~ tworzą nowe wyzwania dla cyberbezpieczeństwa i ***jednocześnie*** zapewniają ~~rozwiązania~~ ***produkty i procesy***. Ocena i zatwierdzenie odporności istniejących lub przyszłych systemów ICT będzie wymagać testowania ~~rozwiązań~~ ***produktów i procesów*** w zakresie bezpieczeństwa pod kątem ataków na urządzenia HPC i urządzenia kwantowe. Centrum Kompetencji, sieć***, europejskie centra innowacji cyfrowych*** i środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinny pomagać w rozwijaniu i rozpowszechnianiu najnowszych ~~rozwiązań~~ ***produktów i procesów, w tym podwójnego zastosowania,*** w zakresie cyberbezpieczeństwa***, w szczególności tych, które pomagają organizacjom stale budować zdolności, odporność i należyte zarządzanie. Centrum Kompetencji i sieć powinny stymulować cały cykl innowacji i przyczyniać się do eliminowania „doliny śmierci" w obszarze innowacji z zakresu technologii i usług w dziedzinie cyberbezpieczeństwa***. Jednocześnie Centrum Kompetencji ~~i sieć~~***, sieć*** i ***środowisko*** powinny służyć twórcom rozwiązań i operatorom w sektorach krytycznych takich jak sektor transportowy, energetyczny, zdrowia, finansowy, administracji, telekomunikacyjny, wytwórczy, obrony i przestrzeni kosmicznej, aby pomóc im w stawianiu czoła wyzwaniom związanym z cyberbezpieczeństwem***, a także powinny badać różne motywy ataków na integralność sieci i systemów informatycznych, takie jak przestępczość, szpiegostwo przemysłowe, zniesławienie i dezinformacja***. **[Popr. 17]**

(14a) Ze względu na szybko zmieniający się charakter cyberzagrożeń i cyberbezpieczeństwa Unia musi być w stanie szybko i w sposób ciągły dostosowywać się do nowych zjawisk w tej dziedzinie. W związku z tym Centrum Kompetencji, sieć i środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinny być wystarczająco elastyczne, aby zapewnić wymaganą zdolność reagowania. Powinny one ułatwiać rozwiązania, które pomagają podmiotom utrzymywać stałą możliwość budowy zdolności do zwiększania własnej odporności i odporności Unii. **[Popr. 18]**

(14b) Centrum Kompetencji powinno dążyć do wypracowania wiodącej pozycji Unii i wiedzy fachowej w dziedzinie cyberbezpieczeństwa, by w ten sposób zagwarantować najwyższe normy bezpieczeństwa w Unii, zapewnić ochronę danych, systemów informatycznych, sieci i infrastruktury krytycznej w Unii, tworzyć nowe wysokiej jakości miejsca pracy w tym obszarze, zapobiegać ściąganiu europejskich ekspertów ds. cyberbezpieczeństwa do państw trzecich (drenaż mózgów) oraz wnosić europejską wartość dodaną do już istniejących krajowych środków w zakresie cyberbezpieczeństwa. **[Popr. 19]**

(15) Centrum Kompetencji powinno pełnić szereg kluczowych funkcji. Po pierwsze, Centrum Kompetencji powinno ułatwiać i wspierać koordynację pracy ~~europejskiej~~ sieci ~~kompetencji w dziedzinie cyberbezpieczeństwa~~ oraz wspierać rozwój środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa. Centrum powinno realizować technologiczny plan w dziedzinie cyberbezpieczeństwa ***oraz gromadzić i udostępniać wiedzę fachową***

([8]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. L 194 z 19.7.2016, s. 1).

i ułatwiać dostęp do wiedzy fachowej zebranej w ramach sieci i środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa***, a także ułatwiać dostęp do infrastruktury cyberbezpieczeństwa***. Po drugie, Centrum powinno wdrażać odpowiednie części programów „Cyfrowa Europa" i „Horyzont Europa" poprzez przydzielanie dotacji, zwykle na podstawie konkurencyjnych zaproszeń do składania wniosków. Po trzecie, Centrum Kompetencji powinno ułatwiać wspólne inwestycje Unii, państw członkowskich lub przemysłu***, a także oferować obywatelom i przedsiębiorstwom możliwości wspólnych szkoleń i programy podnoszenia świadomości zgodnie z programem „Cyfrowa Europa" w celu pokonania luki w umiejętnościach. Szczególną uwagę powinno zwracać na stworzenie MŚP odpowiednich warunków do działania w obszarze cyberbezpieczeństwa***. **[Popr. 20]**

(16) Centrum Kompetencji powinno stymulować i wspierać ***długoterminową strategiczną*** współpracę i koordynację działań środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa, które obejmowałoby dużą, otwartą***, interdyscyplinarną*** i zróżnicowaną grupę podmiotów ***europejskich*** zaangażowanych w technologię cyberbezpieczeństwa. Środowisko to powinno obejmować w szczególności podmioty prowadzące badania naukowe, ***w tym badania nad etycznymi aspektami cyberbezpieczeństwa,*** branże po stronie podaży, branże po stronie popytu***, w tym MŚP,*** i sektor publiczny. Środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa powinno wnieść wkład w działania i plan prac Centrum Kompetencji i powinno również korzystać z działań na rzecz tworzenia środowiska prowadzonych przez Centrum Kompetencji i sieć, ale nie powinno być pod innymi względami uprzywilejowane w zakresie zaproszeń do składania wniosków lub zaproszeń do składania ofert. **[Popr. 21]**

(16a) Centrum Kompetencji powinno zapewniać ENISA odpowiednie wsparcie w realizacji zadań określonych w dyrektywie (UE) 2016/1148 („dyrektywa w sprawie bezpieczeństwa sieci i informacji") oraz w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2019/XXX (9) („akt ws. cyberbezpieczeństwa"). W związku z tym ENISA powinna przekazywać Centrum Kompetencji odpowiednie dane w ramach zadania polegającego na określeniu priorytetów w zakresie finansowania. **[Popr. 22]**

(17) Aby odpowiedzieć na potrzeby ***sektora publicznego oraz*** zarówno branż po stronie podaży, jak i branż po stronie popytu, zadanie Centrum Kompetencji dotyczące zapewnienia wiedzy z zakresu cyberbezpieczeństwa i pomocy technicznej ***sektorowi publicznemu oraz*** gałęziom przemysłu powinno odnosić się zarówno do produktów***, procesów*** i usług ICT, jak i wszystkich innych przemysłowych i technologicznych produktów i ~~rozwiązań~~ ***procesów***, do których ma zostać włączone cyberbezpieczeństwo. ***W szczególności Centrum Kompetencji powinno ułatwiać wdrażanie dynamicznych rozwiązań na poziomie przedsiębiorstw, skupiających się na budowaniu zdolności całych organizacji, w tym ludzi, procesów i technologii, w celu skutecznej ochrony organizacji przed stale zmieniającymi się cyberzagrożeniami.*** **[Popr. 23]**

(17a) Centrum Kompetencji powinno przyczyniać się do powszechnego wdrażania najnowocześniejszych produktów i rozwiązań z zakresu cyberbezpieczeństwa, w szczególności tych, które są uznawane na szczeblu międzynarodowym. **[Popr. 24]**

(18) Chociaż Centrum Kompetencji i sieć powinny mieć na celu osiągnięcie synergii ***i koordynacji*** między cyberbezpieczeństwem cywilnym i cyberbezpieczeństwem obronnym, projekty finansowane w ramach programu „Horyzont Europa" będą wdrażane zgodnie z rozporządzeniem XXX [rozporządzenie w sprawie programu „Horyzont Europa"], w którym przewidziano, że działania w zakresie badań naukowych i innowacji przeprowadzane w ramach programu „Horyzont Europa" powinny dotyczyć głównie zastosowań cywilnych. **[Popr. 25]**

(19) Aby zapewnić ustrukturyzowaną i zrównoważoną współpracę, relacje między Centrum Kompetencji a krajowymi ośrodkami koordynacji powinny opierać się na porozumieniu umownym***, które należy zharmonizować na poziomie Unii***. **[Popr. 26]**

(20) Należy stworzyć odpowiednie przepisy, aby zagwarantować odpowiedzialność i przejrzystość działania Centrum Kompetencji ***oraz finansowanych przedsiębiorstw***. **[Popr. 27]**

(20a) Realizacja projektów wdrożeniowych, w szczególności dotyczących infrastruktury i zdolności wdrażanych na szczeblu europejskim lub w drodze wspólnych zamówień, może zostać podzielona na różne fazy wdrażania, np. oddzielne przetargi na architekturę sprzętu i oprogramowania, ich produkcję oraz obsługę i konserwację, przy czym przedsiębiorstwa mogą uczestniczyć tylko w jednym z etapów i wymagane jest, aby beneficjenci na jednym lub kilku z tych etapów spełniali określone warunki dotyczące własności lub kontroli przez podmioty europejskie. **[Popr. 28]**

---

(9) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/… z dnia … w sprawie „Agencji UE ds. cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa") (Dz.U. L…) (2017/0225(COD)).

Środa, 17 kwietnia 2019 r.

(20b) ***Centrum Kompetencji powinno dążyć do jak największej synergii z ENISA, będącą wyspecjalizowaną agencją Unii ds. cyberbezpieczeństwa, a Rada Zarządzająca powinna konsultować się z ENISA – z uwagi na jej doświadczenie w tej dziedzinie – we wszystkich kwestiach dotyczących cyberbezpieczeństwa, w szczególności w odniesieniu do projektów związanych z badaniami naukowymi.*** **[Popr. 29]**

(20c) ***W procedurze mianowania przedstawiciela do Rady Zarządzającej Parlament Europejski powinien zawrzeć szczegółowe informacje na temat mandatu, obejmującego obowiązek regularnego składania sprawozdań Parlamentowi Europejskiemu lub właściwym komisjom.*** **[Popr. 30]**

(21) W świetle wiedzy fachowej w dziedzinie cyberbezpieczeństwa, jaką posiadają odpowiednio Wspólne Centrum Badawcze Komisji oraz Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), ***a także aby zapewnić możliwie największą synergię,*** powinny one odgrywać aktywną rolę w środowisku posiadającym kompetencje w dziedzinie cyberbezpieczeństwa i Radzie Konsultacyjnej ds. Przemysłowych i Naukowych. ***ENISA powinna nadal realizować swoje cele strategiczne, zwłaszcza w dziedzinie certyfikacji cyberbezpieczeństwa, określone w rozporządzeniu (UE) 2019/XXX [akt ws. cyberbezpieczeństwa] ([10]), natomiast Centrum Kompetencji powinno działać jako organ operacyjny w dziedzinie cyberbezpieczeństwa.*** **[Popr. 31]**

(22) W przypadku gdy krajowy ośrodek koordynacji i podmioty wchodzące w skład środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa otrzymują wkład finansowy z budżetu ogólnego Unii, powinny podać do wiadomości publicznej fakt, że odpowiednie działania podejmowane są w kontekście obecnej inicjatywy.

(23) Wkład Unii na rzecz Centrum Kompetencji powinien sfinansować połowę kosztów związanych z założeniem oraz działaniami administracyjnymi i koordynacyjnymi Centrum Kompetencji. Aby uniknąć podwójnego finansowania, działania te nie powinny jednocześnie korzystać ze środków pochodzących z innych unijnych programów.

(24) Rada Zarządzająca Centrum Kompetencji, składająca się z przedstawicieli państw członkowskich i Komisji, powinna określać ogólny kierunek działalności Centrum Kompetencji oraz zapewniać wykonywanie przez nie jego zadań zgodnie z niniejszym rozporządzeniem. Rada Zarządzająca powinna posiadać uprawnienia niezbędne do uchwalania budżetu, kontroli jego wykonania, przyjmowania stosownych przepisów finansowych, ustalania przejrzystych procedur pracy w zakresie podejmowania decyzji przez Centrum Kompetencji, przyjmowania planu prac Centrum Kompetencji i wieloletniego planu strategicznego odzwierciedlającego priorytety w realizacji celów i zadań Centrum Kompetencji, uchwalania jej regulaminu wewnętrznego, powoływania dyrektora wykonawczego oraz podejmowania decyzji o przedłużeniu jego kadencji lub jej zakończeniu. ***Aby wykorzystać synergię, ENISA powinna być stałym obserwatorem w Radzie Zarządzającej i powinna wnosić wkład w prace Centrum Kompetencji, w tym w drodze konsultacji w sprawie wieloletniego planu strategicznego oraz w sprawie planu prac i wykazu działań wybranych do finansowania.*** **[Popr. 32]**

(24a) ***Rada Zarządzająca powinna dążyć do promowania Centrum Kompetencji w skali globalnej, aby zwiększyć jego atrakcyjność i uczynić z niego światowej klasy podmiot doskonałości w dziedzinie cyberbezpieczeństwa.*** **[Popr. 33]**

(25) Aby Centrum Kompetencji mogło prawidłowo i skutecznie funkcjonować, Komisja i państwa członkowskie powinny zapewnić, aby osoby, które mają zostać powołane na członków Rady Zarządzającej, posiadały odpowiednią zawodową wiedzę fachową i doświadczenie w obszarach funkcyjnych. Komisja i państwa członkowskie powinny również dołożyć starań, by ograniczyć rotację swoich przedstawicieli w Radzie Zarządzającej, tak aby zapewnić ciągłość jej pracy***, a także powinny dążyć do osiągnięcia równowagi płci***. **[Popr. 34]**

(25a) ***Waga głosu Komisji w głosowaniach nad decyzjami Rady Zarządzającej powinna być współmierna do wkładu z budżetu Unii na rzecz Centrum Kompetencji, zgodnie z odpowiedzialnością Komisji za zapewnienie właściwego zarządzania budżetem Unii w interesie Unii, jak określono w traktatach.*** **[Popr. 35]**

([10]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/… z dnia … w sprawie „Agencji UE ds. cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa") (Dz.U. L…) (2017/0225(COD)).

(26) Sprawne funkcjonowanie Centrum Kompetencji wymaga, aby dyrektor wykonawczy był mianowany ***w przejrzysty sposób*** na podstawie swoich osiągnięć oraz udokumentowanych kompetencji administracyjnych i zarządczych, a także odpowiednich kompetencji i doświadczenia w zakresie cyberbezpieczeństwa, oraz aby pełnił swoje obowiązki w sposób całkowicie niezależny. **[Popr. 36]**

(27) Centrum Kompetencji powinno posiadać organ doradczy w postaci Rady Konsultacyjnej ds. Przemysłowych i Naukowych w celu zapewnienia regularnego ***i odpowiednio przejrzystego*** dialogu z sektorem prywatnym, organizacjami konsumenckimi i innymi odpowiednimi zainteresowanymi stronami. ***Centrum powinno także zapewniać dyrektorowi wykonawczemu i Radzie Zarządzającej niezależne doradztwo w zakresie wdrażania i zamówień.*** Rada Konsultacyjna ds. Przemysłowych i Naukowych powinna skupiać się na zagadnieniach istotnych dla zainteresowanych stron i kierować na nie uwagę Rady Zarządzającej Centrum Kompetencji. Skład Rady Konsultacyjnej ds. Przemysłowych i Naukowych oraz przydzielone jej zadania, takie jak zasięganie jej opinii w sprawie planu prac, powinny zapewniać wystarczającą reprezentację zainteresowanych stron w pracach Centrum Kompetencji. ***Każdej kategorii zainteresowanych stron z branży należy przydzielić minimalną liczbę miejsc, ze szczególnym uwzględnieniem reprezentacji MŚP.*** **[Popr. 37]**

(28) Centrum Kompetencji ~~powinno~~ ***i jego działalność powinny*** korzystać ze szczególnej wiedzy fachowej oraz szerokiego i odpowiedniego udziału zainteresowanych stron, stworzonego w ramach umownego partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa w trakcie trwania programu „Horyzont 2020”***, a także projektów pilotażowych w ramach programu „Horyzont 2020”dotyczących sieci kompetencji w dziedzinie cyberbezpieczeństwa,*** za pośrednictwem swojej Rady Konsultacyjnej ds. Przemysłowych i Naukowych. ***W stosownych przypadkach Centrum Kompetencji oraz Rada Konsultacyjna ds. Przemysłowych i Naukowych powinny rozważyć odwzorowanie istniejących struktur, np. w formie grup roboczych.*** **[Popr. 38]**

(28a) Centrum Kompetencji i jego organy powinny wykorzystywać doświadczenia i wkład poprzednich i obecnych inicjatyw, takich jak umowne partnerstwo publiczno-prywatne (cPPP) w dziedzinie cyberbezpieczeństwa, Europejska Organizacja ds. Cyberbezpieczeństwa (ECSO) oraz projekt pilotażowy i działanie przygotowawcze dotyczące audytów wolnego i otwartego oprogramowania (EU FOSSA). **[Popr. 39]**

(29) W Centrum Kompetencji powinny obowiązywać przepisy dotyczące zapobiegania konfliktom interesów ***oraz ich identyfikacji*** i ~~zarządzania nimi~~ ***eliminowania w odniesieniu do jego członków, organów i personelu, Rady Zarządzającej, a także Rady Konsultacyjnej ds. Przemysłowych i Naukowych oraz środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa. Państwa członkowskie powinny zadbać o zapobieganie konfliktom interesów oraz ich identyfikację i eliminowanie w odniesieniu do krajowych ośrodków koordynacji***. Centrum Kompetencji powinno również stosować odpowiednie przepisy unijne dotyczące publicznego dostępu do dokumentów zawarte w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 1049/2001 ([11]). Przetwarzanie danych osobowych przez Centrum Kompetencji będzie podlegać przepisom rozporządzenia Parlamentu Europejskiego i Rady (UE) nr XXX/2018. Centrum Kompetencji powinno przestrzegać przepisów mających zastosowanie do instytucji Unii oraz przepisów krajowych dotyczących postępowania z informacjami, w szczególności ze szczególnie chronionymi informacjami jawnymi i informacjami niejawnymi UE. **[Popr. 40]**

(30) Interesy finansowe Unii i państw członkowskich powinny być chronione w całym cyklu wydatków za pomocą proporcjonalnych środków, w tym poprzez zapobieganie nieprawidłowościom, ich wykrywanie i prowadzenie dochodzeń w sprawach nieprawidłowości, odzyskiwanie utraconych, nienależnie wypłaconych lub nieprawidłowo wykorzystanych funduszy oraz, w stosownych przypadkach, nakładanie kar administracyjnych i pieniężnych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE, EURATOM) nr XXX ([12]) [rozporządzenie finansowe].

(31) Centrum Kompetencji powinno działać w otwarty i przejrzysty sposób pozwalający mu na czas udostępniać ~~wszelkie stosowne~~ ***wyczerpujące*** informacje, jak również promować swoje działania, w tym działania informacyjne i upowszechnianie wiedzy wśród społeczeństwa***. Powinno przekazywać opinii publicznej i wszelkim zainteresowanym stronom wykaz członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa oraz podawać do wiadomości publicznej deklaracje interesów złożone zgodnie z art. 42***. Regulamin wewnętrzny organów Centrum Kompetencji powinien być dostępny publicznie. **[Popr. 41]**

([11]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1049/2001 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).

([12]) [dodać tytuł i odniesienie do Dz.U.].

Środa, 17 kwietnia 2019 r.

(31a) Wskazane jest, aby zarówno Centrum Kompetencji, jak i krajowe ośrodki koordynacji w możliwie największym stopniu monitorowały i stosowały międzynarodowe standardy w celu zachęcania do wypracowania globalnych najlepszych praktyk. **[Popr. 42]**

(32) Audytor wewnętrzny Komisji powinien mieć w stosunku do Centrum Kompetencji takie same uprawnienia jak w stosunku do Komisji.

(33) Komisja, Centrum Kompetencji, Europejski Trybunał Obrachunkowy i Europejski Urząd ds. Zwalczania Nadużyć Finansowych powinny uzyskać dostęp do wszystkich niezbędnych informacji i pomieszczeń, aby prowadzić audyty i dochodzenia dotyczące dotacji, umów i porozumień podpisanych przez Centrum Kompetencji.

(33a) Należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej w odniesieniu do zdefiniowania elementów umów między Centrum Kompetencji i krajowymi ośrodkami koordynacji oraz w odniesieniu do określenia kryteriów oceny podmiotów i ich akredytacji jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa ([13]). W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(34) ~~Ponieważ cele~~ ***Cele*** niniejszego rozporządzenia, a mianowicie ***podniesienie konkurencyjności i zdolności Unii w dziedzinie cyberbezpieczeństwa w wyniku większego upowszechnienia produktów, procesów i usług z zakresu cyberbezpieczeństwa i dzięki temu zmniejszenie zależności cyfrowej Unii,*** utrzymanie i rozwijanie technologicznych i przemysłowych zdolności Unii w dziedzinie cyberbezpieczeństwa, zwiększanie konkurencyjności unijnego sektora cyberbezpieczeństwa i uczynienia z cyberbezpieczeństwa przewagi konkurencyjnej innych gałęzi przemysłu Unii, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie z uwagi na rozproszenie istniejących, ograniczonych zasobów oraz niezbędną wielkość inwestycji, lecz ze względu na uniknięcie niepotrzebnego powielania tych wysiłków, pomoc w osiąganiu masy krytycznej inwestycji i zapewnienie, by finansowanie publiczne wykorzystywano w sposób optymalny, mogą być lepiej realizowane na ~~szczeblu unijnym,~~ ***poziomie Unii. Ponadto jedynie działania na poziomie Unii mogą zapewnić najwyższy poziom cyberbezpieczeństwa we wszystkich państwach członkowskich, a tym samym zlikwidować istniejące w niektórych państwach członkowskich luki w zakresie bezpieczeństwa, które stwarzają luki w zakresie bezpieczeństwa w całej Unii. W związku z powyższym*** Unia może ~~przyjąć środki~~ ***podjąć działania*** zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności~~, o której mowa~~ ***określoną*** w tym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tego celu,**.** **[Popr. 44]**

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

OGÓLNE PRZEPISY I ZASADY CENTRUM KOMPETENCJI ORAZ SIECI

Artykuł 1

Przedmiot

1. Na mocy niniejszego rozporządzenia ustanawia się Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych („Centrum Kompetencji") oraz sieć krajowych ośrodków koordynacji ***(„sieć")***, a także określa się przepisy dotyczące nominacji krajowych ośrodków koordynacji i tworzenia środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa ***(„środowisko")***. ***Centrum Kompetencji i sieć wnoszą wkład w ogólną odporność i świadomość zagrożeń dla cyberbezpieczeństwa w Unii, przy pełnym uwzględnieniu skutków społecznych***. **[Popr. 45]**

([13]) Dz.U. L 123 z 12.5.2016, s. 1.

2. Centrum Kompetencji wnosi wkład we wdrażanie części dotyczącej cyberbezpieczeństwa programu „Cyfrowa Europa" ustanowionego rozporządzeniem nr XXX ***([14])***, w szczególności we wdrażanie działań związanych z art. 6 rozporządzenia (UE) nr XXX [program „Cyfrowa Europa"], a także we wdrażanie programu „Horyzont Europa" ustanowionego rozporządzeniem nr XXX ***([15])***, w szczególności filaru II pkt 2.2.6 załącznika I do decyzji nr XXX ustanawiającej program szczegółowy służący realizacji programu ramowego w zakresie badań naukowych i innowacji „Horyzont Europa" [numer referencyjny programu szczegółowego].

~~3. Siedziba Centrum Kompetencji znajduje się w [Brukseli w Belgii].~~ **[Popr. 46]**

~~4. Centrum Kompetencji posiada osobowość prawną. We wszystkich państwach członkowskich centrum ma zdolność prawną o najszerszym zakresie przyznawanym osobom prawnym zgodnie z ustawodawstwem danego państwa członkowskiego. Może ono zwłaszcza nabywać i zbywać nieruchomości i ruchomości oraz być stroną w postępowaniach sądowych.~~ **[Popr. 47]**

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „cyberbezpieczeństwo" oznacza ~~ochronę~~ ***wszystkie działania niezbędne do ochrony przed zagrożeniami dla cyberbezpieczeństwa*** sieci i systemów informatycznych, ich użytkowników ~~i innych~~ ***oraz*** osób ~~przed zagrożeniami dla cyberbezpieczeństwa~~***, których zagrożenia te dotyczą***; **[Popr. 48]**

1a) „cyberobrona" i „wymiar obronny cyberbezpieczeństwa" oznaczają wyłącznie defensywną i reaktywną technologię cyberobrony, której celem jest ochrona przed cyberzagrożeniami infrastruktury krytycznej, sieci wojskowych i systemów informatycznych, ich użytkowników i osób, których dotyczą zagrożenia, obejmującą orientację sytuacyjną, wykrywanie zagrożeń i kryminalistykę cyfrową; **[Popr. 183]**

2) „produkty i ~~rozwiązania w dziedzinie cyberbezpieczeństwa"~~ ***procesy"*** oznaczają ***komercyjne i niekomercyjne*** produkty, usługi lub procesy ICT, których szczególnym celem jest ochrona ~~przed zagrożeniami dla cyberbezpieczeństwa~~ ***danych,*** sieci i systemów informatycznych, ich użytkowników oraz ***innych*** osób~~, których zagrożenia te dotyczą~~ ***przed zagrożeniami dla cyberbezpieczeństwa***; **[Popr. 49]**

2a) „zagrożenie dla cyberbezpieczeństwa" oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą uszkodzić lub zakłócić sieci i systemy informatyczne, ich użytkowników oraz osoby, których zagrożenie to dotyczy, albo w inny sposób niekorzystnie wpływać na te sieci i systemy informatyczne, użytkowników i osoby, których zagrożenie to dotyczy; **[Popr. 50]**

3) „organ publiczny" oznacza jednostkę administracji rządowej lub innej administracji publicznej, w tym publiczne organy doradcze na szczeblu krajowym, regionalnym lub lokalnym, bądź osobę fizyczną lub prawną, która na mocy prawa ***unijnego i*** krajowego sprawuje publiczne funkcje administracyjne, łącznie ze szczególnymi obowiązkami; **[Popr. 51]**

4) ~~„uczestniczące~~ ***„finansujące*** państwo członkowskie" oznacza państwo członkowskie, które dobrowolnie wnosi wkład finansowy w koszty administracyjne i operacyjne Centrum Kompetencji.**; [Popr. 52]**

4a) „europejskie centra innowacji cyfrowych" oznaczają podmiot prawny w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/XXX ([16]). **[Popr. 53]**

Artykuł 3

Misja Centrum i sieci

1. Centrum Kompetencji i sieć pomagają Unii:

a) w ~~utrzymaniu i~~ rozwijaniu ***fachowych*** technologicznych ~~i~~, przemysłowych***, społecznych, akademickich i naukowych*** zdolności ***i możliwości*** w dziedzinie cyberbezpieczeństwa niezbędnych do zabezpieczenia jej jednolitego rynku cyfrowego ***i dalszej ochrony danych unijnych obywateli, przedsiębiorstw i administracji publicznych***; **[Popr. 54]**

([14]) [dodać pełny tytuł i odniesienie do Dz.U.]
([15]) [dodać pełny tytuł i odniesienie do Dz.U.]
([16]) ***Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/XXX ustanawiające program „Cyfrowa Europa" na lata 2021–2027 (Dz.U. L …) (2018/0227(COD)).***

***aa) w zwiększaniu odporności i niezawodności infrastruktury sieci i systemów informatycznych, w tym infrastruktury krytycznej, internetu oraz powszechnie używanego sprzętu komputerowego i oprogramowania w Unii;* [Popr. 55]**

b) w zwiększaniu konkurencyjności unijnego sektora cyberbezpieczeństwa i uczynieniu z cyberbezpieczeństwa ~~przewagi konkurencyjnej~~ ***atutu konkurencyjnego*** innych gałęzi przemysłu Unii. **[Popr. 56]**

***ba) w zwiększaniu świadomości zagrożeń dla cyberbezpieczeństwa oraz związanych z nimi społecznych i etycznych implikacji i obaw w Unii oraz w niwelowaniu luki kompetencyjnej w zakresie cyberbezpieczeństwa w Unii;* [Popr. 57]**

***bb) w rozwoju wiodącej pozycji Unii w dziedzinie cyberbezpieczeństwa i zapewnieniu najwyższych norm cyberbezpieczeństwa w całej Unii;* [Popr. 58]**

***bc) we wzmacnianiu konkurencyjności i zdolności Unii przy jednoczesnym ograniczaniu jej zależności cyfrowej w drodze większego upowszechniania produktów, procesów i usług z zakresu cyberbezpieczeństwa opracowanych w Unii;* [Popr. 59]**

***bd) w zwiększaniu zaufania obywateli, konsumentów i przedsiębiorstw do środowiska cyfrowego, a tym samym przyczynianiu się do osiągnięcia celów strategii jednolitego rynku cyfrowego;* [Popr. 60]**

2. W stosownych przypadkach Centrum Kompetencji realizuje swoje zadania we współpracy z siecią krajowych ośrodków koordynacji i środowiskiem posiadającym kompetencje w dziedzinie cyberbezpieczeństwa.

Artykuł 4

Cele i zadania Centrum

Cele i związane z nimi zadania Centrum Kompetencji są następujące:

1. ~~ułatwianie i pomoc w koordynacji pracy~~ ***utworzenie*** sieci ~~krajowych ośrodków koordynacji („sieć”)~~, o której mowa w art. 6, oraz ~~pracy~~ środowiska ~~posiadającego kompetencje w dziedzinie cyberbezpieczeństwa~~, o którym mowa w art. 8***, a także zarządzanie nimi i pomoc w ich działaniu***; **[Popr. 61]**

2. ~~wnoszenie wkładu we wdrażanie~~ ***koordynowanie wdrażania*** części dotyczącej cyberbezpieczeństwa programu „Cyfrowa Europa” ustanowionego rozporządzeniem nr XXX ([17]), w szczególności działań związanych z art. 6 rozporządzenia (UE) nr XXX [program „Cyfrowa Europa”], oraz programu „Horyzont Europa” ustanowionego rozporządzeniem nr XXX ([18]), w szczególności pkt 2.2.6 filaru II załącznika I do decyzji nr XXX ustanawiającej program szczegółowy służący realizacji programu ramowego w zakresie badań naukowych i innowacji „Horyzont Europa” [numer referencyjny programu szczegółowego], oraz innych unijnych programów, jeżeli przewidziano to w aktach prawnych Unii***, a także wnoszenie wkładu we wdrażanie działań finansowanych z Europejskiego Funduszu Obrony ustanowionego rozporządzeniem (UE) 2019/XXX***; **[Popr. 62]**

3. poszerzanie ***zwiększanie odporności, zdolności, poszerzanie*** możliwości, wiedzy i ulepszanie infrastruktury w zakresie cyberbezpieczeństwa z korzyścią dla ***społeczeństwa,*** gałęzi przemysłu, sektora publicznego i środowisk naukowych dzięki wykonywaniu następujących zadań***, z wykorzystaniem najnowocześniejszej infrastruktury przemysłowej i badawczej w zakresie cyberbezpieczeństwa oraz powiązanych z nią usług***: **[Popr. 63]**

   a) ~~w odniesieniu do nowoczesnej infrastruktury przemysłowej i badawczej w zakresie cyberbezpieczeństwa i~~ ***nabywanie, ulepszanie, obsługa i udostępnianie systemów Centrum Kompetencji oraz*** związanych z ~~nią~~ ***nimi*** usług – ~~nabywanie, ulepszanie, obsługa takiej infrastruktury oraz udostępnianie jej~~ i ~~związanych z nią usług~~ ***na sprawiedliwych warunkach***, ***otwarcie*** i ***jawnie*** szerokiemu kręgowi użytkowników z sektora przemysłu w całej Unii, ~~w tym~~ ***szczególnie*** MŚP, sektorowi publicznemu oraz społeczności badawczej i naukowej; **[Popr. 64]**

([17]) [dodać pełny tytuł i odniesienie do Dz.U.]
([18]) [dodać pełny tytuł i odniesienie do Dz.U.]

b) ~~w odniesieniu do nowoczesnej infrastruktury przemysłowej i badawczej w zakresie cyberbezpieczeństwa i związanych z nią usług~~ ***zapewnianie*** wsparcia innym podmiotom, w tym wsparcia finansowego, jeżeli chodzi o nabywanie, ulepszanie, obsługę ~~takiej infrastruktury oraz~~ ***i*** udostępnianie ~~jej~~ ***takich systemów*** i związanych z ~~nią~~ ***nimi*** usług szerokiemu kręgowi użytkowników z sektora przemysłu w całej Unii, ~~w tym~~ ***szczególnie*** MŚP, sektorowi publicznemu oraz społeczności badawczej i naukowej; **[Popr. 65]**

ba) zapewnianie wsparcia finansowego oraz pomocy technicznej przedsiębiorstwom typu start-up, MŚP, mikroprzedsiębiorstwom, stowarzyszeniom, indywidualnym ekspertom i obywatelskim projektom technicznym w dziedzinie cyberbezpieczeństwa; **[Popr. 66]**

bb) finansowanie audytów kodów bezpieczeństwa oprogramowania i powiązanych udoskonaleń w odniesieniu do projektów dotyczących wolnego i otwartego oprogramowania, powszechnie wykorzystywanego na potrzeby infrastruktury, produktów i procesów; **[Popr. 67]**

c) ~~zapewnianie sektorowi przemysłu i organom publicznym~~ ***ułatwianie wymiany*** wiedzy z zakresu cyberbezpieczeństwa oraz pomocy technicznej ***między innymi wśród społeczeństwa obywatelskiego, sektora przemysłu, organów publicznych oraz społeczności akademickiej i naukowej***, w szczególności poprzez wspieranie działań mających na celu ułatwianie dostępu do wiedzy fachowej dostępnej w sieci i w środowisku posiadającym kompetencje w dziedzinie cyberbezpieczeństwa ***w celu poprawy cyberodporności w Unii***; **[Popr. 68]**

ca) promowanie „uwzględniania bezpieczeństwa na etapie projektowania" jako zasady w procesie tworzenia, utrzymywania, eksploatacji i aktualizacji infrastruktury, produktów i usług, w szczególności przez wspieranie najnowocześniejszych metod bezpiecznego projektowania, odpowiednich testów i audytów bezpieczeństwa, i łącznie z obowiązkiem producenta lub dostawcy do niezwłocznego udostępnienia aktualizacji mających na celu usunięcie nowych luk lub zagrożeń, również po szacowanym okresie użytkowania produktu, lub umożliwienia stronie trzeciej tworzenia i dostarczania takich aktualizacji; **[Popr. 69]**

cb) wspomaganie polityki w zakresie udziału w tworzeniu kodów źródłowych oraz jej opracowywanie, w szczególności w odniesieniu do organów publicznych, które korzystają z projektów dotyczących wolnego i otwartego oprogramowania; **[Popr. 70]**

cc) zbliżanie zainteresowanych stron z przemysłu, związków zawodowych, środowisk akademickich, organizacji badawczych i podmiotów publicznych w celu zapewnienia długoterminowej współpracy w zakresie opracowywania i wdrażania produktów i procesów w dziedzinie cyberbezpieczeństwa, w tym łączenia zasobów i dzielenia się zasobami oraz informacjami dotyczącymi takich produktów i procesów, w stosownych przypadkach; **[Popr. 71]**

4. wnoszenie wkładu w powszechne wdrażanie w całej ~~gospodarce~~ ***Unii*** nowoczesnych ***i zrównoważonych*** produktów i ~~rozwiązań~~ ***procesów*** w dziedzinie cyberbezpieczeństwa dzięki wykonywaniu następujących zadań: **[Popr. 72]**

a) stymulowanie badań naukowych w dziedzinie cyberbezpieczeństwa, rozwoju cyberbezpieczeństwa, a także absorpcji unijnych produktów i ~~rozwiązań~~ ***całościowych procesów*** w dziedzinie cyberbezpieczeństwa ~~przez organy publiczne i branże wykorzystujące te produkty i rozwiązania~~ ***w całym cyklu innowacji, między innymi przez organy publiczne, przemysł*** i ***rynek***; **[Popr. 73]**

b) wspomaganie organów publicznych, branż po stronie popytu i innych użytkowników w ***zwiększaniu odporności dzięki*** przyjmowaniu i wdrażaniu ~~najnowszych rozwiązań~~ ***najnowocześniejszych produktów i procesów*** w dziedzinie cyberbezpieczeństwa; **[Popr. 74]**

c) wspieranie w szczególności organów publicznych w organizacji udzielania zamówień publicznych lub przeprowadzanie zamówień na ~~nowoczesne~~ ***najnowocześniejsze*** produkty i ~~rozwiązania~~ ***procesy*** w dziedzinie cyberbezpieczeństwa w imieniu organów publicznych***, w tym przez zapewnianie wsparcia na potrzeby zamówień, aby zwiększyć bezpieczeństwo inwestycji publicznych i płynących z nich korzyści***; **[Popr. 75]**

d) zapewnianie wsparcia finansowego i pomocy technicznej przedsiębiorstwom typu start-up ***i MŚP, mikroprzedsiębiorstwom, indywidualnym ekspertom, projektom dotyczącym powszechnie wykorzystywanego wolnego i otwartego oprogramowania*** oraz ~~MŚP~~ ***obywatelskim projektom technicznym*** w dziedzinie cyberbezpieczeństwa***, aby poszerzać wiedzę fachową*** w ~~celu~~ ***dziedzinie cyberbezpieczeństwa, połączyć*** ich ~~połączenia z~~ ***z*** potencjalnymi rynkami i ~~przyciągnięcia inwestycji~~ ***możliwościami wdrażania, a także aby przyciągać inwestycje***; **[Popr. 76]**

Środa, 17 kwietnia 2019 r.

5. poprawa zrozumienia kwestii cyberbezpieczeństwa i wnoszenie wkładu w ograniczanie niedoborów kwalifikacji ***oraz wzmocnienie poziomu kwalifikacji*** w zakresie cyberbezpieczeństwa w Unii dzięki realizacji następujących zadań: **[Popr. 77]**

-a) wspieranie, w stosownych przypadkach, realizacji celu szczegółowego 4 – zaawansowane umiejętności cyfrowe – programu „Cyfrowa Europa" we współpracy z europejskimi centrami innowacji cyfrowych; **[Popr. 78]**

a) wspieranie dalszego rozwoju***, łączenia i wymiany*** umiejętności ***i kompetencji*** w dziedzinie cyberbezpieczeństwa, ***na wszystkich odpowiednich poziomach kształcenia***, ***wspieranie celu polegającego na osiągnięciu równowagi płci, ułatwianie osiągnięcia wspólnego wysokiego poziomu wiedzy*** w ***zakresie cyberbezpieczeństwa oraz przyczynianie się do budowania odporności użytkowników i infrastruktury w całej Unii w koordynacji z siecią oraz, w*** stosownych przypadkach ~~z udziałem odpowiednich agencji~~***, we współpracy*** z ***odpowiednimi agencjami*** i ~~organów~~ ***organami*** UE, w tym ~~Agencji~~ ***Agencją*** Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji ***ENISA***; **[Popr. 79]**

6. przyczynianie się do wzmacniania badań naukowych i rozwoju w dziedzinie cyberbezpieczeństwa w Unii poprzez:

a) zapewnianie wsparcia finansowego na wysiłki badawcze w dziedzinie cyberbezpieczeństwa, których podstawą jest wspólny, stale oceniany i ulepszany wieloletni ~~program~~ ***plan*** dotyczący strategii, przemysłu, technologii i badań naukowych***, o którym mowa w art. 13***; **[Popr. 80]**

b) wspieranie dużych projektów badawczych i demonstracyjnych dotyczących możliwości technologicznych nowej generacji w dziedzinie cyberbezpieczeństwa we współpracy z przemysłem***, społecznością akademicką*** i ***naukową, sektorem publicznym i organami publicznymi, w tym*** z siecią ***i środowiskiem***; **[Popr. 81]**

ba) zapewnianie poszanowania praw podstawowych i etycznego postępowania w projektach badań naukowych w dziedzinie cyberbezpieczeństwa finansowanych przez Centrum Kompetencji; **[Popr. 82]**

bb) monitorowanie zgłoszeń o lukach w zabezpieczeniach wykrytych przez środowisko i ułatwianie ujawniania luk, opracowywania łat, poprawek i rozwiązań oraz ich dystrybucja; **[Popr. 83]**

bc) monitorowanie we współpracy z ENISA wyników badań w zakresie algorytmów samouczących się stosowanych w szkodliwych działaniach w cyberprzestrzeni oraz wspieranie wdrażania dyrektywy (UE) 2016/1148; **[Popr. 84]**

bd) wspieranie badań naukowych w dziedzinie cyberprzestępczości; **[Popr. 85]**

be) wspieranie badań naukowych i opracowania produktów i procesów, które można swobodnie analizować i wykorzystywać oraz którymi można się dzielić, zwłaszcza w dziedzinie zweryfikowanego i dającego się zweryfikować sprzętu i oprogramowania, w ścisłej współpracy z przemysłem, siecią i środowiskiem; **[Popr. 86]**

c) wspieranie badań naukowych i innowacji w celu ***formalnej i nieformalnej*** standaryzacji ***i certyfikacji*** technologii cyberbezpieczeństwa***, w połączeniu z istniejącymi pracami i w stosownych przypadkach w ścisłej współpracy z europejskimi organizacjami normalizacyjnymi, jednostkami certyfikującymi i ENISA***; **[Popr. 87]**

ca) zapewnienie specjalnego wsparcia dla MŚP poprzez ułatwienie im dostępu do wiedzy i szkoleń dzięki dostosowanemu do potrzeb dostępowi do rezultatów prac badawczo-rozwojowych wzmacnianych przez Centrum Kompetencji i sieć w celu zwiększenia konkurencyjności; **[Popr. 88]**

7. zacieśnienie współpracy między kręgami cywilnymi i kręgami obronnymi w ***odniesieniu*** do technologii i aplikacji podwójnego zastosowania w dziedzinie cyberbezpieczeństwa dzięki wykonywaniu następujących zadań***, reaktywnych i defensywnych technologii, aplikacji i usług cyberobrony***: **[Popr. 184]**

a) wspieranie państw członkowskich i zainteresowanych podmiotów naukowych i przemysłowych w zakresie badań naukowych, rozwoju i wdrażania;

b) wnoszenie wkładu we współpracę między państwami członkowskimi dzięki wspieraniu kształcenia, szkolenia i ćwiczeń;

c) łączenie zainteresowanych stron, aby wspierać synergie między badaniami i rynkami w zakresie cyberbezpieczeństwa w wymiarach cywilnym i obronnym;

8. zwiększanie synergii między wymiarem cywilnym i wymiarem obronnym cyberbezpieczeństwa w odniesieniu do Europejskiego Funduszu Obronnego dzięki wykonywaniu następujących zadań***, reaktywnych i defensywnych technologii, aplikacji i usług cyberobrony***: **[Popr. 185]**

a) doradztwo, dzielenie się wiedzą fachową oraz ułatwianie współpracy między zainteresowanymi stronami;

b) zarządzanie międzynarodowymi projektami w dziedzinie cyberobrony na wniosek państw członkowskich i tym samym działanie jako kierownik projektu w rozumieniu rozporządzenia XXX [rozporządzenie ustanawiające Europejski Fundusz Obronny];

ba) pomaganie i doradzanie Komisji w związku z wdrażaniem rozporządzenia (UE) 2019/XXX [przekształcenie rozporządzenia (WE) nr 428/2009 zgodnie z wnioskiem COM(2016)0616]. **[Popr. 89]**

8a. zapewnianie wkładu w wysiłki Unii mające na celu wzmocnienie współpracy międzynarodowej w zakresie cyberbezpieczeństwa przez:

a) ułatwianie udziału Centrum Kompetencji w konferencjach międzynarodowych i organizacjach rządowych, jak również udziału w pracach międzynarodowych organizacji normalizacyjnych;

b) współpracę z państwami trzecimi i organizacjami międzynarodowymi w odpowiednich ramach współpracy międzynarodowej. **[Popr. 90]**

Artykuł 5

Inwestowanie w infrastrukturę, możliwości, produkty lub ~~rozwiązania~~ ***procesy*** oraz ich wykorzystanie **[Popr. 91]**

1. W przypadku gdy Centrum Kompetencji zapewnia finansowanie infrastruktury, możliwości, produktów lub ~~rozwiązań~~ ***procesów*** zgodnie z art. 4 ust. 3 i 4 w formie ***zamówień,*** dotacji lub nagrody, w planie prac Centrum Kompetencji mogą być określone w szczególności: **[Popr. 92]**

a) ***szczegółowe*** zasady dotyczące funkcjonowania infrastruktury lub możliwości, w tym w stosownych przypadkach dotyczące powierzenia obsługi podmiotowi zajmującemu się hostingiem, w oparciu o kryteria, które określa Centrum Kompetencji; **[Popr. 93]**

b) zasady dotyczące dostępu do infrastruktury lub możliwości oraz ich wykorzystania;

ba) szczegółowe przepisy regulujące różne fazy wdrażania; **[Popr. 94]**

bb) zasada, aby w wyniku wkładu Unii dostęp był otwarty w największym możliwym zakresie, a zamknięty tylko w koniecznym i aby możliwe było ponowne wykorzystanie. **[Popr. 95]**

2. Centrum Kompetencji może być odpowiedzialne za ogólne wykonanie odpowiednich działań związanych ze wspólnym udzielaniem zamówień, w tym za przedkomercyjne zamówienia publiczne w imieniu członków sieci~~, członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa lub innych osób trzecich reprezentujących użytkowników produktów i rozwiązań w dziedzinie cyberbezpieczeństwa~~. W tym celu Centrum Kompetencji może być wspierane przez co najmniej jeden krajowy ośrodek koordynacji ~~lub~~ członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa ***lub odpowiednie europejskie centra innowacji cyfrowych***. **[Popr. 96]**

Artykuł 6

Wyznaczenie krajowych ośrodków koordynacji

-1. W każdym państwie członkowskim ustanawia się jeden krajowy ośrodek koordynacji. **[Popr. 97]**

1. Do dnia [data] każde państwo członkowskie wyznacza podmiot, który będzie pełnił rolę krajowego ośrodka koordynacji do celów niniejszego rozporządzenia, i powiadamia o tym Komisję.

2. Na podstawie oceny dotyczącej spełnienia przez ten podmiot kryteriów określonych w ust. 4 Komisja w ciągu sześciu miesięcy od nominacji przekazanej przez państwo członkowskie wydaje decyzję przewidującą akredytację podmiotu jako krajowego ośrodka koordynacji lub odrzucającą nominację. Komisja publikuje wykaz krajowych ośrodków koordynacji.

3. Państwa członkowskie mogą w dowolnym momencie wyznaczyć nowy podmiot, który będzie pełnił rolę krajowego ośrodka koordynacji do celów niniejszego rozporządzenia. Ust. 1 i 2 mają zastosowanie do wyznaczenia nowego podmiotu.

4. Wyznaczony krajowy ośrodek koordynacji posiada możliwość wspierania Centrum Kompetencji oraz sieci w wypełnianiu ich misji określonej w art. 3 niniejszego rozporządzenia. Ośrodki dysponują techniczną wiedzą fachową w dziedzinie cyberbezpieczeństwa lub bezpośrednim dostępem do niej oraz mają możliwość skutecznego angażowania przemysłu, sektora publicznego***, środowiska akademickiego*** i społeczności badawczej ***oraz obywateli*** i współpracy z nimi. ***Komisja wydaje wytyczne zawierające informacje szczegółowe na temat procedury oceny i wyjaśniające zastosowanie kryteriów.*** **[Popr. 98]**

5. Relacje między Centrum Kompetencji i krajowymi ośrodkami koordynacji opierają się na umowach podpisanych między Centrum Kompetencji i każdym z krajowych ośrodków koordynacji. ~~W umowie określa się~~ ***Umowa zawiera ten sam zestaw zharmonizowanych ogólnych warunków określających*** reguły dotyczące relacji między Centrum Kompetencji i każdym z krajowych ośrodków koordynacji oraz podziału zadań między nimi***, a także warunki szczególne dostosowane do specyfiki danego krajowego ośrodka koordynacji***. **[Popr. 99]**

5a. Komisja przyjmuje, zgodnie z art. 45a, akty delegowane w celu uzupełnienia niniejszego rozporządzenia przez ustanowienie zharmonizowanych ogólnych warunków umownych, o których mowa w ust. 5 niniejszego artykułu, w tym ich formatu. **[Popr. 100]**

6. Sieć krajowych ośrodków koordynacji składa się ze wszystkich krajowych ośrodków koordynacji wyznaczonych przez państwa członkowskie.

Artykuł 7

Zadania krajowych ośrodków koordynacji

1. Cele i związane z nimi zadania krajowych ośrodków koordynacji są następujące:

a) wspieranie Centrum Kompetencji w osiąganiu jego celów, a w szczególności w ***ustanawianiu i*** koordynowaniu działań środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa; **[Popr. 101]**

b) ułatwianie ***społeczeństwu obywatelskiemu,*** przemysłowi***, w szczególności przedsiębiorstwom typu start-up*** i ***MŚP, społeczności akademickiej i badawczej oraz*** innym podmiotom na szczeblu państwa członkowskiego udziału w projektach transgranicznych ***oraz promowanie go i zachęcanie do niego***; **[Popr. 102]**

ba) funkcjonowanie – we współpracy z innymi podmiotami realizującymi podobne zadania – jako punkt kompleksowej obsługi w zakresie produktów i procesów w dziedzinie cyberbezpieczeństwa finansowanych w ramach innych programów unijnych, takich jak InvestEU lub program na rzecz jednolitego rynku, w szczególności w przypadku MŚP; **[Popr. 103]**

c) udział wspólnie z Centrum Kompetencji w określaniu i eliminowaniu ~~stojących przed przemysłem~~ wyzwań w dziedzinie cyberbezpieczeństwa, które dotyczą konkretnych sektorów; **[Popr. 104]**

ca) prowadzenie ścisłej współpracy z krajowymi organizacjami normalizacyjnymi w celu wsparcia absorpcji istniejących norm i zaangażowania wszystkich zainteresowanych stron, w szczególności MŚP, w ustalanie nowych norm; **[Popr. 105]**

d) pełnienie roli punktu kontaktowego na szczeblu krajowym na potrzeby środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa i Centrum Kompetencji;

e) dążenie do tworzenia synergii z odpowiednimi działaniami na szczeblu krajowym i regionalnym;

f) wdrażanie poszczególnych działań, na które Centrum Kompetencji przyznało dotacje, w tym poprzez zapewnianie wsparcia finansowego osobom trzecim zgodnie z art. 204 rozporządzenia XXX [nowe rozporządzenie finansowe] na warunkach określonych w odnośnych umowach o udzielenie dotacji;

fa) promowanie i rozpowszechnianie wspólnych minimalnych programów nauczania w dziedzinie cyberbezpieczeństwa we współpracy z właściwymi organami w państwach członkowskich; **[Popr. 107]**

g) promowanie i rozpowszechnianie przez sieć, środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa i Centrum Kompetencji odpowiednich wyników prac na szczeblu krajowym ~~i~~, regionalnym ***lub lokalnym***; **[Popr. 108]**

h) ocena wniosków o włączenie do środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa składanych przez podmioty ***i osoby fizyczne*** mające siedzibę ***lub zamieszkałe*** w tym samym państwie członkowskim co ośrodek koordynacji. **[Popr. 109]**

2. Do celów określonych w lit. f) wsparcie finansowe dla osób trzecich może być zapewniane w którejkolwiek z form określonych w art. 125 rozporządzenia XXX [nowe rozporządzenie finansowe], w tym w formie kwot ryczałtowych.

3. Krajowe ośrodki koordynacji mogą otrzymać od Unii dotacje zgodnie z art. 195 lit. d) rozporządzenia XXX [nowe rozporządzenie finansowe] w związku z wykonywaniem zadań określonych w niniejszym artykule.

4. W stosownych przypadkach krajowe ośrodki koordynacji współpracują za pośrednictwem sieci ***i z właściwymi europejskimi centrami innowacji cyfrowych*** w celu realizacji zadań, o których mowa w ust. 1 ~~lit. a), b), c), e) i g)~~. **[Popr. 110]**

Artykuł 8

Środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa

1. Środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa wnosi swój wkład w misję Centrum Kompetencji, jak określono w art. 3, oraz wzmacnia***, gromadzi, udostępnia*** i rozpowszechnia wiedzę fachową z zakresu cyberbezpieczeństwa w całej Unii***, a także zapewnia techniczną wiedzę fachową***. **[Popr. 111]**

2. W skład środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa wchodzą ~~organizacje~~ ***społeczeństwo obywatelskie, środowisko*** przemysłowe ***po stronie zarówno popytu***, ***jak i podaży, w tym MSP, środowisko*** akademickie i ~~organizacje~~ naukowe ~~non-profit, a także stowarzyszenia~~ ***, stowarzyszenia użytkowników, indywidualni eksperci***, ***właściwe europejskie organizacje normalizacyjne*** oraz ***inne stowarzyszenia, a także*** podmioty publiczne i inne podmioty zajmujące się kwestiami operacyjnymi i technicznymi ***w obszarze cyberbezpieczeństwa***. Środowisko to skupia główne zainteresowane strony, jeżeli chodzi o technologiczne***, przemysłowe, akademickie*** i ~~przemysłowe~~ ***naukowe oraz społeczne*** zdolności ***i możliwości*** w dziedzinie cyberbezpieczeństwa w Unii. W jego skład wchodzą krajowe ośrodki koordynacji, ***europejskie centra innowacji cyfrowych,*** a także unijne instytucje i organy posiadające odpowiednią wiedzę fachową***, zgodnie z art. 10 niniejszego rozporządzenia***. **[Popr. 112]**

3. Jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa można akredytować jedynie podmioty ***i osoby fizyczne***, które mają siedzibę w Unii~~. Podmioty te~~***, na terenie Europejskiego Obszaru Gospodarczego (EOG) lub Europejskiego Stowarzyszenia Wolnego Handlu. Wnioskodawcy*** muszą wykazać, że ~~dysponują wiedzą~~ ***mogą zapewnić wiedzę*** fachową z zakresu cyberbezpieczeństwa w co najmniej jednej z następujących dziedzin: **[Popr. 113]**

a) ~~badania~~ ***środowisko akademickie lub badania*** naukowe; **[Popr. 114]**

b) rozwój przemysłu;

c) szkolenie i kształcenie;

ca) etyka; **[Popr. 115]**

cb) formalna i techniczna standaryzacja oraz specyfikacje. **[Popr. 116]**

Środa, 17 kwietnia 2019 r.

4. Centrum Kompetencji akredytuje podmioty ustanowione na mocy prawa krajowego ***lub osoby fizyczne*** jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa po przeprowadzeniu przez ***Centrum Kompetencji,*** krajowy ośrodek koordynacji państwa członkowskiego, w którym ma siedzibę dany podmiot ***lub w którym zamieszkuje osoba fizyczna***, ***zharmonizowanej*** oceny, czy podmiot ten spełnia kryteria określone w ust. 3. Akredytacja nie jest ograniczona czasowo, ale Centrum Kompetencji może ją w każdym momencie cofnąć, jeżeli samo Centrum lub właściwy krajowy ośrodek koordynacji uzna, że podmiot ***lub osoba fizyczna*** nie spełnia kryteriów określonych w ust. 3 lub podlega odpowiednim przepisom określonym w art. 136 rozporządzenia XXX [nowe rozporządzenie finansowe]. ***Krajowe ośrodki koordynacji państw członkowskich dążą do osiągnięcia zrównoważonej reprezentacji zainteresowanych stron w środowisku, aktywnie stymulując uczestnictwo w niewystarczająco reprezentowanych kategoriach, szczególnie MŚP, i grupach osób fizycznych.*** **[Popr. 117]**

4a. Komisja przyjmuje akty delegowane zgodnie z art. 45a, aby uzupełnić niniejsze rozporządzenie dzięki dokładniejszemu określeniu kryteriów, o których mowa w ust. 3 niniejszego artykułu i na podstawie których wnioskodawcy są wybierani, oraz procedury oceny i akredytacji jednostek, które spełniają kryteria określone w ust. 4 niniejszego artykułu. **[Popr. 118]**

5. Centrum Kompetencji akredytuje odpowiednie organy, agencje i urzędy Unii jako członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa po przeprowadzeniu oceny, czy dany podmiot spełnia kryteria określone w ust. 3. Akredytacja nie jest ograniczona czasowo, ale Centrum Kompetencji może ją w każdym momencie cofnąć, jeżeli uzna, że podmiot nie spełnia kryteriów określonych w ust. 3 lub podlega odpowiednim przepisom określonym w art. 136 rozporządzenia XXX [nowe rozporządzenie finansowe].

6. W pracach prowadzonych w ramach środowiska mogą brać udział przedstawiciele Komisji.

Artykuł 9

Zadania członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa

Członkowie środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa:

1) wspierają Centrum Kompetencji w wypełnianiu misji i osiąganiu celów określonych w art. 3 i 4 oraz ściśle współpracują w tym celu z Centrum Kompetencji i właściwymi krajowymi ośrodkami koordynacji;

2) uczestniczą w działaniach promowanych przez Centrum Kompetencji i krajowe ośrodki koordynacji;

3) w stosownych przypadkach uczestniczą w grupach roboczych ustanowionych przez Radę Zarządzającą Centrum Kompetencji w celu realizacji poszczególnych działań określonych w planie prac Centrum Kompetencji;

4) w stosownych przypadkach wspierają Centrum Kompetencji i krajowe ośrodki koordynacji w promowaniu poszczególnych projektów;

5) promują i rozpowszechniają stosowne wyniki działań i projektów prowadzonych w ramach społeczności.

5a) wspierają Centrum Kompetencji dzięki zgłaszaniu i ujawnianiu luk w zabezpieczeniach, pomocy w ich łagodzeniu i doradzaniu w zakresie eliminowania takich słabych punktów, w tym poprzez certyfikację w ramach systemów przyjętych zgodnie z rozporządzeniem (UE) 2019/XXX [akt ws. cyberbezpieczeństwa]. **[Popr. 119]**

Artykuł 10

Współpraca Centrum Kompetencji z instytucjami, organami, urzędami i agencjami Unii

1. ***W celu zapewnienia spójności i komplementarności*** Centrum Kompetencji współpracuje z odpowiednimi instytucjami, organami, urzędami i agencjami Unii, w tym z ~~Agencją Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji~~ ***ENISA***, z zespołem reagowania na incydenty komputerowe (CERT-UE), Europejską Służbą Działań Zewnętrznych, ze Wspólnym Centrum Badawczym Komisji, Agencją Wykonawczą ds. Badań Naukowych, Agencją Wykonawczą ds. Innowacyjności i Sieci, ***odpowiednimi europejskimi centrami innowacji cyfrowych,*** Europejskim Centrum ds. Walki z Cyberprzestępczością w Europolu oraz z Europejską Agencją Obrony ***w odniesieniu do projektów, usług i kompetencji podwójnego zastosowania***. **[Popr. 120]**

2. Taka współpraca ma miejsce w ramach uzgodnień roboczych. Uzgodnienia te ~~należy uprzednio przedłożyć do zatwierdzenia~~ ***przyjmuje Rada Zarządzająca po uprzednim zatwierdzeniu*** przez Komisję. **[Popr. 121]**

ROZDZIAŁ II

ORGANIZACJA CENTRUM KOMPETENCJI

Artykuł 11

Członkostwo i struktura

1. Członkami Centrum Kompetencji są Unia reprezentowana przez Komisję i państwa członkowskie.

2. Struktura Centrum Kompetencji składa się z:

a) Rady Zarządzającej, która wykonuje zadania określone w art. 13;

b) dyrektora wykonawczego, który wykonuje zadania określone w art. 16;

c) Rady Konsultacyjnej ds. Przemysłowych i Naukowych, która pełni funkcje określone w art. 20.

SEKCJA I

RADA ZARZĄDZAJĄCA

Artykuł 12

Skład Rady Zarządzającej

1. W skład Rady Zarządzającej wchodzi po jednym przedstawicielu każdego państwa członkowskiego***, jeden przedstawiciel wyznaczony przez Parlament Europejski do roli obserwatora*** oraz ~~pięciu~~ ***czterech*** przedstawicieli Komisji w imieniu Unii***, przy czym dąży się do zachowania równowagi płci wśród członków Rady i ich zastępców***. **[Popr. 122]**

2. Każdy z członków Rady Zarządzającej posiada zastępcę, który reprezentuje członka w przypadku jego nieobecności.

3. Członków Rady Zarządzającej i ich zastępców powołuje się, biorąc pod uwagę ich wiedzę z dziedziny ~~technologii~~ ***cyberbezpieczeństwa***, a także odpowiednie umiejętności kierownicze, administracyjne i w zakresie zarządzania budżetem. Komisja oraz państwa członkowskie dokładają starań, aby ograniczyć rotację swoich przedstawicieli w Radzie Zarządzającej w celu zapewnienia ciągłości pracy Rady. Komisja oraz państwa członkowskie mają na celu osiągnięcie zrównoważonej reprezentacji mężczyzn i kobiet w Radzie Zarządzającej. **[Popr. 123]**

4. Kadencja członków Rady Zarządzającej i ich zastępców trwa cztery lata. Kadencja ta jest odnawialna.

5. Członkowie Rady Zarządzającej działają w sposób niezależny i przejrzysty w interesie Centrum Kompetencji, chroniąc jego cele i misję, tożsamość, autonomię i spójność.

6. ~~Komisja~~ ***Rada Zarządzająca*** może, w stosownych przypadkach, zapraszać obserwatorów, w tym przedstawicieli odpowiednich unijnych organów, urzędów i agencji ***a także członków środowiska***, do udziału w posiedzeniach Rady Zarządzającej. **[Popr. 124]**

7. ~~Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (~~ENISA~~) jest stałym obserwatorem~~ ***oraz Rada Konsultacyjna ds. Przemysłowych i Naukowych są stałymi obserwatorami*** w Radzie Zarządzającej***, zapewniając doradztwo bez prawa głosu. Rada Zarządzająca w najwyższym stopniu uwzględnia opinie wyrażone przez stałych obserwatorów***. **[Popr. 125]**

Środa, 17 kwietnia 2019 r.

Artykuł 13

Zadania Rady Zarządzającej

1. Rada Zarządzająca ponosi ogólną odpowiedzialność za strategiczną orientację i operacje Centrum Kompetencji oraz nadzoruje realizację jego działalności.

2. Rada Zarządzająca uchwala swój regulamin wewnętrzny. Regulamin ten zawiera szczegółowe procedury ustalania i unikania konfliktów interesów i zapewnia poufność wszelkich informacji szczególnie chronionych.

3. Rada Zarządzająca podejmuje niezbędne decyzje strategiczne, a w szczególności:

a) przyjmuje wieloletni plan strategiczny obejmujący zestawienie głównych priorytetów oraz planowanych inicjatyw Centrum Kompetencji, w tym oszacowanie potrzeb finansowych i źródeł finansowania***, uwzględniając doradztwo ENISA***; **[Popr. 126]**

b) na podstawie wniosku dyrektora wykonawczego przyjmuje plan prac Centrum Kompetencji, roczne sprawozdanie finansowe i bilans oraz roczne sprawozdanie z działalności***, uwzględniając doradztwo ENISA***; **[Popr. 127]**

c) przyjmuje szczegółowe przepisy finansowe Centrum Kompetencji zgodnie z [art. 70 RF];

d) przyjmuje procedurę powoływania dyrektora wykonawczego;

e) przyjmuje ~~kryteria i~~ procedury oceny i akredytacji podmiotów jako członków środowiska ~~posiadającego kompetencje w dziedzinie cyberbezpieczeństwa~~; **[Popr. 128]**

ea) przyjmuje uzgodnienia robocze, o których mowa w art. 10 ust. 2; **[Popr. 129]**

f) powołuje, zwalnia i przedłuża kadencję dyrektora wykonawczego, udziela mu wskazówek i monitoruje jego działania oraz powołuje księgowego;

g) przyjmuje roczny budżet Centrum Kompetencji, w tym odpowiedni plan zatrudnienia wskazujący liczbę stanowisk czasowych według grupy funkcyjnej i grupy zaszeregowania, liczbę pracowników kontraktowych i oddelegowanych ekspertów krajowych, wyrażone w ekwiwalentach pełnego czasu pracy;

ga) przyjmuje dla Centrum Kompetencji przepisy dotyczące przejrzystości; **[Popr. 130]**

h) przyjmuje przepisy dotyczące konfliktów interesów;

i) ustanawia grupy robocze złożone z członków środowiska ~~posiadającego kompetencje w dziedzinie cyberbezpieczeństwa~~***, uwzględniając doradztwo stałych obserwatorów***; **[Popr. 131]**

j) powołuje członków Rady Konsultacyjnej ds. Przemysłowych i Naukowych;

k) ustanawia funkcję audytu wewnętrznego zgodnie z rozporządzeniem delegowanym Komisji (UE) nr 1271/2013 ([19]);

l) promuje ***współpracę*** Centrum Kompetencji ~~w skali globalnej, aby zwiększyć jego atrakcyjność i uczynić~~ z ~~niego światowej klasy podmiot doskonałości w dziedzinie cyberbezpieczeństwa~~ ***globalnymi podmiotami***; **[Popr. 132]**

m) tworzy politykę komunikacyjną Centrum Kompetencji na podstawie zalecenia dyrektora wykonawczego;

n) odpowiada za monitorowanie odpowiednich działań następczych wynikających z wniosków z ocen retrospektywnych;

o) w stosownych przypadkach ustanawia przepisy wykonawcze do regulaminu pracowniczego i warunków zatrudnienia zgodnie z art. 31 ust. 3;

p) w stosownych przypadkach określa zasady dotyczące delegowania ekspertów krajowych do Centrum Kompetencji oraz wykorzystania stażystów zgodnie z art. 32 ust. 2;

([19]) Rozporządzenie delegowane Komisji (UE) nr 1271/2013 z dnia 30 września 2013 r. w sprawie ramowego rozporządzenia finansowego dotyczącego organów, o których mowa w art. 208 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 966/2012 (Dz.U. L 328 z 7.12.2013, s. 42).

q) przyjmuje przepisy bezpieczeństwa dla Centrum Kompetencji;

r) przyjmuje strategię zwalczania nadużyć finansowych~~, która jest proporcjonalna~~ ***i korupcji, proporcjonalną*** do istniejących w tym zakresie zagrożeń, **z *uwzględnieniem analizy*** ~~uwzględniając analizę~~ kosztów i ~~korzyści~~ ***korzyści*** ~~w odniesieniu do~~ środków, które mają zostać wdrożone***, jak również przyjmuje kompleksowe środki ochrony osób zgłaszających przypadki naruszenia prawa Unii zgodnie*** z ***mającym zastosowanie ustawodawstwem Unii***; **[Popr. 133]**

s) przyjmuje ***wyczerpującą definicję wkładów finansowych państw członkowskich oraz*** metodę obliczania ~~wkładu finansowego~~ ***kwoty dobrowolnych wkładów*** państw członkowskich***, które mogą być rozliczane jako wkłady finansowe zgodnie z tą definicją; takie obliczenia przeprowadza się na koniec każdego roku budżetowego***; **[Popr. 134]**

t) odpowiada za każde zadanie nieprzydzielone żadnemu konkretnemu organowi Centrum Kompetencji; może przydzielać takie zadania każdemu organowi Centrum Kompetencji.

Artykuł 14

Przewodniczący i posiedzenia Rady Zarządzającej

1. Rada Zarządzająca***, starając się zachować równowagę płci,*** wybiera na okres dwóch lat przewodniczącego i zastępcę przewodniczącego spośród tych członków, którzy mają prawo głosu. Kadencję przewodniczącego i zastępcy przewodniczącego można jednokrotnie przedłużyć na podstawie decyzji Rady Zarządzającej. Jeżeli jednak w dowolnym momencie swojej kadencji stracą oni status członka Rady Zarządzającej, kadencja ich kończy się automatycznie w tym samym dniu. Zastępca przewodniczącego zastępuje z urzędu przewodniczącego, jeżeli przewodniczący nie jest w stanie pełnić swoich obowiązków. Przewodniczący bierze udział w głosowaniu. **[Popr. 135]**

2. Rada Zarządzająca odbywa swoje zwykłe posiedzenia co najmniej trzy razy w roku. Rada może zwoływać posiedzenia nadzwyczajne na wniosek Komisji, na wniosek co najmniej jednej trzeciej wszystkich swoich członków, na wniosek przewodniczącego lub na wniosek dyrektora wykonawczego w ramach wykonywania jego zadań.

3. Dyrektor wykonawczy ma prawo uczestniczenia w obradach, o ile Rada Zarządzająca nie postanowi inaczej, lecz bez prawa głosu. ~~Rada Zarządzająca może zapraszać na poszczególne posiedzenia również inne osoby w charakterze obserwatorów.~~ **[Popr. 136]**

~~4. Członkowie Rady Konsultacyjnej ds. Przemysłowych i Naukowych mogą brać udział w posiedzeniach Rady Zarządzającej, na zaproszenie przewodniczącego, bez prawa głosu.~~ **[Popr. 137]**

5. Członkowie Rady Zarządzającej i ich zastępcy mogą korzystać podczas posiedzeń z pomocy doradców lub ekspertów, z zastrzeżeniem przepisów regulaminu wewnętrznego.

6. Centrum Kompetencji zapewnia Radzie Zarządzającej obsługę sekretariatu.

~~Artykuł 15~~

~~Zasady głosowania Rady Zarządzającej~~

~~1. Unia posiada 50 % praw głosu. Głosy Unii są niepodzielne.~~

~~2. Każde uczestniczące państwo członkowskie posiada jeden głos.~~

~~3. Rada Zarządzająca podejmuje decyzje większością co najmniej 75 % wszystkich głosów, w tym głosów członków nieobecnych, reprezentujących co najmniej 75 % całkowitych wkładów finansowych na rzecz Centrum Kompetencji. Wkład finansowy oblicza się na podstawie zaproponowanych przez państwa członkowskie szacowanych wydatków, o których mowa w art. 17 ust. 2 lit. c), oraz na podstawie sprawozdania na temat wartości wkładów uczestniczących państw członkowskich, o którym mowa w art. 22 ust. 5.~~

~~4. Jedynie przedstawiciele Komisji i przedstawiciele uczestniczących państw członkowskich posiadają prawo głosu.~~

~~5. Przewodniczący bierze udział w głosowaniu.~~ **[Popr. 138]**

Środa, 17 kwietnia 2019 r.

Artykuł 15a

Zasady głosowania Rady Zarządzającej

1. Decyzje poddawane pod głosowanie mogą dotyczyć:

a) zarządzania i organizacji Centrum Kompetencji i sieci;

b) przydziału środków budżetowych na rzecz Centrum Kompetencji i sieci;

c) wspólnych działań szeregu państw członkowskich, z ewentualnym wkładem z budżetu Unii zgodnie z decyzją o przydziale, o której mowa w lit. b).

2. Rada Zarządzająca podejmuje decyzje większością co najmniej 75 % głosów wszystkich członków. Głosy Unii, która reprezentowana jest przez Komisję, są niepodzielne.

3. W przypadku decyzji, o których mowa w ust. 1 lit. a), każde państwo członkowskie jest reprezentowane i posiada takie same równe prawa głosu. Jeżeli chodzi o pozostałe głosy (w obrębie puli 100 %), Unia powinna posiadać co najmniej 50 % praw głosu odpowiadających jej wkładowi finansowemu.

4. W przypadku decyzji wchodzących w zakres ust. 1 lit. b) lub c) lub jakiejkolwiek innej decyzji nienależącej do żadnej innej kategorii wymienionej w ust. 1 Unia posiada co najmniej 50 % praw głosu odpowiadających jej wkładowi finansowemu. Tylko finansujące państwa członkowskie mają prawo głosu odpowiadające wkładowi finansowemu danego państwa.

5. Jeżeli przewodniczący został wybrany spośród przedstawicieli państw członkowskich, przewodniczący bierze udział w głosowaniu jako przedstawiciel swojego państwa członkowskiego. **[Popr. 139]**

SEKCJA II

DYREKTOR WYKONAWCZY

Artykuł 16

Mianowanie, zwolnienie lub przedłużenie kadencji dyrektora wykonawczego

1. Dyrektor wykonawczy musi dysponować wiedzą fachową i cieszyć się szerokim uznaniem w dziedzinach, w których Centrum Kompetencji prowadzi działalność.

2. Dyrektor wykonawczy zatrudniany jest w Centrum Kompetencji na czas określony, zgodnie z art. 2 lit. a) warunków zatrudnienia innych pracowników.

3. Rada Zarządzająca w ramach otwartej***, przejrzystej*** i ~~przejrzystej~~ ***niedyskryminującej*** procedury wyboru mianuje dyrektora wykonawczego z listy kandydatów zaproponowanych przez Komisję ***oraz kandydatur z państw członkowskich zgłoszonych z myślą o zachowaniu równości płci***. **[Popr. 140]**

4. Do celów zawarcia umowy z dyrektorem wykonawczym Centrum Kompetencji jest reprezentowane przez przewodniczącego Rady Zarządzającej.

5. Kadencja dyrektora wykonawczego trwa ~~cztery lata~~ ***pięć lat***. Przed upływem tego okresu Komisja przeprowadza ocenę, w której uwzględnia ocenę wykonywania zadań przez dyrektora wykonawczego oraz przyszłe zadania i wyzwania Centrum Kompetencji. **[Popr. 141]**

6. Rada Zarządzająca, działając na wniosek Komisji, w którym uwzględniono ocenę, o której mowa w ust. 5, może przedłużyć kadencję dyrektora wykonawczego jednokrotnie na okres nie dłuższy niż ~~cztery lata~~ ***pięć lat***. **[Popr. 142]**

7. Dyrektor wykonawczy, którego kadencję przedłużono, nie może brać udziału w kolejnej procedurze wyboru na to samo stanowisko.

8. Dyrektor wykonawczy zostaje odwołany ze stanowiska jedynie na mocy decyzji Rady Zarządzającej działającej na wniosek ***swoich członków lub na wniosek*** Komisji. **[Popr. 143]**

Artykuł 17

Zadania dyrektora wykonawczego

1. Dyrektor wykonawczy jest odpowiedzialny za działalność Centrum Kompetencji i za bieżące zarządzanie nim oraz pełni funkcję jego przedstawiciela prawnego. Dyrektor wykonawczy jest odpowiedzialny przed Radą Zarządzającą i swoje obowiązki pełni całkowicie niezależnie w zakresie przyznanych mu uprawnień.

2. W szczególności dyrektor wykonawczy realizuje w niezależny sposób następujące zadania:

a) wykonuje decyzje przyjęte przez Radę Zarządzającą;

b) wspiera działania Rady Zarządzającej, pomaga sekretariatowi w organizacji posiedzeń oraz przekazuje wszelkie informacje, które są niezbędne do wykonania jej obowiązków;

c) przygotowuje i przedkłada Radzie Zarządzającej do przyjęcia, po konsultacjach z Radą Zarządzającą***, Radą Konsultacyjną ds. Przemysłowych*** i ***Naukowych, ENISA i*** Komisją, projekt wieloletniego planu strategicznego oraz projekt rocznego planu prac Centrum Kompetencji, uwzględniając zakres zaproszeń do składania wniosków, zaproszeń do wyrażenia zainteresowania i zaproszeń do składania ofert potrzebnych do celów realizacji planu prac oraz powiązane szacunki wydatków proponowane przez państwa członkowskie i Komisję; **[Popr. 144]**

d) opracowuje i przedkłada Radzie Zarządzającej do przyjęcia projekt budżetu rocznego, w tym powiązanego z nim planu zatrudnienia, określającego liczbę stanowisk czasowych według grupy funkcyjnej i grupy zaszeregowania oraz liczbę pracowników kontraktowych i oddelegowanych ekspertów krajowych, wyrażone w ekwiwalentach pełnego czasu pracy;

e) realizuje plan prac i składa sprawozdania z jego realizacji Radzie Zarządzającej;

f) przygotowuje projekt rocznego sprawozdania z działalności Centrum Kompetencji, uwzględniając informacje na temat powiązanych wydatków;

g) zapewnia wdrożenie skutecznych procedur monitorowania i oceny związanych z funkcjonowaniem Centrum Kompetencji;

h) przygotowuje plan działania w następstwie wniosków z ocen retrospektywnych oraz przedkłada Komisji ***i Parlamentowi Europejskiemu*** co dwa lata sprawozdania z postępów; **[Popr. 145]**

i) przygotowuje, negocjuje i zawiera umowy z krajowymi ośrodkami koordynacji;

j) jest odpowiedzialny za kwestie administracyjne, finansowe i pracownicze, w tym za wykonanie budżetu Centrum Kompetencji, należycie uwzględniając wskazówki otrzymane od komórki audytu wewnętrznego w ramach uprawnień przekazanych przez Radę Zarządzającą;

k) zatwierdza ogłaszanie zaproszeń do składania wniosków i zarządza nimi – zgodnie z planem prac – oraz zarządza umowami o udzielenie dotacji i decyzjami o udzieleniu dotacji;

l) zatwierdza***, po zasięgnięciu opinii Rady Konsultacyjnej ds. Przemysłowych i Naukowych i ENISA,*** wykaz działań wybranych do finansowania w oparciu o listę rankingową ustaloną przez zespół niezależnych ekspertów; **[Popr. 146]**

m) zatwierdza ogłaszanie zaproszeń do składania ofert i zarządza nimi – zgodnie z planem prac – oraz zarządza umowami;

n) zatwierdza oferty wybrane do finansowania;

o) przedkłada komórce audytu wewnętrznego, a następnie Radzie Zarządzającej, projekt rocznego sprawozdania finansowego oraz bilansu;

p) zapewnia przeprowadzanie oceny ryzyka oraz stosowanie środków w zakresie zarządzania ryzykiem;

q) popisuje poszczególne umowy o udzielenie dotacji, decyzje i umowy;

r) podpisuje umowy w sprawie zamówienia publicznego;

s) przygotowuje plan działania na podstawie wniosków ze sprawozdań z kontroli wewnętrznej lub zewnętrznej, a także z dochodzeń przeprowadzanych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF), oraz składa sprawozdania z postępów prac dwa razy w roku Komisji i ***Parlamentowi Europejskiemu oraz*** regularnie Radzie Zarządzającej; **[Popr. 147]**

t) przygotowuje projekt przepisów finansowych mających zastosowanie do Centrum Kompetencji;

u) ustanawia skuteczny i efektywny system kontroli wewnętrznych i zapewnia jego funkcjonowanie oraz zgłasza Radzie Zarządzającej wszelkie istotne zmiany w tym systemie;

v) zapewnia skuteczną komunikację z instytucjami Unii***oraz przedstawia sprawozdanie Parlamentowi Europejskiemu i Radzie na wniosek***; **[Popr. 148]**

w) podejmuje wszelkie pozostałe działania potrzebne do oceny postępów Centrum Kompetencji w realizacji jego misji i celów określonych w art. 3 i 4 niniejszego rozporządzenia;

x) wykonuje wszelkie inne zadania powierzone lub zlecone mu przez Radę Zarządzającą.

SEKCJA III

RADA KONSULTACYJNA DS. PRZEMYSŁOWYCH I NAUKOWYCH

Artykuł 18

Skład Rady Konsultacyjnej ds. Przemysłowych i Naukowych

1. Rada Konsultacyjna ds. Przemysłowych i Naukowych liczy nie więcej niż ~~16~~ ***25*** członków. Członków mianuje Rada Zarządzająca spośród przedstawicieli podmiotów będących częścią środowiska ~~posiadającego kompetencje w dziedzinie cyberbezpieczeństwa~~ ***lub poszczególnych członków. Kwalifikują się jedynie przedstawiciele podmiotów, które nie są kontrolowane przez państwo trzecie lub podmioty z państw trzecich, z wyjątkiem państw EOG i EFTA. Mianowanie odbywa się zgodnie z otwartą, przejrzystą i niedyskryminacyjną procedurą. W składzie Rady dąży się do osiągnięcia równowagi płci i zapewnia zrównoważoną reprezentację grup zainteresowanych stron reprezentujących przemysł, środowisko akademickie i społeczeństwo obywatelskie***. **[Popr. 149]**

2. Członkowie Rady Konsultacyjnej ds. Przemysłowych i Naukowych posiadają wiedzę fachową albo w dziedzinach badań nad cyberbezpieczeństwem, rozwoju przemysłu, ~~zawodów regulowanych albo we~~ ***albo oferowaniu, realizowaniu lub*** wdrażaniu ~~rozwiązań~~ ***usług świadczonych*** w ~~tych obszarach~~ ***ramach zawodów regulowanych lub produktów z tym związanych***. Rada Zarządzająca szczegółowo określa wymogi dotyczące takiej wiedzy fachowej. **[Popr. 150]**

3. Procedury dotyczące powoływania jej członków przez Radę Zarządzającą oraz funkcjonowania Rady Konsultacyjnej określa się w regulaminie wewnętrznym Centrum Kompetencji i podaje do wiadomości publicznej.

4. Kadencja członków Rady Konsultacyjnej ds. Przemysłowych i Naukowych trwa trzy lata. Kadencja ta jest odnawialna.

5. Przedstawiciele Komisji oraz ~~Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji mogą brać udział~~ ***ENISA są zapraszani do udziału*** w pracach Rady Konsultacyjnej ds. Przemysłowych i Naukowych i ~~zapewniać im~~ ***zapewniają jej*** wsparcie. ***W indywidualnych przypadkach Rada może zaprosić dodatkowych przedstawicieli ze środowiska w charakterze obserwatora, doradców lub ekspertów.*** **[Popr. 151]**

Artykuł 19

Funkcjonowanie Rady Konsultacyjnej ds. Przemysłowych i Naukowych

1. Posiedzenia Rady Konsultacyjnej ds. Przemysłowych i Naukowych odbywają się co najmniej ~~dwa~~ ***trzy*** razy w roku. **[Popr. 152]**

2. Rada Konsultacyjna ds. Przemysłowych i Naukowych ~~może doradzać~~ ***przedstawia wskazówki*** Radzie Zarządzającej w sprawie tworzenia, w razie potrzeby, grup roboczych ds. konkretnych kwestii istotnych dla pracy Centrum Kompetencji ~~koordynowanych całościowo~~ ***, w przypadkach gdy kwestie te wchodzą w zakres zadań i obszarów kompetencji określonych w art. 20 i gdy są konieczne z uwagi na ogólną koordynację*** przez co najmniej jednego członka Rady Konsultacyjnej ds. Przemysłowych i Naukowych. **[Popr. 153]**

3. Rada Konsultacyjna ds. Przemysłowych i Naukowych wybiera swojego przewodniczącego.

4. Rada Konsultacyjna ds. Przemysłowych i Naukowych przyjmuje swój regulamin wewnętrzny, obejmujący powołanie przedstawicieli, którzy w stosownych przypadkach reprezentują Radę Konsultacyjną, oraz określający okres, na jaki zostali powołani.

Artykuł 20

Zadania Rady Konsultacyjnej ds. Przemysłowych i Naukowych

Rada Konsultacyjna ds. Przemysłowych i Naukowych ***regularnie*** doradza Centrum Kompetencji w kwestiach dotyczących prowadzenia jego działalności i wykonuje następujące zadania: **[Popr. 154]**

1) zapewnia dyrektorowi wykonawczemu i Radzie Zarządzającej doradztwo strategiczne i ~~uwagi dotyczące przygotowywania~~ ***wkład we wdrażanie planów przez Centrum Kompetencji, jego ukierunkowanie i działalność w obszarach przemysłu i nauki, a także w przygotowanie*** planu prac i wieloletniego planu strategicznego w terminach ustalonych przez Radę Zarządzającą; **[Popr. 155]**

1a) zapewnia doradztwo na rzecz Rady Zarządzającej w zakresie tworzenia grup roboczych zajmujących się szczególnymi kwestiami związanymi z pracą Centrum Kompetencji; **[Popr. 156]**

2) organizuje konsultacje publiczne otwarte dla wszystkich zainteresowanych stron z sektora publicznego i prywatnego, dla których cyberbezpieczeństwo stanowi przedmiot zainteresowania, aby zebrać informacje na potrzeby strategicznego doradztwa, o którym mowa w ust. 1;

3) promuje przesyłanie informacji zwrotnych na temat planu prac i wieloletniego planu strategicznego Centrum Kompetencji oraz je gromadzi***, a także doradza Radzie Zarządzającej na temat możliwości poprawy strategicznego ukierunkowania i działania Centrum Kompetencji***. **[Popr. 157]**

ROZDZIAŁ III

PRZEPISY FINANSOWE

Artykuł 21

Wkład finansowy Unii

1. Wkład Unii na pokrycie administracyjnych i operacyjnych kosztów Centrum Kompetencji obejmuje następujące kwoty:

a) ~~1 981 668 000~~ ***1 780 954 875 EUR w cenach z 2018 r. (1 998 696 000*** EUR ***w cenach bieżących)*** z programu „Cyfrowa Europa", w tym do wysokości ***21 385 465 EUR w cenach z 2018 r. (***23 746 000 EUR ***w cenach bieżących)*** na pokrycie kosztów administracyjnych; **[Popr. 158]**

b) kwotę pochodzącą z programu „Horyzont Europa", w tym na pokrycie kosztów administracyjnych, która zostanie określona z uwzględnieniem procesu planowania strategicznego, który zostanie przeprowadzony na podstawie art. 6 ust. 6 rozporządzenia XXX [rozporządzenie w sprawie programu „Horyzont Europa"].

ba) kwotę pochodzącą z Europejskiego Funduszu Obronnego na działania Centrum Kompetencji związane z obronnością, w tym na koszty administracyjne, takie jak koszty, jakie może ponieść Centrum Kompetencji, gdy występuje w charakterze kierownika projektu w przypadku działań prowadzonych w ramach Europejskiego Funduszu Obronnego. **[Popr. 159]**

Środa, 17 kwietnia 2019 r.

2. Maksymalny wkład Unii wypłaca się ze środków w budżecie ogólnym Unii przeznaczonych na [program „Cyfrowa Europa”] ~~i na~~ program szczegółowy służący realizacji programu „Horyzont Europa”, ustanowiony decyzją XXX***, Europejski Fundusz Obronny oraz na inne programy i projekty wchodzące w zakres Centrum Kompetencji i sieci***. **[Popr. 160]**

3. Centrum Kompetencji realizuje działania dotyczące cyberbezpieczeństwa w ramach [programu „Cyfrowa Europa”] oraz [programu „Horyzont Europa”] zgodnie z art. 62 lit. c) ppkt (iv) rozporządzenia (UE, Euratom) XXX ([20]) [rozporządzenie finansowe].

4. Wkład finansowy Unii ***z programu „Cyfrowa Europa” i programu „Horyzont Europa”*** nie pokrywa zadań, o których mowa w art. 4 ust. 8 lit. b). ***Zadania te realizowane są ze środków pochodzących z Europejskiego Funduszu Obronnego.*** **[Popr. 161]**

Artykuł 22

Wkład uczestniczących państw członkowskich

1. Uczestniczące państwa członkowskie wnoszą łączny wkład na poczet kosztów operacyjnych i administracyjnych Centrum Kompetencji co najmniej w kwotach, o których mowa w art. 21 ust. 1 niniejszego rozporządzenia.

2. Na potrzeby oszacowania wkładów, o których mowa w art. 23 ust. 1 oraz ust. 3 lit. b) ppkt (ii), koszty ustala się zgodnie z praktykami księgowymi zwyczajowo stosowanymi przez dane państwa członkowskie przy obliczaniu kosztów, standardami rachunkowości obowiązującymi w danym państwie członkowskim, a także obowiązującymi międzynarodowymi standardami rachunkowości oraz międzynarodowymi standardami sprawozdawczości finansowej. Koszty poświadcza niezależny audytor zewnętrzny powołany przez dane państwo członkowskie. Jeżeli poświadczenie budzi jakiekolwiek wątpliwości, Centrum Kompetencji może zweryfikować metodę wyceny.

3. W przypadku gdy uczestniczące państwo członkowskie nie wykonuje swoich zobowiązań dotyczących uzgodnionego wkładu finansowego, dyrektor wykonawczy sporządza pismo w tej sprawie i ustala w nim rozsądny termin, w którym takie niewykonanie zobowiązania ma zostać naprawione. W przypadku gdy niewykonanie zobowiązania nie zostanie naprawione we wskazanym terminie, dyrektor wykonawczy zwołuje posiedzenie Rady Zarządzającej, która podejmuje decyzję, czy uczestniczącemu państwu członkowskiemu, które nie wywiązuje się ze swoich zobowiązań, należy odebrać prawo głosu, bądź czy należy zastosować inne środki do czasu wywiązania się przez nie z zobowiązania. Prawo głosu uczestniczącego państwa członkowskiego, które nie wywiązuje się ze swoich zobowiązań, zawiesza się do czasu wywiązania się z nich.

4. Komisja może zakończyć, w proporcjonalnym stopniu ograniczyć lub zawiesić wypłacanie wkładu finansowego Unii na rzecz Centrum Kompetencji, jeżeli uczestniczące państwa członkowskie nie wnoszą swojego wkładu, o którym mowa w ust. 1, ***lub*** wnoszą go jedynie częściowo***. Zakończenie, ograniczenie*** lub ~~spóźniają się z jego wniesieniem.~~ ***zawieszenie przez Komisję wypłacania wkładu finansowego Unii jest proporcjonalne pod względem kwoty i czasu do ograniczenia, zakończenia lub zawieszenia wypłacania wkładów państw członkowskich.*** **[Popr. 162]**

5. Do dnia 31 stycznia każdego roku uczestniczące państwa członkowskie składają Radzie Zarządzającej sprawozdanie na temat wartości wkładów, o których mowa w ust. 1 i które zostały wniesione w każdym poprzednim roku budżetowym.

Artykuł 23

Koszty i zasoby Centrum Kompetencji

1. Centrum Kompetencji jest wspólnie finansowane przez Unię i państwa członkowskie za pomocą wkładów finansowych wypłacanych w transzach i wkładów obejmujących koszty poniesione przez krajowe ośrodki koordynacji oraz beneficjentów w związku z realizacją działań, których koszty nie są zwracane przez Centrum Kompetencji.

2. Koszty administracyjne Centrum Kompetencji nie przekraczają [kwota] EUR i są pokrywane z wkładów finansowych podzielonych równo w skali rocznej między Unię i uczestniczące państwa członkowskie. Ewentualna niewykorzystana część wkładu na pokrycie kosztów administracyjnych może zostać przeznaczona na pokrycie kosztów operacyjnych Centrum Kompetencji.

3. Koszty operacyjne Centrum Kompetencji są pokrywane ze środków pochodzących z:

a) wkładu finansowego Unii;

([20]) [dodać pełny tytuł i odniesienie do Dz.U.]

b) wkładów uczestniczących państw członkowskich w postaci:

(i) wkładów finansowych; oraz

(ii) w stosownych przypadkach wkładów rzeczowych uczestniczących państw członkowskich na pokrycie kosztów poniesionych przez krajowe ośrodki koordynacji oraz beneficjentów w związku z realizacją działań po odliczeniu wkładu Centrum Kompetencji i wszelkich innych wkładów Unii przeznaczonych na pokrycie tych kosztów;

4. Na zasoby uwzględnione w budżecie Centrum Kompetencji składają się następujące wkłady:

a) wkłady finansowe ***Unii i*** uczestniczących państw członkowskich na pokrycie kosztów administracyjnych; **[Popr. 163]**

b) wkłady finansowe ***Unii i*** uczestniczących państw członkowskich na pokrycie kosztów operacyjnych; **[Popr. 164]**

c) wszelkie przychody osiągane przez Centrum Kompetencji;

d) wszelkie inne wkłady finansowe, zasoby i przychody.

5. Wszelkie odsetki uzyskane z wkładów wypłaconych na rzecz Centrum Kompetencji przez uczestniczące państwa członkowskie uznaje się za jego przychód.

6. Wszystkie zasoby Centrum Kompetencji i jego działania służą osiągnięciu celów określonych w art. 4.

7. Wszystkie aktywa wytworzone przez Centrum Kompetencji lub przekazane mu na potrzeby realizacji jego celów stanowią własność Centrum Kompetencji.

8. Poza przypadkiem likwidacji Centrum Kompetencji na rzecz uczestniczących członków Centrum Kompetencji nie dokonuje się żadnych wypłat ewentualnej nadwyżki przychodów nad wydatkami.

8a. Centrum Kompetencji współpracuje ściśle z innymi instytucjami, agencjami i organami Unii w celu wykorzystania synergii i w odpowiednich przypadkach zmniejszenia kosztów administracyjnych. **[Popr. 165]**

Artykuł 24

Zobowiązania finansowe

Zobowiązania finansowe Centrum Kompetencji nie przekraczają kwoty zasobów finansowych dostępnych w jego budżecie lub zadeklarowanych na rzecz tego budżetu przez jego członków.

Artykuł 25

Rok budżetowy

Rok budżetowy trwa od dnia 1 stycznia do dnia 31 grudnia.

Artykuł 26

Ustanowienie budżetu

1. Każdego roku dyrektor wykonawczy sporządza projekt preliminarza dochodów i wydatków Centrum Kompetencji na następny rok budżetowy oraz przekazuje ten projekt Radzie Zarządzającej wraz z projektem planu zatrudnienia. Dochody i wydatki muszą się równoważyć. Wydatki Centrum Kompetencji obejmują wydatki na personel, administrację, infrastrukturę i działania operacyjne. Wydatki administracyjne utrzymywane są na jak najniższym poziomie.

2. Każdego roku Rada Zarządzająca opracowuje na podstawie projektu preliminarza dochodów i wydatków, o którym mowa w ust. 1, preliminarz dochodów i wydatków Centrum Kompetencji w następnym roku budżetowym.

3. Do dnia 31 stycznia każdego roku Rada Zarządzająca przesyła Komisji preliminarz, o którym mowa w ust. 2, stanowiący część projektu jednolitego dokumentu programowego.

Środa, 17 kwietnia 2019 r.

4. Na podstawie tego preliminarza Komisja wprowadza do projektu budżetu Unii przewidywane kwoty, które uważa za niezbędne w związku z planem zatrudnienia, oraz kwotę wkładu, który ma zostać wniesiony z budżetu ogólnego, oraz przedkłada ten projekt Parlamentowi Europejskiemu i Radzie zgodnie z art. 313 i 314 TFUE.

5. Parlament Europejski i Rada zatwierdzają środki przewidziane na wkład na rzecz Centrum Kompetencji.

6. Parlament Europejski i Rada przyjmują plan zatrudnienia Centrum Kompetencji.

7. Rada Zarządzająca przyjmuje budżet Centrum wraz z planem prac. Budżet staje się ostateczny po ostatecznym przyjęciu budżetu ogólnego Unii. W stosownych przypadkach Rada Zarządzająca dostosowuje budżet i plan prac Centrum Kompetencji zgodnie z budżetem ogólnym Unii.

Artykuł 27

Przedstawienie sprawozdania finansowego Centrum Kompetencji i udzielenie absolutorium

Przedstawienie wstępnego i ostatecznego sprawozdania finansowego Centrum Kompetencji oraz udzielenie absolutorium przebiegają zgodnie z zasadami i terminarzem wynikającymi z rozporządzenia finansowego oraz jego przepisów finansowych przyjętych zgodnie z art. 29.

Artykuł 28

Sprawozdawczość operacyjna i finansowa

1. Dyrektor wykonawczy co roku przekazuje Radzie Zarządzającej sprawozdanie z wykonania swoich obowiązków zgodnie z przepisami finansowymi Centrum Kompetencji.

2. W ciągu dwóch miesięcy od zakończenia każdego roku budżetowego dyrektor wykonawczy przedkłada Radzie Zarządzającej do zatwierdzenia roczne sprawozdanie z działalności dotyczące postępów poczynionych przez Centrum Kompetencji w poprzednim roku kalendarzowym, w szczególności w odniesieniu do planu prac na dany rok. Sprawozdanie to zawiera m.in. informacje dotyczące następujących kwestii:

a) przeprowadzonych działań operacyjnych i powiązanych wydatków;

b) proponowanych działań, w tym w podziale na rodzaje uczestników, w tym MŚP, i na państwa członkowskie;

c) działań wybranych do finansowania, w tym w podziale na rodzaje uczestników, w tym MŚP, i na państwa członkowskie, ze wskazaniem wkładu Centrum Kompetencji na rzecz poszczególnych uczestników i działań;

d) postępów w kierunku realizacji celów określonych w art. 4 i propozycji dalszych działań niezbędnych do zrealizowania tych celów.

3. Po zatwierdzeniu przez Radę Zarządzającą roczne sprawozdanie z działalności jest podawane do wiadomości publicznej.

Artykuł 29

Przepisy finansowe

Centrum Kompetencji przyjmuje swoje szczegółowe przepisy finansowe zgodnie z art. 70 rozporządzenia XXX [nowe rozporządzenie finansowe].

Artykuł 30

Ochrona interesów finansowych

1. W trakcie realizacji działań finansowanych na podstawie niniejszego rozporządzenia Centrum Kompetencji stosuje odpowiednie środki w celu zapewnienia ochrony interesów finansowych Unii przeciw nadużyciom finansowym, korupcji i wszelkim innym nielegalnym działaniom, w drodze ***regularnych i*** skutecznych kontroli oraz, w razie wykrycia nieprawidłowości, w drodze odzyskiwania kwot nienależnie wypłaconych, a także, w stosownych przypadkach, skutecznych, proporcjonalnych i odstraszających sankcji administracyjnych. **[Popr. 166]**

2. Centrum Kompetencji zapewnia pracownikom Komisji i innym upoważnionym przez Komisję osobom, a także Trybunałowi Obrachunkowemu, dostęp do swoich obiektów i pomieszczeń oraz do wszelkich informacji, włącznie z informacjami w formacie elektronicznym, niezbędnych do przeprowadzenia ich audytów.

3. Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) może przeprowadzać dochodzenia, w tym kontrole na miejscu i inspekcje, zgodnie z przepisami i procedurami określonymi w rozporządzeniu Rady (Euratom, WE) nr 2185/96 ([21]) oraz rozporządzeniu Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 ([22]), aby ustalić, czy miały miejsce nadużycia finansowe, korupcja lub jakakolwiek inna nielegalna działalność na szkodę interesów finansowych Unii w związku z finansowaniem umowy o udzielenie dotacji lub zamówienia – bezpośrednio lub pośrednio – zgodnie z niniejszym rozporządzeniem.

4. Nie naruszając przepisów ust. 1, 2 i 3 niniejszego artykułu, w zamówieniach i umowach o udzielenie dotacji wynikających z wykonania niniejszego rozporządzenia zamieszcza się postanowienia wyraźnie upoważniające Komisję, Centrum Kompetencji, Trybunał Obrachunkowy i OLAF do prowadzenia takich audytów i dochodzeń zgodnie z ich odpowiednimi uprawnieniami. W przypadku gdy realizację działania zlecono na zewnątrz lub przekazano do podwykonawstwa w całości lub w części lub gdy realizacja działania wymaga udzielenia zamówienia publicznego lub udzielenia wsparcia finansowego osobie trzeciej, w umowie o udzielenie dotacji określa się zobowiązanie wykonawcy lub beneficjenta do uzyskania od każdej zaangażowanej osoby trzeciej wyraźnej akceptacji tych uprawnień Komisji, Centrum Kompetencji, Trybunału Obrachunkowego i OLAF-u.

ROZDZIAŁ IV

PERSONEL CENTRUM KOMPETENCJI

Artykuł 31

Personel

1. Do pracowników Centrum Kompetencji mają zastosowanie: regulamin pracowniczy urzędników i warunki zatrudnienia innych pracowników Unii Europejskiej określone w rozporządzeniu Rady (EWG, Euratom, EWWiS) nr 259/68 ([23]) („regulamin pracowniczy urzędników" i „warunki zatrudnienia") oraz przepisy przyjęte wspólnie przez instytucje Unii do celów stosowania regulaminu pracowniczego urzędników i warunków zatrudnienia.

2. W odniesieniu do personelu Centrum Kompetencji Rada Zarządzająca korzysta z uprawnień powierzonych organowi powołującemu na podstawie regulaminu pracowniczego oraz z uprawnień powierzonych organowi właściwemu do zawierania umów o pracę na podstawie warunków zatrudnienia („uprawnień organu powołującego").

3. Zgodnie z art. 110 regulaminu pracowniczego Rada Zarządzająca przyjmuje na podstawie art. 2 ust. 1 regulaminu pracowniczego i art. 6 warunków zatrudnienia decyzję przekazującą odpowiednie uprawnienia organu powołującego dyrektorowi wykonawczemu i określającą warunki, na jakich można zawiesić przekazanie tych uprawnień. Dyrektor wykonawczy jest uprawniony do dalszego przekazywania tych uprawnień.

4. Jeżeli wymagają tego szczególne okoliczności, Rada Zarządzająca może w drodze decyzji tymczasowo zawiesić przekazanie uprawnień organu powołującego dyrektorowi wykonawczemu i każde dalsze przekazanie przez niego tych uprawnień. W takich przypadkach Rada Zarządzająca samodzielnie wykonuje uprawnienia organu powołującego lub przekazuje je jednemu ze swoich członków lub też członkowi personelu Centrum Kompetencji innemu niż dyrektor wykonawczy.

([21]) Rozporządzenie Rady (Euratom, WE) nr 2185/96 z dnia 11 listopada 1996 r. w sprawie kontroli na miejscu oraz inspekcji przeprowadzanych przez Komisję w celu ochrony interesów finansowych Wspólnot Europejskich przed nadużyciami finansowymi i innymi nieprawidłowościami (Dz.U. L 292 z 15.11.1996, s. 2).

([22]) Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 z dnia 11 września 2013 r. dotyczące dochodzeń prowadzonych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) oraz uchylające rozporządzenie (WE) nr 1073/1999 Parlamentu Europejskiego i Rady i rozporządzenie Rady (Euratom) nr 1074/1999 (Dz.U. L 248 z 18.9.2013, s. 1).

([23]) Rozporządzenie Rady (EWG, Euratom, EWWiS) nr 259/68 z dnia 29 lutego 1968 r. ustanawiające regulamin pracowniczy urzędników Wspólnot Europejskich i warunki zatrudnienia innych pracowników Wspólnot oraz ustanawiające specjalne środki stosowane tymczasowo wobec urzędników Komisji (Dz.U. L 56 z 4.3.1968, s. 1).

5. Rada Zarządzająca przyjmuje odpowiednie przepisy wykonawcze dotyczące regulaminu pracowniczego i warunków zatrudnienia zgodnie z art. 110 regulaminu pracowniczego.

6. Zasoby kadrowe określa się w planie zatrudnienia Centrum Kompetencji, w którym wskazuje się liczbę stanowisk czasowych w podziale na grupy funkcyjne i grupy zaszeregowania oraz liczbę pracowników kontraktowych w przeliczeniu na ekwiwalenty pełnego czasu pracy, zgodnie z rocznym budżetem Centrum Kompetencji.

7. ~~Personel Centrum Kompetencji składa się z~~ ***Centrum Kompetencji dąży do osiągnięcia równowagi płci wśród swojego personelu. W skład*** personelu ~~zatrudnionego~~ ***wchodzi personel zatrudniony*** na czas określony ~~i personelu kontraktowego~~ ***i personel kontraktowy***. **[Popr. 167]**

8. Centrum Kompetencji ponosi wszystkie koszty związane z pracownikami.

Artykuł 32

Oddelegowani eksperci krajowi i inni pracownicy

1. Centrum Kompetencji może korzystać z pomocy oddelegowanych ekspertów krajowych lub innych pracowników niezatrudnionych przez Centrum Kompetencji.

2. Rada Zarządzająca przyjmuje decyzję określającą zasady oddelegowania ekspertów krajowych do Centrum Kompetencji w porozumieniu z Komisją.

Artykuł 33

Przywileje i immunitety

Do Centrum Kompetencji i jego pracowników zastosowanie ma Protokół nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej załączony do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej.

ROZDZIAŁ V

WSPÓLNE PRZEPISY

Artykuł 34

Przepisy bezpieczeństwa

1. Do uczestnictwa we wszystkich działaniach finansowanych przez Centrum Kompetencji ma zastosowanie art. 12 ust. 7 rozporządzenia (UE) nr XXX [program „Cyfrowa Europa"].

2. Do działań finansowanych w ramach programu „Horyzont Europa" zastosowanie mają następujące szczególne przepisy bezpieczeństwa:

a) do celów określonych w art. 34 ust. 1 [Własność i ochrona] rozporządzenia (UE) nr XXX [„Horyzont Europa"], jeżeli przewidziano to w planie prac, udzielanie licencji niewyłącznych może zostać ograniczone do osób trzecich mających siedzibę lub uznanych za mające siedzibę w państwie członkowskim i znajdujących się pod kontrolą państw członkowskich lub obywateli państw członkowskich;

b) do celów określonych w art. 36 ust. 4 lit. b) [Przeniesienie własności i udzielanie licencji] rozporządzenia (UE) nr XXX [„Horyzont Europa"] przeniesienie własności lub udzielenie licencji na rzecz podmiotu prawnego z siedzibą w państwie stowarzyszonym lub w Unii, ale kontrolowanego z państw trzecich, również stanowi podstawę do zgłoszenia sprzeciwu wobec przeniesienia prawa własności rezultatów lub wobec udzielenia wyłącznej licencji w odniesieniu do rezultatów;

c) do celów określonych w art. 37 ust. 3 lit. a) [Prawa dostępu] rozporządzenia (UE) nr XXX [„Horyzont Europa"], jeżeli przewidziano to w planie prac, udzielanie dostępu do rezultatów i posiadanej istniejącej wiedzy może zostać ograniczone jedynie do podmiotów prawnych mających siedzibę lub uznanych za mające siedzibę w państwie członkowskim i znajdujących się pod kontrolą państw członkowskich lub obywateli państw członkowskich;

ca) Art. 22 [Własność wyników], art. 23 [Własność wyników] i art. 30 [Stosowanie zasad dotyczących informacji niejawnych] rozporządzenia (UE) 2019/XXX [Europejski Fundusz Obronny] stosuje się do udziału Centrum Kompetencji we wszystkich działaniach związanych z obronnością, o ile zostało to przewidziane w planie prac, a przyznawanie licencji niewyłącznych ogranicza się do osób trzecich z siedzibą w państwach członkowskich lub uznanych za prowadzących działalność w państwach członkowskich i kontrolowanych przez państwa członkowskie lub obywateli państw członkowskich. **[Popr. 168]**

Artykuł 35

Przejrzystość

1. Centrum Kompetencji wykonuje swoje działania przy zachowaniu ~~wysokiego~~ ***najwyższego*** stopnia przejrzystości. **[Popr. 169]**

2. Centrum Kompetencji ~~zapewnia~~ ***dopilnowuje***, aby ~~społeczeństwo~~ ***opinia publiczna*** i wszelkie inne zainteresowane strony otrzymywały ***w terminie wyczerpujące,*** odpowiednie, obiektywne, wiarygodne i łatwo dostępne informacje, w szczególności dotyczące wyników ~~jej pracy~~ ***pracy Centrum Kompetencji, sieci, Rady Konsultacyjnej ds. Przemysłowych i Naukowych oraz środowiska***. Centrum Kompetencji podaje również do wiadomości publicznej deklaracje interesów złożone zgodnie z art. ~~41~~ **42**. **[Popr. 170]**

3. Rada Zarządzająca, działając na wniosek dyrektora wykonawczego, może upoważnić zainteresowane strony do obserwowania przebiegu niektórych działań Centrum Kompetencji.

4. Centrum Kompetencji określa w regulaminie wewnętrznym praktyczne ustalenia w zakresie wdrażania zasad przejrzystości, o których mowa w ust. 1 i 2. W przypadku działań finansowanych w ramach programu „Horyzont Europa" w tym względzie zostaną należycie wzięte pod uwagę przepisy zawarte w załączniku III do rozporządzenia w sprawie programu „Horyzont Europa".

Artykuł 36

Przepisy bezpieczeństwa w zakresie ochrony informacji niejawnych i szczególnie chronionych informacji jawnych

1. Nie naruszając przepisów art. 35, Centrum Kompetencji nie ujawnia osobom trzecim przetwarzanych lub otrzymywanych przez siebie informacji, w odniesieniu do których w całości lub w części zgłoszono uzasadniony wniosek o zachowanie poufności.

2. Członkowie Rady Zarządzającej, dyrektor wykonawczy, członkowie Rady Konsultacyjnej ds. Przemysłowych i Naukowych, eksperci zewnętrzni uczestniczący w pracach grup roboczych ad hoc oraz członkowie personelu Centrum podlegają wymogom dotyczącym poufności określonym w art. 339 Traktatu o funkcjonowaniu Unii Europejskiej, nawet po zakończeniu pełnienia swoich obowiązków.

3. Rada Zarządzająca Centrum Kompetencji przyjmuje po zatwierdzeniu przez Komisję przepisy bezpieczeństwa Centrum Kompetencji oparte na zasadach i przepisach zawartych w przepisach bezpieczeństwa Komisji dotyczących ochrony informacji niejawnych UE (EUCI) oraz szczególnie chronionych informacji jawnych, w tym między innymi przepisy dotyczące przetwarzania i przechowywania takich informacji określone w decyzjach Komisji (UE, Euratom) 2015/443 ([24]) i 2015/444 ([25]).

4. Centrum Kompetencji może podjąć wszelkie niezbędne środki w celu ułatwienia mającej istotne znaczenie dla jego zadań wymiany informacji z Komisją i państwami członkowskimi oraz, w stosownych przypadkach, z właściwymi agencjami i organami Unii. Wszelkie ustalenia administracyjne poczynione w tym celu w sprawie udostępniania EUCI lub, jeżeli nie ma takiego porozumienia, jakiekolwiek nadzwyczajne doraźne udostępnienie EUCI muszą zostać uprzednio zatwierdzone przez Komisję.

Artykuł 37

Dostęp do dokumentów

1. Do dokumentów będących w posiadaniu Centrum Kompetencji ma zastosowanie rozporządzenie (WE) nr 1049/2001.

2. Rada Zarządzająca przyjmuje ustalenia dotyczące wykonania rozporządzenia (WE) nr 1049/2001 w ciągu sześciu miesięcy od ustanowienia Centrum Kompetencji.

([24]) Decyzja Komisji (UE, Euratom) 2015/443 z dnia 13 marca 2015 r. w sprawie bezpieczeństwa w Komisji (Dz.U. L 72 z 17.3.2015, s. 41).

([25]) Decyzja Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 72 z 17.3.2015, s. 53).

3. Decyzje podjęte przez Centrum Kompetencji na podstawie art. 8 rozporządzenia (WE) nr 1049/2001 mogą być przedmiotem skarg składanych do Europejskiego Rzecznika Praw Obywatelskich na podstawie art. 228 Traktatu o funkcjonowaniu Unii Europejskiej lub skarg wnoszonych do Trybunału Sprawiedliwości Unii Europejskiej na podstawie art. 263 Traktatu o funkcjonowaniu Unii Europejskiej.

Artykuł 38

Monitorowanie, ocena i przegląd

1. Centrum Kompetencji zapewnia, aby jego działania, w tym działania zarządzane za pośrednictwem krajowych ośrodków koordynacji i sieci, podlegały stałemu i systematycznemu monitorowaniu i okresowej ocenie. Centrum Kompetencji zapewnia, aby dane dotyczące monitorowania wdrażania i rezultatów programów gromadzono efektywnie, skutecznie i terminowo, a na odbiorców środków unijnych i państwa członkowskie nakłada się proporcjonalne wymogi sprawozdawcze. Wyniki oceny podaje się do publicznej wiadomości.

2. Komisja przeprowadza śródokresową ocenę Centrum Kompetencji po uzyskaniu wystarczających informacji na temat wdrażania niniejszego rozporządzenia, jednak nie później niż w ciągu trzech i pół roku od rozpoczęcia wdrażania niniejszego rozporządzenia. Komisja przygotowuje sprawozdanie z tej oceny i przedkłada to sprawozdanie Parlamentowi Europejskiemu i Radzie do dnia 31 grudnia 2024 r. Centrum Kompetencji i państwa członkowskie dostarczają Komisji informacje niezbędne do przygotowania przedmiotowego sprawozdania.

3. Ocena, o której mowa w ust. 2, obejmuje ocenę rezultatów osiągniętych przez Centrum Kompetencji z uwzględnieniem jego celów, mandatu i zadań***, skuteczności i wydajności***. Jeżeli Komisja uzna, że kontynuacja prac Centrum Kompetencji jest uzasadniona pod względem jego założonych celów, mandatu i zadań, może zaproponować przedłużenie mandatu Centrum Kompetencji określonego w art. 46. **[Popr. 171]**

4. Na podstawie wniosków z oceny śródokresowej, o której mowa w ust. 2, Komisja może postąpić zgodnie z [art. 22 ust. 5] lub podjąć dowolne inne właściwe działania.

5. Monitorowanie, ocena, stopniowe wycofywanie i odnawianie wkładu finansowego z programu „Horyzont Europa" przebiega zgodnie z przepisami zawartymi w art. 8, 45 i 47 oraz w załączniku III do rozporządzenia w sprawie programu „Horyzont Europa" oraz z uzgodnionym trybem realizacji.

6. Monitorowanie i ocena wkładu z programu „Cyfrowa Europa" oraz sprawozdawczość w tym zakresie podlegają przepisom zawartym w art. 24 i 25 programu „Cyfrowa Europa".

7. W przypadku likwidacji Centrum Kompetencji Komisja przeprowadza ocenę końcową Centrum Kompetencji w ciągu sześciu miesięcy od likwidacji Centrum Kompetencji, ale nie później niż po upływie dwóch lat od uruchomienia procedury likwidacji, o której mowa w art. 46 niniejszego rozporządzenia. Wnioski z tej oceny końcowej przedstawia się Parlamentowi Europejskiemu i Radzie.

Artykuł 38a

Osobowość prawna Centrum Kompetencji

1. Centrum Kompetencji posiada osobowość prawną.

2. We wszystkich państwach członkowskich Centrum Kompetencji ma zdolność prawną o najszerszym zakresie przyznawanym osobom prawnym zgodnie z ustawodawstwem danego państwa członkowskiego. Może ono zwłaszcza nabywać i zbywać nieruchomości i ruchomości oraz być stroną w postępowaniach sądowych. **[Popr. 172]**

Artykuł 39

Odpowiedzialność Centrum Kompetencji

1. Odpowiedzialność umowną Centrum Kompetencji reguluje prawo właściwe dla danej umowy, decyzji lub danego zamówienia.

2. W zakresie odpowiedzialności pozaumownej Centrum Kompetencji naprawia szkody wyrządzone przez swoich pracowników podczas wykonywania przez nich obowiązków służbowych, zgodnie z ogólnymi zasadami wspólnymi dla systemów prawnych państw członkowskich.

3. Wszelkie wypłaty dokonywane przez Centrum Kompetencji z tytułu odpowiedzialności, o której mowa w ust. 1 i 2, a także poniesione w związku z tym koszty i wydatki, uznaje się za wydatki Centrum Kompetencji i pokrywa się z jego środków.

4. Centrum Kompetencji ponosi wyłączną odpowiedzialność za swoje zobowiązania.

Artykuł 40

Właściwość Trybunału Sprawiedliwości Unii Europejskiej i prawo właściwe

1. Trybunał Sprawiedliwości Unii Europejskiej jest właściwy:

1) na podstawie wszelkich klauzul arbitrażowych zamieszczonych w umowach lub kontraktach zawieranych przez Centrum Kompetencji lub decyzjach przez nie podejmowanych;

2) w sporach dotyczących odszkodowań za szkody wyrządzone przez pracowników Centrum Kompetencji podczas wykonywania przez nich obowiązków służbowych;

3) w sporach między Centrum Kompetencji a członkami jego personelu w granicach i przy zachowaniu warunków określonych w regulaminie pracowniczym.

2. W odniesieniu do wszelkich kwestii nieobjętych przepisami niniejszego rozporządzenia lub innymi aktami prawnymi Unii zastosowanie ma prawo państwa członkowskiego, w którym znajduje się siedziba Centrum Kompetencji.

Artykuł 41

Odpowiedzialność członków i ubezpieczenie

1. Odpowiedzialność finansowa członków za długi Centrum Kompetencji jest ograniczona do kwoty już wniesionych przez nich wkładów na poczet kosztów administracyjnych.

2. Centrum Kompetencji zawiera i podtrzymuje odpowiednie umowy ubezpieczeniowe.

Artykuł 42

Konflikty interesów

Rada Zarządzająca Centrum Kompetencji przyjmuje zasady, których celem jest zapobieganie konfliktom interesów ***oraz ich identyfikacja*** i ~~zarządzanie nimi~~ ***eliminowanie*** w odniesieniu do członków, organów i ~~personelu Centrum Kompetencji. Zasady te zawierają przepisy służące unikaniu konfliktów interesów przez przedstawicieli członków pełniących obowiązki w Radzie~~ ***personelu, w tym dyrektora wykonawczego, Rady*** Zarządzającej ~~oraz w Radzie~~ ***, a także Rady*** Konsultacyjnej ds. Przemysłowych i Naukowych ~~zgodnie z rozporządzeniem XXX [nowe rozporządzenie finansowe]~~ ***oraz środowiska***. **[Popr. 173]**

Państwa członkowskie zapewniają zapobieganie konfliktom interesów oraz ich identyfikację i eliminowanie w odniesieniu do krajowych ośrodków koordynacji. **[Popr. 174]**

Zasady, o których mowa w akapicie pierwszym, są zgodne z rozporządzeniem (UE, Euratom) 2018/1046. **[Popr. 175]**

Artykuł 43

Ochrona danych osobowych

1. Przetwarzanie danych osobowych przez Centrum Kompetencji podlega przepisom rozporządzenia Parlamentu Europejskiego i Rady (UE) nr XXX/2018.

2. Rada Zarządzająca przyjmuje środki wykonawcze, o których mowa w art. xx ust. 3 rozporządzenia (UE) nr XXX/2018. Rada Zarządzająca może przyjąć dodatkowe środki niezbędne do stosowania przez Centrum Kompetencji rozporządzenia (UE) nr XXX/2018.

Środa, 17 kwietnia 2019 r.

Artykuł 44

Siedziba i wsparcie ze strony przyjmującego państwa członkowskiego **[Popr. 176]**

Siedzibę Centrum Kompetencji określa się w drodze procedury podlegającej demokratycznej kontroli, na podstawie przejrzystych kryteriów i zgodnie z prawem Unii. **[Popr. 177]**

Przyjmujące państwo członkowskie zapewnia możliwie najlepsze warunki dla zagwarantowania właściwego funkcjonowania Centrum Kompetencji, w tym jedną lokalizację, a także dodatkowe warunki takie jak dostępność odpowiedniej infrastruktury szkolnej dla dzieci członków personelu, odpowiedni dostęp do rynku pracy, zabezpieczenie społeczne i opiekę zdrowotną zarówno dla dzieci, jak i dla partnerów. **[Popr. 178]**

Centrum Kompetencji i ***przyjmujące*** państwo członkowskie ~~[Belgia]~~, w którym znajduje się jego siedziba, ~~mogą dokonać~~ ***dokonują*** ustaleń administracyjnych w sprawie przywilejów i immunitetów oraz innego wsparcia udzielanego Centrum Kompetencji przez to państwo członkowskie. **[Popr. 179]**

ROZDZIAŁ VII

PRZEPISY KOŃCOWE

Artykuł 45

Początek funkcjonowania

1. Komisja odpowiada za ustanowienie Centrum Kompetencji i jego początkowe funkcjonowanie do momentu osiągnięcia przez nie zdolności operacyjnej do wykonywania własnego budżetu. Zgodnie z prawem Unii Komisja przeprowadza wszystkie niezbędne działania przy pomocy właściwych organów Centrum Kompetencji.

2. Do celów określonych w ust. 1, do czasu objęcia obowiązków przez dyrektora wykonawczego w wyniku mianowania go przez Radę Zarządzającą zgodnie z art. 16, Komisja może wyznaczyć tymczasowego dyrektora wykonawczego i wykonywać obowiązki powierzone dyrektorowi wykonawczemu, któremu może pomagać ograniczona liczba urzędników Komisji. Komisja może tymczasowo wyznaczyć ograniczoną liczbę swoich urzędników.

3. Tymczasowy dyrektor wykonawczy może zatwierdzać wszelkie płatności w ramach środków przydzielonych w rocznym budżecie Centrum Kompetencji po zatwierdzeniu przez Radę Zarządzającą oraz może podejmować decyzje, udzielać zamówień i zawierać umowy, w tym umowy o pracę po przyjęciu planu zatrudnienia Centrum Kompetencji.

4. Tymczasowy dyrektor wykonawczy — w porozumieniu z dyrektorem wykonawczym Centrum Kompetencji i za zgodą Rady Zarządzającej — określa datę uzyskania przez Centrum Kompetencji zdolności do wykonywania własnego budżetu. Począwszy od tej daty, Komisja przestaje podejmować zobowiązania i dokonywać płatności z tytułu działań Centrum Kompetencji.

Artykuł 45a

Wykonywanie przekazanych uprawnień

1. ***Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych podlega warunkom określonym w niniejszym artykule.***

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 6 ust. 5a i art. 8 ust. 4b, powierza się Komisji na czas nieokreślony od … [data wejścia w życie rozporządzenia].

3. Przekazanie uprawnień, o którym mowa w art. 6 ust. 5a i art. 8 ust. 4b, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna następnego dnia po jej opublikowaniu w Dzienniku Urzędowym Unii Europejskiej lub w późniejszym terminie określonym w tej decyzji. Nie wpływa ona na ważność już obowiązujących aktów delegowanych.

4. Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.

5. Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6. Akt delegowany przyjęty na podstawie art. 6 ust. 5a i art. 8 ust. 4b wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o dwa miesiące z inicjatywy Parlamentu Europejskiego lub Rady. **[Popr. 180]**

Artykuł 46

Czas trwania

1. Centrum Kompetencji ustanawia się na okres od dnia 1 stycznia 2021 r. do dnia 31 grudnia 2029 r.

2. Pod koniec tego okresu, o ile w drodze przeglądu niniejszego rozporządzenia nie postanowiono inaczej, wszczyna się procedurę likwidacji. Procedurę likwidacji wszczyna się automatycznie, jeśli Unia lub wszystkie uczestniczące państwa członkowskie wystąpią z Centrum Kompetencji.

3. Do celów przeprowadzenia postępowania mającego na celu likwidację Centrum Kompetencji, Rada Zarządzająca wyznacza co najmniej jednego likwidatora, który działa zgodnie z jej decyzjami.

4. W ramach likwidacji Centrum Kompetencji jego aktywa wykorzystuje się do pokrycia jego zobowiązań oraz wydatków związanych z jego likwidacją. Wszelką nadwyżkę rozdziela się między Unię oraz uczestniczące państwa członkowskie proporcjonalnie do ich wkładu finansowego na rzecz Centrum Kompetencji. Każda taka nadwyżka przydzielona Unii jest zwracana do budżetu Unii.

Artykuł 47

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

Przewodniczący

W imieniu Rady

Przewodniczący