I

(Akty ustawodawcze)

ROZPORZĄDZENIA

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2021/887

z dnia 20 maja 2021 r.

ustanawiające Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa 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,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

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

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([2]),

a także mając na uwadze, co następuje:

(1) Większość ludności Unii Europejskiej ma dostęp do internetu. Życie codzienne ludzi i gospodarki stają się coraz bardziej zależne od technologii cyfrowych. Obywatele i przedsiębiorstwa są w coraz większym stopniu narażeni są na poważne incydenty w zakresie cyberbezpieczeństwa i wiele przedsiębiorstw w Unii doświadcza co najmniej jednego incydentu w zakresie cyberbezpieczeństwa każdego roku. Wskazuje to na potrzebę zbudowania odporności, zwiększenia możliwości technologicznych i przemysłowych oraz stosowania wysokich standardów cyberbezpieczeństwa i kompleksowych rozwiązań w tym zakresie, obejmujących ludzi, produkty, procesy i technologie w Unii, a także na konieczność osiągnięcia przez Unię wiodącej pozycji w dziedzinie cyberbezpieczeństwa i uzyskania autonomii cyfrowej. Cyberbezpieczeństwo można również poprawić poprzez podnoszenie świadomości na temat cyberzagrożeń i poprzez rozwijanie w całej Unii kompetencji, zdolności i możliwości, przy pełnym uwzględnieniu skutków i wątpliwości społecznych i etycznych.

(2) Unia stale intensyfikuje swoje działania w celu rozwiązania rosnących wyzwań w zakresie cyberbezpieczeństwa, realizując strategię cyberbezpieczeństwa przedstawioną przez Komisję i Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (zwanego dalej „Wysokim Przedstawicielem") w ich wspólnym komunikacie do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 7 lutego 2013 r. pt. „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń" (zwana dalej „strategią cyberbezpieczeństwa z 2013 r."). Strategia ta miała na celu promowanie niezawodnego, bezpiecznego i otwartego ekosystemu cyfrowego. W 2016 r. Unia przyjęła pierwsze środki w dziedzinie cyberbezpieczeństwa poprzez dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 ([3]) w sprawie bezpieczeństwa sieci i systemów informatycznych.

([1]) Dz.U. C 159 z 10.5.2019, s. 63.

([2]) Stanowisko Parlamentu Europejskiego z dnia 17 kwietnia 2019 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz stanowisko Rady w pierwszym czytaniu z dnia 20 kwietnia 2021 r. (dotychczas nieopublikowane w Dzienniku Urzędowym). Stanowisko Parlamentu Europejskiego z dnia 19 maja 2021 r. (dotychczas nieopublikowane w Dzienniku Urzędowym).

([3]) 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).

(3) We wrześniu 2017 r. Komisja i Wysoki Przedstawiciel przedstawili wspólny komunikat do Parlamentu Europejskiego i Rady pt. „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej", aby jeszcze bardziej wzmocnić odporność, prewencję i reakcję Unii w przypadku 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 obywatelom, konsumentom i przedsiębiorstwom zaufania, pewności i ochrony online oraz umożliwienia istnienia wolnego, bezpieczniejszego i podlegającego przepisom prawa internetu, a także zadeklarowali zamiar powszechniejszego korzystania z rozwiązań w zakresie otwartego oprogramowania i otwartych standardów przy (prze)budowie systemów i rozwiązań w zakresie technologii informacyjno-komunikacyjnych (ICT), w szczególności aby uniknąć uzależnienia od jednego dostawcy, w tym rozwiązań i standardów opracowanych lub promowanych w ramach unijnych programów na rzecz interoperacyjności i standaryzacji, takich jak ISA[2].

(5) Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (zwane dalej „Centrum Kompetencji") ustanowione w niniejszym rozporządzeniu powinno przyczyniać się do zwiększenia bezpieczeństwa sieci i systemów informatycznych, w tym internetu i innych rodzajów infrastruktury krytycznych dla funkcjonowania społeczeństwa, takich jak systemy w dziedzinach transportu, zdrowia, energii, infrastruktury cyfrowej, wody, rynków finansowych i bankowości.

(6) Znaczne zakłócenie funkcjonowania sieci i systemów informatycznych może wpływać na poszczególne państwa członkowskie i na Unię jako całość. Wysoki poziom bezpieczeństwa sieci i systemów informatycznych w całej Unii ma zatem zasadnicze znaczenie zarówno dla społeczeństwa, jak i gospodarki. Obecnie Unia jest uzależniona od dostawców cyberbezpieczeństwa spoza Europy. W strategicznym interesie Unii leży jednak zapewnienie, aby utrzymała i rozwijała ona podstawowe zdolności badawcze i technologiczne w dziedzinie cyberbezpieczeństwa w celu zabezpieczenia sieci i systemów informatycznych wykorzystywanych przez obywateli i przedsiębiorstwa, a w szczególności w celu ochrony sieci i systemów informatycznych o znaczeniu krytycznym oraz świadczenia kluczowych usług w zakresie cyberbezpieczeństwa.

(7) Chociaż Unia dysponuje rozległą wiedzą fachową i doświadczeniem w zakresie badań naukowych, technologii i rozwoju przemysłu w dziedzinie cyberbezpieczeństwa, to wysiłki środowisk przemysłowych i badawczych są rozproszone, brak im też koordynacji i wspólnej misji, co stanowi przeszkodę dla konkurencyjności oraz skutecznej ochrony sieci i systemów w tej dziedzinie. Należy skupić takie wysiłki i wiedzę fachową, połączyć je w sieć i wykorzystać w wydajny sposób, aby wzmocnić i uzupełnić istniejące zdolności i umiejętności badawcze, technologiczne i przemysłowe na poziomie unijnym i krajowym. Choć sektor ICT stoi w obliczu ważnych wyzwań, takich jak zaspokojenie popytu na wykwalifikowanych pracowników, może skorzystać on na tym, że będzie reprezentował różnorodność całego społeczeństwa oraz charakteryzował się zrównoważoną reprezentacją płci, różnorodnością etniczną i niedyskryminacją osób z niepełnosprawnościami, jak również na tym, że będzie ułatwiał przyszłym ekspertom w dziedzinie cyberbezpieczeństwa dostęp do wiedzy i szkoleń, w tym do kształcenia takich ekspertów w warunkach pozaformalnych, na przykład w ramach projektów dotyczących wolnego i otwartego oprogramowania, projektów z dziedziny technologii obywatelskiej, przedsiębiorstw typu start-up i mikroprzedsiębiorstw.

(8) Małe i średnie przedsiębiorstwa (MŚP) są kluczowymi interesariuszami w unijnym sektorze cyberbezpieczeństwa i ze względu na swoją elastyczność mogą zapewniać najnowocześniejsze rozwiązania. Jednakże MŚP, które nie specjalizują się w cyberbezpieczeństwie, są również bardziej podatne na incydenty w zakresie cyberbezpieczeństwa ze względu na duże wymagania w zakresie inwestycji i zasobów wiedzy niezbędnych do wprowadzenia skutecznych rozwiązań w dziedzinie cyberbezpieczeństwa. W związku z tym konieczne jest, aby Centrum Kompetencji i sieć krajowych ośrodków koordynacji (zwana dalej „Siecią") zapewniły MŚP wsparcie, ułatwiając im dostęp do wiedzy i personalizując dostęp do wyników prac badawczo-rozwojowych, tak aby umożliwić MŚP wystarczające zabezpieczenie się, a tym spośród nich, które działają w dziedzinie cyberbezpieczeństwa, umożliwić konkurencyjność i wnoszenie wkładu w zdobywanie przez Unię wiodącej pozycji w dziedzinie cyberbezpieczeństwa.

(9) Wiedza fachowa istnieje również poza kontekstem przemysłowym i badawczym. Projekty niekomercyjne i przedkomercyjne, nazywane projektami z dziedziny „technologii obywatelskiej", wykorzystują otwarte standardy, otwarte dane oraz wolne i otwarte oprogramowanie w interesie społeczeństwa i dobra publicznego.

(10) Cyberbezpieczeństwo to niejednorodna dziedzina. Do interesariuszy zalicza się podmioty publiczne, państwa członkowskie i Unię, a także podmioty z sektora przemysłu, podmioty społeczeństwa obywatelskiego, takie jak związki zawodowe, stowarzyszenia konsumenckie, środowisko wolnego i otwartego oprogramowania oraz środowisko akademickie i badawcze oraz inne podmioty.

(11) W swoich konkluzjach przyjętych w listopadzie 2017 r. Rada wezwała Komisję do szybkiego opracowania oceny skutków na temat możliwych wariantów stworzenia sieci centrów kompetencji w dziedzinie cyberbezpieczeństwa i Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie Cyberbezpieczeństwa oraz do przedstawienia do połowy 2018 r. wniosku dotyczącego odpowiedniego instrumentu prawnego w celu stworzenia takiej sieci i takiego centrum.

(12) Unia nadal nie dysponuje wystarczającymi technologicznymi i przemysłowymi zdolnościami i możliwościami, by w sposób autonomiczny zabezpieczyć swoją gospodarkę i infrastrukturę krytyczną oraz stać się światowym liderem w dziedzinie cyberbezpieczeństwa. Poziom strategicznej i trwałej koordynacji oraz współpracy między sektorami przemysłu, środowiskami badawczymi w dziedzinie cyberbezpieczeństwa i rządami jest niewystarczający. W Unii występuje problem niewystarczających inwestycji i ograniczonego dostępu do wiedzy, umiejętności i infrastruktury w tej dziedzinie, zaś niewiele unijnych wyników badań naukowych i innowacji w dziedzinie cyberbezpieczeństwa przekłada się na rozwiązania rynkowe szeroko wykorzystywane w gospodarce.

(13) Ustanowienie Centrum Kompetencji i Sieci, mających mandat do realizacji środków wspierających technologie przemysłowe oraz środków w dziedzinie badań naukowych i innowacji, stanowi najlepszy sposób osiągnięcia celów niniejszego rozporządzenia, przy jednoczesnym zapewnieniu maksymalnych skutków gospodarczych, społecznych i środowiskowych oraz zabezpieczeniu interesów Unii.

(14) Centrum Kompetencji powinno być głównym unijnym instrumentem służącym skupianiu inwestycji w badania naukowe, technologię i rozwój przemysłu w dziedzinie cyberbezpieczeństwa oraz wdrażaniu odpowiednich projektów i inicjatyw razem z Siecią. Centrum Kompetencji powinno zarządzać wsparciem finansowym na działania związane z cyberbezpieczeństwem z Programu ramowego w zakresie badań naukowych i innowacji „Horyzont Europa" ustanowionego rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/695 ([4]) (zwanego dalej „programem Horyzont Europa") oraz programu „Cyfrowa Europa" ustanowionego rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/694 ([5]) i w stosownych przypadkach powinno być otwarte na inne programy. Podejście to powinno przyczynić się do tworzenia synergii i koordynowania wsparcia finansowego związanego z inicjatywami Unii w dziedzinie badań naukowych i rozwoju, innowacji i rozwoju technologiczno-przemysłowego w dziedzinie cyberbezpieczeństwa oraz unikać zbędnego powielania działań.

(15) Istotne zapewnienie poszanowania praw podstawowych i zasad etycznego postępowanie w ramach projektów badawczych w dziedzinie cyberbezpieczeństwa wspieranych przez Centrum Kompetencji.

(16) Centrum Kompetencji nie powinno wykonywać zadań operacyjnych w dziedzinie cyberbezpieczeństwa, takich jak zadania należące do zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), w tym zadań w zakresie monitorowania cyberincydentów i reagowania na nie. Centrum Kompetencji powinno być jednak w stanie ułatwiać rozwój infrastruktur ICT służących sektorom przemysłu, w szczególności MŚP, środowiskom badawczym, społeczeństwu obywatelskiemu i sektorowi publicznemu, w zgodzie z misją i celami określonymi w niniejszym rozporządzeniu. Podczas gdy zespoły CSIRT i inni interesariusze dążą do propagowania zgłaszania i ujawniania podatności, Centrum Kompetencji i członkowie społeczności kompetentnej w zakresie cyberbezpieczeństwa (zwanej dalej „Społecznością") powinni mieć możliwość wspierania tych interesariuszy na ich wniosek w granicach swoich zadań oraz unikając powielania działań z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (zwaną dalej „agencją ENISA") ustanowioną rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 ([6]).

(17) W celu zarządzania Społecznością i jej reprezentowania w ramach Centrum Kompetencji, Centrum Kompetencji, Społeczność i Sieć mają korzystać z doświadczenia oraz szerokiej reprezentacji odpowiednich interesariuszy powstałej w wyniku umownego partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa między Komisją a Europejską Organizacją ds. Cyberbezpieczeństwa (ECSO) na okres trwania programu Horyzont 2020 - programu ramowego w zakresie badań naukowych i innowacji (2014–2020) ustanowionego rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1291/2013 ([7]) oraz z wniosków wyciągniętych z czterech projektów pilotażowych zainicjowanych na początku 2019 r. w ramach programu „Horyzont 2020", mianowicie CONCORDIA, ECHO, SPARTA i CyberSec4Europe, a także z projektu pilotażowego i działania przygotowawczego w ramach audytów wolnego i otwartego oprogramowania (EU FOSSA).

(18) Z uwagi na rozmiar wyzwania związanego z cyberbezpieczeństwem oraz inwestycje w zdolności i możliwości w zakresie cyberbezpieczeństwa dokonane w innych częściach świata należy zachęcać Unię i państwa członkowskie do zwiększania wsparcia finansowego na badania naukowe, rozwój i działania wdrożeniowe w tej dziedzinie. Aby osiągnąć korzyści skali i porównywalny poziom ochrony w całej Unii, państwa członkowskie powinny skupić swoje wysiłki w wymiarze unijnym poprzez aktywne przyczynianie się do działalności Centrum Kompetencji i Sieci.

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/695 z dnia 28 kwietnia 2021 r. ustanawiające Program ramowy w zakresie badań naukowych i innowacji „Horyzont Europa" oraz zasady uczestnictwa i upowszechniania obowiązujące w tym programie oraz uchylające rozporządzenia (UE) nr 1290/2013 i (UE) nr 1291/2013 (Dz.U. L 170 z 12.5.2021, s. 1).

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa" oraz uchylające decyzję (UE) 2015/2240 (Dz.U. L 166 z 11.5.2021, s. 1).

([6]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz.U. L 151 z 7.6.2019, s. 15).

([7]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1291/2013 z dnia 11 grudnia 2013 r. ustanawiające „Horyzont 2020" – program ramowy w zakresie badań naukowych i innowacji (2014–2020) oraz uchylające decyzję nr 1982/2006/WE (Dz.U. L 347 z 20.12.2013, s. 104).

(19) W celu wspierania unijnej konkurencyjności i wysokich norm cyberbezpieczeństwa na arenie międzynarodowej Centrum Kompetencji i Społeczność powinny dążyć do wymiany ze społecznością międzynarodową informacji na temat wydarzeń w dziedzinie cyberbezpieczeństwa, w tym w dziedzinie produktów i procesów, standardów i norm technicznych, tam gdzie ma to związek z misją, celami i zadaniami Centrum Kompetencji. Na potrzeby niniejszego rozporządzenia stosowne normy techniczne mogą obejmować tworzenie oprogramowania wzorcowego, w tym oprogramowania opublikowanego w ramach otwartych licencji standardowych.

(20) Siedziba Centrum Kompetencji znajduje się w Bukareszcie.

(21) Przygotowując swój roczny program prac (zwany dalej „rocznym programem prac"), Centrum Kompetencji powinno poinformować Komisję o swoich potrzebach dotyczących współfinansowania, w oparciu o planowane przez państwa członkowskie wkłady na współfinansowanie wspólnych działań, tak aby Komisja była w stanie uwzględnić wkład Unii w odpowiedniej wysokości podczas przygotowywania projektu budżetu ogólnego Unii na kolejny rok.

(22) W procesie przygotowywania przez Komisję programu prac dla programu „Horyzont Europa" w zakresie kwestii związanych z cyberbezpieczeństwem, w tym w kontekście procesu konsultacji z interesariuszami, a w szczególności przed przyjęciem tego programu prac, Komisja powinna należycie uwzględnić wkład Centrum Kompetencji oraz przekazać ten wkład komitetowi programu „Horyzont Europa".

(23) Aby umożliwić Centrum Kompetencji pełnienie jego roli w dziedzinie cyberbezpieczeństwa i ułatwić zaangażowanie Sieci oraz by zapewnić silną pozycję państw członkowskich w zakresie zarządzania, Centrum Kompetencji należy ustanowić jako organ Unii mający osobowość prawną, do którego ma mieć zastosowanie rozporządzenie delegowane Komisji (UE) 2019/715 ([8]). Centrum Kompetencji powinno pełnić podwójną rolę: podejmować konkretne, ustanowione w niniejszym rozporządzeniu zadania w odniesieniu do przemysłu, technologii i badań naukowych w dziedzinie cyberbezpieczeństwa oraz zarządzać środkami finansowymi na rzecz cyberbezpieczeństwa pochodzącymi z różnych programów, w szczególności z programu „Horyzont Europa" i programu „Cyfrowa Europa", oraz ewentualnie także z innych programów unijnych. Zarządzanie to musi być zgodne z przepisami mającymi zastosowanie do tych programów. Biorąc jednak pod uwagę, że finansowanie funkcjonowania Centrum Kompetencji będzie pochodziło przede wszystkim z programu „Horyzont Europa" i z programu „Cyfrowa Europa", konieczne jest, by na potrzeby wykonania budżetu Centrum Kompetencji było uznawane za partnerstwo, w tym na etapie programowania.

(24) Ze względu na wkład Unii, dostęp do wyników działań Centrum Kompetencji i do wyników projektów ma być otwarty w największym możliwym zakresie i zamknięty tylko w zakresie koniecznym, a w odpowiednich przypadkach możliwe ma być ponowne wykorzystywanie takich wyników.

(25) Centrum Kompetencji powinno ułatwiać i koordynować pracę Sieci. W skład Sieci powinien wchodzić jeden krajowy ośrodek koordynacji z każdego państwa członkowskiego. Krajowe ośrodki koordynacji, które zostały uznane przez Komisję za posiadające niezbędne zdolności w zakresie zarządzania środkami finansowymi w celu realizacji misji i celów określonych w niniejszym rozporządzeniu, powinny otrzymywać bezpośrednie wsparcie finansowe Unii, w tym dotacje przyznawane bez zaproszenia do składania wniosków, w celu realizacji ich działań związanych z niniejszym rozporządzeniem.

(26) Krajowymi ośrodkami koordynacji wyznaczanymi przez państwa członkowskie powinny być podmioty sektora publicznego lub podmioty z większościowym udziałem tego sektora, wypełniające zadania administracji publicznej na mocy prawa krajowego, w tym w drodze przekazania uprawnień. Powinna istnieć możliwość, aby funkcje krajowego ośrodka koordynacji w danym państwie członkowskim wypełniał podmiot pełniący również inne funkcje wymagane prawem Unii, takie jak funkcja krajowego właściwego organu, pojedynczego punktu kontaktowego w rozumieniu dyrektywy (UE) 2016/1148 lub innego rozporządzenia unijnego, albo funkcja centrum innowacji cyfrowych w rozumieniu rozporządzenia (UE) 2021/694. Inne podmioty sektora publicznego lub podmioty wypełniające zadania administracji publicznej w danym państwie członkowskim powinny być w stanie wspierać krajowy ośrodek koordynacji w wykonywaniu jego funkcji.

(27) Krajowe ośrodki koordynacji powinny posiadać niezbędne zdolności administracyjne, powinny dysponować wiedzą fachową w zakresie przemysłu, technologii i badań naukowych w dziedzinie cyberbezpieczeństwa lub mieć dostęp do takiej wiedzy i powinny być zdolne do efektywnych kontaktów z przemysłem, sektorem publicznym i środowiskiem badawczym oraz do koordynowania z nimi swoich działań.

(28) Kształcenie w państwach członkowskich powinno uwzględniać znaczenie posiadania odpowiedniej wiedzy na temat cyberbezpieczeństwa i odpowiednich umiejętności w tym zakresie. W tym celu, z uwzględnieniem roli agencji ENISA i bez uszczerbku dla kompetencji państw członkowskich w dziedzinie edukacji, krajowe ośrodki koordynacji – obok odpowiednich organów publicznych i interesariuszy – powinny przyczyniać się do propagowania i upowszechniania programów kształcenia w dziedzinie cyberbezpieczeństwa.

([8]) Rozporządzenie delegowane Komisji (UE) 2019/715 z dnia 18 grudnia 2018 r. w sprawie ramowego rozporządzenia finansowego dotyczącego organów utworzonych na podstawie TFUE oraz Traktatu Euratom, o których mowa w art. 70 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 (Dz.U. L 122 z 10.5.2019, s. 1).

(29) Krajowe ośrodki koordynacji powinny mieć możliwość otrzymywania od Centrum Kompetencji dotacji w celu zapewniania stronom trzecim wsparcia finansowego w formie dotacji. Koszty bezpośrednie ponoszone przez krajowe ośrodki koordynacji w zakresie udzielania wsparcia finansowego stronom trzecim i zarządzania takim wsparciem kwalifikują się do finansowania w ramach odpowiednich programów.

(30) Centrum Kompetencji, Sieć i Społeczność powinny pomagać w rozwijaniu i upowszechnianiu najnowszych produktów, usług i procesów w dziedzinie cyberbezpieczeństwa. Jednocześnie Centrum Kompetencji i Sieć powinny promować możliwości w dziedzinie cyberbezpieczeństwa, którymi dysponują branże po stronie popytu, szczególnie poprzez wspieranie twórców rozwiązań i operatorów w sektorach takich jak sektor transportu, energii, zdrowia, finansowy, administracji, telekomunikacyjny, wytwórczy i kosmiczny, aby pomóc takim twórcom rozwiązań i operatorom w stawianiu czoła wyzwaniom związanym z cyberbezpieczeństwem, takim jak uwzględnianie bezpieczeństwa na etapie projektowania. Centrum Kompetencji i Sieć powinny również wspierać standaryzację i wdrażanie produktów, usług i procesów w dziedzinie cyberbezpieczeństwa, a jednocześnie promować w stosownych przypadkach wdrażanie europejskich ram certyfikacji cyberbezpieczeństwa określonych w rozporządzeniu (UE) 2019/881.

(31) 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 Społeczność powinny być na tyle elastyczne, aby zapewnić wymaganą zdolność reagowania na takie zjawiska. Powinny one sprzyjać projektom, które pomagają podmiotom w stałym tworzeniu zdolności do zwiększania swojej odporności i odporności Unii.

(32) Centrum Kompetencji powinno być wsparciem dla Społeczności. Centrum Kompetencji powinno realizować części programu „Horyzont Europa" i programu „Cyfrowa Europa" dotyczące cyberbezpieczeństwa zgodnie z wieloletnim programem prac Centrum Kompetencji (zwanym dalej „wieloletnim programem prac"), rocznym programem prac oraz procesem planowania strategicznego w ramach programu „Horyzont Europa" poprzez udzielanie dotacji i innych form finansowania, głównie na podstawie zapewniających konkurencję zaproszeń do składania wniosków. Centrum Kompetencji powinno również ułatwiać przekazywanie wiedzy fachowej w ramach Sieci i Społeczności oraz wspierać wspólne inwestycje Unii, państw członkowskich lub przemysłu. Szczególną wagę powinno przykładać do wspierania MŚP w dziedzinie cyberbezpieczeństwa, a także do działań mających pomagać w przezwyciężeniu luki kompetencyjnej.

(33) Pomoc techniczna w zakresie przygotowania projektów powinna być udzielana w sposób w pełni obiektywny i przejrzysty, tak by zapewnić, iż wszyscy potencjalni beneficjenci otrzymają te same informacje, i ma unikać konfliktów interesów.

(34) Centrum Kompetencji powinno stymulować i wspierać długoterminową strategiczną współpracę i koordynację działań Społeczności, które to współpraca i koordynacja obejmowałyby dużą, otwartą, interdyscyplinarną i zróżnicowaną grupę europejskich interesariuszy zaangażowanych w technologię cyberbezpieczeństwa. Do Społeczności powinny należeć podmioty prowadzące badania naukowe, sektory przemysłu i sektor publiczny. Społeczność powinna wnosić wkład w działania Centrum Kompetencji oraz w wieloletni program prac i roczny program prac, działając w szczególności za pośrednictwem Strategicznej Grupy Doradczej. Społeczność powinna również korzystać z prowadzonych przez Centrum Kompetencji i Sieć działań na rzecz tworzenia wspólnoty, nie powinna być jednak uprzywilejowana w zakresie zaproszeń do składania wniosków lub zaproszeń do składania ofert. Członkami Społeczności powinny być podmioty zbiorowe i organizacje. Jednocześnie, aby odnosić korzyści z całej wiedzy fachowej w zakresie cyberbezpieczeństwa w Unii, Centrum Kompetencji i jego organy powinny mieć również możliwość wykorzystywać wiedzę fachową osób fizycznych występujących w roli ekspertów ad-hoc.

(35) Centrum Kompetencji powinno współpracować i zapewniać synergię z agencją ENISA i powinno otrzymywać od agencji ENISA odpowiedni wkład przy określaniu priorytetów w zakresie finansowania.

(36) Aby odpowiedzieć zarówno na podaż, jak i popyt w dziedzinie cyberbezpieczeństwa, zadanie Centrum Kompetencji dotyczące zapewnienia wiedzy z zakresu cyberbezpieczeństwa i pomocy technicznej na rzecz przemysłu powinno odnosić się zarówno do produktów, procesów i usług ICT, jak i wszystkich innych technologicznych produktów i procesów, do których ma zostać włączone cyberbezpieczeństwo. Na swój wniosek sektor publiczny mógłby również korzystać ze wsparcia ze strony Centrum Kompetencji.

(37) W celu osiągnięcia stabilnego środowiska cyberbezpieczeństwa ważne jest, aby w procesach tworzenia, utrzymywania, eksploatacji i aktualizacji infrastruktur, produktów i usług obowiązywała zasada uwzględniania bezpieczeństwa na etapie projektowania, szczególnie poprzez wspieranie najnowocześniejszych metod bezpiecznego projektowania, odpowiednich testów i audytów bezpieczeństwa, udostępnianie aktualizacji mających na celu niezwłoczne usuwanie znanych podatności lub zagrożeń, oraz, w miarę możliwości, umożliwianie stronom trzecim tworzenia i dostarczania takich aktualizacji po zakończeniu przewidzianego okresu użytkowania produktów. Bezpieczeństwo uwzględniane na etapie projektowania należy zapewniać w całym cyklu życia produktu, usługi lub procesu ICT oraz poprzez takie procesy projektowania, które nieustannie ewoluują, by ograniczać ryzyko szkody w przypadku wykorzystania w złej wierze.

(38) Chociaż Centrum Kompetencji i Sieć powinny mieć na celu wzmocnienie synergii i koordynacji między cyberbezpieczeństwem w sferze cywilnej i w sferze wojskowej, realizowane na podstawie niniejszego rozporządzenia projekty finansowane w ramach programu „Horyzont Europa" powinny być wdrażane zgodnie z rozporządzeniem (UE) 2021/695, w którym przewidziano, że działania w zakresie badań naukowych i innowacji przeprowadzane w ramach programu „Horyzont Europa" mają dotyczyć wyłącznie zastosowań cywilnych.

(39) Niniejsze rozporządzenie ma zastosowanie przede wszystkim do kwestii cywilnych, ale działania państw członkowskich na podstawie niniejszego rozporządzenia mogą odzwierciedlać specyfikę państw członkowskich w przypadkach, gdy polityka cyberbezpieczeństwa prowadzona jest przez organy wykonujące zarówno zadania w sferze cywilnej, jak i wojskowej; należy w tych działaniach dążyć do komplementarności i unikać pokrywania się działań z instrumentami finansowania związanymi z obronnością.

(40) Niniejsze rozporządzenie powinno zapewnić odpowiedzialność i przejrzystość działania Centrum Kompetencji oraz finansowanych przedsięwzięć, zgodnie z rozporządzeniami w sprawie odpowiednich programów.

(41) Realizacja projektów wdrożeniowych, w szczególności projektów wdrożeniowych, które dotyczą infrastruktury i zdolności wdrażanych na poziomie unijnym lub w drodze wspólnych zamówień, może być dzielona na różne etapy wdrażania, takie jak oddzielne przetargi na architekturę sprzętu i oprogramowania, ich produkcję oraz obsługę i konserwację, przy czym przedsiębiorstwa będą mogły uczestniczyć tylko w jednym z etapów; w odpowiednich przypadkach może być wymagane, aby beneficjenci na jednym lub kilku z tych etapów spełniali określone warunki dotyczące własności lub kontroli przez podmioty europejskie.

(42) W działaniach Centrum Kompetencji, w tym w opracowywaniu Programu działań, aktywną rolę powinna odgrywać agencja ENISA z uwagi na jej wiedzę fachową w dziedzinie cyberbezpieczeństwa i jej mandat do pełnienia roli punktu odniesienia w zakresie doradztwa i wiedzy fachowej w dziedzinie cyberbezpieczeństwa na rzecz instytucji, organów i jednostek organizacyjnych Unii oraz na rzecz odpowiednich unijnych interesariuszy, a także z uwagi na zbieranie przekazywanych informacji w ramach jej zadań, przy czym należy unikać powielania wysiłków; tę rolę agencja ENISA może pełnić szczególnie dzięki temu, że pełni funkcję stałego obserwatora w Radzie Zarządzającej Centrum Kompetencji. Przy opracowywaniu Programu działań, rocznego programu prac i wieloletniego programu prac Dyrektor Wykonawczy Centrum Kompetencji i Rada Zarządzająca powinni uwzględnić stosowne doradztwo strategiczne i informacje przekazane przez agencję ENISA zgodnie z regulaminem wewnętrznym Rady Zarządzającej.

(43) W przypadku gdy krajowe ośrodki koordynacji i podmioty należące do Społeczności otrzymują wkład finansowy z budżetu ogólnego Unii, powinny one podać do wiadomości publicznej fakt, że odpowiednie działania podejmowane są w kontekście niniejszego rozporządzenia.

(44) Koszty związane z ustanowieniem Centrum Kompetencji oraz jego działaniami administracyjnymi i koordynacyjnymi powinny być finansowane przez Unię oraz przez państwa członkowskie – proporcjonalnie do dobrowolnych wkładów państw członkowskich we wspólne działania. Aby uniknąć podwójnego finansowania, działania te nie powinny jednocześnie korzystać ze środków pochodzących z innych programów unijnych.

(45) Rada Zarządzająca, która powinna się składać z przedstawicieli państw członkowskich i Komisji, powinna określać ogólny kierunek działalności Centrum Kompetencji oraz zapewniać wykonywanie przez Centrum Kompetencji jego zadań zgodnie z niniejszym rozporządzeniem. Rada Zarządzająca powinna przyjąć Program działań.

(46) Rada Zarządzająca powinna mieć uprawnienia niezbędne do uchwalania budżetu Centrum Kompetencji. Rada Zarządzająca powinna kontrolować wykonanie budżetu, przyjmować stosowne zasady finansowe i ustalać przejrzyste procedury działania w procesie podejmowania decyzji przez Centrum Kompetencji, w tym przyjmowanie rocznego programu prac i wieloletniego programu prac zgodnie z Programem działań. Rada Zarządzająca powinna również przyjąć swój regulamin wewnętrzny, powoływać Dyrektora Wykonawczego oraz podejmować decyzje o przedłużeniu jego kadencji lub jej zakończeniu.

(47) Rada Zarządzająca powinna sprawować nadzór nad działaniami o charakterze strategicznym Centrum Kompetencji i jego działaniami w zakresie wdrożenia oraz powinna zapewniać ich spójność. W swoim sprawozdaniu rocznym Centrum Kompetencji powinno położyć szczególny nacisk na osiągnięte przez siebie cele strategiczne i w razie potrzeby zaproponować działania na rzecz dalszej poprawy realizacji tych celów strategicznych.

(48) Do prawidłowego i skutecznego funkcjonowania Centrum Kompetencji Komisja i państwa członkowskie powinny zapewnić, aby osoby, które mają zostać powołane na członków Rady Zarządzającej, miały odpowiednią zawodową wiedzę fachową i doświadczenie w obszarach funkcyjnych. Komisja i państwa członkowskie powinny również dołożyć starań, aby w celu zapewnienia ciągłości jej pracy ograniczyć rotację swoich przedstawicieli w Radzie Zarządzającej.

(49) W świetle szczególnego statusu Centrum Kompetencji i spoczywającej na nim odpowiedzialności za wdrażanie środków finansowych Unii, w szczególności pochodzących z programu „Horyzont Europa" i programu „Cyfrowa Europa", Komisja powinna dysponować w Radzie Zarządzającej 26 % całkowitej liczby głosów w odniesieniu do decyzji dotyczących zaangażowania środków finansowych Unii w celu maksymalizacji unijnej wartości dodanej tych decyzji, przy jednoczesnym zapewnieniu ich legalności i zgodności z priorytetami Unii.

(50) Sprawne funkcjonowanie Centrum Kompetencji wymaga, aby Dyrektor Wykonawczy był powoływany w przejrzysty sposób na podstawie swoich osiągnięć oraz miał udokumentowane kompetencje administracyjne i umiejętności kierownicze, a także odpowiednie kompetencje i doświadczenie w zakresie cyberbezpieczeństwa, oraz aby pełnił swoje obowiązki w sposób całkowicie niezależny.

(51) Centrum Kompetencji powinno korzystać ze wsparcia Strategicznej Grupy Doradczej. Grupa powinna udzielać tego wsparcia w oparciu o regularny dialog między Centrum Kompetencji a Społecznością, która powinna składać się z przedstawicieli sektora prywatnego, organizacji konsumenckich, środowiska akademickiego i innych odpowiednich interesariuszy. Strategiczna Grupa Doradcza powinna skupiać się na zagadnieniach istotnych dla interesariuszy i kierować na nie uwagę Rady Zarządzającej i Dyrektora Wykonawczego. Zadania Strategicznej Grupy Doradczej powinny obejmować zapewnianie doradztwa w zakresie Programu działań, rocznego programu prac i wieloletniego programu prac. Reprezentacja różnych interesariuszy w Strategicznej Grupie Doradczej powinna być zrównoważona, ze szczególnym uwzględnieniem MŚP, tak by zapewnić odpowiednią reprezentację interesariuszy w pracach Centrum Kompetencji.

(52) Wkłady państw członkowskich w zasoby Centrum Kompetencji mogą mieć charakter finansowy lub rzeczowy. Wkładem finansowym może być na przykład dotacja przyznana przez dane państwo członkowskie beneficjentowi z tego państwa, stanowiąca uzupełnienie wsparcia finansowego Unii dla projektu w ramach rocznego programu prac. Natomiast wkład rzeczowy byłby zwykle wnoszony w przypadkach, gdy podmiot z państwa członkowskiego sam jest beneficjentem wsparcia finansowego Unii. Na przykład, jeśli Unia dofinansowuje działania krajowego ośrodka koordynacji z zastosowaniem poziomu finansowania wynoszącego 50 %, pozostałe koszty zostaną ujęte jako wkład rzeczowy. Innym przykładem będzie sytuacja, gdy podmiot z państwa członkowskiego otrzymuje wsparcie finansowe Unii na utworzenie lub modernizację infrastruktury, którą interesariusze będą wykorzystywać wspólnie, zgodnie z rocznym programem prac; powiązane koszty niesubsydiowane ujmowane będą w takim wypadku jako wkłady rzeczowe.

(53) Zgodnie z odpowiednimi przepisami rozporządzenia delegowanego (UE) 2019/715 dotyczącego konfliktów interesów Centrum Kompetencji powinno przyjąć przepisy dotyczące zapobiegania konfliktom interesów, ich identyfikowania i rozwiązywania oraz zarządzania nimi, w odniesieniu do swoich członków, organów i personelu, Rady Zarządzającej, a także Strategicznej Grupy Doradczej i Społeczności. Państwa członkowskie powinny zapewnić zapobieganie konfliktom interesów oraz ich identyfikację i rozstrzyganie w odniesieniu do krajowych ośrodków koordynacji, zgodnie z przepisami krajowymi. Centrum Kompetencji powinno również stosować odpowiednie unijne przepisy dotyczące publicznego dostępu do dokumentów zawarte w rozporządzeniu Parlamentu Europejskiego i Rady (WE) nr 1049/2001 ([9]). Przetwarzanie danych osobowych przez Centrum Kompetencji powinno podlegać przepisom rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 ([10]). Centrum Kompetencji powinno przestrzegać przepisów unijnych mających zastosowanie do instytucji Unii oraz prawa krajowego dotyczącego przetwarzania informacji, w szczególności przetwarzania szczególnie chronionych informacji jawnych i informacji niejawnych UE.

(54) 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) 2018/1046 ([11]) (zwanym dalej „rozporządzeniem finansowym").

(55) Centrum Kompetencji powinno działać w otwarty i przejrzysty sposób. Powinno ono na czas udostępniać wszelkie stosowne informacje i promować swoją działalność, w tym realizować działania informacyjne i upowszechnianie wiedzy wśród społeczeństwa. Regulaminy wewnętrzne Rady Zarządzającej Centrum Kompetencji oraz Strategicznej Grupy Doradcze powinno podać się do wiadomości publicznej.

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

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

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

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

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

(58) Ponieważ cele niniejszego rozporządzenia, a mianowicie wzmocnienie konkurencyjności i zdolności Unii, utrzymanie i rozwijanie badawczych, technologicznych i przemysłowych zdolności Unii w dziedzinie cyberbezpieczeństwa, zwiększanie konkurencyjności unijnego sektora cyberbezpieczeństwa i sprawienie, by cyberbezpieczeństwo stało się elementem decydującym o przewadze konkurencyjnej pozostałych sektorów przemysłu Unii, nie mogą zostać osiągnięte w sposób wystarczający przez same państwa członkowskie z uwagi na rozproszenie istniejących ograniczonych zasobów oraz wymaganą skalę inwestycji, a jednocześnie mogą zostać w lepszym stopniu osiągnięte na poziomie unijnym, dzięki uniknięciu niepotrzebnego powielania tych wysiłków, pomocy w osiągnięciu masy krytycznej inwestycji, zapewnieniu optymalnego sposobu wykorzystania finansowania publicznego i promowaniu wysokiego poziomu cyberbezpieczeństwa we wszystkich państwach członkowskich, Unia może przyjąć środki zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej (TUE). Zgodnie z zasadą proporcjonalności, o której mowa w przywołanym artykule, niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

Ogólne przepisy I zasady centrum kompetencji oraz sieci

Artykuł 1

Przedmiot i zakres

1. Niniejszym rozporządzeniem ustanawia się Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (zwane dalej „Centrum Kompetencji") oraz sieć krajowych ośrodków koordynacji (zwaną dalej „Siecią"). W niniejszym rozporządzeniu ustanawia się przepisy dotyczące wyznaczania krajowych ośrodków koordynacji, jak również przepisy regulujące tworzenie społeczności kompetentnej w zakresie cyberbezpieczeństwa (zwanej dalej „Społecznością").

2. Centrum Kompetencji odgrywa podstawową rolę we wdrażaniu części programu „Cyfrowa Europa" dotyczącej cyberbezpieczeństwa, w szczególności w odniesieniu do działań związanych z art. 6 rozporządzenia (UE) 2021/694, i przyczynia się do wdrażania programu „Horyzont Europa", w szczególności w odniesieniu do pkt 3.1.3 filaru II opisanego w załączniku I do decyzji Rady (UE) 2021/764 ([12]).

3. Państwa członkowskie wspólnie wnoszą wkład w prace Centrum Kompetencji i prace Sieci.

4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla kompetencji państw członkowskich w zakresie bezpieczeństwa publicznego, obronności i bezpieczeństwa narodowego oraz dla działań państwa w dziedzinie prawa karnego.

Artykuł 2

Definicje

Na potrzeby niniejszego rozporządzenia stosuje się następujące definicje:

1) „cyberbezpieczeństwo" oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami;

2) „sieci i systemy informatyczne" oznaczają sieci i systemy informatyczne zgodnie z definicją w art. 4 pkt 1 dyrektywy (UE) 2016/1148;

3) „produkty, usługi i procesy w dziedzinie cyberbezpieczeństwa" oznaczają komercyjne i niekomercyjne produkty, usługi lub procesy ICT, których konkretnym zadaniem jest ochrona sieci i systemów informatycznych lub zapewnianie poufności, integralności i dostępności danych przetwarzanych lub przechowywanych w sieciach i systemach informatycznych, a także których zadaniem jest zapewnianie cyberbezpieczeństwa użytkowników takich systemów i innych osób przed cyberzagrożeniami;

4) „cyberzagrożenie" oznacza potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć na sieci i systemy informatyczne, użytkowników takich systemów oraz inne osoby;

([12]) Decyzja Rady (UE) 2021/764 z dnia 10 maja 2021 r. ustanawiająca program szczegółowy służący realizacji programu ramowego w zakresie badań naukowych i innowacji „Horyzont Europa" oraz uchylająca decyzję 2013/743/UE (Dz.U. L 167 I z 12.5.2021, s. 1).

5) „wspólne działanie" oznacza działanie, które jest ujęte w rocznym programie prac, i które otrzymuje wsparcie finansowe z programu „Horyzont Europa", programu „Cyfrowa Europa" lub innych programów unijnych, a także wsparcie finansowe lub rzeczowe ze strony co najmniej jednego z państw członkowskich, i które to działanie jest realizowane za pośrednictwem projektów z udziałem beneficjentów mających siedzibę w tych państwach członkowskich i otrzymujących wsparcie finansowe lub rzeczowe od tych państw członkowskich;

6) „wkład rzeczowy" oznacza koszty kwalifikowalne poniesione przez krajowe ośrodki koordynacji i inne podmioty publiczne uczestniczące w projektach finansowanych na podstawie niniejszego rozporządzenia, które to koszty nie są finansowane z wkładu Unii ani z wkładów finansowych państw członkowskich;

7) „europejskie centrum innowacji cyfrowych" oznacza europejskie centrum innowacji cyfrowych zgodnie z definicją w art. 2 lit. e) rozporządzenia (UE) 2021/694;

8) „Program działań" oznacza kompleksową i zrównoważoną strategię na rzecz przemysłu, technologii i badań naukowych w dziedzinie cyberbezpieczeństwa, w której określa się strategiczne zalecenia dotyczące rozwoju i wzrostu europejskiego sektora przemysłu, technologii i badań naukowych w dziedzinie cyberbezpieczeństwa oraz priorytety strategiczne działań Centrum Kompetencji i która nie jest wiążąca w odniesieniu do decyzji, które mają być podejmowane w sprawie rocznych programów prac;

9) „pomoc techniczna" oznacza pomoc oferowaną przez Centrum Kompetencji na rzecz krajowych ośrodków koordynacji lub Społeczności w celu realizacji ich zadań, świadczoną poprzez zapewnianie wiedzy lub ułatwianie dostępu do wiedzy fachowej w zakresie przemysłu, technologii i badań naukowych w dziedzinie cyberbezpieczeństwa, ułatwianie tworzenia sieci kontaktów, podnoszenie świadomości oraz promowanie współpracy, lub oznacza pomoc techniczną oferowaną przez Centrum Kompetencji wraz z krajowymi ośrodkami koordynacji na rzecz interesariuszy w odniesieniu do przygotowywania projektów uwzględniających misję Centrum Kompetencji i Sieci oraz cele Centrum Kompetencji.

Artykuł 3

Misja Centrum Kompetencji i Sieci

1. Misją Centrum Kompetencji i Sieci jest pomoc Unii w:

a) wzmocnieniu jej wiodącej pozycji i autonomii strategicznej w dziedzinie cyberbezpieczeństwa poprzez utrzymanie i rozwijanie badawczych, naukowych, społecznych, technologicznych i przemysłowych zdolności i możliwości Unii w dziedzinie cyberbezpieczeństwa, niezbędnych, by zwiększyć zaufanie i bezpieczeństwo, w tym poufność, integralność i dostępność danych na jednolitym rynku cyfrowym;

b) wspieraniu unijnych zdolności, możliwości i umiejętności technologicznych w zakresie odporności i niezawodności infrastruktury sieci i systemów informatycznych, w tym infrastruktury krytycznej oraz powszechnie używanego sprzętu komputerowego i oprogramowania w Unii; oraz

c) zwiększaniu globalnej konkurencyjności unijnego sektora cyberbezpieczeństwa, zapewnianiu wysokich norm cyberbezpieczeństwa w Unii i sprawieniu, by cyberbezpieczeństwo stało się elementem decydującym o przewadze konkurencyjnej pozostałych sektorów przemysłu Unii.

2. W odpowiednich przypadkach Centrum Kompetencji i Sieć realizują swoje zadania we współpracy z agencją ENISA i Społecznością.

3. Centrum Kompetencji zgodnie z aktami prawnymi ustanawiającymi odpowiednie programy, w szczególności program „Horyzont Europa" i program „Cyfrowa Europa", wykorzystuje odpowiednie zasoby finansowe Unii w taki sposób, aby przyczyniać się do realizacji misji określonej w ust. 1.

Artykuł 4

Cele Centrum Kompetencji

1. Celem ogólnym Centrum Kompetencji jest wspieranie badań naukowych, innowacji i wdrażania rozwiązań w dziedzinie cyberbezpieczeństwa w celu realizacji misji określonej w art. 3.

2. Centrum Kompetencji ma następujące cele szczegółowe:

a) zwiększanie zdolności, możliwości, wiedzy i infrastruktury w zakresie cyberbezpieczeństwa służących stosownie do przypadku sektorom przemysłu, w szczególności MŚP, środowiskom badawczym, sektorowi publicznemu i społeczeństwu obywatelskiemu;

b) propagowanie cyberodporności, upowszechnianie stosowania najlepszych praktyk w zakresie cyberbezpieczeństwa, zasady uwzględniania bezpieczeństwa na etapie projektowania i certyfikacji bezpieczeństwa produktów i usług cyfrowych, w sposób uzupełniający wysiłki innych podmiotów publicznych;

c) przyczynianie się do silnego europejskiego ekosystemu cyberbezpieczeństwa, łączącego wszystkich odpowiednich interesariuszy.

3. Centrum Kompetencji realizuje cele szczegółowe, o których mowa w ust. 2, poprzez:

a) określanie zaleceń strategicznych dotyczących badań naukowych, innowacji i wdrażania rozwiązań w dziedzinie cyberbezpieczeństwa zgodnie z prawem Unii oraz określanie strategicznych priorytetów działań Centrum Kompetencji;

b) realizowanie działań w ramach odpowiednich unijnych programów finansowania zgodnie z odpowiednimi programami prac i aktami ustawodawczymi Unii ustanawiającymi te programy finansowania;

c) sprzyjanie współpracy i koordynacji między krajowymi ośrodkami koordynacji oraz ze Społecznością i w ramach Społeczności; oraz

d) nabywanie i obsługę – w odpowiednich i stosownych przypadkach – infrastruktury i usług ICT, jeżeli jest to konieczne do realizacji zadań określonych w art. 5 i zgodnie z odpowiednimi programami prac określonymi w art. 5 ust. 3 lit. b).

Artykuł 5

Zadania Centrum Kompetencji

1. W celu realizacji swojej misji i celów Centrum Kompetencji wykonuje następujące zadania:

a) zadania o charakterze strategicznym; oraz

b) zadania o charakterze wdrożeniowym.

2. Zadania o charakterze strategicznym, o których mowa w ust. 1 lit. a), obejmują:

a) opracowanie i monitorowanie realizacji Programu działań;

b) w oparciu o Program działań i wieloletni program prac, przy unikaniu powielania działań z agencją ENISA i z uwzględnieniem potrzeby tworzenia synergii między częścią programu „Horyzont Europa" i programu „Cyfrowa Europa" dotyczącą cyberbezpieczeństwa a innymi częściami tych programów:

(i) określanie priorytetów prac Centrum Kompetencji w zakresie:

1) zwiększenia skali badań naukowych i innowacji w dziedzinie cyberbezpieczeństwa z uwzględnieniem całego cyklu innowacji oraz skali wdrażania rozwiązań będących owocem tych badań naukowych i innowacji;

2) rozwijania przemysłowych, technologicznych i badawczych zdolności i możliwości w dziedzinie cyberbezpieczeństwa oraz infrastruktury;

3) wzmacniania umiejętności i kompetencji w dziedzinie cyberbezpieczeństwa i technologii w przemyśle oraz badaniach naukowych i na wszystkich odpowiednich poziomach edukacji, przy wspieraniu równowagi płci;

4) wdrażania produktów, usług i procesów w dziedzinie cyberbezpieczeństwa;

5) udzielania wsparcia na rzecz wprowadzania na rynek produktów, usług i procesów z zakresu cyberbezpieczeństwa przyczyniających się do realizacji misji określonej w art. 3;

6) udzielania wsparcia na rzecz przyjmowania i wdrażania najnowocześniejszych produktów, usług i procesów z zakresu cyberbezpieczeństwa przez organy publiczne na ich wniosek, przez sektory przemysłu po stronie popytu i innych użytkowników;

(ii) wspieranie sektora cyberbezpieczeństwa, w szczególności MŚP, w celu wzmocnienia doskonałości, zdolności i konkurencyjności Unii w odniesieniu do cyberbezpieczeństwa, w tym z myślą o połączeniu z potencjalnymi rynkami i możliwościami w zakresie wdrażania oraz przyciąganiu inwestycji; oraz

(iii) zapewnianie wsparcia oraz pomocy technicznej zajmującym się cyberbezpieczeństwem przedsiębiorstwom typu start-up, MŚP, mikroprzedsiębiorstwom, stowarzyszeniom, indywidualnym ekspertom oraz projektom z dziedziny technologii obywatelskiej;

c) zapewnianie synergii i współpracy pomiędzy odpowiednimi instytucjami, organami i jednostkami organizacyjnymi Unii, w szczególności z agencją ENISA, przy jednoczesnym unikaniu powielania działań z tymi instytucjami, organami i jednostkami organizacyjnymi Unii;

d) koordynowanie krajowych ośrodków koordynacji za pośrednictwem Sieci i zapewnianie regularnej wymiany wiedzy fachowej;

e) zapewnianie państwom członkowskim, na ich wniosek, doradztwa fachowego w zakresie przemysłu, technologii i badań naukowych w dziedzinie cyberbezpieczeństwa, w tym w odniesieniu do zamówień publicznych i wdrażania technologii;

f) ułatwianie współpracy i dzielenia się wiedzą fachową między wszystkimi odpowiednimi interesariuszami, w szczególności między członkami Społeczności;

g) udział w unijnych, krajowych i międzynarodowych konferencjach, targach i forach związanych z misją, celami i zadaniami Centrum Kompetencji w celu wymiany poglądów i stosownych najlepszych praktyk z innymi uczestnikami;

h) ułatwianie wykorzystywania wyników projektów w zakresie badań naukowych i innowacji w działaniach związanych z rozwojem produktów, usług i procesów w dziedzinie cyberbezpieczeństwa, przy unikaniu rozdrobnienia i powielania wysiłków oraz propagowanie dobrych praktyk, produktów, usług i procesów w dziedzinie cyberbezpieczeństwa, w szczególności opracowanych przez MŚP i wykorzystujących otwarte oprogramowanie;

3. Zadania o charakterze wdrożeniowym, o których mowa w ust. 1 lit. b), obejmują:

a) koordynowanie i zarządzanie pracami Sieci i Społeczności w celu realizacji misji określonej w art. 3, w szczególności wspieranie w Unii przedsiębiorstw typu start-up, MŚP, mikroprzedsiębiorstw, stowarzyszeń i projektów z dziedziny technologii obywatelskiej zajmujących się cyberbezpieczeństwem i ułatwianie im dostępu do wiedzy fachowej, finansowania, inwestycji i rynków;

b) ustanowienie i wdrażanie rocznego programu prac, zgodnie z Programem działań i wieloletnim programem prac, w odniesieniu do części dotyczących cyberbezpieczeństwa:

   (i) programu „Cyfrowa Europa", w szczególności w odniesieniu do działań związanych z art. 6 rozporządzenia (UE) 2021/694;

   (ii) wspólnych działań otrzymujących wsparcie na podstawie przepisów dotyczących cyberbezpieczeństwa zawartych w programie „Horyzont Europa", w szczególności w odniesieniu do pkt 3.1.3 filaru II opisanego w załączniku I do decyzji (UE) 2021/764, zgodnie z wieloletnim programem prac i procesem planowania strategicznego programu „Horyzont Europa"; oraz

   (iii) innych programów, jeżeli zostało to przewidziane w odpowiednich aktach ustawodawczych Unii;

c) wspieranie, w odpowiednich przypadkach, realizacji celu szczegółowego 4 – „Zaawansowane umiejętności cyfrowe" określonego w art. 7 rozporządzenia (UE) 2021/694 we współpracy z europejskimi centrami innowacji cyfrowych;

d) zapewnianie Komisji doradztwa fachowego na temat cyberbezpieczeństwa w przemyśle, technologii i badaniach naukowych, gdy Komisja przygotowuje projekty programów prac zgodnie z art. 13 decyzji (UE) 2021/764;

e) przeprowadzanie lub umożliwianie wdrażania infrastruktury ICT i ułatwianie nabywania takiej infrastruktury – służącej społeczeństwu, sektorom przemysłu i sektorowi publicznemu, na wniosek państw członkowskich, środowisk badawczych i operatorów usług kluczowych, między innymi dzięki wkładom państw członkowskich i finansowaniu unijnemu w ramach wspólnych działań, zgodnie z Programem działań, rocznym programem prac i wieloletnim programem prac;

f) podnoszenie świadomości na temat misji Centrum Kompetencji i Sieci oraz celów i zadań Centrum Kompetencji;

g) bez uszczerbku dla cywilnego charakteru projektów, które mają być finansowane w ramach programu „Horyzont Europa" oraz zgodnie z rozporządzeniami (UE) 2021/695 i (UE) 2021/694, wzmacnianie synergii i koordynacji między cywilnymi a obronnymi aspektami cyberbezpieczeństwa poprzez ułatwianie wymiany:

   (i) wiedzy i informacji w odniesieniu do technologii i aplikacji podwójnego zastosowania;

   (ii) rezultatów, wymogów i najlepszych praktyk; oraz

   (iii) informacji w odniesieniu do priorytetów odpowiednich programów unijnych.

4. Centrum Kompetencji wypełnia zadania określone w ust. 1 w ścisłej współpracy z Siecią.

5. Zgodnie z art. 6 rozporządzenia (UE) 2021/695 i z zastrzeżeniem umowy o przyznanie wkładu zdefiniowanej w art. 2 pkt 18 rozporządzenia finansowego, Centrum Kompetencji można powierzyć zadanie realizowania tych części dotyczących cyberbezpieczeństwa w ramach programu „Horyzont Europa", które nie są współfinansowane przez państwa członkowskie, a w szczególności w odniesieniu do pkt 3.1.3 filaru II opisanego w załączniku I do decyzji (UE) 2021/764.

Artykuł 6

Wyznaczenie krajowych ośrodków koordynacji

1. Do dnia 29 grudnia 2021 r. każde państwo członkowskie wyznacza jeden podmiot, który spełnia kryteria określone w ust. 5, aby pełnił rolę krajowego ośrodka koordynacji na potrzeby niniejszego rozporządzenia. Każde państwo członkowskie niezwłocznie powiadamia o wyznaczonym podmiocie Radę Zarządzającą Centrum Kompetencji. Podmiotem tym może być podmiot już istniejący w tym państwie członkowskim.

Termin określony w akapicie pierwszym niniejszego ustępu przedłuża się o okres, w którym Komisja ma wydać opinię, o której mowa w ust. 2.

2. Państwo członkowskie może w dowolnym momencie zwrócić się do Komisji o opinię na temat spełniania wymaganych zdolności przez podmiot, który to państwo członkowskie wyznaczyło lub zamierza wyznaczyć na swój krajowy ośrodek koordynacji, w zakresie zarządzania środkami finansowymi w celu realizacji misji i celów określonych w niniejszym rozporządzeniu. Komisja przekazuje temu państwu członkowskiemu swoją opinię w ciągu trzech miesięcy od otrzymania jego wniosku.

3. Na podstawie dokonanego przez państwo członkowskie zgłoszenia dotyczącego podmiotu, o którym mowa w ust. 1, Rada Zarządzająca – nie później niż trzy miesiące od tego zgłoszenia – umieszcza ten podmiot w wykazie jako krajowy ośrodek koordynacji. Centrum Kompetencji publikuje wykaz wyznaczonych krajowych ośrodków koordynacji.

4. Państwa członkowskie mogą w dowolnym momencie wyznaczyć nowy podmiot, który będzie pełnił rolę krajowego ośrodka koordynacji na potrzeby niniejszego rozporządzenia. Do wyznaczenia nowego podmiotu mają zastosowanie ust. 1, 2 i 3.

5. Krajowy ośrodek koordynacji musi być podmiotem sektora publicznego lub podmiotem, w którym większościowy udział ma państwo członkowskie, realizującym zadania administracji publicznej na mocy prawa krajowego, w tym na podstawie przekazania uprawnień, i mającym zdolności wspierania Centrum Kompetencji i Sieci w wypełnianiu ich misji określonej w art. 3 niniejszego rozporządzenia. Ośrodek musi dysponować wiedzą fachową z zakresu badań naukowych i technologii w dziedzinie cyberbezpieczeństwa lub też mieć dostęp do takiej wiedzy. Musi on być zdolny do utrzymywania skutecznych kontaktów z przemysłem, sektorem publicznym, środowiskiem akademickim i badawczym oraz obywatelami, a także z organami wyznaczonymi na podstawie dyrektywy (UE) 2016/1148, oraz do koordynowania z nimi swoich działań.

6. Krajowy ośrodek koordynacji może w dowolnym momencie wystąpić z wnioskiem o uznanie, że posiada on wymagane zdolności w zakresie zarządzania środkami finansowymi w celu realizacji misji i celów określonych w niniejszym rozporządzeniu, zgodnie z rozporządzeniami (UE) 2021/695 i (UE) 2021/694. W ciągu trzech miesięcy od otrzymania takiego wniosku Komisja ocenia, czy krajowy ośrodek koordynacji ma takie zdolności i wydaje decyzję.

W przypadku gdy Komisja, zgodnie z procedurą określoną w ust. 2, wydała pozytywną opinię państwu członkowskiemu, opinię tę uznaje się za decyzję uznającą wskazany podmiot za posiadający wymagane zdolności na potrzeby niniejszego ustępu.

Najpóźniej do dnia 29 sierpnia 2021 r. Komisja, po konsultacji z Radą Zarządzającą, wydaje wytyczne w sprawie oceny, o której mowa w akapicie pierwszym, zawierające wyszczególnienie warunków uznawania i opisujące sposób wydawania opinii i przeprowadzania ocen.

Przed wydaniem opinii, o której mowa w ust. 2, i decyzji, o której mowa w akapicie pierwszym niniejszego ustępu, Komisja uwzględnia informacje i dokumentację przedstawione przez krajowy ośrodek koordynacji występujący z wnioskiem.

Decyzja o odmowie uznania, że krajowy ośrodek koordynacji posiada wymagane zdolności do zarządzania środkami finansowymi w celu wypełnienia misji i celów określonych w niniejszym rozporządzeniu jest należycie uzasadniana i wskazuje wymogi, których występujący z wnioskiem krajowy ośrodek koordynacji jeszcze nie spełnił, co uzasadnia decyzję o odmowie uznania. Krajowy ośrodek koordynacji, którego wniosek o uznanie został odrzucony, może w dowolnym momencie ponownie przedłożyć swój wniosek uzupełniony dodatkowymi informacjami.

Państwa członkowskie informują Komisję o zmianach, które nastąpiły w odniesieniu do krajowego ośrodka koordynacji, takich jak skład krajowego ośrodka koordynacji, formę prawną krajowego ośrodka koordynacji lub inne istotne aspekty, które wpływają na jego zdolności w zakresie zarządzania środkami finansowymi w celu wypełnienia misji i celów określonych w niniejszym rozporządzeniu. Po otrzymaniu takich informacji Komisja może odpowiednio zmienić swoją decyzję o uznaniu lub odmowie uznania krajowego ośrodka koordynacji jako posiadającego wymagane zdolności do odpowiedniego zarządzania środkami finansowymi.

7. Sieć składa się ze wszystkich krajowych ośrodków koordynacji, które zostały zgłoszone Radzie Zarządzającej przez państwa członkowskie.

Artykuł 7

Zadania krajowych ośrodków koordynacji

1. Krajowe ośrodki koordynacji mają następujące zadania:

a) pełnienie roli punktu kontaktowego na poziomie krajowym dla Społeczności, by wspierać Centrum Kompetencji w realizacji jego misji i celów, a w szczególności w koordynowaniu działań Społeczności poprzez koordynowanie działań członków Społeczności w swoich państwach członkowskich;

b) zapewnianie wiedzy fachowej i aktywne wnoszenie wkładu na rzecz realizacji zadań o charakterze strategicznym określonych w art. 5 ust. 2, z uwzględnieniem odpowiednich krajowych i regionalnych wyzwań dla cyberbezpieczeństwa występujących w poszczególnych sektorach;

c) promowanie uczestnictwa społeczeństwa obywatelskiego, sektorów przemysłu, w szczególności przedsiębiorstw typu start-up i MŚP, środowiska akademickiego i środowiska badawczego oraz innych interesariuszy na poziomie krajowym w projektach transgranicznych i w działaniach z dziedziny cyberbezpieczeństwa finansowanych na podstawie odpowiednich programów unijnych oraz zachęcanie do tego uczestnictwa i jego ułatwianie;

d) zapewnianie interesariuszom pomocy technicznej poprzez udzielanie im wsparcia na etapie składania wniosków dotyczących projektów zarządzanych przez Centrum Kompetencji – w odniesieniu do jego misji i celów oraz z pełnym poszanowaniem zasad należytego zarządzania finansami, w szczególności zasad dotyczących konfliktów interesów;

e) dążenie do tworzenia synergii z odpowiednimi działaniami na poziomie krajowym, regionalnym i lokalnym, na przykład w ramach krajowych polityk w zakresie badań naukowych, rozwoju i innowacji w dziedzinie cyberbezpieczeństwa, w szczególności polityk ujętych w krajowych strategiach cyberbezpieczeństwa;

f) wdrażanie poszczególnych działań, na które Centrum Kompetencji przyznało dotacje, w tym poprzez zapewnianie wsparcia finansowego dla stron trzecich zgodnie z art. 204 rozporządzenia finansowego na warunkach określonych w odnośnych umowach o udzielenie dotacji;

g) bez uszczerbku dla kompetencji państw członkowskich w dziedzinie edukacji i z uwzględnieniem odpowiednich zadań agencji ENISA – nawiązywanie kontaktów z organami krajowymi z myślą o potencjalnym wkładzie w promowanie i upowszechnianie programów kształcenia w dziedzinie cyberbezpieczeństwa;

h) promowanie i rozpowszechnianie – na poziomie krajowym, regionalnym lub lokalnym – odpowiednich wyników prac prowadzonych przez Sieć, Społeczność i Centrum Kompetencji;

i) ocena wniosków o włączenie do Społeczności składanych przez podmioty mające siedzibę w tym samym państwie członkowskim co krajowy ośrodek koordynacji;

j) popieranie i promowanie zaangażowania odpowiednich podmiotów w działania inicjowane przez Centrum Kompetencji, Sieć i Społeczność oraz monitorowanie, w odpowiednich przypadkach, poziomu zaangażowania w zakresie badań naukowych, rozwoju i zastosowań w dziedzinie cyberbezpieczeństwa oraz wysokości publicznego wsparcia finansowego udzielonego na działania w tej dziedzinie.

2. Na potrzeby ust. 1 lit. f) niniejszego artykułu wsparcie finansowe dla stron trzecich może być zapewniane w którejkolwiek z form wkładu Unii określonych w art. 125 rozporządzenia finansowego, w tym w formie płatności ryczałtowych.

3. Na podstawie decyzji, o której mowa w art. 6 ust. 6 niniejszego rozporządzenia, krajowe ośrodki koordynacji mogą otrzymać od Unii dotacje zgodnie z art. 195 akapit pierwszy lit. d) rozporządzenia finansowego w związku z wykonywaniem zadań określonych w niniejszym artykule.

4. W stosownych przypadkach krajowe ośrodki koordynacji współpracują za pośrednictwem Sieci.

Artykuł 8

Społeczność kompetentna w zakresie cyberbezpieczeństwa

1. Społeczność wnosi wkład w określoną w art. 3 misję Centrum Kompetencji i Sieci oraz wzmacnia i upowszechnia w całej Unii wiedzę fachową z zakresu cyberbezpieczeństwa i dzieli się tą wiedzą w całej Unii.

2. W skład Społeczności wchodzą organizacje przemysłowe, w tym MŚP, organizacje akademickie i badawcze, inne odpowiednie stowarzyszenia społeczeństwa obywatelskiego, a także, w odpowiednich przypadkach, odpowiednie europejskie organizacje normalizacyjne, podmioty publiczne i inne podmioty zajmujące się aspektami operacyjnymi i technicznymi cyberbezpieczeństwa, oraz w stosownych przypadkach – interesariusze z sektorów powiązanych z cyberbezpieczeństwem i mierzących się z wyzwaniami w tej dziedzinie. Społeczność skupia głównych interesariuszy w zakresie unijnych zdolności technologicznych, przemysłowych, akademickich i badawczych w dziedzinie cyberbezpieczeństwa. Społeczność obejmuje krajowe ośrodki koordynacji, w stosownych przypadkach europejskie centra innowacji cyfrowych, a także instytucje, organy i jednostki organizacyjne Unii dysponujące odpowiednią wiedzą fachową, takie jak agencja ENISA.

3. Jako członków Społeczności rejestruje się jedynie podmioty, które mają siedzibę w państwach członkowskich. Podmioty te muszą wykazać, że mogą przyczyniać się do realizacji misji, i dysponować wiedzą fachową z zakresu cyberbezpieczeństwa w co najmniej jednej z następujących dziedzin:

a) środowisko akademickie, badania naukowe lub innowacje;

b) rozwój przemysłowy lub rozwój produktów;

c) szkolenie i kształcenie;

d) bezpieczeństwo informacji lub operacje w zakresie reagowania na incydenty;

e) etyka;

f) formalna i techniczna standaryzacja oraz specyfikacje.

4. Centrum Kompetencji rejestruje podmioty, na ich wniosek, jako członków Społeczności po przeprowadzeniu przez krajowy ośrodek koordynacji państwa członkowskiego, w którym dane podmioty mają siedzibę, oceny, celem potwierdzenia czy te podmioty spełniają kryteria określone w ust. 3 niniejszego artykułu. W ocenie tej uwzględnia się również odpowiednie krajowe oceny bezpieczeństwa przeprowadzone przez właściwe organy krajowe. Rejestracja taka nie jest ograniczona czasowo, ale Centrum Kompetencji może ją w każdym momencie odwołać, jeżeli właściwy krajowy ośrodek koordynacji uzna, że dany podmiot nie spełnia już kryteriów określonych w ust. 3 niniejszego artykułu lub podlega art. 136 rozporządzenia finansowego, lub że motywują to uzasadnione względy bezpieczeństwa. W przypadku gdy członkostwo w Społeczności zostaje odwołane ze względów bezpieczeństwa, decyzja o tym odwołaniu musi być proporcjonalna i uzasadniona. Krajowe ośrodki koordynacji dążą do osiągnięcia zrównoważonej reprezentacji interesariuszy w Społeczności i aktywnie zachęcają do uczestnictwa, w szczególności MŚP.

5. Krajowe ośrodki koordynacji zachęca się do współpracy za pośrednictwem Sieci w celu zharmonizowania sposobu, w jaki stosują kryteria określone w ust. 3 oraz procedury oceny i rejestracji podmiotów, o których mowa w ust. 4.

6. Centrum Kompetencji rejestruje odpowiednie instytucje, organy i jednostki organizacyjne Unii jako członków Społeczności po przeprowadzeniu oceny celem potwierdzenia, czy dana instytucja, organ lub jednostka organizacyjna Unii spełnia kryteria określone w ust. 3 niniejszego artykułu. Rejestracja nie jest ograniczona czasowo, ale Centrum Kompetencji może ją w każdym momencie odwołać, jeżeli uzna, że instytucja, organ lub jednostka organizacyjna Unii nie spełniają już kryteriów określonych w ust. 3 niniejszego artykułu lub podlegają art. 136 rozporządzenia finansowego.

7. W pracach Społeczności mogą uczestniczyć przedstawiciele instytucji, organów oraz jednostek organizacyjnych Unii.

8. Podmiot zarejestrowany jako członek Społeczności wyznacza swoich przedstawicieli w celu zapewnienia skutecznego dialogu. Przedstawiciele ci muszą mieć wiedzę fachową w zakresie badań naukowych, technologii i przemysłu w dziedzinie cyberbezpieczeństwa. Rada Zarządzająca może doprecyzować przedmiotowe wymogi, jednak nie może nadmiernie ograniczać podmiotów w wyznaczaniu przedstawicieli.

9. Społeczność za pośrednictwem swoich grup roboczych, a szczególnie Strategicznej Grupy Doradczej, zapewnia Dyrektorowi Wykonawczemu i Radzie Zarządzającej doradztwo strategiczne w zakresie Programu działań, rocznego i wieloletniego programu prac zgodnie z regulaminem wewnętrznym Rady Zarządzającej.

Artykuł 9

Zadania członków Społeczności

Członkowie Społeczności:

a) wspierają Centrum Kompetencji w wypełnianiu jego misji i osiąganiu jego celów oraz ściśle współpracują w tym względzie z Centrum Kompetencji i krajowymi ośrodkami koordynacji;

b) w stosownych przypadkach uczestniczą w działaniach formalnych lub nieformalnych oraz w grupach roboczych, o których mowa w art. 13 ust. 3 lit. n), w celu realizacji poszczególnych działań przewidzianych w rocznym programie prac; oraz

c) w stosownych przypadkach wspierają Centrum Kompetencji i krajowe ośrodki koordynacji w promowaniu poszczególnych projektów.

Artykuł 10

Współpraca Centrum Kompetencji z innymi instytucjami, organami i jednostkami organizacyjnymi Unii oraz organizacjami międzynarodowymi

1. W celu zapewnienia spójności i komplementarności oraz unikania powielania wysiłków Centrum Kompetencji współpracuje z odpowiednimi instytucjami, organami i jednostkami organizacyjnymi Unii, w tym z agencją ENISA, Europejską Służbą Działań Zewnętrznych, Dyrekcją Generalną Wspólnego Centrum Badawczego Komisji, Europejską Agencją Wykonawczą ds. Badań Naukowych, Agencją Wykonawczą Europejskiej Rady ds. Badań Naukowych, Europejską Agencją Wykonawczą ds. Zdrowia i Cyfryzacji ustanowioną decyzją wykonawczą Komisji (UE) 2021/173 ([13]), odpowiednimi europejskimi centrami innowacji cyfrowych, Europejskim Centrum ds. Walki z Cyberprzestępczością w Agencji Unii Europejskiej ds. Współpracy Organów Ścigania, ustanowionej rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/794 ([14]), Europejską Agencją Obrony – w odniesieniu do zadań określonych w art. 5 niniejszego rozporządzenia – oraz z innymi odpowiednimi podmiotami unijnymi. W odpowiednich przypadkach Centrum Kompetencji może również współpracować z organizacjami międzynarodowymi.

2. Współpraca, o której mowa w ust. 1 niniejszego artykułu, może odbywać się w ramach uzgodnień dotyczących współpracy. Uzgodnienia te są przedkładane do zatwierdzenia Radzie Zarządzającej. Wymiana informacji niejawnych odbywa się w ramach porozumień administracyjnych zawartych zgodnie z art. 36 ust. 3.

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 zapewnia realizację celów określonych w art. 4 i zadań określonych w art. 5, i obejmuje:

a) Radę Zarządzającą;

b) Dyrektora Wykonawczego;

c) Strategiczną Grupę Doradczą.

([13]) Decyzja wykonawcza Komisji (UE) 2021/173 z dnia 12 lutego 2021 r. ustanawiająca Europejską Agencję Wykonawczą ds. Klimatu, Infrastruktury i Środowiska, Europejską Agencję Wykonawczą ds. Zdrowia i Cyfryzacji, Europejską Agencję Wykonawczą ds. Badań Naukowych, Europejską Radę ds. Innowacji i Agencję Wykonawczą ds. MŚP, Agencję Wykonawczą Europejskiej Rady ds. Badań Naukowych i Europejską Agencję Wykonawczą ds. Edukacji i Kultury oraz uchylająca decyzje wykonawcze 2013/801/UE, 2013/771/UE, 2013/778/UE, 2013/779/UE, 2013/776/UE i 2013/770/UE (Dz.U. L 50 z 15.2.2021, s. 9).

([14]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.5.2016, s. 53).

Sekcja I

Rada Zarządzająca

Artykuł 12

Skład Rady Zarządzającej

1. W skład Rady Zarządzającej wchodzi po jednym przedstawicielu każdego państwa członkowskiego oraz dwóch przedstawicieli Komisji, którzy działają w imieniu Unii.

2. Każdy z członków Rady Zarządzającej ma zastępcę. Zastępca reprezentuje członka pod jego nieobecność.

3. Na członków Rady Zarządzającej powołanych przez państwa członkowskie i ich zastępców wybiera się pracowników sektora publicznego z danego państwa członkowskiego w oparciu o ich wiedzę z zakresu badań naukowych, technologii i przemysłu w dziedzinie cyberbezpieczeństwa, umiejętność zapewnienia przez nich koordynacji działań i stanowisk z odpowiednim krajowym ośrodkiem koordynacji, lub ich odpowiednie umiejętności kierownicze, administracyjne i w zakresie zarządzania budżetem. Komisja powołuje swoich członków Rady Zarządzającej i ich zastępców w oparciu o ich wiedzę z dziedziny cyberbezpieczeństwa, technologii lub odpowiednie umiejętności kierownicze, administracyjne i w zakresie zarządzania budżetem, a także z uwagi na umiejętność zapewnienia koordynacji, synergii oraz, w miarę możliwości, wspólnych inicjatyw pomiędzy różnymi, sektorowymi i horyzontalnymi obszarami polityki Unii, które dotyczą cyberbezpieczeństwa. Komisja oraz państwa członkowskie dokładają starań, aby ograniczyć rotację swoich przedstawicieli w Radzie Zarządzającej w celu zapewnienia ciągłości pracy Rady. Komisja oraz państwa członkowskie dążą do osiągnięcia zrównoważonej reprezentacji mężczyzn i kobiet w Radzie Zarządzającej.

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

5. Członkowie Rady Zarządzającej działają w niezależny i przejrzysty sposób na rzecz ochrony misji, celów, tożsamości i autonomii Centrum Kompetencji oraz zapewnienia, aby działania Centrum Kompetencji były spójne z jego misją i celami.

6. Rada Zarządzająca może do udziału w swoich posiedzeniach zapraszać, w odpowiednich przypadkach, obserwatorów, w tym przedstawicieli odpowiednich instytucji, organów i jednostek organizacyjnych Unii oraz członków Społeczności.

7. Przedstawiciel agencji ENISA jest stałym obserwatorem w Radzie Zarządzającej. Rada Zarządzająca może zaprosić do udziału w swoich posiedzeniach przedstawiciela Strategicznej Grupy Doradczej.

8. Dyrektor Wykonawczy bierze udział w posiedzeniach Rady Zarządzającej, ale nie przysługuje mu prawo głosu.

Artykuł 13

Zadania Rady Zarządzającej

1. Rada Zarządzająca ponosi ogólną odpowiedzialność za strategiczne ukierunkowanie i działalność Centrum Kompetencji, nadzoruje realizację jego działań oraz jest odpowiedzialna za każde zadanie, które nie zostało wyraźnie przydzielone Dyrektorowi Wykonawczemu.

2. Rada Zarządzająca przyjmuje swój regulamin wewnętrzny. Ten regulamin wewnętrzny zawiera szczegółowe procedury identyfikowania i unikania konfliktów interesów i zapewnia poufność informacji szczególnie chronionych.

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

a) opracowania i przyjęcia Programu działań i monitorowania jego wdrażania;

b) kierowania się priorytetami polityki unijnej i Programem działań, przyjęcia wieloletniego programu prac zawierającego wspólne priorytety w obszarze przemysłu, technologii i badań naukowych, które określono w oparciu o potrzeby zidentyfikowane przez państwa członkowskie we współpracy ze Społecznością i które wymagają udzielenia unijnego wsparcia finansowego, obejmujące technologie i obszary kluczowe dla rozwijania własnych możliwości Unii w dziedzinie cyberbezpieczeństwa;

c) przyjęcia rocznego programu prac w zakresie wdrażania odpowiednich unijnych środków finansowych, w szczególności pochodzących z dotyczących cyberbezpieczeństwa części programu „Horyzont Europa" – w zakresie, w jakim są one dobrowolnie współfinansowane przez państwa członkowskie – i programu „Cyfrowa Europa", zgodnie z wieloletnim programem prac Centrum Kompetencji i procesem planowania strategicznego w ramach programu „Horyzont Europa";

d) przyjęcia – na podstawie wniosku Dyrektora Wykonawczego – rocznego sprawozdania finansowego i bilansu Centrum Kompetencji oraz rocznego sprawozdania z działalności;

e) przyjęcia szczegółowych zasad finansowych Centrum Kompetencji zgodnie z art. 70 rozporządzenia finansowego;

f) przydzielenia, w ramach rocznego programu prac, środków z budżetu Unii na tematy wspólnych działań Unii i państw członkowskich;

g) opisu wspólnych działań, o których mowa w lit. f) niniejszego akapitu, oraz określenia warunków realizacji takich wspólnych działań w ramach rocznego programu prac i zgodnie z decyzjami, o których mowa w lit. f) niniejszego akapitu, oraz zgodnie z rozporządzeniami (UE) 2021/695 i (UE) 2021/694;

h) przyjęcia procedury powoływania Dyrektora Wykonawczego oraz powołania, odwoływania i przedłużania kadencji Dyrektora Wykonawczego, a także przekazywania mu wytycznych i monitorowania wykonywania przez niego zadań;

i) przyjęcia wytycznych dotyczących oceny i rejestracji podmiotów jako członków Społeczności;

j) przyjęcia uzgodnień roboczych, o których mowa w art. 10 ust. 2;

k) powołania księgowego;

l) przyjęcia rocznego budżetu Centrum Kompetencji, w tym odpowiedniego planu zatrudnienia wskazującego liczbę stanowisk czasowych według grupy funkcyjnej i grupy zaszeregowania wraz z liczbą pracowników kontraktowych i oddelegowanych ekspertów krajowych, wyrażoną w ekwiwalentach pełnego czasu pracy;

m) przyjęcia dla Centrum Kompetencji zasad dotyczących przejrzystości oraz zasad dotyczących zapobiegania konfliktom interesów i zarządzania nimi, w tym w odniesieniu do członków Rady Zarządzającej, zgodnie z art. 42 rozporządzenia delegowanego (UE) 2019/715;

n) ustanowienia grup roboczych w ramach Społeczności, w odpowiednich przypadkach z uwzględnieniem doradztwa świadczonego przez Strategiczną Grupę Doradczą;

o) powołania członków Strategicznej Grupy Doradczej;

p) przyjęcia zasad dotyczących zwrotu wydatków poniesionych przez członków Strategicznej Grupy Doradczej;

q) ustanowienia mechanizmu monitorowania w celu zapewnienia, by wdrażanie odpowiednich środków finansowych zarządzanych przez Centrum Kompetencji było zgodne z Programem działań, misją i wieloletnim programem prac oraz zgodne z zasadami programów, z których pochodzą odpowiednie środki finansowe;

r) zapewnienia regularnego dialogu i ustanowienia skutecznego mechanizmu współpracy ze Społecznością;

s) opracowania polityki komunikacyjnej Centrum Kompetencji na podstawie zalecenia Dyrektora Wykonawczego;

t) w stosownych przypadkach ustanowienia przepisów wdrażających regulamin pracowniczy urzędników i warunki zatrudnienia innych pracowników Unii Europejskiej określonych w rozporządzeniu Rady (EWG, Euratom, EWWiS) nr 259/68 ([15]) (zwane dalej „regulaminem pracowniczym" i „warunkami zatrudnienia") zgodnie z art. 30 ust. 3 niniejszego rozporządzenia;

u) w stosownych przypadkach ustanawiania zasad dotyczących delegowania ekspertów krajowych do Centrum Kompetencji oraz wykorzystania stażystów zgodnie z art. 31 ust. 2;

v) przyjęcia zasad bezpieczeństwa dla Centrum Kompetencji;

w) przyjęcia strategii dotyczącej zwalczania nadużyć finansowych i korupcji proporcjonalnej do ryzyka nadużyć finansowych i korupcji, a także przyjęcia, zgodnie z mającym zastosowanie ustawodawstwem Unii, kompleksowych środków ochrony osób, które zgłaszają naruszenia prawa Unii, z uwzględnieniem analizy kosztów i korzyści środków, które mają zostać przyjęte;

x) w razie konieczności przyjmowania metodologii obliczania dobrowolnego wkładu finansowego i rzeczowego państw członkowskich uczestniczących w finansowaniu zgodnie z rozporządzeniami (UE) 2021/695 i (UE) 2021/694 lub innym mającym zastosowanie ustawodawstwem;

([15]) Dz.U. L 56 z 4.3.1968, s. 1.

y) w kontekście rocznego programu prac i wieloletniego programu prac, zapewnienia spójności i synergii z tymi częściami programów „Cyfrowa Europa" i „Horyzont Europa", które nie są zarządzane przez Centrum Kompetencji, a także z innymi programami unijnymi;

z) przyjęcia rocznego sprawozdania z realizacji strategicznych celów i priorytetów Centrum Kompetencji, w razie potrzeby wraz z zaleceniem służącym ich lepszej realizacji.

W zakresie, w jakim roczny program prac zawiera wspólne działania, przedstawia on również informacje na temat dobrowolnych wkładów państw członkowskich na rzecz wspólnych działań. W odpowiednich przypadkach we wnioskach, a w szczególności w projekcie rocznego programu prac ocenia się potrzebę zastosowania zasad bezpieczeństwa określonych w art. 33 niniejszego rozporządzenia, w tym procedury samooceny bezpieczeństwa zgodnie z art. 20 rozporządzenia (UE) 2021/695

4. W odniesieniu do decyzji określonych w ust. 3 lit. a), b) i c) Dyrektor Wykonawczy i Rada Zarządzająca uwzględniają stosowne doradztwo strategiczne i wkład agencji ENISA zgodnie z regulaminem wewnętrznym Rady Zarządzającej.

5. Rada Zarządzająca odpowiada za zapewnianie odpowiedniego wykonywania zaleceń zawartych w sprawozdaniu z realizacji i ocenie, o których mowa w art. 38 ust. 2 i 4.

Artykuł 14

Przewodniczący i posiedzenia Rady Zarządzającej

1. Rada Zarządzająca wybiera na okres trzech lat przewodniczącego i zastępcę przewodniczącego spośród swoich członków. Kadencję przewodniczącego i zastępcy przewodniczącego można jednokrotnie przedłużyć decyzją Rady Zarządzającej. Jeżeli jednak w dowolnym momencie swojej kadencji przewodniczący lub zastępca przewodniczącego straci status członka Rady Zarządzającej, jego kadencja kończy się automatycznie w tym samym momencie. Zastępca przewodniczącego zastępuje z urzędu przewodniczącego, jeżeli przewodniczący nie jest w stanie pełnić swoich obowiązków. Przewodniczący bierze udział w głosowaniu.

2. Rada Zarządzająca odbywa 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. O ile Rada Zarządzająca nie postanowi inaczej, Dyrektor Wykonawczy Rady Zarządzającej uczestniczy w obradach, ale nie ma prawa głosu.

4. Rada Zarządzająca może zapraszać na poszczególne posiedzenia również inne osoby w charakterze obserwatorów.

5. Przewodniczący Rady Zarządzającej może zaprosić przedstawicieli Społeczności do udziału w posiedzeniach Rady Zarządzającej, ale nie mają oni prawa głosu.

6. Podczas posiedzeń członkom Rady Zarządzającej i ich zastępcom mogą towarzyszyć doradcy lub eksperci, z zastrzeżeniem postanowień regulaminu wewnętrznego Rady Zarządzającej.

7. Centrum Kompetencji zapewnia Radzie Zarządzającej obsługę sekretariatu.

Artykuł 15

Zasady głosowania Rady Zarządzającej

1. W toku swoich dyskusji Rada Zarządzająca stosuje podejście oparte na konsensusie. Jeśli członkowie Rady Zarządzającej nie są w stanie osiągnąć konsensusu, przeprowadza się głosowanie.

2. Jeśli Rada Zarządzająca nie osiągnie konsensusu w danej sprawie, podejmuje ona swoje decyzje większością co najmniej 75 % głosów wszystkich swoich członków, przy czym przedstawicieli Komisji uznaje się w takim przypadku za jednego członka. Nieobecny członek Rady Zarządzającej może przekazać swój głos swojemu zastępcy, a w przypadku nieobecności zastępcy – innemu członkowi. Żaden członek Rady Zarządzającej nie może reprezentować więcej niż jednego innego członka.

3. Decyzje Rady Zarządzającej w sprawie wspólnych działań i zarządzania nimi, o których mowa w art. 13 ust. 3 lit. f) i g), podejmuje się w następujący sposób:

a) decyzje o przydzieleniu środków z budżetu Unii na wspólne działania, o których mowa w art. 13 ust. 3 lit. f), oraz decyzje o włączeniu takich wspólnych działań do rocznego programu prac podejmuje się zgodnie z ust. 2 niniejszego artykułu;

b) decyzje dotyczące opisu wspólnych działań i decyzje określające warunki ich realizacji, o których mowa w art. 13 ust. 3 lit. g), podejmowane są przez uczestniczące państwa członkowskie i Komisję, a prawa głosu członków są proporcjonalne do ich odpowiedniego wkładu w dane wspólne działanie obliczanego zgodnie z metodologią przyjętą na podstawie art. 13 ust. 3 lit. x).

4. W odniesieniu do decyzji podejmowanych na podstawie art. 13 ust. 3 lit. b), c), d), e), f), k), l), p), q), t), u), w), x) i y) Komisja dysponuje 26 % całkowitej liczby głosów w ramach Rady Zarządzającej.

5. W przypadku decyzji innych niż decyzje, o których mowa w ust. 3 lit. b) i ust. 4, każdemu państwu członkowskiemu i Unii przysługuje jeden głos. Głos w imieniu Unii oddają wspólnie dwaj przedstawiciele Komisji.

6. Przewodniczący bierze udział w głosowaniu.

Sekcja II

Dyrektor Wykonawczy

Artykuł 16

Powołanie, odwoływanie Dyrektora Wykonawczego i przedłużanie jego kadencji

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

2. Dyrektor Wykonawczy zatrudniany jest w Centrum Kompetencji jako pracownik na czas określony, zgodnie z art. 2 lit. a) warunków zatrudnienia.

3. Rada Zarządzająca w ramach otwartej, przejrzystej i niedyskryminującej procedury wyboru powołuje Dyrektora Wykonawczego z listy kandydatów zaproponowanych przez Komisję.

4. Na potrzeby zawarcia umowy z Dyrektorem Wykonawczym przedstawicielem Centrum Kompetencji jest przewodniczący Rady Zarządzającej.

5. Kadencja Dyrektora Wykonawczego trwa cztery lata. Przed upływem tego okresu Komisja przeprowadza ocenę, w której uwzględnia ocenę wykonywania zadań przez Dyrektora Wykonawczego oraz przyszłe zadania i wyzwania Centrum Kompetencji.

6. Rada Zarządzająca, działając na wniosek Komisji uwzględniający ocenę, o której mowa w ust. 5, może jednorazowo przedłużyć kadencję Dyrektora Wykonawczego na okres nie dłuższy niż cztery lata.

7. Dyrektor Wykonawczy, którego kadencję przedłużono, nie bierze udziału w kolejnej procedurze wyboru na to samo stanowisko.

8. Dyrektor Wykonawczy może zostać odwołany ze stanowiska jedynie decyzją Rady Zarządzającej działającej na wniosek Komisji lub na wniosek co najmniej 50 % państw członkowskich.

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 odpowiada przed Radą Zarządzającą i w zakresie przyznanych mu uprawnień pełni swoje obowiązki całkowicie niezależnie. Dyrektorowi Wykonawczemu wsparcia udziela personel Centrum Kompetencji.

2. Dyrektor Wykonawczy realizuje w niezależny sposób co najmniej następujące zadania:

a) wykonuje decyzje przyjęte przez Radę Zarządzającą;

b) wspiera działania Rady Zarządzającej, zapewnia obsługę sekretariatu przy organizacji jej posiedzeń oraz przekazuje wszystkie informacje, które są niezbędne do wykonywania jej obowiązków;

c) przygotowuje i przedkłada Radzie Zarządzającej do przyjęcia – po konsultacjach z Radą Zarządzającą i Komisją, z uwzględnieniem wkładu krajowych ośrodków koordynacji oraz Społeczności – Program działań oraz zgodne z Programem działań projekty rocznego programu prac i wieloletniego programu prac Centrum Kompetencji, uwzględniając zakres zaproszeń do składania wniosków, zaproszeń do wyrażenia zainteresowania i zaproszeń do składania ofert potrzebnych w celu realizacji rocznego programu prac oraz powiązane szacunkowe kwoty wydatków zgodnie z propozycjami państw członkowskich i Komisji;

d) opracowuje i przedkłada Radzie Zarządzającej do przyjęcia projekt budżetu rocznego, obejmujący związany z nim plan zatrudnienia, o którym mowa w art. 13 ust. 3 lit. l), określający 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 roczny program prac i wieloletni program prac i składa Radzie Zarządzającej sprawozdania z ich realizacji;

f) przygotowuje projekt rocznego sprawozdania z działalności Centrum Kompetencji, uwzględniający informacje na temat powiązanych wydatków i realizacji Programu działań oraz wieloletniego programu prac; w razie potrzeby sprawozdaniu temu towarzyszą propozycje dotyczące kolejnych usprawnień w zakresie realizacji lub przeformułowania strategicznych celów i priorytetów;

g) zapewnia wdrożenie skutecznych procedur monitorowania i oceny funkcjonowania Centrum Kompetencji;

h) przygotowuje plan działania będący następstwem wniosków ze sprawozdania z realizacji oraz oceny, o których mowa w art. 38 ust. 2 i 4, oraz co dwa lata przedkłada Parlamentowi Europejskiemu i Komisji sprawozdanie z postępów;

i) przygotowuje i zawiera umowy z krajowymi ośrodkami koordynacji;

j) odpowiada za kwestie administracyjne, finansowe i pracownicze, w tym za wykonanie budżetu Centrum Kompetencji, przy należytym uwzględnieniu wskazówek otrzymanych od odpowiedniej komórki audytu wewnętrznego, zgodnie z decyzjami o których mowa w art. 13 ust. 3 lit. e), l), t), u), v) i w);

k) zatwierdza ogłaszanie zaproszeń do składania wniosków i zarządza nimi – zgodnie z rocznym programem prac – oraz administruje wynikającymi z tych zaproszeń umowami o udzielenie dotacji i decyzjami o udzieleniu dotacji;

l) zatwierdza wykaz działań wybranych do finansowania w oparciu o listę rankingową ustaloną przez zespół niezależnych ekspertów;

m) zatwierdza ogłaszanie zaproszeń do składania ofert i zarządza nimi – zgodnie z rocznym programem prac – oraz administruje zawartymi w ich rezultacie umowami;

n) zatwierdza oferty wybrane do finansowania;

o) przedkłada odpowiedniej 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) podpisuje poszczególne umowy o udzielenie dotacji, decyzje i umowy;

r) podpisuje umowy w sprawie zamówień publicznych;

s) przygotowuje plan działania na podstawie wniosków ze sprawozdań z audytów wewnętrznych lub zewnętrznych, a także z dochodzeń przeprowadzanych przez Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) ustanowiony decyzją Komisji 1999/352/WE, EWWiS, Euratom ([16]), oraz składa sprawozdania z postępów prac: dwa razy w roku Komisji, a regularnie – Radzie Zarządzającej;

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

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

([16]) Decyzja Komisji 1999/352/WE, EWWiS, Euratom z dnia 28 kwietnia 1999 r. ustanawiająca Europejski Urząd ds. Zwalczania Nadużyć Finansowych (OLAF) (Dz.U. L 136 z 31.5.1999, s. 20).

v) zapewnia skuteczną komunikację z instytucjami Unii oraz – na wniosek – przedstawia sprawozdanie Parlamentowi Europejskiemu i Radzie;

w) podejmuje inne działania potrzebne do oceny realizacji misji i celów Centrum Kompetencji;

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

Sekcja III

Strategiczna Grupa Doradcza

Artykuł 18

Skład Strategicznej Grupy Doradczej

1. Strategiczna Grupa Doradcza liczy nie więcej niż 20 członków. Członkowie są powoływani przez Radę Zarządzającą na podstawie wniosku Dyrektora Wykonawczego spośród przedstawicieli członków Społeczności, z wyjątkiem przedstawicieli instytucji, organów i jednostek organizacyjnych Unii. Kwalifikują się jedynie przedstawiciele członków Społeczności, którzy nie są kontrolowani przez państwo trzecie lub przez podmiot mający siedzibę w państwie trzecim. Powołanie odbywa się zgodnie z otwartą, przejrzystą i niedyskryminacyjną procedurą. Rada Zarządzająca dąży do tego, by skład Strategicznej Grupy Doradczej w zrównoważony sposób reprezentował Społeczność: podmioty naukowe, przemysłowe i społeczeństwa obywatelskiego, sektory przemysłu znajdujące się po stronie popytu i po stronie podaży, duże przedsiębiorstwa i MŚP, a także zapewniał zrównoważoną reprezentację pod względem pochodzenia geograficznego i płci. Dąży ona do również do równowagi wewnątrzsektorowej, mając na uwadze spójność Unii i wszystkich państw członkowskich w zakresie badań naukowych, przemysłu i technologii w dziedzinie cyberbezpieczeństwa. Skład Strategicznej Grupy Doradczej musi umożliwiać wszechstronny, ciągły i trwały dialog między Społecznością a Centrum Kompetencji.

2. Członkowie Strategicznej Grupy Doradczej dysponują wiedzą fachową w dziedzinie badań naukowych dotyczących cyberbezpieczeństwa, rozwoju przemysłu, oferowania, realizacji lub wdrażania profesjonalnych usług lub produktów. Rada Zarządzająca określa szczegółowe wymagania w zakresie takiej wiedzy fachowej.

3. Procedury dotyczące powoływania członków oraz funkcjonowania Strategicznej Grupy Doradczej określa się w regulaminie wewnętrznym Rady Zarządzającej i podaje do wiadomości publicznej.

4. Kadencja członków Strategicznej Grupy Doradczej trwa dwa lata. Kadencja ta jest odnawialna jeden raz.

5. Przedstawiciele Komisji i innych instytucji, organów i jednostek organizacyjnych Unii, w szczególności agencji ENISA, mogą być zapraszani przez Strategiczną Grupę Doradczą do udziału w jej pracach i do wspierania ich. W indywidualnych przypadkach Strategiczna Grupa Doradcza może zapraszać dodatkowych przedstawicieli Społeczności w charakterze odpowiednio obserwatora, doradcy lub eksperta, w celu uwzględnienia dynamiki zmian w dziedzinie cyberbezpieczeństwa. Członkowie Rady Zarządzającej mogą uczestniczyć w posiedzeniach Strategicznej Grupy Doradczej w charakterze obserwatorów.

Artykuł 19

Funkcjonowanie Strategicznej Grupy Doradczej

1. Strategiczna Grupa Doradcza spotyka się co najmniej trzy razy do roku.

2. Strategiczna Grupa Doradcza udziela Radzie Zarządzającej porad w sprawie tworzenia w ramach Społeczności grup roboczych, zgodnie z art. 13 ust. 3 lit. n), zajmujących się szczególnymi kwestiami związanymi z pracą Centrum Kompetencji, o ile kwestie te wiążą się bezpośrednio z zakresem zadań i obszarów kompetencji określonych w art. 20. W razie potrzeby takie grupy robocze podlegają ogólnej koordynacji ze strony co najmniej jednego członka Strategicznej Grupy Doradczej.

3. Strategiczna Grupa Doradcza wybiera przewodniczącego zwykłą większością głosów swoich członków.

4. Obsługę sekretariatu Strategicznej Grupy Doradczej zapewnia Dyrektor Wykonawczy wraz z personelem Centrum Kompetencji przy wykorzystaniu dostępnych zasobów i przy należytym uwzględnieniu ogólnego obciążenia pracą Centrum Kompetencji. Zasoby przeznaczone na wsparcie Strategicznej Grupy Doradczej są wskazane w projekcie budżetu rocznego.

5. Strategiczna Grupa Doradcza przyjmuje swój regulamin wewnętrzny zwykłą większością głosów swoich członków.

Artykuł 20

Zadania Strategicznej Grupy Doradczej

Strategiczna Grupa Doradcza regularnie doradza Centrum Kompetencji w kwestiach dotyczących prowadzenia działalności Centrum Kompetencji oraz zapewnia komunikację ze Społecznością i innymi odpowiednimi interesariuszami. Strategiczna Grupa Doradcza wykonuje również następujące zadania:

a) uwzględniając wkład Społeczności oraz – w stosownych przypadkach – wkłady grup roboczych, o których mowa w art. 13 ust. 3 lit. n), zapewnia i w sposób ciągły aktualizuje strategiczne doradztwo i wkład dla Dyrektora Wykonawczego i Rady Zarządzającej, dotyczące Programu działań, rocznego programu prac oraz wieloletniego programu prac, w terminach ustalonych przez Radę Zarządzającą;

b) zapewnia Radzie Zarządzającej doradztwo w zakresie tworzenia – w ramach Społeczności i zgodnie z art. 13 ust. 3 lit. n) – grup roboczych zajmujących się szczególnymi kwestiami związanymi z pracą Centrum Kompetencji;

c) z zastrzeżeniem zatwierdzenia przez Radę Zarządzającą decyduje o przeprowadzeniu i zajmuje się organizacją konsultacji publicznych otwartych dla wszystkich interesariuszy z sektora publicznego i prywatnego związanych z obszarem cyberbezpieczeństwa, aby zebrać informacje na potrzeby strategicznego doradztwa, o którym mowa w lit. a).

ROZDZIAŁ III

Przepisy finansowe

Artykuł 21

Wkład finansowy Unii i państw członkowskich

1. Centrum Kompetencji jest finansowane przez Unię, natomiast wspólne działania są finansowane przez Unię i z dobrowolnych wkładów państw członkowskich.

2. Koszty administracyjne i operacyjne wspólnych działań są pokrywane przez Unię i państwa członkowskie wnoszące wkład we wspólne działania zgodnie z rozporządzeniami (UE) 2021/695 i (UE) 2021/694.

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

a) do 1 649 566 000 EUR z programu „Cyfrowa Europa", w tym do 32 000 000 EUR na pokrycie kosztów administracyjnych;

b) kwotę z programu „Horyzont Europa", w tym na pokrycie kosztów administracyjnych wspólnych działań, równą kwocie wniesionej przez państwa członkowskie zgodnie z ust. 7 niniejszego artykułu, ale nieprzekraczającą kwoty ustalonej w procesie planowania strategicznego w ramach programu „Horyzont Europa", które należy przeprowadzić zgodnie z art. 6 ust. 6 rozporządzenia (UE) 2021/695, w rocznym programie prac lub w wieloletnim programie prac.

c) kwotę pochodzącą z innych odpowiednich programów Unii wymaganą do realizacji zadań lub osiągnięcia celów Centrum Kompetencji, z zastrzeżeniem decyzji podejmowanych zgodnie z aktami prawnymi Unii ustanawiającymi te programy.

4. Maksymalny wkład Unii wypłaca się ze środków w budżecie ogólnym Unii przeznaczonych na program „Cyfrowa Europa", program szczegółowy służący realizacji programu „Horyzont Europa", ustanowiony decyzją (UE) 2021/764, oraz inne programy i projekty objęte zakresem zadań Centrum Kompetencji lub Sieci.

5. Centrum Kompetencji realizuje działania dotyczące cyberbezpieczeństwa przewidziane w programie „Cyfrowa Europa" oraz programie „Horyzont Europa" zgodnie z art. 62 ust. 1 akapit pierwszy lit. c) ppkt (iv) rozporządzenia finansowego.

6. Przy obliczaniu maksymalnego wkładu finansowego Unii, o którym mowa w ust. 3 i 4, nie uwzględnia się wkładów z programów unijnych innych niż programy, o których mowa w tych ustępach, które to wkłady stanowią część unijnego współfinansowania na rzecz programu wdrażanego przez jedno z państw członkowskich.

7. Państwa członkowskie dobrowolnie uczestniczą we wspólnych działaniach, wnosząc swoje dobrowolne wkłady finansowe lub rzeczowe. Jeżeli państwo członkowskie uczestniczy we wspólnym działaniu, wkład finansowy tego państwa pokrywa koszty administracyjne proporcjonalnie do wkładu tego państwa w dane wspólne działanie. Koszty administracyjne wspólnych działań pokrywane są z wkładów finansowych. Koszty operacyjne wspólnych działań mogą być pokrywane z wkładów finansowych lub rzeczowych na zasadach określonych w programie „Horyzont Europa" i w programie „Cyfrowa Europa". Wkłady każdego państwa członkowskiego mogą przybrać formę wsparcia udzielanego przez to państwo członkowskie w ramach danego wspólnego działania beneficjentom mającym siedzibę w tym państwie członkowskim. Wkłady rzeczowe państw członkowskich obejmują koszty kwalifikowalne poniesione przez krajowe ośrodki koordynacji i inne podmioty publiczne w ramach uczestnictwa w projektach finansowanych na mocy

niniejszego rozporządzenia, pomniejszone o wkłady Unii na rzecz tych kosztów. W przypadku projektów finansowanych z programu „Horyzont Europa" koszty kwalifikowalne oblicza się zgodnie z art. 36 rozporządzenia (UE) 2021/695. W przypadku projektów finansowanych z programu „Cyfrowa Europa" koszty kwalifikowalne oblicza się zgodnie z rozporządzeniem finansowym.

Przewidywaną całkowitą kwotę dobrowolnych wkładów państw członkowskich we wspólne działania realizowane w ramach programu „Horyzont Europa", w tym wkładów finansowych na rzecz kosztów administracyjnych, ustala się w celu jej uwzględnienia w procesie planowania strategicznego w ramach programu „Horyzont Europa", które przeprowadza się zgodnie z art. 6 ust. 6 rozporządzenia (UE) 2021/695, z wykorzystaniem informacji przekazanych przez Radę Zarządzającą. W odniesieniu do działań w ramach programu „Cyfrowa Europa", bez uszczerbku dla art. 15 rozporządzenia (UE) 2021/694, państwa członkowskie mogą wnieść wkład w koszty Centrum Kompetencji, które współfinansowane są ze środków programu „Cyfrowa Europa"; wkład ten jest mniejszy niż kwoty określone w ust. 3 lit. a) niniejszego artykułu.

8. Współfinansowanie krajowe przez państwa członkowskie na rzecz działań otrzymujących wsparcie z programów unijnych innych niż program „Horyzont Europa" i program „Cyfrowa Europa" uznaje się za krajowe wkłady państw członkowskich w takim zakresie, w jakim są one częścią wspólnych działań i zostały uwzględnione w programie prac Centrum Kompetencji.

9. Na potrzeby oszacowania wkładów, o których mowa w ust. 3 niniejszego artykułu i w art. 22 ust. 2 lit. b), koszty ustala się zgodnie ze zwyczajową praktyką księgowania kosztów stosowaną przez dane państwa członkowskie, standardami rachunkowości obowiązującymi w danym państwie członkowskim, a także mającymi zastosowanie międzynarodowymi standardami rachunkowości i międzynarodowymi standardami sprawozdawczości finansowej. Koszty poświadcza niezależny audytor zewnętrzny wyznaczony przez dane państwo członkowskie. Jeśli w odniesieniu do danego poświadczenia powstanie jakakolwiek niejasność, Centrum Kompetencji może zweryfikować metodę wyceny.

10. W przypadku gdy którekolwiek z państw członkowskich nie wypełni swoich zobowiązań w zakresie wkładu finansowego lub rzeczowego na rzecz wspólnych działań, Dyrektor Wykonawczy powiadamia o tym dane państwo członkowskie pisemnie i ustala rozsądny termin, w którym takie niewypełnienie zobowiązania ma zostać naprawione. Jeśli sytuacja ta nie zostanie naprawiona we wskazanym terminie, Dyrektor Wykonawczy zwołuje posiedzenie Rady Zarządzającej, by zdecydować, czy uczestniczącemu państwu członkowskiemu, które nie wypełnia swoich zobowiązań, należy odebrać prawo głosu, lub czy należy zastosować inne środki do czasu wypełnienia przez to państwo członkowskie jego zobowiązań. Związane ze wspólnymi działaniami prawa głosu państwa członkowskiego, które nie wypełnia swoich zobowiązań, zawiesza się do czasu wypełnienia tych zobowiązań.

11. Komisja może zakończyć, proporcjonalnie ograniczyć lub zawiesić wypłacanie wkładu finansowego Unii na rzecz wspólnych działań, jeżeli państwa członkowskie uczestniczące w finansowaniu nie wnoszą swojego wkładu, o którym mowa w ust. 3 lit. b), wnoszą go jedynie częściowo lub spóźniają się z jego wniesieniem. Zakończenie, ograniczenie lub zawieszenie przez Komisję wypłacania wkładu finansowego Unii jest proporcjonalne pod względem kwoty i czasu do niewniesienia wkładu, wniesienia go jedynie częściowo lub spóźnienia się z jego wniesieniem przez państwo członkowskie.

12. Do dnia 31 stycznia każdego roku państwa członkowskie uczestniczące w finansowaniu informują Radę Zarządzającą o wartości wkładów, o których mowa w ust. 7, wniesionych w poprzednim roku budżetowym na rzecz wspólnych działań z Unią.

Artykuł 22

Koszty i zasoby Centrum Kompetencji

1. Koszty administracyjne Centrum Kompetencji są co do zasady pokrywane z wnoszonego co roku wkładu finansowego Unii. Dodatkowe wkłady finansowe są wnoszone przez uczestniczące w finansowaniu państwa członkowskie proporcjonalnie do dobrowolnych wkładów tych państw we wspólne działania. Jeśli część wkładu na pokrycie kosztów administracyjnych pozostanie niewykorzystana, może zostać przeznaczona na pokrycie kosztów operacyjnych Centrum Kompetencji.

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

a) wkładu finansowego Unii;

b) dobrowolnych finansowych lub rzeczowych wkładów dokonywanych przez państwa członkowskie uczestniczące w finansowaniu w związku ze wspólnymi działaniami.

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

a) wkłady finansowe Unii na rzecz kosztów operacyjnych i administracyjnych;

b) dobrowolne wkłady finansowe dokonywane przez państwa członkowskie uczestniczące w finansowaniu na rzecz kosztów administracyjnych w związku ze wspólnymi działaniami;

c) dobrowolne wkłady finansowe dokonywane przez państwa członkowskie uczestniczące w finansowaniu na rzecz kosztów operacyjnych w związku ze wspólnymi działaniami;

d) przychody osiągane przez Centrum Kompetencji;

e) inne wkłady finansowe, zasoby lub przychody.

4. Odsetki uzyskane z wkładów wpłaconych na rzecz Centrum Kompetencji przez państwa członkowskie uczestniczące w finansowaniu uznaje się za przychód Centrum Kompetencji.

5. Wszystkie zasoby Centrum Kompetencji i jego działania służą osiągnięciu jego celów.

6. Wszystkie aktywa wytworzone przez Centrum Kompetencji lub przekazane mu na potrzeby realizacji jego celów stanowią własność Centrum Kompetencji. Bez uszczerbku dla mających zastosowanie przepisów odpowiedniego programu finansowania prawo własności aktywów wytworzonych lub nabytych w ramach wspólnych działań określa się zgodnie z art. 15 ust. 3 lit. b).

7. Poza przypadkiem likwidacji Centrum Kompetencji, nadwyżki przychodów nad wydatkami pozostają własnością Centrum Kompetencji i nie wypłaca się ich na rzecz członków Centrum Kompetencji uczestniczących w finansowaniu.

8. Centrum Kompetencji współpracuje ściśle z innymi instytucjami, organami i jednostkami organizacyjnymi Unii, uwzględniając należycie ich odpowiednie mandaty i nie powielając istniejących mechanizmów współpracy, aby wykorzystać synergię, oraz – tam, gdzie to możliwe i właściwe – ograniczyć koszty administracyjne.

Artykuł 23

Zobowiązania finansowe

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

Artykuł 24

Rok budżetowy

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

Artykuł 25

Uchwalanie budżetu

1. Każdego roku Dyrektor Wykonawczy sporządza projekt preliminarza przychodów i wydatków Centrum Kompetencji na następny rok budżetowy oraz przekazuje ten projekt Radzie Zarządzającej wraz z projektem planu zatrudnienia, o którym mowa w art. 13 ust. 3 lit. l). Przychody 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, w tym poprzez przesunięcia personelu lub stanowisk.

2. Każdego roku Rada Zarządzająca na podstawie projektu preliminarza przychodów i wydatków, o którym mowa w ust. 1, opracowuje preliminarz przychodów i wydatków Centrum Kompetencji na następny rok budżetowy.

3. Do dnia 31 stycznia każdego roku Rada Zarządzająca przesyła Komisji preliminarz, o którym mowa w ust. 2 niniejszego artykułu, stanowiący część projektu jednolitego dokumentu programowego, o którym mowa w art. 32 ust. 1 rozporządzenia delegowanego (UE) 2019/715.

4. Na podstawie preliminarza, o którym mowa w ust. 2 niniejszego artykułu, Komisja wprowadza do projektu budżetu Unii szacunkowe kwoty, które uważa za niezbędne w związku z planem zatrudnienia, o którym mowa w art. 13 ust. 3 lit. l) niniejszego rozporządzenia, oraz kwotę wkładu, który ma zostać wniesiony z budżetu ogólnego, i przedkłada ten projekt Parlamentowi Europejskiemu i Radzie zgodnie z art. 313 i 314 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE).

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

6. Parlament Europejski i Rada przyjmują plan zatrudnienia, o którym mowa w art. 13 ust. 3 lit. l).

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

Artykuł 26

Przedstawienie sprawozdania finansowego Centrum Kompetencji i udzielenie absolutorium

Przedstawienie wstępnego i ostatecznego sprawozdania finansowego Centrum Kompetencji oraz udzielenie absolutorium odbywają się zgodnie z zasadami i terminarzem wynikającymi z rozporządzenia finansowego oraz zasad finansowych Centrum Kompetencji.

Artykuł 27

Sprawozdawczość operacyjna i finansowa

1. Dyrektor Wykonawczy co roku przekazuje Radzie Zarządzającej sprawozdanie z wykonania swoich obowiązków zgodnie z zasadami 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 rocznego programu prac na odnośny rok i realizacji strategicznych celów i priorytetów Centrum Kompetencji. Sprawozdanie to obejmuje informacje dotyczące następujących kwestii:

a) przeprowadzonych działań operacyjnych i powiązanych wydatków;

b) zgłoszonych działań, z uwzględnieniem podziału na rodzaje uczestników, w tym MŚP, i na państwa członkowskie;

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

d) realizacji misji i celów określonych w niniejszym rozporządzeniu oraz propozycji dalszych działań niezbędnych do zrealizowania tej misji i tych celów;

e) spójności zadań o charakterze wdrożeniowym z Programem działań i wieloletnim programem prac.

3. Po zatwierdzeniu przez Radę Zarządzającą roczne sprawozdanie z działalności podaje się do wiadomości publicznej.

Artykuł 28

Zasady finansowe

Centrum Kompetencji przyjmuje swoje szczegółowe zasady finansowe zgodnie z art. 70 rozporządzenia finansowego.

Artykuł 29

Ochrona interesów finansowych Unii

1. W trakcie realizacji działań finansowanych na podstawie niniejszego rozporządzenia Centrum Kompetencji stosuje odpowiednie środki zapobiegawcze w celu zapewnienia ochrony interesów finansowych Unii przeciw nadużyciom finansowym, korupcji i wszelkim innym nielegalnym działaniom, w drodze regularnych i skutecznych kontroli oraz, w przypadku wykrycia nieprawidłowości, w drodze odzyskiwania kwot nienależnie wypłaconych, a także – w odpowiednich przypadkach – skutecznych, proporcjonalnych i odstraszających kar administracyjnych.

2. Centrum Kompetencji zapewnia personelowi 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. OLAF może – zgodnie z przepisami i procedurami ustanowionymi w rozporządzeniu Rady (Euratom, WE) nr 2185/96 ([17]) oraz rozporządzeniu Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 ([18]) – przeprowadzać dochodzenia, w tym kontrole na miejscu i inspekcje, aby ustalić, czy przy okazji bezpośredniego lub pośredniego finansowania – na podstawie niniejszego rozporządzenia – umowy o udzielenie dotacji lub zamówienia miały miejsce nadużycia finansowe, korupcja lub jakakolwiek inna nielegalna działalność na szkodę interesów finansowych Unii.

4. Bez uszczerbku dla ust. 1, 2 i 3 w umowach i umowach o udzielenie dotacji wynikających z wykonywania niniejszego rozporządzenia zamieszcza się postanowienia wyraźnie upoważniające Komisję, Centrum Kompetencji, Trybunał Obrachunkowy i OLAF do prowadzenia takich audytów i dochodzeń w zakresie ich odpowiednich uprawnień. 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 stronie trzeciej, w umowie lub umowie o udzielenie dotacji określa się zobowiązanie wykonawcy lub beneficjenta do uzyskania od każdej zaangażowanej strony trzeciej wyraźnej akceptacji tych uprawnień Komisji, Centrum Kompetencji, Trybunału Obrachunkowego i OLAF.

ROZDZIAŁ IV

Personel Centrum kompetencji

Artykuł 30

Personel

1. Do personelu Centrum Kompetencji mają zastosowanie regulamin pracowniczy i warunki zatrudnienia oraz przepisy przyjęte wspólnie przez instytucje Unii na potrzeby stosowania regulaminu pracowniczego i warunków zatrudnienia.

2. W odniesieniu do personelu Centrum Kompetencji Rada Zarządzająca wykonuje uprawnienia przyznane na mocy regulaminu pracowniczego organowi powołującemu oraz na mocy warunków zatrudnienia organowi właściwemu do zawierania umów o pracę (zwane dalej „uprawnieniami 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 Dyrektorowi Wykonawczemu uprawnień organu powołującego 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.

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, o którym mowa w art. 13 ust. 3 lit. l); w planie tym wskazuje się liczbę stanowisk czasowych w podziale na grupy funkcyjne i grupy zaszeregowania oraz liczbę pracowników kontraktowych wyrażoną w ekwiwalentach pełnego czasu pracy, zgodnie z rocznym budżetem Centrum Kompetencji.

7. Zasoby ludzkie potrzebne Centrum Kompetencji zapewnia się w pierwszym rzędzie poprzez przesunięcia personelu lub stanowisk z instytucji, organów i jednostek organizacyjnych Unii, a dodatkowe zasoby ludzkie pozyskuje się w drodze rekrutacji. Personel Centrum Kompetencji może składać się z pracowników zatrudnionych na czas określony i pracowników kontraktowych.

([17]) 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).

([18]) 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).

8. Centrum Kompetencji ponosi wszystkie koszty związane z personelem.

Artykuł 31

Oddelegowani eksperci krajowi i inni pracownicy

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

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

Artykuł 32

Przywileje i immunitety

Do Centrum Kompetencji i jego personelu zastosowanie ma Protokół nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej załączony do TUE i do TFUE.

ROZDZIAŁ V

Wspólne przepisy

Artykuł 33

Przepisy bezpieczeństwa

1. Do uczestnictwa we wszystkich działaniach finansowanych przez Centrum Kompetencji ma zastosowanie art. 12 rozporządzenia (UE) 2021/694.

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

a) na potrzeby art. 38 ust. 1 rozporządzenia (UE) 2021/695 udzielanie licencji niewyłącznych – jeżeli zostało przewidziane w rocznym programie prac – może zostać ograniczone do stron trzecich mających siedzibę lub uznawanych za mające siedzibę w państwie członkowskim i kontrolowanych przez to państwo członkowskie lub przez obywateli tego państwa członkowskiego;

b) na potrzeby art. 40 ust. 4 lit. b) akapit pierwszy rozporządzenia (UE) 2021/695 przeniesienie własności lub udzielenie licencji na rzecz podmiotu prawnego z siedzibą w państwie stowarzyszonym lub w Unii, ale kontrolowanego z państw trzecich, stanowi podstawę do sprzeciwu wobec przeniesienia prawa własności rezultatów lub wobec udzielenia wyłącznej licencji w odniesieniu do rezultatów;

c) na potrzeby art. 41 ust. 7 lit. a) akapit pierwszy rozporządzenia (UE) 2021/695 udzielanie dostępu do praw zdefiniowanych w art. 2 pkt 9 tego rozporządzenia – jeżeli zostało przewidziane w rocznym programie prac – może zostać ograniczone do podmiotów prawnych mających siedzibę lub uznawanych za mające siedzibę w państwie członkowskim i znajdujących się pod kontrolą tego państwa członkowskiego lub obywateli tego państwa członkowskiego.

Artykuł 34

Przejrzystość

1. Centrum Kompetencji wykonuje swoje działania przy zachowaniu wysokiego stopnia przejrzystości.

2. Centrum Kompetencji zapewnia, aby opinia publiczna i wszelkie inne zainteresowane strony otrzymywały w stosownym czasie odpowiednie, obiektywne, wiarygodne i łatwo dostępne informacje, dotyczące w szczególności wyników jego pracy. Podaje ono również do wiadomości publicznej deklaracje interesów złożone zgodnie z art. 43. Te wymogi mają także zastosowanie do krajowych ośrodków koordynacji, Społeczności oraz Strategicznej Grupy Doradczej zgodnie z odpowiednimi przepisami.

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 Rady Zarządzającej oraz Strategicznej Grupy Doradczej praktyczne ustalenia w zakresie wdrażania zasad przejrzystości, o których mowa w ust. 1 i 2 niniejszego artykułu. W odniesieniu do działań finansowanych z programu „Horyzont Europa" te zasady i ustalenia uwzględniają rozporządzenie (UE) 2021/695.

Artykuł 35

Równowaga płci

W ramach wdrażania niniejszego rozporządzenia, przy wskazywaniu kandydatów lub proponowaniu przedstawicieli, Komisja, państwa członkowskie i inni interesariusze instytucjonalni oraz z sektora prywatnego wybierają przedstawicieli spośród kilku kandydatów, jeśli to możliwe, i dążą do zapewnienia równowagi płci.

Artykuł 36

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

1. Po zatwierdzeniu przez Komisję, Rada Zarządzająca przyjmuje przepisy bezpieczeństwa Centrum Kompetencji. Te przepisy bezpieczeństwa oparte są na zasadach i przepisach bezpieczeństwa zawartych w decyzjach Komisji (UE, Euratom) 2015/443 ([19]) i (UE, Euratom) 2015/444 ([20]).

2. Członkowie Rady Zarządzającej, Dyrektor Wykonawczy, eksperci zewnętrzni uczestniczący w pracach grup roboczych ad hoc oraz członkowie personelu Centrum Kompetencji podlegają wymogom dotyczącym poufności określonym w art. 339 TFUE, nawet po zakończeniu pełnienia swoich obowiązków.

3. Centrum Kompetencji może podjąć niezbędne środki w celu ułatwienia wymiany informacji – mających istotne znaczenie dla jego zadań – z Komisją i państwami członkowskimi oraz, w stosownych przypadkach, z właściwymi instytucjami, organami i jednostkami organizacyjnymi Unii. Zawarte w tym celu porozumienia administracyjne dotyczące udostępniania informacji niejawnych UE (zwanych dalej „EUCI") lub, jeżeli nie ma takiego porozumienia, nadzwyczajne doraźne udostępnienie EUCI są uprzednio zatwierdzane 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 do dnia 29 grudnia 2021 r.

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 TFUE lub skarg wnoszonych do Trybunału Sprawiedliwości Unii Europejskiej na podstawie art. 263 TFUE.

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 unijnych programów finansowania, o których mowa w art. 4 ust. 3 lit. b), gromadzono efektywnie, skutecznie i terminowo, a na odbiorców środków finansowych Unii i państwa członkowskie nakłada proporcjonalne wymogi sprawozdawcze. Wnioski z oceny podaje się do publicznej wiadomości.

2. Z chwilą, gdy dostępne będą wystarczające informacje na temat wdrażania niniejszego rozporządzenia, i w każdym przypadku nie później jednak niż 30 miesięcy od daty określonej w art. 46 ust. 4 Komisja sporządza sprawozdanie z realizacji dotyczące działań Centrum Kompetencji, uwzględniając wstępny wkład przekazany przez Radę Zarządzającą, krajowe ośrodki koordynacji i Społeczność. Komisja przedkłada to sprawozdanie z realizacji Parlamentowi Europejskiemu i Radzie do dnia 30 czerwca 2024 r. Centrum Kompetencji i państwa członkowskie dostarczają Komisji informacje niezbędne do przygotowania tego sprawozdania.

3. Sprawozdanie z realizacji, o którym mowa w ust. 2, obejmuje ocenę:

a) zdolności operacyjnych Centrum Kompetencji w odniesieniu do jego misji, celów, mandatu i zadań oraz ocenę współpracy i koordynacji z innymi interesariuszami, w szczególności krajowymi ośrodkami koordynacji, Społecznością i agencją ENISA;

([19]) 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).

([20]) 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).

b) wyników osiągniętych przez Centrum Kompetencji w odniesieniu do misji, celów, mandatu i zadań, a w szczególności w zakresie efektywności Centrum Kompetencji w zarządzaniu środkami finansowymi Unii i gromadzeniu wiedzy fachowej;

c) spójności zadań o charakterze wdrożeniowym z Programem działań i wieloletnim programem prac;

d) koordynacji i współpracy Centrum Kompetencji z komitetami programowymi programów „Horyzont Europa" i „Cyfrowa Europa", w szczególności w zakresie zwiększania spójności i synergii w odniesieniu do Programu działań, rocznego programu prac i wieloletniego programu prac, programu „Horyzont Europa" i programu „Cyfrowa Europa";

e) wspólnych działań.

4. Po przedłożeniu sprawozdania z realizacji, o którym mowa w ust. 2 niniejszego artykułu, Komisja dokonuje oceny Centrum Kompetencji, uwzględniając wstępny wkład przekazany przez Radę Zarządzającą, krajowe ośrodki koordynacji oraz Społeczność. Ocena ta odwołuje się do ocen, o których mowa w ust. 3 niniejszego artykułu, lub w razie potrzeby je aktualizuje; przeprowadza się ją przed upływem okresu, o którym mowa w art. 47 ust. 1, w celu ustalenia w odpowiednim terminie, czy mandat Centrum Kompetencji powinien zostać przedłużony poza ten okres. W ocenie zostaną przeanalizowane aspekty prawne i administracyjne mandatu Centrum Kompetencji oraz potencjał w zakresie tworzenia synergii z innymi instytucjami, organami i jednostkami organizacyjnymi Unii i uniknięcia rozdrobnienia ich działań.

Jeżeli Komisja uzna, że kontynuacja prac Centrum Kompetencji jest uzasadniona ze względu na jego misję, cele, mandat i zadania, może przygotować wniosek ustawodawczy dotyczący przedłużenia mandatu Centrum Kompetencji określonego w art. 47.

5. Na podstawie wniosków ze sprawozdania z realizacji, o którym mowa w ust. 2, Komisja może podjąć stosowne działania.

6. Monitorowanie, ocena, stopniowe wycofywanie i odnawianie wkładu finansowego z programu „Horyzont Europa" odbywa się zgodnie z art. 10, 50 i 52 rozporządzenia (UE) 2021/695 oraz z zatwierdzonymi ustaleniami w zakresie realizacji.

7. Monitorowanie, sprawozdawczość i ocenę wkładu z programu „Cyfrowa Europa" przeprowadza się zgodnie z art. 24 i 25 rozporządzenia (UE) 2021/694.

8. W przypadku likwidacji Centrum Kompetencji Komisja przeprowadza jego ocenę końcową w ciągu sześciu miesięcy od tej likwidacji, a w każdym przypadku nie później jednak niż dwa lata od uruchomienia procedury likwidacji, o której mowa w art. 47. Wnioski z tej oceny końcowej przedstawia się Parlamentowi Europejskiemu i Radzie.

Artykuł 39

Osobowość prawna Centrum Kompetencji

1. Centrum Kompetencji ma osobowość prawną.

2. W każdym państwie członkowskim Centrum Kompetencji ma zdolność prawną o najszerszym zakresie przyznawanym osobom prawnym na mocy prawa danego państwa członkowskiego. Może ono w szczególności nabywać i zbywać nieruchomości i ruchomości oraz być stroną w postępowaniach sądowych.

Artykuł 40

Odpowiedzialność Centrum Kompetencji

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

2. W zakresie odpowiedzialności pozaumownej szkody wyrządzone przez swój personel podczas wykonywania przez niego obowiązków służbowych Centrum Kompetencji naprawia zgodnie z ogólnymi zasadami wspólnymi dla systemów prawnych państw członkowskich.

3. 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 zasobów.

4. Centrum Kompetencji ponosi wyłączną odpowiedzialność za wykonanie swoich zobowiązań.

Artykuł 41

Właściwość Trybunału Sprawiedliwości Unii Europejskiej i prawo właściwe

1. Trybunał Sprawiedliwości Unii Europejskiej jest właściwy:

a) do wydawania wyroków na podstawie wszelkich klauzul arbitrażowych zamieszczonych w decyzjach przyjętych przez Centrum Kompetencji lub w zawieranych przez nie umowach;

b) w sporach dotyczących odszkodowań za szkody wyrządzone przez personel Centrum Kompetencji podczas wykonywania przez niego obowiązków służbowych;

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

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

Artykuł 42

Odpowiedzialność Unii i państw członkowskich oraz ubezpieczenie

1. Odpowiedzialność finansowa Unii i państw członkowskich za długi Centrum Kompetencji jest ograniczona do wysokości wkładów już wniesionych przez nich na poczet kosztów administracyjnych.

2. Centrum Kompetencji zawiera i utrzymuje odpowiednie umowy ubezpieczeniowe.

Artykuł 43

Konflikty interesów

Rada Zarządzająca przyjmuje zasady, których celem jest zapobieganie konfliktom interesów - oraz identyfikowanie i rozwiązywanie ich - w odniesieniu do członków, organów i personelu Centrum, w tym Dyrektora Wykonawczego. Zasady te zawierają postanowienia służące unikaniu konfliktów interesów w odniesieniu do przedstawicieli członków pełniących obowiązki w Radzie Zarządzającej, a także w Strategicznej Grupie Doradczej, zgodnie z rozporządzeniem finansowym, w tym postanowienia dotyczące deklaracji interesów. W kwestii konfliktów interesów krajowe ośrodki koordynacji podlegają prawu krajowemu.

Artykuł 44

Ochrona danych osobowych

1. Przetwarzanie danych osobowych przez Centrum Kompetencji podlega rozporządzeniu (UE) 2018/1725.

2. Rada Zarządzająca przyjmuje środki wykonawcze, o których mowa w art. 45 ust. 3 rozporządzenia (UE) 2018/1725. Rada Zarządzająca może przyjąć dodatkowe środki niezbędne do stosowania tego rozporządzenia przez Centrum Kompetencji.

Artykuł 45

Wsparcie ze strony przyjmującego państwa członkowskiego

Centrum Kompetencji i przyjmujące państwo członkowskie, w którym znajduje się siedziba Centrum, mogą zawrzeć porozumienie administracyjne w sprawie przywilejów i immunitetów oraz innego wsparcia udzielanego Centrum Kompetencji przez to państwo członkowskie.

ROZDZIAŁ VI

Przepisy końcowe

Artykuł 46

Początek funkcjonowania

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

2. Na potrzeby ust. 1 niniejszego artykułu, Komisja może wyznaczyć tymczasowego Dyrektora Wykonawczego do czasu objęcia obowiązków przez Dyrektora Wykonawczego w wyniku powołania przez Radę Zarządzającą zgodnie z art. 16. Tymczasowy Dyrektor Wykonawczy wykonuje obowiązki Dyrektora Wykonawczego; może on otrzymywać przy tym wsparcie ze strony ograniczonej liczby pracowników Komisji. Komisja może tymczasowo oddelegować ograniczoną liczbę swoich pracowników do Centrum Kompetencji.

3. Tymczasowy Dyrektor Wykonawczy może zatwierdzać wszelkie płatności w ramach środków przydzielonych w rocznym budżecie Centrum Kompetencji po przyjęciu przez Radę Zarządzającą oraz może zawierać umowy, w tym umowy o pracę, oraz przyjmować decyzje, po przyjęciu planu zatrudnienia, o którym mowa w art. 13 ust. 3 lit. l).

4. Tymczasowy Dyrektor Wykonawczy – w porozumieniu z Dyrektorem Wykonawczym i z zastrzeżeniem zgody 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 47

Czas trwania

1. Centrum Kompetencji ustanawia się na okres od dnia 28 czerwca 2021 r. do dnia 31 grudnia 2029 r.

2. O ile mandat Centrum Kompetencji nie zostanie przedłużony zgodnie z art. 38 ust. 4, pod koniec okresu, o którym mowa w ust. 1 niniejszego artykułu, wszczyna się automatycznie procedurę likwidacji.

3. Na potrzeby przeprowadzenia postępowania mającego na celu likwidację Centrum Kompetencji, Rada Zarządzająca powołuje 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. Nadwyżki rozdziela się między Unię oraz uczestniczące w finansowaniu państwa członkowskie proporcjonalnie do ich wkładu finansowego na rzecz Centrum Kompetencji. Nadwyżkę przydzieloną Unii zwraca się do budżetu Unii.

Artykuł 48

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 20 maja 2021 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
D.M. SASSOLI	A.P. ZACARIAS
Przewodniczący	*Przewodniczący*