2023/2841

18.12.2023

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE, Euratom) 2023/2841

z dnia 13 grudnia 2023 r.

w sprawie ustanowienia środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i jednostkach organizacyjnych Unii

PARLAMENT EUROPEJSKI i RADA UNII EUROPEJSKIEJ,

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

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

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą [1],

a także mając na uwadze, co następuje:

(1) W epoce cyfrowej technologie informacyjno-komunikacyjne stanowią podstawę otwartej, efektywnej i niezależnej administracji europejskiej. Rozwój technologii oraz coraz większa złożoność i wzajemne powiązanie systemów cyfrowych zwiększają ryzyko w cyberprzestrzeni, sprawiając, że podmioty Unii są bardziej podatne na cyberzagrożenia i incydenty, co z kolei stanowi zagrożenie dla ciągłości ich działania i zdolności do zabezpieczenia ich danych. Mimo że coraz częstsze korzystanie z usług chmurowych, wszechobecne korzystanie z technologii informacyjno-komunikacyjnych (ICT), wysoki poziom cyfryzacji, praca zdalna oraz rozwój technologii i możliwości łączenia się z siecią stanowią trzon wszystkich działań podmiotów Unii, ich odporność cyfrowa nie rozwinęła się jeszcze w wystarczającym stopniu.

(2) Krajobraz cyberzagrożeń, z jakimi mierzą się podmioty Unii, podlega ciągłym zmianom. Stosowane przez agresorów taktyki, techniki i sposoby działania ciągle ewoluują, natomiast główne motywy takich ataków prawie się nie zmieniają – ich celem jest kradzież cennych, nieujawnionych informacji, osiągnięcie korzyści finansowych, manipulowanie opinią publiczną czy też osłabienie infrastruktury cyfrowej. Tempo, w jakim agresorzy przeprowadzają cyberataki, stale rośnie, a ich działania są coraz bardziej wyrafinowane i zautomatyzowane oraz ukierunkowane na obszary wystawione na ataki, które stale się powiększają, i mają na celu szybkie wykorzystanie luk i podatności.

(3) Środowiska ICT podmiotów Unii są współzależne i występują w nich zintegrowane przepływy danych, a ich użytkownicy ściśle ze sobą współpracują. Te powiązania oznaczają, że wszelkie zakłócenia, nawet początkowo ograniczone do jednego podmiotu Unii, mogą mieć szerszy efekt kaskadowy, potencjalnie powodując dalekosiężne i długotrwałe negatywne skutki dla pozostałych podmiotów Unii. Ponadto środowiska ICT niektórych podmiotów Unii są połączone ze środowiskami ICT państw członkowskich, co powoduje, że incydent w podmiocie unijnym może stanowić ryzyko w cyberprzestrzeni dla środowisk ICT państw członkowskich i odwrotnie. Dzielenie się informacjami dotyczącymi konkretnych incydentów może ułatwić wykrywanie podobnych cyberzagrożeń lub incydentów uderzających w państwa członkowskie.

(4) Podmioty Unii stanowią atrakcyjne cele i muszą stawiać czoła dysponującym wysokimi umiejętnościami i znaczącymi zasobami agresorom, a także innym zagrożeniom. Jednocześnie istnieją znaczne różnice między tymi podmiotami, jeżeli chodzi o poziom cyberodporności, dojrzałość systemów cyberodporności oraz zdolność do wykrywania szkodliwych działań w cyberprzestrzeni i reagowania na nie. Aby dobrze funkcjonować, podmioty Unii muszą zatem osiągnąć wysoki wspólny poziom cyberbezpieczeństwa dzięki wdrożeniu środków cyberbezpieczeństwa współmiernych do zidentyfikowanego ryzyka w cyberprzestrzeni, wymianie informacji i współpracy.

[1] Stanowisko Parlamentu Europejskiego z dnia 21 listopada 2023 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 8 grudnia 2023 r.

(5) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 ([2]) ma na celu dalszą poprawę cyberodporności podmiotów publicznych i prywatnych, właściwych organów i instytucji, jak również całej Unii, a także dalsze zwiększenie ich zdolności reagowania na incydenty. Należy zatem zapewnić, by podobnymi środkami objęto podmioty Unii poprzez ustanowienie przepisów zgodnych z dyrektywą (UE) 2022/2555 i odzwierciedlających przewidziany w niej poziom ambicji.

(6) Aby osiągnąć wysoki wspólny poziom cyberbezpieczeństwa, konieczne jest aby każdy podmiot Unii ustanowił wewnętrzne ramy zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli (zwane dalej „Ramami"), które umożliwią skuteczne i ostrożne zarządzanie wszelkiego rodzaju ryzykiem w cyberprzestrzeni, z uwzględnieniem ciągłości działania i zarządzania kryzysowego. w Ramach należy określić politykę w zakresie cyberbezpieczeństwa, w tym cele i priorytety, w odniesieniu do bezpieczeństwa sieci i systemów informatycznych, obejmującą całe jawne środowisko ICT. Ramy powinny być oparte na podejściu uwzględniającym wszystkie zagrożenia, które ma na celu ochronę sieci i systemów informatycznych oraz środowiska fizycznego tych sieci i systemów przed takimi zdarzeniami jak kradzież, pożar, powódź, awaria telekomunikacyjna bądź awaria zasilania lub nieuprawniony dostęp fizyczny do związanej z informacjami i przetwarzaniem informacji należącej do podmiotu Unii, jej uszkodzenie i ingerencja w nią, które to zdarzenia mogłyby naruszyć dostępność, autentyczność, integralność lub poufność danych przechowywanych, przekazywanych, przetwarzanych lub dostępnych za pośrednictwem sieci i systemów informatycznych.

(7) Do celów zarządzania ryzykiem w cyberprzestrzeni stwierdzonym dzięki Ramom każdy podmiot Unii powinien podjąć odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne. Środki te powinny dotyczyć poszczególnych dziedzin oraz środków zarządzania ryzykiem w cyberprzestrzeni określonych w niniejszym rozporządzeniu, aby wzmocnić cyberbezpieczeństwo każdego podmiotu Unii.

(8) Zasoby i ryzyko w cyberprzestrzeni zidentyfikowane dzięki Ramom, a także wnioski wyciągnięte z regularnych ocen dojrzałości w zakresie cyberbezpieczeństwa powinny zostać odzwierciedlone w planie dotyczącym cyberbezpieczeństwa ustanowionym przez każdy podmiot Unii. Plan dotyczący cyberbezpieczeństwa powinien obejmować przyjęte środki zarządzania ryzykiem w cyberprzestrzeni.

(9) Z racji tego, że dbanie o cyberbezpieczeństwo jest procesem ciągłym, adekwatność i skuteczność środków podejmowanych na mocy niniejszego rozporządzenia powinna być regularnie oceniana w świetle zmieniającego się ryzyka w cyberprzestrzeni oraz zmieniających się zasobów i dojrzałości podmiotów Unii w zakresie cyberbezpieczeństwa. Ramy powinny być poddawane regularnemu przeglądowi, co najmniej co cztery lata, natomiast plan dotyczący cyberbezpieczeństwa powinien być poddawany przeglądowi co dwa lata lub, w razie potrzeby, częściej w następstwie ocen dojrzałości w zakresie cyberbezpieczeństwa lub każdej istotnej zmiany Ram.

(10) Środki zarządzania ryzykiem w cyberprzestrzeni wprowadzone przez podmioty Unii powinny obejmować strategie mające na celu zapewnienie w miarę możliwości przejrzystości kodu źródłowego, z uwzględnieniem ochrony praw osób trzecich lub podmiotów Unii. Strategie te powinny być współmierne do ryzyka w cyberprzestrzeni i mają ułatwiać analizę cyberzagrożeń, nie nakładając jednocześnie obowiązku ujawniania kodu osoby trzeciej ani nie przyznając praw dostępu do niego w zakresie wykraczającym poza mające zastosowanie warunki umowne.

(11) Narzędzia i aplikacje z zakresu cyberbezpieczeństwa oparte na otwartym oprogramowaniu mogą przyczynić się do większej otwartości. Otwarte standardy ułatwiają interoperacyjność między narzędziami bezpieczeństwa z korzyścią dla bezpieczeństwa zainteresowanych stron. Narzędzia i aplikacje z zakresu cyberbezpieczeństwa oparte na otwartym oprogramowaniu mogą umożliwić pozyskanie szerszej społeczności programistów, co pozwoli na dywersyfikację dostawców. Otwarte oprogramowanie może prowadzić do bardziej przejrzystego procesu weryfikacji narzędzi związanych z cyberbezpieczeństwem oraz do kierowanego przez społeczność procesu wykrywania podatności. Podmioty Unii powinny zatem móc promować wykorzystywanie otwartego oprogramowania i otwartych standardów przez prowadzenie polityki związanej z wykorzystywaniem otwartych danych i otwartego oprogramowania na zasadzie bezpieczeństwa dzięki przejrzystości.

([2]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz.U. L 333 z 27.12.2022, s. 80).

(12) Zróżnicowanie podmiotów Unii wymaga elastyczności w procesie wdrażania niniejszego rozporządzenia. Środki na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa przewidziane w niniejszym rozporządzeniu nie powinny obejmować żadnych obowiązków bezpośrednio kolidujących z wykonywaniem przez podmioty Unii ich misji lub naruszających ich autonomię instytucjonalną. Dlatego podmioty te powinny ustanowić własne Ramy, a także przyjąć własne środki zarządzania ryzykiem w cyberprzestrzeni i plany dotyczące cyberbezpieczeństwa. Przy wdrażaniu takich środków należy odpowiednio uwzględnić istniejące synergie między podmiotami Unii, aby odpowiednio zarządzać zasobami oraz zoptymalizować koszty. Należy również zwrócić szczególną uwagę, by środki te nie oddziaływały negatywnie na sprawność wymiany informacji oraz współpracę między podmiotami Unii oraz między podmiotami Unii a ich odpowiednikami z państw członkowskich.

(13) Aby zoptymalizować wykorzystanie zasobów, w niniejszym rozporządzeniu należy przewidzieć możliwość współpracy dwóch lub większej liczby podmiotów Unii o podobnej strukturze przy przeprowadzaniu ich ocen dojrzałości w zakresie cyberbezpieczeństwa.

(14) Aby uniknąć nakładania nieproporcjonalnie dużych obciążeń finansowych i administracyjnych na podmioty Unii, wymogi w zakresie zarządzania ryzykiem w cyberprzestrzeni powinny być proporcjonalne do ryzyka w cyberprzestrzeni dla danych sieci i systemów informatycznych oraz powinny uwzględniać najnowszy stan wiedzy na temat takich środków. Każdy podmiot Unii powinien dążyć do przeznaczenia odpowiedniego odsetka swojego budżetu przewidzianego na ICT na poprawę swojego poziomu cyberbezpieczeństwa. w dłuższej perspektywie należy dążyć do osiągnięcia orientacyjnego celu w wysokości co najmniej 10 %. w ocenie dojrzałości w zakresie cyberbezpieczeństwa należy przeanalizować, czy wydatki danego podmiotu Unii na cyberbezpieczeństwo są proporcjonalne do ryzyka w cyberprzestrzeni, z jakim ten podmiot się mierzy. Bez uszczerbku dla przepisów dotyczących rocznego budżetu Unii na mocy traktatów, w swoim wniosku dotyczącym pierwszego budżetu rocznego, który ma zostać przyjęty po wejściu w życie niniejszego rozporządzenia, przy ocenie potrzeb budżetowych i kadrowych podmiotów Unii wynikających z ich preliminarza wydatków Komisja powinna uwzględnić obowiązki wynikające z niniejszego rozporządzenia.

(15) W celu osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa konieczne jest, by cyberbezpieczeństwo było objęte nadzorem kierownictwa najwyższego szczebla każdego podmiotu Unii. Kierownictwo najwyższego szczebla podmiotu Unii powinno być odpowiedzialne za wdrożenie niniejszego rozporządzenia, w tym za ustanowienie Ram, podejmowanie środków zarządzania ryzykiem w cyberprzestrzeni oraz zatwierdzanie planu dotyczącego cyberbezpieczeństwa. Uwzględnienie kultury cyberbezpieczeństwa, tj. codziennej praktyki w dziedzinie cyberbezpieczeństwa, jest nieodłączną częścią Ram oraz odpowiednich środków zarządzania ryzykiem w cyberprzestrzeni we wszystkich podmiotach Unii.

(16) Zasadnicze znaczenie ma bezpieczeństwo sieci i systemów informatycznych przetwarzających informacje niejawne UE (EUCI). Podmioty Unii, które przetwarzają EUCI, mają obowiązek stosowania kompleksowych ram regulacyjnych służących ochronie takich informacji, w tym szczególnych zasad zarządzania, polityk i procedur zarządzania ryzykiem. Sieci i systemy informatyczne przetwarzające EUCI muszą spełniać bardziej rygorystyczne normy bezpieczeństwa niż sieci i systemy i informatyczne przetwarzające informacje jawne. Dlatego sieci i systemy informatyczne przetwarzające EUCI są bardziej odporne na cyberzagrożenia i incydenty. w związku z tym, uznając potrzebę wspólnych ram w tym zakresie, niniejsze rozporządzenie nie powinno jednak mieć zastosowania do sieci i systemów informatycznych przetwarzających EUCI. Jednakże na wyraźny wniosek podmiotu Unii zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE) powinien mieć możliwość udzielenia temu podmiotowi Unii pomocy w związku z incydentami w niejawnych środowiskach ICT.

(17) Podmioty Unii powinny przeprowadzić ocenę ryzyka w cyberprzestrzeni związanego z relacjami z dostawcami i usługodawcami, w tym dostawcami usług przechowywania i przetwarzania danych lub usług zarządzanych w zakresie bezpieczeństwa, oraz wprowadzić odpowiednie środki w celu wyeliminowania tego ryzyka. Środki w zakresie cyberbezpieczeństwa powinny być szczegółowo określane w wytycznych lub zaleceniach wydawanych przez CERT-UE. Przy określaniu środków i wytycznych powinno się należycie uwzględniać stan wiedzy oraz, w stosownych przypadkach, odpowiednie normy europejskie i międzynarodowe, a także odpowiednie prawo Unii i strategie unijne, w tym oceny ryzyka w cyberprzestrzeni i zalecenia wydane przez Grupę Współpracy ustanowioną na mocy art. 14 dyrektywy (UE) 2022/2555, takie jak unijna skoordynowana ocena ryzyka cyberbezpieczeństwa sieci

5G i unijny zestaw narzędzi na potrzeby cyberbezpieczeństwa sieci 5G. Ponadto, biorąc pod uwagę krajobraz cyberzagrożeń i znaczenie budowania cyberodporności podmiotów Unii, można wprowadzić wymóg certyfikacji odpowiednich produktów, usług i procesów ICT zgodnie ze specjalnymi europejskimi programami certyfikacji cyberbezpieczeństwa przyjętymi na podstawie art. 49 rozporządzenia (UE) 2019/881 Parlamentu Europejskiego i Rady ([3]).

(18) W maju 2011 r. sekretarze generalni instytucji i organów Unii postanowili utworzyć zespół ds. wstępnej konfiguracji CERT-UE, pod nadzorem międzyinstytucjonalnej rady sterującej. w lipcu 2012 r. sekretarze generalni potwierdzili ustalenia praktyczne i zgodzili się co do utrzymania CERT-UE jako stałego podmiotu, tak aby dalej wspomagał poprawę ogólnego poziomu bezpieczeństwa technologii informacyjnej w instytucjach, organach i agencjach Unii jako przykład dostrzegalnej współpracy międzyinstytucjonalnej w dziedzinie cyberbezpieczeństwa. We wrześniu 2012 r. powołano CERT-UE jako grupę zadaniową Komisji z mandatem międzyinstytucjonalnym. w grudniu 2017 r. instytucje i organy Unii zawarły porozumienie międzyinstytucjonalne w sprawie organizacji i funkcjonowania CERT-UE ([4]). Niniejsze rozporządzenie powinno przewidywać kompleksowy zestaw przepisów dotyczących organizacji, funkcjonowania i działania CERT-UE. Przepisy niniejszego rozporządzenia mają pierwszeństwo przed postanowieniami porozumienia międzyinstytucjonalnego w sprawie organizacji i funkcjonowania CERT-UE, które zostało zawarte w grudniu 2017 r.

(19) Należy zmienić nazwę CERT-UE na Służbę ds. Cyberbezpieczeństwa Instytucji, Organów i Jednostek Organizacyjnych Unii, zachowując jednak skrót „CERT-UE" ze względu na jego rozpoznawalność.

(20) Oprócz powierzenia CERT-UE większej liczby zadań i rozszerzenia jego roli niniejsze rozporządzenie ustanawia Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa (IICB), w celu ułatwienia osiągnięcia wysokiego wspólnego poziomu cyberbezpieczeństwa przez podmioty Unii. IICB powinno posiadać wyłączny mandat do monitorowania i wspierania wdrażania niniejszego rozporządzenia przez podmioty Unii oraz do sprawowania nadzoru nad realizacją ogólnych priorytetów i celów przez CERT-UE i zapewniania CERT-UE strategicznego kierunku działania. IICB powinno zatem zagwarantować, że instytucje Unii będą należycie reprezentowane, a w jej skład powinni wchodzić przedstawiciele organów i jednostek organizacyjnych Unii za pośrednictwem sieci agencji UE (EUAN). Organizacja i funkcjonowanie IICB powinny być dodatkowo uregulowane poprzez regulamin wewnętrzny, który może obejmować dalsze doprecyzowanie kwestii regularnych posiedzeń IICB, w tym corocznych zgromadzeń na poziomie politycznym, podczas których dzięki obecności przedstawicieli kierownictwa najwyższego szczebla każdego z członków IICB można by prowadzić dyskusje strategiczne dotyczące IICB i formułować strategiczne wskazówki dla IICB. IICB powinno ponadto móc ustanowić komitet wykonawczy, który będzie wspierał IICB w jego pracach, oraz przekazać mu niektóre z zadań i uprawnień IICB, zwłaszcza w przypadku zadań wymagających szczególnej wiedzy fachowej jego członków, na przykład zatwierdzanie katalogu usług i jego późniejszych aktualizacji, warunków umów o gwarantowanym poziomie usług, ocen dokumentów i sprawozdań przedkładanych IICB przez podmioty Unii zgodnie z niniejszym rozporządzeniem lub zadań związanych z przygotowywaniem wydawanych przez IICB decyzji dotyczących środków zapewniania zgodności oraz z monitorowaniem ich wdrażania. IICB powinno ustanowić regulamin wewnętrzny komitetu wykonawczego, w tym jego zadania i uprawnienia.

(21) Celem IICB jest wspieranie podmiotów Unii w poprawie stanu ich cyberbezpieczeństwa poprzez wdrażanie niniejszego rozporządzenia. Aby wspierać podmioty Unii, IICB powinno udzielać wskazówek szefowi CERT-UE, przyjmować wieloletnią strategię podnoszenia poziomu cyberbezpieczeństwa w podmiotach Unii, ustanowić metodykę i inne aspekty dobrowolnych wzajemnych ocen oraz ułatwić ustanowienie nieformalnej grupy lokalnych urzędników ds. cyberbezpieczeństwa, wspieranej przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), w celu wymiany najlepszych praktyk i informacji w związku z wdrażaniem niniejszego rozporządzenia.

([3]) 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).

([4]) Porozumienie między Parlamentem Europejskim, Radą Europejską, Radą Unii Europejskiej, Komisją Europejską, Trybunałem Sprawiedliwości Unii Europejskiej, Europejskim Bankiem Centralnym, Europejskim Trybunałem Obrachunkowym, Europejską Służbą Działań Zewnętrznych, Europejskim Komitetem Ekonomiczno-Społecznym, Europejskim Komitetem Regionów i Europejskim Bankiem Inwestycyjnym w sprawie organizacji i funkcjonowania zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE) (Dz.U. C 12 z 13.1.2018, s. 1).

(22) Aby osiągnąć wysoki poziom cyberbezpieczeństwa we wszystkich podmiotach Unii, interesy organów i jednostek organizacyjnych Unii, które posiadają własne środowisko ICT, powinny być reprezentowane w IICB przez trzech przedstawicieli wyznaczonych przez EUAN. Bezpieczeństwo przetwarzania danych osobowych, a tym samym również ich cyberbezpieczeństwo, stanowi podstawę ochrony danych. w świetle synergii między ochroną danych a cyberbezpieczeństwem Europejski Inspektor Ochrony Danych powinien być reprezentowany w IICB jako podmiot Unii podlegający niniejszemu rozporządzeniu, dysponujący szczególną wiedzą fachową w dziedzinie ochrony danych, w tym bezpieczeństwa sieci łączności elektronicznej. Biorąc pod uwagę znaczenie innowacji i konkurencyjności w dziedzinie cyberbezpieczeństwa, w IICB powinno być reprezentowane Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa. z uwagi na rolę ENISA jako centrum wiedzy specjalistycznej w dziedzinie cyberbezpieczeństwa oraz wsparcie zapewniane przez ENISA, a także z uwagi na znaczenie cyberbezpieczeństwa unijnej infrastruktury kosmicznej i usług kosmicznych, w IICB powinny być reprezentowane ENISA i Agencja Unii Europejskiej ds. Programu Kosmicznego. w świetle roli przydzielonej CERT-UE na mocy niniejszego rozporządzenia szef CERT-UE powinien być zapraszany przez przewodniczącego IICB na wszystkie posiedzenia IICB, z wyjątkiem przypadków, w których IICB omawia kwestie związane bezpośrednio z szefem CERT-UE.

(23) IICB powinno monitorować przestrzeganie niniejszego rozporządzenia, jak również wdrażanie wytycznych i zaleceń oraz wezwań do działania. w kwestiach technicznych IICB powinny wspierać techniczne grupy doradcze działające w składzie, który IICB uzna za stosowny. Te techniczne grupy doradcze powinny ściśle współpracować z CERT-UE, podmiotami Unii oraz innymi zainteresowanymi stronami, jeżeli zajdzie taka potrzeba.

(24) W przypadku gdy IICB stwierdzi, że dany podmiot Unii nie wdrożył należycie niniejszego rozporządzenia lub wytycznych, zaleceń lub wezwań do działania wydanych na podstawie niniejszego rozporządzenia, IICB powinno mieć możliwość – bez uszczerbku dla wewnętrznych procedur danego podmiotu Unii – zastosowania środków zapewniania zgodności. IICB powinno stosować środki zapewniania zgodności stopniowo, tj. najpierw przyjąć najmniej surowy środek, mianowicie uzasadnioną opinię, oraz wyłącznie w razie potrzeby, przyjmować coraz bardziej rygorystyczne środki, aż po najpoważniejszy z nich, mianowicie zalecenie tymczasowego zawieszenia przepływu danych do danego podmiotu Unii. Takie zalecenie powinno być stosowane wyłącznie w wyjątkowych przypadkach długotrwałego, umyślnego, uporczywego lub poważnego naruszenia niniejszego rozporządzenia przez dany podmiot Unii.

(25) Uzasadniona opinia stanowi najmniej surowy środek zapewnienia zgodności mający na celu wyeliminowanie stwierdzonych luk we wdrażaniu niniejszego rozporządzenia. w nawiązaniu do uzasadnionej opinii IICB powinno mieć możliwość udzielenia wskazówek mających na celu wsparcie podmiotu Unii w zadbaniu o to, aby jego Ramy, środki zarządzania ryzykiem w cyberprzestrzeni, plan dotyczący cyberbezpieczeństwa i zgłaszanie incydentów były zgodne z niniejszym rozporządzeniem, a następnie wydania ostrzeżenia w celu wyeliminowania przez podmiot Unii stwierdzonych niedociągnięć w określonym terminie. Jeżeli niedociągnięcia wskazane w ostrzeżeniu nie zostaną w wystarczającym stopniu usunięte, IICB powinna mieć możliwość wydania uzasadnionego powiadomienia.

(26) IICB powinno móc zalecić przeprowadzenie audytu podmiotu Unii. Podmiot Unii powinien móc wykorzystać do tego celu własną jednostkę audytu wewnętrznego. IICB powinno również móc zażądać, by audyt został przeprowadzony przez zewnętrznego audytora, w tym przez wspólnie uzgodnionego dostawcę usług z sektora prywatnego.

(27) W wyjątkowych przypadkach długotrwałego, umyślnego, uporczywego lub poważnego naruszania niniejszego rozporządzenia przez podmiot Unii IICB powinno móc – jako ostateczny środek – wydać wszystkim państwom członkowskim i podmiotom Unii zalecenie, aby tymczasowo zawiesić przepływy danych do tego podmiotu Unii, dopóki nie zaprzestanie on tego naruszenia. Takie zalecenie powinno być przekazywane za pomocą odpowiednich i bezpiecznych kanałów komunikacji.

(28) Aby zapewnić prawidłowe wdrożenie niniejszego rozporządzenia, IICB powinno, jeżeli uzna, że naruszenie niniejszego rozporządzenia przez podmiot Unii, które miało charakter długotrwały, było spowodowane bezpośrednio działaniami lub zaniechaniami członka jego personelu, w tym członka kierownictwa najwyższego szczebla, zwrócić się do danego podmiotu Unii o podjęcie odpowiednich działań, w tym o rozważenie podjęcia działań o charakterze dyscyplinarnym, zgodnie z zasadami i procedurami określonymi w regulaminie pracowniczym urzędników Unii Europejskiej i warunkach zatrudnienia innych pracowników Unii Europejskiej, ustanowionym rozporządzeniem Rady (EWG, Euratom, EWWiS) nr 259/68 ([5]) (zwanym dalej „regulaminem pracowniczym") oraz z innymi mającymi zastosowanie przepisami i procedurami.

(29) CERT-UE powinien przyczyniać się do bezpieczeństwa środowiska ICT wszystkich podmiotów Unii. Rozważając, czy na wniosek podmiotu Unii zapewnić doradztwo techniczne lub wkład techniczny w odpowiednich kwestiach dotyczących polityki, CERT-UE powinien zapewnić, że nie będzie to stanowić żadnej przeszkody dla realizacji innych zadań powierzonych mu na mocy niniejszego rozporządzenia. CERT-UE powinien działać po stronie podmiotów Unii jako odpowiednik koordynatora wyznaczonego na potrzeby skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1 dyrektywy (UE) 2022/2555.

(30) CERT-UE powinien wspierać realizację działań na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa, przedstawiając propozycje wytycznych i zaleceń dla IICB lub wydając wezwania do działania. Takie wytyczne i zalecenia powinny być zatwierdzane przez IICB. w razie potrzeby CERT-UE powinien wydawać wezwania do działania opisujące pilne środki w zakresie bezpieczeństwa, do których wprowadzenia w określonym terminie wzywa się podmioty Unii. IICB powinno polecać CERT-UE wydawanie, wycofywanie lub zmianę propozycji wytycznych lub zaleceń lub wezwań do działania.

(31) CERT-UE powinien również wypełniać przewidzianą dla niego w dyrektywie (UE) 2022/2555 rolę dotyczącą współpracy i wymiany informacji z siecią zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), ustanowioną na mocy art. 15 tej dyrektywy. Ponadto, zgodnie z zaleceniem Komisji (UE) 2017/1584 ([6]), CERT-UE powinien współpracować z odpowiednimi zainteresowanymi stronami przy prowadzeniu działań podejmowanych w reakcji na incydenty oraz koordynować te działania. Aby przyczynić się do wysokiego poziomu cyberbezpieczeństwa w całej Unii, CERT-UE powinien prowadzić wymianę informacji dotyczących konkretnych incydentów ze swoimi odpowiednikami z państw członkowskich. CERT-UE powinien również współpracować z innymi odpowiednikami, zarówno publicznymi, jak i prywatnymi, w tym z Organizacją Traktatu Północnoatlantyckiego, pod warunkiem uzyskania uprzedniej zgody IICB.

(32) Wspierając cyberbezpieczeństwo na poziomie operacyjnym, CERT-UE powinien korzystać z dostępnej wiedzy fachowej ENISA w ramach ustrukturyzowanej współpracy przewidzianej w rozporządzeniu (UE) 2019/881. w stosownych przypadkach należy poczynić specjalne ustalenia między oboma podmiotami, aby określić sposób praktycznej realizacji takiej współpracy i uniknąć powielania działań. CERT-UE powinien współpracować z ENISA w obszarze analizy cyberzagrożeń i regularnie udostępniać ENISA swoje sprawozdanie dotyczące krajobrazu zagrożeń.

(33) CERT-UE powinien móc współpracować i prowadzić wymianę informacji z zainteresowanymi społecznościami zajmującymi się cyberbezpieczeństwem w Unii i w jej państwach członkowskich, aby wzmocnić współpracę operacyjną i umożliwić istniejącym sieciom wykorzystanie ich pełnego potencjału w zakresie ochrony Unii.

(34) Ponieważ usługi i zadania CERT-UE leżą w interesie podmiotów Unii, każdy podmiot Unii, który ponosi wydatki na ICT, powinien wnosić odpowiedni wkład na poczet kosztów tych usług i zadań. Wkład ten pozostaje bez uszczerbku dla autonomii budżetowej podmiotów Unii.

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

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

(35) Wiele cyberataków jest częścią szerszych kampanii, których celem są grupy podmiotów Unii lub wspólnoty interesów, do których należą podmioty Unii. Aby umożliwić aktywne wykrywanie incydentów, reagowanie na nie lub wprowadzanie środków ograniczających ryzyko, a także usuwanie skutków incydentów, podmioty Unii powinny móc powiadamiać CERT-UE o incydentach, cyberzagrożeniach, podatnościach i potencjalnych zdarzeniach dla cyberbezpieczeństwa oraz przekazywać odpowiednie szczegółowe informacje techniczne, które umożliwiają wykrycie lub ograniczenie ryzyka wystąpienia podobnych incydentów, cyberzagrożeń, podatności i potencjalnych zdarzeń dla cyberbezpieczeństwa w innych podmiotach Unii, a także reagowanie na nie. Kierując się podejściem przewidzianym w dyrektywie (UE) 2022/2555, należy nałożyć na podmioty Unii obowiązek przekazywania wczesnego ostrzeżenia do CERT-UE w ciągu 24 godzin od powzięcia wiedzy o znaczącym incydencie. Taka wymiana informacji powinna umożliwić CERT-UE rozpowszechnienie tej informacji wśród innych podmiotów Unii, jak również wśród ich właściwych odpowiedników, aby pomóc w ochronie środowisk ICT podmiotów Unii i ich odpowiedników przed podobnymi incydentami.

(36) W niniejszym rozporządzeniu określono wieloetapowe podejście do zgłaszania znaczących incydentów, aby zapewnić odpowiednią równowagę między szybkim zgłaszaniem, które pomaga zahamować potencjalne rozprzestrzenienie się znaczących incydentów i pozwala podmiotom Unii zwrócić się o pomoc, a szczegółowym zgłaszaniem, które umożliwia wyciągnięcie cennych wniosków z poszczególnych incydentów i z czasem poprawia cyberodporność poszczególnych podmiotów Unii, a także przyczynia się do ogólnej poprawy stanu ich cyberbezpieczeństwa. w tym względzie niniejsze rozporządzenie powinno obejmować zgłaszanie incydentów, które – w oparciu o wstępną ocenę przeprowadzoną przez dany podmiot Unii – mogą doprowadzić do dotkliwych zakłóceń operacyjnych w funkcjonowaniu bądź do strat finansowych dla tego podmiotu Unii lub też dotknąć inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe lub niemajątkowe. w takiej wstępnej ocenie należy wziąć pod uwagę między innymi sieci i systemy informatyczne, których dotyczy incydent, a w szczególności ich znaczenie dla funkcjonowania danego podmiotu Unii, dotkliwość i charakterystykę techniczną cyberzagrożenia oraz bazowe podatności, które są wykorzystywane, a także doświadczenie danego podmiotu Unii z podobnymi incydentami. Wskaźniki takie jak stopień, w jakim zakłócone jest funkcjonowanie podmiotu Unii, czas trwania incydentu lub liczba dotkniętych nim osób fizycznych lub prawnych, mogą odegrać ważną rolę w ustaleniu, czy zakłócenie operacyjne jest dotkliwe.

(37) Ponieważ infrastruktura oraz sieci i systemy informatyczne odpowiedniego podmiotu Unii i państwa członkowskiego, w którym znajduje się ten podmiot, są powiązane, kluczowe znaczenie ma, by to państwo członkowskie zostało bez zbędnej zwłoki poinformowane o wystąpieniu znaczącego incydentu w tym podmiocie Unii. w tym celu podmiot Unii, którego dotyczy incydent, powinien poinformować wszystkich właściwych odpowiedników z państw członkowskich wyznaczonych lub ustanowionych na podstawie art. 8 i 10 dyrektywy (UE) 2022/2555 o wystąpieniu znaczącego incydentu, który zgłasza on CERT-UE. w przypadku gdy CERT-UE dowie się o wystąpieniu znaczącego incydentu w danym państwie członkowskim, powinien on powiadomić właściwego odpowiednika w tym państwie członkowskim.

(38) Należy wdrożyć mechanizm zapewniający skuteczną wymianę informacji, koordynację i współpracę podmiotów Unii w przypadku poważnych incydentów, obejmujący wyraźne określenie ról i odpowiedzialności podmiotów Unii, których to dotyczy. Przedstawiciel Komisji w IICB powinien, z zastrzeżeniem planu zarządzania kryzysami w cyberprzestrzeni, być punktem kontaktowym ułatwiającym IICB wymianę istotnych informacji dotyczących poważnych incydentów z europejską siecią organizacji łącznikowych ds. kryzysów cyberbezpieczeństwa (EU-CyCLONe), wnosząc wkład we wspólną orientację sytuacyjną. Rola przedstawiciela Komisji w IICB jako punktu kontaktowego powinna pozostawać bez uszczerbku dla odrębnej i szczególnej roli Komisji w EU-CyCLONe zgodnie z art. 16 ust. 2 dyrektywy (UE) 2022/2555.

(39) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 ([7]) ma zastosowanie do przetwarzania danych osobowych na podstawie niniejszego rozporządzenia. Przetwarzanie danych osobowych może odbywać się w związku ze środkami przyjętymi w kontekście zarządzania ryzykiem w cyberprzestrzeni, postępowania w przypadku podatności i obsługi incydentów, wymiany informacji na temat incydentów, cyberzagrożeń i podatności oraz koordynacji i współpracy w zakresie reagowania na incydenty. Takie środki mogą wymagać przetwarzania niektórych kategorii danych osobowych, takich jak adresy IP, adresy URL, nazwy domen, adresy poczty elektronicznej, role organizacyjne osoby, której dane dotyczą, znaczniki czasu, przedmioty korespondencji za pośrednictwem

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

poczty elektronicznej lub nazwy plików. Wszystkie środki podejmowane na podstawie niniejszego rozporządzenia powinny być zgodne z ramami ochrony danych i prywatności, a podmioty Unii, CERT-UE i, w stosownych przypadkach, IICB powinny wprowadzić wszelkie odpowiednie zabezpieczenia techniczne i organizacyjne w celu zapewnienia takiej zgodności w sposób rozliczalny.

(40) Niniejsze rozporządzenie ustanawia podstawę prawną przetwarzania danych osobowych przez podmioty Unii, CERT-UE oraz, w stosownych przypadkach, IICB do celów wykonywania ich zadań i wypełniania obowiązków wynikających z niniejszego rozporządzenia, zgodnie z art. 5 ust. 1 lit. b) rozporządzenia (UE) 2018/1725. CERT-UE może działać jako podmiot przetwarzający lub administrator w zależności od zadań, które wykonuje na podstawie rozporządzenia (UE) 2018/1725.

(41) W niektórych przypadkach, aby wypełnić obowiązki wynikające z niniejszego rozporządzenia w celu zapewnienia wysokiego poziomu cyberbezpieczeństwa, w szczególności w kontekście postępowania w przypadku podatności i obsługi incydentów, podmioty Unii i CERT-UE mogą mieć obowiązek przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 10 ust. 1 rozporządzenia (UE) 2018/1725. Niniejsze rozporządzenie ustanawia podstawę prawną przetwarzania szczególnych kategorii danych osobowych przez podmioty Unii i CERT-UE zgodnie z art. 10 ust. 2 lit. g) rozporządzenia (UE) 2018/1725. Przetwarzanie szczególnych kategorii danych osobowych na podstawie niniejszego rozporządzenia powinno być ściśle proporcjonalne do zamierzonego celu. z zastrzeżeniem warunków określonych w art. 10 ust. 2 lit. g) tego rozporządzenia podmioty Unii i CERT-UE powinny mieć możliwość przetwarzania takich danych wyłącznie w niezbędnym zakresie i w przypadkach wyraźnie przewidzianych w niniejszym rozporządzeniu. Przetwarzając szczególne kategorie danych osobowych, podmioty Unii i CERT-UE powinny przestrzegać istoty prawa do ochrony danych oraz przewidzieć odpowiednie i konkretne środki ochrony praw podstawowych i interesów osób, których dane dotyczą.

(42) Na mocy art. 33 rozporządzenia (UE) 2018/1725 podmioty Unii i CERT-UE powinny, uwzględniając stan wiedzy, koszty wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw i wolności osób fizycznych o różnym prawdopodobieństwie i wadze, wdrożyć odpowiednie środki techniczne i organizacyjne zapewniające odpowiedni poziom bezpieczeństwa danych osobowych, takie jak ograniczenie praw dostępu w oparciu o zasadę wiedzy koniecznej, stosowanie zasad ścieżki audytu, przyjęcie łańcucha kontroli, przechowywanie danych w kontrolowanym środowisku podlegającym audytowi, znormalizowane procedury operacyjne i środki ochrony prywatności, takie jak pseudonimizacja lub szyfrowanie. Środków tych nie należy wdrażać w sposób mający wpływ na cele obsługi incydentu i na rzetelność dowodów. w przypadku gdy podmiot Unii lub CERT-UE przekazuje dane osobowe związane z incydentem, w tym szczególne kategorie danych osobowych, odpowiednikowi lub partnerowi do celów niniejszego rozporządzenia, takie przekazywanie powinno być zgodne z rozporządzeniem (UE) 2018/1725. w przypadku gdy szczególne kategorie danych osobowych są przekazywane osobie trzeciej, podmioty Unii i CERT-UE powinny zapewnić stosowanie przez tę osobę trzecią środków dotyczących ochrony danych osobowych na poziomie równoważnym z rozporządzeniem (UE) 2018/1725.

(43) Dane osobowe przetwarzane do celów niniejszego rozporządzenia powinny być zatrzymywane jedynie tak długo, jak jest to konieczne zgodnie z rozporządzeniem (UE) 2018/1725. Podmioty Unii oraz, w stosownych przypadkach, CERT-UE, działając w roli administratora, powinny ustalić okresy zatrzymywania danych, które są ograniczone do tego, co jest konieczne do osiągnięcia określonych celów. w szczególności w odniesieniu do danych osobowych gromadzonych na potrzeby obsługi incydentów podmioty Unii i CERT-UE powinny dokonywać rozróżnienia między danymi osobowymi, które są gromadzone w celu wykrywania cyberzagrożeń w ich środowiskach ICT, aby zapobiec incydentowi, a danymi osobowymi, które są gromadzone w celu złagodzenia lub usunięcia skutków incydentu bądź zareagowania na niego. w przypadku wykrywania cyberzagrożeń należy wziąć pod uwagę czas, przez jaki agresor może pozostać niewykryty w systemie. w przypadku łagodzenia lub usuwania skutków incydentu bądź reagowania na niego należy rozważyć, czy dane osobowe są niezbędne do śledzenia i obsługi powtarzających się incydentów lub incydentów o podobnym charakterze, w przypadku których można wykazać korelację.

(44) Postępowanie z informacjami przez podmioty Unii oraz CERT-UE powinno być zgodne z mającymi zastosowanie przepisami dotyczącymi bezpieczeństwa informacji. Uwzględnienie bezpieczeństwa zasobów ludzkich wśród środków zarządzania ryzykiem w cyberprzestrzeni powinno być również zgodne z mającymi zastosowanie przepisami.

(45) Do celu udostępniania informacji stosuje się widoczne oznaczenia wskazujące, że odbiorcy tych informacji mają stosować granice udostępniania w oparciu, w szczególności, o umowy o zachowanie poufności lub nieformalne ustalenia dotyczące zachowania poufności, takie jak kod poufności TLP lub inne wyraźne oznaczenia ustalone przez źródło danych. Kod poufności TLP należy rozumieć jako narzędzie służące informowaniu o ograniczeniach w dalszym rozpowszechnianiu informacji. Jest on wykorzystywany niemal we wszystkich CSIRT oraz w niektórych ośrodkach analizy i wymiany informacji.

(46) Niniejsze rozporządzenie należy poddawać regularnej ocenie w świetle przyszłych negocjacji dotyczących wieloletnich ram finansowych umożliwiających podjęcie dalszych decyzji w odniesieniu do funkcjonowania i roli instytucjonalnej CERT-UE, w tym ewentualnego ustanowienia CERT-UE jako urzędu Unii.

(47) IICB, z pomocą CERT-UE, powinno dokonywać przeglądu i oceny wdrażania niniejszego rozporządzenia oraz przedkładać Komisji sprawozdania zawierające jej ustalenia. Na tej podstawie Komisja powinna przedkładać sprawozdania Parlamentowi Europejskiemu, Radzie, Europejskiemu Komitetowi Ekonomiczno-Społecznemu i Komitetowi Regionów. Sprawozdania te, przygotowywane przy udziale IICB, powinny zawierać ocenę stosowności włączenia sieci i systemów informatycznych przetwarzających EUCI, do zakresu stosowania niniejszego rozporządzenia, w szczególności w przypadku braku wspólnych dla podmiotów Unii przepisów dotyczących bezpieczeństwa informacji.

(48) Zgodnie z zasadą proporcjonalności konieczne i stosowne jest przyjęcie przepisów dotyczących cyberbezpieczeństwa dla podmiotów Unii, aby osiągnąć podstawowy cel, jakim jest osiągnięcie ogólnie wysokiego wspólnego poziomu cyberbezpieczeństwa w podmiotach Unii. Niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia założonego celu, zgodnie z art. 5 ust. 4 Traktatu o Unii Europejskiej.

(49) Niniejsze rozporządzenie odzwierciedla fakt, że podmioty Unii różnią się pod względem wielkości i zdolności, w tym pod względem zasobów finansowych i ludzkich.

(50) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 17 maja 2022 r. ([8]),

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot

Niniejszym rozporządzeniem ustanawia się środki mające na celu osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa w podmiotach Unii w odniesieniu do:

a) ustanowienia przez każdy podmiot Unii wewnętrznych ram zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli zgodnie z art. 6;

b) zarządzania ryzykiem w cyberprzestrzeni, zgłaszania incydentów i wymiany informacji;

c) organizacji, funkcjonowania i działania Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa ustanowionej na mocy art. 10, a także organizacji, funkcjonowania i działania Służby ds. Cyberbezpieczeństwa Instytucji, Organów i Jednostek Organizacyjnych Unii (CERT-UE);

d) monitorowania wdrażania niniejszego rozporządzenia.

([8]) Dz.U. C 258 z 5.7.2022, s. 10.

Artykuł 2

Zakres

1. Niniejsze rozporządzenie stosuje się do podmiotów Unii, do Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa ustanowionej na mocy art. 10 oraz do CERT-UE.

2. Niniejsze rozporządzenie stosuje się bez uszczerbku dla autonomii instytucjonalnej wynikającej z Traktatów.

3. Z wyjątkiem art. 13 ust. 8 niniejszego rozporządzenia nie stosuje się do sieci i systemów informatycznych przetwarzających informacje niejawne UE (EUCI).

Artykuł 3

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „podmioty Unii" oznaczają instytucje, organy i jednostki administracyjne Unii ustanowione Traktatem o Unii Europejskiej, Traktatem o funkcjonowaniu Unii Europejskiej (TFUE) lub Traktatem ustanawiającym Europejską Wspólnotę Energii Atomowej lub na podstawie tych traktatów;

2) „sieci i systemy informatyczne" oznaczają sieci i systemy informatyczne zdefiniowane w art. 6 pkt 1 dyrektywy (UE) 2022/2555;

3) „bezpieczeństwo sieci i systemów informatycznych" oznacza bezpieczeństwo sieci i systemów informatycznych zdefiniowane w art. 6 pkt 2 dyrektywy (UE) 2022/2555;

4) „cyberbezpieczeństwo" oznacza cyberbezpieczeństwo zdefiniowane w art. 2 pkt 1 rozporządzenia (UE) 2019/881;

5) „kierownictwo najwyższego szczebla" oznacza kierownika odpowiedzialnego, organ zarządzający lub organ ds. koordynacji i nadzoru odpowiedzialne za funkcjonowanie danego podmiotu Unii na najwyższym szczeblu administracyjnym, uprawnionego lub uprawnione do przyjmowania lub zatwierdzania decyzji zgodnie z ustaleniami dotyczącymi zarządzania na wysokim szczeblu danego podmiotu Unii, bez uszczerbku dla formalnych obowiązków innych szczebli kierownictwa w zakresie zgodności i zarządzania ryzykiem w cyberprzestrzeni w ramach ich odpowiednich kompetencji;

6) „potencjalne zdarzenie dla cyberbezpieczeństwa" oznacza potencjalne zdarzenie dla cyberbezpieczeństwa zdefiniowane w art. 6 pkt 5 dyrektywy (UE) 2022/2555;

7) „incydent" oznacza incydent zdefiniowany w art. 6 pkt 6 dyrektywy (UE) 2022/2555;

8) „poważny incydent" oznacza incydent, który powoduje zakłócenie o stopniu przekraczającym zdolność reagowania podmiotu Unii i CERT-UE lub który ma znaczący wpływ na co najmniej dwa podmioty Unii;

9) „incydent w cyberbezpieczeństwie na dużą skalę" oznacza incydent w cyberbezpieczeństwie na dużą skalę zdefiniowany w art. 6 pkt 7 dyrektywy (UE) 2022/2555;

10) „obsługa incydentu" oznacza obsługę incydentu zdefiniowaną w art. 6 pkt 8 dyrektywy (UE) 2022/2555;

11) „cyberzagrożenie" oznacza cyberzagrożenie zdefiniowane w art. 2 pkt 8 rozporządzenia (UE) 2019/881;

12) „poważne cyberzagrożenie" oznacza poważne cyberzagrożenie zdefiniowane w art. 6 pkt 11 dyrektywy (UE) 2022/2555;

13) „podatność" oznacza podatność zdefiniowaną w art. 6 pkt 15 dyrektywy (UE) 2022/2555;

14) „ryzyko w cyberprzestrzeni" oznacza ryzyko zdefiniowane w art. 6 pkt 9 dyrektywy (UE) 2022/2555;

15) „usługa chmurowa" oznacza usługę chmurową zdefiniowaną w art. 6 pkt 30 dyrektywy (UE) 2022/2555.

Artykuł 4

Przetwarzanie danych osobowych

1. Przetwarzanie danych osobowych na podstawie niniejszego rozporządzenia przez CERT-UE, Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa ustanowioną na mocy art. 10 i podmioty Unii odbywa się zgodnie z rozporządzeniem (UE) 2018/1725.

2. Realizując zadania lub wypełniając obowiązki wynikające z niniejszego rozporządzenia, CERT-UE, Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa ustanowiona na mocy art. 10 oraz podmioty Unii przetwarzają i wymieniają dane osobowe wyłącznie w niezbędnym zakresie i wyłącznie w celu realizacji tych zadań lub wypełniania tych obowiązków.

3. Przetwarzanie szczególnych kategorii danych osobowych, o którym mowa w art. 10 ust. 1 rozporządzenia (UE) 2018/1725, uznaje się za konieczne ze względów związanych z ważnym interesem publicznym zgodnie z art. 10 ust. 2 lit. g) tego rozporządzenia. Takie dane można przetwarzać wyłącznie w zakresie niezbędnym do wdrożenia środków zarządzania ryzykiem w cyberprzestrzeni, o których mowa w art. 6 i 8, do świadczenia usług przez CERT-UE na podstawie art. 13, do wymiany informacji dotyczących poszczególnych incydentów na podstawie art. 17 ust. 3 i art. 18 ust. 3, do wymiany informacji na podstawie art. 20, do wypełnienia obowiązków w zakresie zgłaszania incydentów na podstawie art. 21, do koordynacji reagowania na incydenty i współpracy na podstawie art. 22 oraz do zarządzania poważnymi incydentami na podstawie art. 23 niniejszego rozporządzenia. Podmioty Unii i CERT-UE, działając w charakterze administratorów danych, stosują środki techniczne zapobiegające przetwarzaniu szczególnych kategorii danych osobowych do innych celów oraz zapewniają odpowiednie i konkretne środki ochrony praw podstawowych i interesów osób, których dane dotyczą.

ROZDZIAŁ II

ŚRODKI NA RZECZ WYSOKIEGO WSPÓLNEGO POZIOMU CYBERBEZPIECZEŃSTWA

Artykuł 5

Wdrożenie środków

1. Do dnia 8 września 2024 r. Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa ustanowiona na mocy art. 10, po konsultacji z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) i po otrzymaniu wskazówek od CERT-UE, wyda podmiotom Unii wytyczne do celów przeprowadzenia wstępnej analizy cyberbezpieczeństwa i ustanowienia wewnętrznych ram zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli zgodnie z art. 6, przeprowadzania ocen dojrzałości w zakresie cyberbezpieczeństwa na podstawie art. 7, stosowania środków zarządzania ryzykiem w cyberprzestrzeni na podstawie art. 8 oraz przyjęcia planu dotyczącego cyberbezpieczeństwa na podstawie art. 9.

2. Wdrażając art. 6–9, podmioty Unii uwzględniają wytyczne, o których mowa w ust. 1 niniejszego artykułu, a także odpowiednie wytyczne i zalecenia przyjęte na podstawie art. 11 i 14.

Artykuł 6

Ramy zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli

1. Do dnia 8 kwietnia 2025 r. każdy podmiot Unii, po przeprowadzeniu wstępnej analizy cyberbezpieczeństwa, takiej jak audyt, ustanawia wewnętrzne ramy zarządzania ryzykiem w cyberprzestrzeni, jego nadzorowania i kontroli (zwane dalej „Ramami"). Ustanowienie Ram nadzoruje kierownictwo najwyższego szczebla podmiotu Unii, które ponosi za nie odpowiedzialność.

2. Ramy obejmują swym zakresem całość jawnego środowiska ICT danego podmiotu Unii (zwanego dalej „środowiskiem ICT"), w tym każde środowisko ICT i sieć technologii operacyjnej znajdujące się w obiektach tego podmiotu, wszelkie aktywa i usługi, które przekazano w ramach outsourcingu do środowisk przetwarzania w chmurze lub których hosting prowadzą strony trzecie, a także urządzenia mobilne, sieci instytucjonalne, sieci biznesowe niepodłączone do internetu oraz wszelkie urządzenia podłączone do tych środowisk. Ramy opierają się na podejściu uwzględniającym wszystkie zagrożenia.

3. Ramy muszą zapewniać wysoki poziom cyberbezpieczeństwa. Ramy określają wewnętrzną politykę w zakresie cyberbezpieczeństwa, w tym cele i priorytety, w odniesieniu do bezpieczeństwa sieci i systemów informatycznych, a także role i obowiązki członków personelu podmiotu Unii, których zadaniem jest zapewnienie skutecznego wdrożenia niniejszego rozporządzenia. Ramy obejmują również mechanizmy pomiaru skuteczności wdrażania.

4. Ramy poddaje się regularnemu przeglądowi w świetle ewolucji ryzyka w cyberprzestrzeni i co najmniej raz na cztery lata. w stosownych przypadkach i na wniosek Międzyinstytucjonalnej Rady ds. Cyberbezpieczeństwa ustanowionej na mocy art. 10 Ramy podmiotu Unii mogą być aktualizowane w oparciu o wskazówki od CERT-UE dotyczące zidentyfikowanych incydentów lub zaobserwowanych ewentualnych luk we wdrażaniu niniejszego rozporządzenia.

5. Kierownictwo najwyższego szczebla każdego podmiotu Unii odpowiada za wdrażanie niniejszego rozporządzenia i nadzoruje wypełnianie przez jego struktury obowiązków związanych z Ramami.

6. W stosownych przypadkach i bez uszczerbku dla swojej odpowiedzialności za wdrażanie niniejszego rozporządzenia kierownictwo najwyższego szczebla każdego podmiotu Unii może przekazać określone obowiązki wynikające z niniejszego rozporządzenia urzędnikom wyższego szczebla w rozumieniu art. 29 ust. 2 regulaminu pracowniczego lub innym urzędnikom na równoważnym szczeblu w danym podmiocie Unii. Niezależnie od takiego przekazania obowiązków dany podmiot Unii może pociągnąć kierownictwo najwyższego szczebla do odpowiedzialności za naruszenia niniejszego rozporządzenia.

7. Każdy podmiot Unii musi posiadać skuteczne mechanizmy zapewniające, aby odpowiedni odsetek budżetu przewidzianego na ICT był przeznaczany na cyberbezpieczeństwo. Przy ustalaniu tego odsetka należy odpowiednio uwzględnić Ramy.

8. Każdy podmiot Unii wyznacza lokalnego urzędnika ds. cyberbezpieczeństwa lub osobę pełniącą równoważną funkcję, która działa jako pojedynczy punkt kontaktowy tego podmiotu w odniesieniu do wszystkich kwestii związanych z cyberbezpieczeństwem. Lokalny urzędnik ds. cyberbezpieczeństwa ułatwia wdrażanie niniejszego rozporządzenia i regularnie składa sprawozdania na temat stanu wdrożenia bezpośrednio kierownictwu najwyższego szczebla. Bez uszczerbku dla pełnionej przez lokalnego urzędnika ds. cyberbezpieczeństwa funkcji pojedynczego punktu kontaktowego w każdym podmiocie Unii, podmiot Unii może przekazać CERT-UE niektóre zadania lokalnego urzędnika ds. cyberbezpieczeństwa związane z wdrażaniem niniejszego rozporządzenia na podstawie umowy o gwarantowanym poziomie usług zawartej między tym podmiotem Unii a CERT-UE lub zadaniami tymi może podzielić się kilka podmiotów Unii. Jeżeli zadania te przekazuje się CERT-UE, Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa ustanowiona na mocy art. 10 decyduje, czy świadczenie tej usługi ma być częścią podstawowych usług CERT-UE, uwzględniając zasoby ludzkie i finansowe danego podmiotu Unii. Każdy podmiot Unii bez zbędnej zwłoki powiadamia CERT-UE o wyznaczeniu lokalnego urzędnika ds. cyberbezpieczeństwa oraz wszelkich zmianach w tym zakresie.

CERT-UE tworzy i aktualizuje listę wyznaczonych lokalnych urzędników ds. cyberbezpieczeństwa.

9. Urzędnicy wyższego szczebla w rozumieniu art. 29 ust. 2 regulaminu pracowniczego lub inni urzędnicy na równoważnym szczeblu w każdym podmiocie Unii, a także wszyscy odpowiedni członkowie personelu, których zadaniem jest wdrażanie środków i wypełnianie obowiązków w zakresie zarządzania ryzykiem w cyberprzestrzeni określonych w niniejszym rozporządzeniu, regularnie uczestniczą w specjalnych szkoleniach, aby zdobyć wystarczającą wiedzę i wystarczające umiejętności umożliwiające zrozumienie i ocenę ryzyka w cyberprzestrzeni i praktyk zarządzania nim oraz ich wpływu na działalność danego podmiotu Unii.

Artykuł 7

Oceny dojrzałości w zakresie cyberbezpieczeństwa

1. Do dnia 8 lipca 2025 r., a następnie co najmniej raz na dwa lata każdy podmiot Unii przeprowadza ocenę dojrzałości w zakresie cyberbezpieczeństwa, obejmującą wszystkie elementy jego środowiska ICT.

2. Oceny dojrzałości w zakresie cyberbezpieczeństwa przeprowadza się w stosownych przypadkach przy pomocy wyspecjalizowanej osoby trzeciej.

3. Podmioty Unii o podobnej strukturze mogą współpracować przy przeprowadzaniu swoich ocen dojrzałości w zakresie cyberbezpieczeństwa.

4. Na podstawie wniosku Międzynarodowej Rady ds. Cyberbezpieczeństwa ustanowionej na mocy art. 10 i za wyraźną zgodą zainteresowanego podmiotu Unii wyniki oceny dojrzałości w zakresie cyberbezpieczeństwa mogą być omawiane w ramach tej rady lub w ramach nieformalnej grupy lokalnych urzędników ds. cyberbezpieczeństwa w celu wyciągnięcia wniosków z doświadczeń oraz wymiany najlepszych praktyk.

Artykuł 8

Środki zarządzania ryzykiem w cyberprzestrzeni

1. Bez zbędnej zwłoki, a w każdym razie do dnia 8 września 2025 r. każdy podmiot Unii pod nadzorem swojego kierownictwa najwyższego szczebla podejmuje odpowiednie i proporcjonalne środki techniczne, operacyjne i organizacyjne, aby zarządzać ryzykiem w cyberprzestrzeni zidentyfikowanym na podstawie Ram oraz aby zapobiec incydentom lub zminimalizować ich skutki. Przy uwzględnieniu najnowszego stanu wiedzy, oraz, w stosownych przypadkach, odpowiednich norm europejskich i międzynarodowych, środki te zapewniają poziom bezpieczeństwa sieci i systemów informatycznych w całym środowisku ICT odpowiedni do istniejącego ryzyka w cyberprzestrzeni. Oceniając proporcjonalność tych środków należycie uwzględnia się stopień narażenia podmiotu Unii na ryzyko w cyberprzestrzeni, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów i ich dotkliwość, w tym ich skutki społeczne, gospodarcze i międzyinstytucjonalne.

2. Wdrażając środki zarządzania ryzykiem w cyberprzestrzeni, podmioty Unii uwzględniają co najmniej następujące kwestie:

a) politykę w zakresie cyberbezpieczeństwa, w tym środki niezbędne do osiągnięcia celów i priorytetów, o których mowa w art. 6 i w ust. 3 niniejszego artykułu;

b) politykę analizy ryzyka w cyberprzestrzeni i bezpieczeństwa systemów informatycznych;

c) cele strategiczne w zakresie korzystania z usług chmurowych;

d) w stosownych przypadkach audyt cyberbezpieczeństwa, który może obejmować ocenę ryzyka w cyberprzestrzeni, podatności i cyberzagrożeń oraz testy penetracyjne przeprowadzane regularnie przez zaufanego usługodawcę z sektora prywatnego;

e) wdrożenie zaleceń wynikających z audytów cyberbezpieczeństwa, o których mowa w lit. d), w drodze aktualizacji zasad dotyczących cyberbezpieczeństwa i aktualizacji polityk;

f) kwestie organizacyjne dotyczące cyberbezpieczeństwa, w tym wyznaczenie ról i obowiązków;

g) zarządzanie aktywami, w tym rejestr zasobów ICT i mapy sieci ICT;

h) bezpieczeństwo zasobów ludzkich i kontrolę dostępu;

i) bezpieczeństwo operacji;

j) bezpieczeństwo łączności;

k) nabywanie, rozbudowę i utrzymywanie systemów, w tym polityki postępowania z podatnościami i ich ujawniania;

l) w miarę możliwości politykę dotyczącą przejrzystości kodu źródłowego;

m) bezpieczeństwo łańcucha dostaw, w tym aspekty związane z bezpieczeństwem relacji między każdym podmiotem Unii a jego bezpośrednimi dostawcami lub usługodawcami;

n) obsługę incydentów oraz współpracę z CERT-UE, na przykład stałe monitorowanie bezpieczeństwa i rejestrowanie danych związanych z bezpieczeństwem;

o) zarządzanie ciągłością działania, na przykład zarządzanie kopiami zapasowymi i przywracanie normalnego działania po wystąpieniu sytuacji nadzwyczajnej, i zarządzanie kryzysowe; oraz

p) promowanie i rozwój programów edukowania, rozwijania umiejętności, podnoszenia świadomości, ćwiczeń i szkoleń w dziedzinie cyberbezpieczeństwa.

Do celów akapitu pierwszego lit. m) podmioty Unii uwzględniają podatności charakterystyczne dla każdego bezpośredniego dostawcy i usługodawcy oraz ogólną jakość produktów i praktyk w zakresie cyberbezpieczeństwa stosowanych przez ich dostawców i usługodawców, w tym ich procedury bezpiecznego opracowywania.

3. Podmioty Unii stosują co najmniej następujące szczegółowe środki zarządzania ryzykiem w cyberprzestrzeni:

a) rozwiązania techniczne umożliwiające pracę zdalną i jej utrzymanie;

b) konkretne kroki zmierzające do przejścia na zasady zerowego zaufania;

c) stosowanie uwierzytelniania wieloskładnikowego jako normy we wszystkich sieciach i systemach informatycznych;

d) wykorzystywanie kryptografii i szyfrowania, w szczególności szyfrowania end-to-end, oraz bezpiecznego podpisu cyfrowego;

e) w stosownych przypadkach bezpieczne systemy łączności głosowej, wizualnej i tekstowej oraz bezpieczne systemy łączności w sytuacjach nadzwyczajnych wewnątrz podmiotu Unii;

f) proaktywne środki wykrywania i usuwania złośliwego oprogramowania i oprogramowania szpiegującego;

g) zabezpieczenie łańcucha dostaw oprogramowania poprzez kryteria regulujące opracowywanie i ocenę bezpiecznego oprogramowania;

h) tworzenie i przyjmowanie programów szkoleń w zakresie cyberbezpieczeństwa dla kierownictwa najwyższego szczebla i członków personelu podmiotu Unii, którym powierzono zadanie zapewnienia skutecznego wdrożenia niniejszego rozporządzenia, przy czym te programy szkoleń muszą być współmierne do przewidzianych zadań i oczekiwanych zdolności;

i) regularne szkolenia z zakresu cyberbezpieczeństwa dla członków personelu;

j) w stosownych przypadkach udział w analizach ryzyka dla wzajemnych połączeń między podmiotami Unii;

k) wzmocnienie zasad udzielania zamówień publicznych, aby ułatwić osiągnięcie wysokiego wspólnego poziomu cyberbezpieczeństwa poprzez:

   (i) usunięcie barier umownych, które ograniczają wymianę pochodzących od dostawców usług ICT informacji na temat incydentów, podatności i cyberzagrożeń z CERT-UE;

   (ii) zobowiązania umowne do zgłaszania incydentów, podatności i cyberzagrożeń, a także do ustanowienia odpowiedniego mechanizmu reagowania na incydenty i ich monitorowania.

Artykuł 9

Plany dotyczące cyberbezpieczeństwa

1. Zgodnie z wnioskami z oceny dojrzałości w zakresie cyberbezpieczeństwa przeprowadzonej na podstawie art. 7, a także z uwzględnieniem aktywów i ryzyka w cyberprzestrzeni zidentyfikowanych dzięki Ramom oraz środków zarządzania ryzykiem w cyberprzestrzeni przyjętych na podstawie art. 8 kierownictwo najwyższego szczebla każdego podmiotu Unii zatwierdza – bez zbędnej zwłoki, a w każdym razie do dnia 8 stycznia 2026 r. – plan dotyczący cyberbezpieczeństwa. Plan dotyczący cyberbezpieczeństwa ma na celu zwiększenie ogólnego poziomu cyberbezpieczeństwa danego podmiotu Unii, a tym samym przyczynia się do zwiększenia wysokiego wspólnego poziomu cyberbezpieczeństwa wewnątrz podmiotów Unii. Plan dotyczący cyberbezpieczeństwa obejmuje co najmniej środki zarządzania ryzykiem w cyberprzestrzeni podjęte na podstawie art. 8. Plan dotyczący cyberbezpieczeństwa poddaje się przeglądowi co dwa lata lub, w razie potrzeby, częściej w następstwie ocen dojrzałości w zakresie cyberbezpieczeństwa przeprowadzonej na podstawie art. 7 lub każdej istotnej zmiany Ram.

2. Plan dotyczący cyberbezpieczeństwa zawiera opracowany przez podmiot Unii plan zarządzania kryzysami w cyberprzestrzeni na wypadek poważnych incydentów.

3. Podmiot Unii przedkłada gotowy plan dotyczący cyberbezpieczeństwa Międzyinstytucjonalnej Radzie ds. Cyberbezpieczeństwa ustanowionej na mocy art. 10.

ROZDZIAŁ III

MIĘDZYINSTYTUCJONALNA RADA DS. CYBERBEZPIECZEŃSTWA

Artykuł 10

Międzyinstytucjonalna Rada ds. Cyberbezpieczeństwa

1. Niniejszym ustanawia się Międzyinstytucjonalną Radę ds. Cyberbezpieczeństwa (IICB).

2. IICB jest odpowiedzialne za:

a) monitorowanie i wspieranie wdrażania niniejszego rozporządzenia przez podmioty Unii;

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

3. W skład IICB wchodzą:

a) po jednym przedstawicielu wyznaczonym przez:

(i) Parlament Europejski;

(ii) Radę Europejską;

(iii) Radę Unii Europejskiej;

(iv) Komisję;

(v) Trybunał Sprawiedliwości Unii Europejskiej;

(vi) Europejski Bank Centralny;

(vii) Trybunał Obrachunkowy;

(viii) Europejską Służbę Działań Zewnętrznych;

(ix) Europejski Komitet Ekonomiczno-Społeczny,

(x) Europejski Komitet Regionów;

(xi) Europejski Bank Inwestycyjny;

(xii) Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa;

(xiii) ENISA;

(xiv) Europejskiego Inspektora Ochrony Danych (EIOD);

(xv) Agencję Unii Europejskiej ds. Programu Kosmicznego;

b) trzech przedstawicieli wyznaczonych przez sieć agencji UE (EUAN) na wniosek jej komitetu doradczego ds. ICT w celu reprezentowania interesów organów i jednostek organizacyjnych Unii, które mają własne środowisko ICT, innych niż te, o których mowa w lit. a).

Podmioty Unii reprezentowane w IICB dążą do osiągnięcia równowagi płci wśród wyznaczonych przedstawicieli.

4. Członkowie IICB mogą być wspomagani przez zastępców. Przewodniczący może zaprosić innych przedstawicieli podmiotów Unii, o których mowa w ust. 3, lub innych podmiotów Unii do udziału w posiedzeniach IICB bez prawa głosu.

5. Szef CERT-UE i przewodniczący Grupy Współpracy, sieci CSIRT i EU-CyCLONe, ustanowionych na podstawie odpowiednio art. 14, 15 i 16 dyrektywy (UE) 2022/2555, lub ich zastępcy mogą uczestniczyć w posiedzeniach IICB w charakterze obserwatorów. w wyjątkowych przypadkach IICB może, zgodnie ze swoim regulaminem wewnętrznym, postanowić inaczej.

6. IICB przyjmuje swój regulamin wewnętrzny.

7. Zgodnie z regulaminem wewnętrznym IICB wyznacza spośród swoich członków przewodniczącego na trzyletnią kadencję. Zastępca przewodniczącego staje się pełnoprawnym członkiem IICB na ten sam okres.

8. IICB co najmniej trzy razy do roku odbywa posiedzenia z inicjatywy swojego przewodniczącego, na wniosek CERT-UE lub na wniosek któregokolwiek z członków IICB.

9. Każdy członek IICB dysponuje jednym głosem. Decyzje IICB zapadają zwykłą większością głosów, chyba że niniejsze rozporządzenie stanowi inaczej. Przewodniczący IICB nie bierze udziału w głosowaniach, z wyjątkiem sytuacji gdy zostanie oddana taka sama liczba głosów za i przeciw, w którym to przypadku przewodniczący może oddać decydujący głos.

10. IICB może stanowić w drodze uproszczonej procedury pisemnej wszczynanej zgodnie ze swoim regulaminem wewnętrznym. w ramach tej procedury daną decyzję uznaje się za zatwierdzoną w terminie ustalonym przez przewodniczącego, chyba że któryś z członków wyrazi sprzeciw.

11. Sekretariat IICB jest prowadzony przez Komisję i podlega przewodniczącemu IICB.

12. Przedstawiciele wyznaczeni przez EUAN przekazują decyzje IICB członkom EUAN. Każdy członek EUAN ma prawo zwracać się do tych przedstawicieli lub przewodniczącego IICB z każdą sprawą, o której jego zdaniem należy poinformować IICB.

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

14. Do dnia 8 stycznia 2025 r., a następnie co roku IICB składa Parlamentowi Europejskiemu i Radzie sprawozdanie, w którym szczegółowo przedstawia postępy we wdrażaniu niniejszego rozporządzenia, a w szczególności zakres współpracy CERT-UE z jego odpowiednikami w każdym z państw członkowskich. Sprawozdanie to stanowi wkład w przedstawiane co dwa lata sprawozdanie o stanie cyberbezpieczeństwa w Unii, przyjmowane na podstawie art. 18 dyrektywy (UE) 2022/2555.

Artykuł 11

Zadania IICB

W ramach swoich obowiązków IICB w szczególności:

a) udziela wskazówek szefowi CERT-UE;

b) skutecznie monitoruje i nadzoruje wdrażanie niniejszego rozporządzenia oraz wspiera podmioty Unii we wzmacnianiu ich cyberbezpieczeństwa, w tym, w stosownych przypadkach, zwraca się do podmiotów Unii i CERT-UE o sporządzenie sprawozdań ad hoc;

c) w następstwie dyskusji strategicznej przyjmuje wieloletnią strategię podniesienia poziomu cyberbezpieczeństwa w podmiotach Unii, regularnie – co najmniej raz na pięć lat – ją ocenia i w razie potrzeby ją zmienia;

d) ustala metodykę i aspekty organizacyjne przeprowadzania dobrowolnych wzajemnych ocen przez podmioty Unii by wyciągnąć wnioski z wspólnych doświadczeń, zwiększyć wzajemne zaufanie, osiągnąć wysoki wspólny poziom cyberbezpieczeństwa, a także zwiększać zdolności podmiotów Unii w zakresie cyberbezpieczeństwa, zapewniając, aby takie wzajemne oceny były przeprowadzane przez ekspertów ds. cyberbezpieczeństwa wyznaczonych przez podmiot Unii inny niż podmiot Unii poddawany ocenie oraz aby metodyka ich przeprowadzania opierała się na art. 19 dyrektywy (UE) 2022/2555 i była, w stosownych przypadkach, dostosowana do potrzeb podmiotów Unii;

e) zatwierdza, na wniosek szefa CERT-UE, roczny program prac CERT-UE i monitoruje jego realizację;

f) zatwierdza, na wniosek szefa CERT-UE, katalog usług CERT-UE oraz jego aktualizacje;

g) zatwierdza, na wniosek szefa CERT-UE, roczny plan dochodów i wydatków, w tym plan zatrudnienia, na potrzeby działalności CERT-UE;

h) zatwierdza, na wniosek szefa CERT-UE, ustalenia dotyczące umów o gwarantowanym poziomie usług;

i) analizuje i zatwierdza sprawozdanie roczne, sporządzone przez szefa CERT-UE, obejmujące działalność CERT-UE i zarządzanie środkami finansowymi przez CERT-UE;

j) zatwierdza i monitoruje kluczowe wskaźniki skuteczności działania w odniesieniu do CERT-UE, określone na wniosek szefa CERT-UE;

k) zatwierdza porozumienia o współpracy, umowy o gwarantowanym poziomie usług lub umowy między CERT-UE a innymi podmiotami zawarte na podstawie art. 18;

l) przyjmuje wytyczne i zalecenia na wniosek CERT-UE zgodnie z art. 14 i zleca CERT-UE wydanie, wycofanie lub zmianę propozycji wytycznych bądź zaleceń, lub wezwania do działania;

m) ustanawia grupy doradztwa technicznego realizujące konkretne zadania, aby wspierać prace IICB, zatwierdza zakres ich uprawnień i zadań i wyznacza ich przewodniczących;

n) otrzymuje i analizuje dokumenty i sprawozdania składane przez podmioty Unii na podstawie niniejszego rozporządzenia, takie jak oceny dojrzałości w zakresie cyberbezpieczeństwa;

o) wspomaga utworzenie nieformalnej grupy lokalnych urzędników podmiotów Unii ds. cyberbezpieczeństwa, wspieranej przez ENISA, aby umożliwić wymianę najlepszych praktyk i informacji dotyczących wdrażania niniejszego rozporządzenia;

p) uwzględniając informacje na temat zidentyfikowanego ryzyka w cyberprzestrzeni i wyciągnięte wnioski przedstawione przez CERT-UE, monitoruje adekwatność ustaleń dotyczących wzajemnych połączeń między środowiskami ICT podmiotów Unii oraz doradza możliwe usprawnienia;

q) ustanawia plan zarządzania kryzysami w cyberprzestrzeni w celu wsparcia – na poziomie operacyjnym – skoordynowanego zarządzania poważnymi incydentami mającymi wpływ na podmioty Unii oraz w celu przyczynienia się do regularnej wymiany istotnych informacji, w szczególności o skutkach i dotkliwości poważnych incydentów oraz o możliwych sposobach łagodzenia ich skutków;

r) koordynuje przyjmowanie planów zarządzania kryzysami w cyberprzestrzeni, o których mowa w art. 9 ust. 2, w poszczególnych podmiotach Unii;

s) przyjmuje zalecenia w odniesieniu do bezpieczeństwa łańcucha dostaw, o którym mowa w art. 8 ust. 2 akapit pierwszy lit. m), z uwzględnieniem wyników skoordynowanego na poziomie Unii szacowania ryzyka krytycznych łańcuchów dostaw, o którym mowa w art. 22 dyrektywy (UE) 2022/2555, w celu wsparcia podmiotów Unii w przyjmowaniu skutecznych i proporcjonalnych środków zarządzania ryzykiem w cyberprzestrzeni.

Artykuł 12

Zapewnianie zgodności

1. IICB na podstawie art. 10 ust. 2 i art. 11 skutecznie monitoruje wdrażanie przez podmioty Unii niniejszego rozporządzenia oraz przyjętych wytycznych, zaleceń i wezwań do działania. IICB może zażądać od podmiotów Unii niezbędnych w tym celu informacji lub dokumentów. w przypadku przyjmowania środków zapewniania zgodności na podstawie niniejszego artykułu dotyczących danego podmiotu Unii, który jest bezpośrednio reprezentowany w IICB, podmiot ten nie ma prawa głosu.

2. W razie gdy IICB stwierdzi, że dany podmiot Unii nie wdrożył należycie niniejszego rozporządzenia lub wytycznych, zaleceń lub wezwań do działania wydanych na podstawie niniejszego rozporządzenia, może – bez uszczerbku dla wewnętrznych procedur danego podmiotu Unii oraz po umożliwieniu temu podmiotowi Unii przedstawienia uwag:

a) przekazać danemu podmiotowi Unii uzasadnioną opinię dotyczącą stwierdzonych niedociągnięć we wdrażaniu niniejszego rozporządzenia;

b) wydać – po konsultacji z CERT-UE – wytyczne dla danego podmiotu Unii, w celu zapewnienia, aby w określonym terminie jego Ramy, środki zarządzania ryzykiem w cyberprzestrzeni, plan dotyczący cyberbezpieczeństwa i zgłaszanie incydentów stały się zgodne z niniejszym rozporządzeniem;

c) wydać ostrzeżenie wzywające podjęcie działań w celu zaradzenia w określonym terminie stwierdzonym niedociągnięciom, zawierające zalecenia co do zmiany środków przyjętych przez dany podmiot Unii na podstawie niniejszego rozporządzenia;

d) wydać danemu podmiotowi Unii uzasadnione powiadomienie, w przypadku gdy w określonym terminie nie podjął on wystarczających działań w celu zaradzenia niedociągnięciom wskazanym w ostrzeżeniu wydanym na podstawie lit. c);

e) wydać:

(i) zalecenie przeprowadzenia audytu; lub

(ii) żądanie przeprowadzenia audytu przez zewnętrznego audytora;

f) w stosownych przypadkach poinformować Trybunał Obrachunkowy, w ramach jego mandatu, o zarzucanym braku zgodności;

g) wydać skierowane do wszystkich państw członkowskich i podmiotów Unii zalecenie tymczasowego zawieszenia przepływów danych do danego podmiotu Unii.

Do celów akapitu pierwszego lit. c) liczbę odbiorców ostrzeżenia odpowiednio się ogranicza, jeżeli jest to konieczne ze względu na ryzyko w cyberprzestrzeni.

Ostrzeżenia i zalecenia wydane na podstawie akapitu pierwszego kieruje się do kierownictwa najwyższego szczebla danego podmiotu Unii.

3. W przypadku gdy IICB przyjmie środki na podstawie ust. 2 akapit pierwszy lit. a)–g), dany podmiot Unii przedstawia szczegółowy opis środków i działań podjętych w celu usunięcia zarzucanych mu niedociągnięć stwierdzonych przez IICB. Podmiot Unii przedkłada ten szczegółowy opis w rozsądnym terminie uzgodnionym z IICB.

4. W przypadku gdy IICB uzna, że naruszenie niniejszego rozporządzenia przez dany podmiot Unii ma charakter długotrwały i wynika bezpośrednio z działań lub zaniechań ze strony urzędnika lub innego pracownika Unii, w tym członka kierownictwa najwyższego szczebla, IICB zwraca się do danego podmiotu Unii o podjęcie odpowiednich działań, w tym z żądaniem, by rozważył podjęcie działań o charakterze dyscyplinarnym zgodnie z przepisami i procedurami ustanowionymi w regulaminie pracowniczym i innymi mającymi zastosowanie przepisami i procedurami. w tym celu IICB przekazuje danemu podmiotowi Unii niezbędne informacje.

5. Jeżeli podmioty Unii powiadomią, że nie są w stanie dotrzymać terminów określonych w art. 6 ust. 1 i w art. 8 ust. 1, IICB może w należycie uzasadnionych przypadkach, uwzględniwszy rozmiar podmiotu Unii, zezwolić na przedłużenie tych terminów.

ROZDZIAŁ IV

CERT-UE

Artykuł 13

Misja i zadania CERT-UE

1. Misją CERT-UE jest przyczynianie się do bezpieczeństwa jawnego środowiska ICT wszystkich podmiotów Unii poprzez doradzanie im w zakresie cyberbezpieczeństwa, pomaganie im w zapobieganiu incydentom, wykrywaniu ich, ich obsłudze, łagodzeniu ich skutków, reagowaniu na nie i usuwaniu ich skutków oraz poprzez pełnienie dla tych podmiotów w roli punktu wymiany informacji na temat cyberbezpieczeństwa i koordynacji reakcji na incydenty.

2. CERT-UE gromadzi, analizuje i udostępnia podmiotom Unii informacje na temat cyberzagrożeń, podatności i incydentów dotyczących jawnej infrastruktury ICT oraz zarządza tymi informacjami. Koordynuje reagowanie na incydenty na poziomie międzyinstytucjonalnym i na poziomie podmiotów Unii, również poprzez świadczenie lub koordynowanie specjalistycznej pomocy operacyjnej.

3. Mając na celu pomoc dla podmiotów Unii, CERT-UE wykonuje następujące zadania:

a) wspiera je we wdrażaniu niniejszego rozporządzenia oraz przyczynia się do koordynacji wdrażania niniejszego rozporządzenia za pomocą środków wymienionych w art. 14 ust. 1 lub poprzez sporządzanie sprawozdań ad hoc, o które zwróci się IICB;

b) świadczy standardowe usługi CSIRT dla podmiotów Unii w formie pakietu usług z zakresu cyberbezpieczeństwa opisanych w katalogu usług (zwane dalej „usługami podstawowymi”);

c) utrzymuje sieć równorzędnych podmiotów i partnerów w celu wspierania usług określonych w art. 17 i 18;

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

e) na podstawie informacji, o których mowa w ust. 2, przyczynia się w ścisłej współpracy z ENISA do uzyskania orientacji sytuacyjnej w zakresie cyberbezpieczeństwa Unii;

f) koordynuje zarządzanie poważnymi incydentami;

g) działa po stronie podmiotów Unii jako odpowiednik koordynatora wyznaczonego na potrzeby skoordynowanego ujawniania podatności na podstawie art. 12 ust. 1 dyrektywy (UE) 2022/2555;

h) na wniosek podmiotu Unii dokonuje proaktywnego nieinwazyjnego skanowania publicznie dostępnych sieci i systemów informatycznych tego podmiotu Unii.

W stosownych przypadkach i z zastrzeżeniem odpowiedniej poufności informacje, o których mowa w akapicie pierwszym lit. e), udostępnia się IICB, sieci CSIRT i Centrum Analiz Wywiadowczych Unii Europejskiej (EU INTCEN).

4. CERT-UE może, zgodnie z odpowiednio art. 17 lub 18, współpracować ze stosownymi społecznościami zajmującymi się cyberbezpieczeństwem w Unii i w jej państwach członkowskich, w tym w następujących obszarach:

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

b) współpraca operacyjna dotycząca sieci CSIRT, w tym w odniesieniu do wzajemnej pomocy;

c) analiza cyberzagrożeń, w tym orientacja sytuacyjna;

d) dowolna kwestia wymagająca fachowej wiedzy technicznej CERT-UE w dziedzinie cyberbezpieczeństwa.

5. W ramach swoich kompetencji CERT-UE prowadzi zorganizowaną współpracę z ENISA w zakresie budowania zdolności, współpracy operacyjnej i długoterminowych analiz strategicznych cyberzagrożeń zgodnie z rozporządzeniem (UE) 2019/881. CERT-UE może współpracować z Europejskim Centrum ds. Walki z Cyberprzestępczością przy Europolu i wymieniać się z nim informacjami.

6. CERT-UE może świadczyć następujące usługi nie opisane w jego katalogu usług (zwane dalej „usługami płatnymi"):

a) usługi wspierające cyberbezpieczeństwo środowiska ICT podmiotów Unii inne niż usługi określone w ust. 3, na podstawie umów o gwarantowanym poziomie usług i z zastrzeżeniem dostępnych zasobów, w szczególności szeroko zakrojone monitorowanie sieci, w tym stanowiące pierwszą linię obrony, całodobowe monitorowanie pod kątem poważnych cyberzagrożeń;

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

c) na wniosek – proaktywne skanowanie sieci i systemów informatycznych danego podmiotu Unii w celu wykrycia podatności o potencjalnym znaczącym wpływie;

d) usługi wspierające bezpieczeństwo środowiska ICT świadczone na rzecz organizacji niebędących podmiotami Unii, lecz ściśle współpracujących z podmiotami Unii, na przykład ze względu na powierzone im zadania lub obowiązki na mocy prawa Unii, na podstawie pisemnych umów i po uprzednim zatwierdzeniu przez IICB.

W odniesieniu do akapitu pierwszego lit. d) po uprzednim zatwierdzeniu przez IICB CERT-UE może w drodze wyjątku zawierać umowy o gwarantowanym poziomie usług z podmiotami innymi niż podmioty Unii.

7. CERT-UE organizuje ćwiczenia w zakresie cyberbezpieczeństwa i może w nich uczestniczyć lub zalecać uczestnictwo w istniejących ćwiczeniach, w stosownych przypadkach w ścisłej współpracy z ENISA, w celu testowania poziomu cyberbezpieczeństwa podmiotów Unii.

8. CERT-UE może udzielać pomocy podmiotom Unii w razie incydentów w sieciach i systemach informatycznych przetwarzających EUCI, o ile zainteresowane podmioty Unii wyraźnie się o to zwrócą zgodnie ze swoimi odpowiednimi procedurami. Udzielanie pomocy przez CERT-UE na podstawie niniejszego ustępu pozostaje bez uszczerbku dla mających zastosowanie przepisów dotyczących ochrony informacji niejawnych.

9. CERT-UE informuje podmioty Unii o swoich procedurach i procesach obsługi incydentów.

10. CERT-UE dostarcza, z zachowaniem wysokiego poziomu poufności i wiarygodności, za pomocą odpowiednich mechanizmów współpracy i podległości służbowej, istotnych i zanonimizowanych informacji o poważnych incydentach i sposobie ich obsługi. Informacje te włącza się do sprawozdania, o którym mowa w art. 10 ust. 14.

11. CERT-UE w ścisłej współpracy z EIOD wspiera zainteresowane podmioty Unii w obsłudze incydentów powodujących naruszenie danych osobowych, bez uszczerbku dla właściwości i zadań EIOD jako organu nadzorczego zgodnie z rozporządzeniem (UE) 2018/1725.

12. CERT-UE może, na wyraźny wniosek jednostek podmiotów Unii zajmujących się poszczególnymi politykami, zapewnić doradztwo techniczne lub wkład techniczny w odpowiednich kwestiach dotyczących polityki.

Artykuł 14

Wytyczne, zalecenia i wezwania do działania

1. CERT-UE wspiera wdrażanie niniejszego rozporządzenia poprzez:

a) wydawanie wezwań do działania opisujących pilne środki w zakresie bezpieczeństwa, do zastosowania których w określonym terminie wzywa się podmioty Unii;

b) przedstawianie IICB propozycji wytycznych skierowanych do wszystkich podmiotów Unii lub do części z nich;

c) przedstawianie IICB propozycji zaleceń skierowanych do poszczególnych podmiotów Unii.

W odniesieniu do akapitu pierwszego lit. a) dany podmiot Unii bez zbędnej zwłoki po otrzymaniu wezwania do działania informuje CERT-UE o sposobie zastosowania pilnych środków w zakresie bezpieczeństwa.

2. Wytyczne i zalecenia mogą obejmować:

a) wspólne metody i model oceny dojrzałości podmiotów Unii w zakresie cyberbezpieczeństwa, w tym odpowiednie skale lub kluczowe wskaźniki skuteczności działania, służące jako punkt odniesienia dla stałych postępów w zakresie cyberbezpieczeństwa we wszystkich podmiotach Unii i ułatwiające traktowanie priorytetowo poszczególnych obszarów cyberbezpieczeństwa i środków z zakresu cyberbezpieczeństwa z uwzględnieniem stanu cyberbezpieczeństwa w poszczególnych podmiotach;

b) ustalenia dotyczące zarządzania ryzykiem w cyberprzestrzeni i ustalenia dotyczące środków zarządzania ryzykiem w cyberprzestrzeni lub usprawnienia tych elementów;

c) ustalenia dotyczące ocen dojrzałości w zakresie cyberbezpieczeństwa i planów dotyczących cyberbezpieczeństwa;

d) w stosownych przypadkach wykorzystywanie wspólnej technologii, architektury, otwartego oprogramowania i powiązanych najlepszych praktyk w celu osiągnięcia interoperacyjności i wspólnych norm, w tym skoordynowanego podejścia do bezpieczeństwa łańcucha dostaw;

e) w stosownych przypadkach informacje ułatwiające posługiwanie się narzędziami udzielania zamówień realizowanych na zasadzie współpracy na zakup odpowiednich usług i produktów z zakresu cyberbezpieczeństwa od zewnętrznych dostawców;

f) ustalenia dotyczące wymiany informacji na podstawie art. 20.

Artykuł 15

Szef CERT-UE

1. Komisja, za zgodą dwóch trzecich członków IICB, mianuje szefa CERT-UE. Na wszystkich etapach procedury mianowania, w szczególności w odniesieniu do przygotowywania ogłoszeń o naborze, rozpatrywania kandydatur oraz powoływania komisji selekcyjnych do celu wyboru na to stanowisko, prowadzi się konsultacje z IICB. Procedura wyboru, w tym ostateczna skrócona lista kandydatów, spośród których ma zostać mianowany szef CERT-UE, musi gwarantować sprawiedliwą reprezentację każdej z płci z uwzględnieniem przedstawionych kandydatur.

2. Szef CERT-UE odpowiada za sprawne funkcjonowanie CERT-UE i działa w ramach kompetencji związanych z jego funkcją oraz pod kierownictwem IICB. Szef CERT-UE regularnie składa sprawozdania przewodniczącemu IICB oraz – na żądanie IICB – składa IICB sprawozdania ad hoc.

3. Szef CERT-UE wspomaga odpowiedzialnego delegowanego urzędnika zatwierdzającego w sporządzaniu rocznego sprawozdania z działalności zawierającego informacje dotyczące finansów i zarządzania, w tym wyniki kontroli, przygotowywanego zgodnie z art. 74 ust. 9 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2018/1046 ([9]) i regularnie składa temu delegowanemu urzędnikowi zatwierdzającemu sprawozdania z realizacji działań, co do których szefowi CERT-UE przekazano uprawnienia na zasadzie subdelegacji.

4. Szef CERT-UE opracowuje co roku plan dochodów i wydatków administracyjnych na potrzeby działalności CERT-UE, projekt rocznego programu prac, projekt katalogu usług CERT-UE, projekt zmian w katalogu usług, projekt warunków umów o gwarantowanym poziomie usług oraz projekt kluczowych wskaźników skuteczności działania CERT-UE, które mają zostać zatwierdzone przez IICB zgodnie z art. 11. Dokonując rewizji wykazu usług w katalogu usług CERT-UE, szef CERT-UE uwzględnia zasoby przydzielone CERT-UE.

5. Szef CERT-UE co najmniej raz do roku przedkłada IICB i przewodniczącemu IICB sprawozdania z działalności i wyników CERT-UE za okres odniesienia, w tym z wykonania budżetu, zawartych umów o gwarantowanym poziomie usług i pisemnych umów, współpracy z odpowiednikami i partnerami oraz z misji podejmowanych przez członków personelu, w tym sprawozdania, o których mowa w art. 11. Sprawozdania te obejmują program prac na kolejny okres, plan dochodów i wydatków, w tym plan zatrudnienia, planowane aktualizacje katalogu usług CERT-UE oraz ocenę spodziewanego wpływu takich aktualizacji na zasoby finansowe i ludzkie.

Artykuł 16

Sprawy finansowe i kadrowe

1. CERT-UE wchodzi w skład struktury administracyjnej jednej z dyrekcji generalnych Komisji, aby korzystać z komisyjnych struktur wsparcia administracyjnego, zarządzania finansowego i rachunkowego, zachowując jednocześnie swój status autonomicznego, międzyinstytucjonalnego dostawcy usług dla wszystkich podmiotów Unii. Komisja informuje IICB o miejscu CERT-UE w strukturze administracyjnej oraz o wszelkich zmianach w tym zakresie. Komisja dokonuje regularnie przeglądu ustaleń administracyjnych dotyczących CERT-UE oraz każdorazowo przed ustanowieniem wieloletnich ram finansowych na podstawie art. 312 TFUE, aby umożliwić podjęcie odpowiednich działań. Przegląd obejmuje możliwość ustanowienia CERT-UE jako urzędu Unii.

2. W kwestii stosowania procedur administracyjnych i finansowych szef CERT-UE działa z upoważnienia Komisji oraz pod nadzorem IICB.

([9]) 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).

3. Zadania i działania CERT-UE, w tym usługi świadczone przez CERT-UE zgodnie z art. 13 ust. 3, 4, 5 i 7 oraz art. 14 ust. 1 na rzecz podmiotów Unii finansowanych w ramach działu wieloletnich ram finansowych dotyczącego europejskiej administracji publicznej, są finansowane z odrębnej linii budżetowej budżetu Komisji. Stanowiska przeznaczone dla CERT-UE wyszczególnia się w przypisie do planu zatrudnienia Komisji.

4. Podmioty Unii inne niż te wymienione w ust. 3 niniejszego artykułu wnoszą roczny wkład finansowy na rzecz CERT-UE w celu pokrycia kosztów usług świadczonych przez CERT-UE na podstawie tego ustępu. Wkłady opierają się na wskazówkach wydanych przez IICB i są przedmiotem uzgodnień zawartych między każdym podmiotem Unii a CERT-UE w umowach o gwarantowanym poziomie usług. Wkłady muszą odzwierciedlać sprawiedliwy i proporcjonalny udział w całkowitych kosztach świadczonych usług. Ujmuje się je w odrębnej linii budżetowej, o której mowa w ust. 3 niniejszego artykułu, jako wewnętrzne dochody przeznaczone na określony cel, jak przewidziano w art. 21 ust. 3 lit. c) rozporządzenia (UE, Euratom) 2018/1046.

5. Koszty usług przewidzianych w art. 13 ust. 6 odzyskuje się od podmiotów Unii korzystających z usług CERT-UE. Dochody przypisuje się do linii budżetowych przeznaczonych na pokrycie kosztów.

Artykuł 17

Współpraca CERT-UE z jego odpowiednikami w państwach członkowskich

1. Bez zbędnej zwłoki CERT-UE współpracuje i prowadzi wymianę informacji ze swoimi odpowiednikami z państw członkowskich, w szczególności z CSIRT wyznaczonymi lub ustanowionymi na podstawie art. 10 dyrektywy (UE) 2022/2555 lub w stosownych przypadkach z właściwymi organami i z pojedynczymi punktami kontaktowymi wyznaczonymi lub ustanowionymi na podstawie art. 8 tej dyrektywy, w zakresie incydentów, cyberzagrożeń, podatności, potencjalnych zdarzeń dla cyberbezpieczeństwa, ewentualnych środków zaradczych oraz najlepszych praktyk, jak również wszystkich kwestii istotnych dla lepszej ochrony środowisk ICT podmiotów Unii, w tym za pośrednictwem sieci CSIRT ustanowionej na podstawie art. 15 dyrektywy (UE) 2022/2555. CERT-UE wspiera Komisję w ramach EU-CyCLONe, ustanowionego na podstawie art. 16 dyrektywy (UE) 2022/2555, w skoordynowanym zarządzaniu kryzysami i incydentami w cyberbezpieczeństwie na dużą skalę.

2. W przypadku gdy CERT-UE dowie się o wystąpieniu znaczącego incydentu na terytorium danego państwa członkowskiego, niezwłocznie powiadamia on właściwego odpowiednika w tym państwie członkowskim, zgodnie z ust. 1.

3. Jeżeli dane osobowe są chronione zgodnie z mającym zastosowanie prawem Unii dotyczącym ochrony danych, CERT-UE bez zbędnej zwłoki, wymienia z odpowiednikami z państw członkowskich stosowne informacje dotyczące konkretnych incydentów, aby ułatwić wykrywanie podobnych cyberzagrożeń lub incydentów lub by przyczynić się do analizy incydentu, co nie wymaga zgody podmiotu Unii, którego dotyczy incydent. CERT-UE wymienia informacje dotyczące konkretnych incydentów, które ujawniają tożsamość celu, wyłącznie w jednej z następujących sytuacji

a) podmiot Unii, którego dotyczy incydent, wyraził zgodę;

b) podmiot Unii, którego dotyczy incydent, nie wyraził zgody przewidzianej w lit. a), lecz ujawnienie tożsamości tego podmiotu Unii mogłoby zwiększyć prawdopodobieństwo uniknięcia incydentów lub złagodzenia ich skutków w innych miejscach;

c) podmiot Unii, którego dotyczy incydent, już podał do wiadomości publicznej, że padł ofiarą incydentu.

Decyzje o wymianie informacji dotyczących konkretnego incydentu, które ujawniają tożsamość celu, w który wymierzony był incydent, podjęte na podstawie akapitu pierwszego lit. b) zatwierdza szef CERT-UE. Przed wydaniem takiej decyzji CERT-UE kontaktuje się na piśmie z podmiotem Unii, którego dotyczy incydent, wyjaśniając, w jaki sposób ujawnienie tożsamości podmiotu pomogłoby uniknąć incydentów lub złagodzić ich skutki w innych miejscach. Szef CERT-UE przedstawia wyjaśnienie i wyraźnie zwraca się do podmiotu Unii o wydanie w określonym terminie oświadczenia, czy wyraża zgodę. Szef CERT-UE informuje również podmiot Unii, że w świetle przedstawionych wyjaśnień zastrzega on sobie prawo do ujawnienia informacji nawet pomimo braku zgody. Przed ujawnieniem informacji informuje się o tym podmiot Unii, którego dotyczy incydent.

Artykuł 18

Współpraca CERT-UE z innymi odpowiednikami

1. CERT-UE może współpracować ze swoimi odpowiednikami w Unii innymi niż te, o których mowa w art. 17, podlegającymi unijnym wymogom w zakresie cyberbezpieczeństwa, w tym z odpowiednikami działającymi w konkretnych sektorach przemysłu, w zakresie narzędzi i metod, takich jak techniki, taktyka, procedury i najlepsze praktyki, a także w zakresie cyberzagrożeń i podatności. CERT-UE zwraca się do IICB o uprzednią – analizowaną indywidualnie dla każdego przypadku – zgodę na podjęcie wszelkiej współpracy z takimi odpowiednikami. w przypadku gdy CERT-UE nawiązuje współpracę z takimi odpowiednikami, informuje wszystkie stosowne odpowiedniki, o których mowa w art. 17 ust. 1, z państwa członkowskiego, w którym dany odpowiednik ma siedzibę. w stosownych przypadkach taką współpracę i jej warunki, w tym dotyczące cyberbezpieczeństwa, ochrony danych i przetwarzania informacji, ustanawia się w szczególnych uzgodnieniach o poufności, takich jak umowy lub porozumienia administracyjne. Uzgodnienia o poufności nie wymagają uprzedniej zgody IICB, ale o ich zawarciu informuje się przewodniczącego IICB. Jeżeli zachodzi pilna i nieuchronna potrzeba wymiany informacji na temat cyberbezpieczeństwa w interesie podmiotów Unii lub innej strony, CERT-UE może wymieniać informacje z podmiotem, którego szczególne kompetencje, zdolności i wiedza fachowa są zasadnie wymagane do udzielenia pomocy w takiej pilnej i nieuchronnej potrzebie, nawet jeżeli CERT-UE nie zawarł z tym podmiotem uzgodnień o poufności. w takich przypadkach CERT-UE natychmiast informuje przewodniczącego IICB i powiadamia IICB w formie regularnych sprawozdań lub spotkań.

2. CERT-UE może współpracować z partnerami, takimi jak podmioty komercyjne, w tym podmioty działające w konkretnych sektorach przemysłu, organizacje międzynarodowe, podmioty krajowe spoza Unii lub indywidualni eksperci, w celu zbierania informacji na temat ogólnych i szczególnych cyberzagrożeń, potencjalnych zdarzeń dla cyberbezpieczeństwa, podatności i ewentualnych środków zaradczych. CERT-UE zwraca się do IICB o uprzednią – analizowaną indywidualnie dla każdego przypadku – zgodę na podjęcie szerszej współpracy z takimi partnerami.

3. CERT-UE może, za zgodą podmiotu Unii, którego dotyczy incydent, i pod warunkiem zawarcia z właściwym odpowiednikiem lub partnerem uzgodnień lub umowy o poufności, przekazać informacje dotyczące konkretnego incydentu odpowiednikom lub partnerom, o których mowa w ust. 1 i 2, wyłącznie w celu przyczynienia się do jego analizy.

ROZDZIAŁ V

OBOWIĄZKI W ZAKRESIE WSPÓŁPRACY I ZGŁASZANIA INCYDENTÓW

Artykuł 19

Postępowanie z informacjami

1. Podmioty Unii oraz CERT-UE przestrzegają obowiązku zachowania tajemnicy zawodowej zgodnie z art. 339 TFUE lub równoważnymi mającymi zastosowanie ramami.

2. Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady ([10]) stosuje się do wniosków o udzielenie publicznego dostępu do dokumentów przechowywanych przez CERT-UE, w tym wynikającego z tego rozporządzenia obowiązku konsultowania się z innymi podmiotami Unii lub – w stosownych przypadkach – z państwami członkowskimi, jeśli przedmiotem wniosku są ich dokumenty.

3. Postępowanie z informacjami przez podmioty Unii oraz CERT-UE musi być zgodne z mającymi zastosowanie przepisami dotyczącymi bezpieczeństwa informacji.

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

Artykuł 20

Mechanizmy wymiany informacji na temat cyberbezpieczeństwa

1. Podmioty Unii mogą dobrowolnie zgłaszać CERT-UE incydenty, cyberzagrożenia, potencjalne zdarzenia dla cyberbezpieczeństwa i podatności, które ich dotyczą, i przekazywać CERT-UE informacje na ten temat. CERT-UE zapewnia dostępność skutecznych środków łączności, charakteryzujących się wysokim poziomem identyfikowalności, poufności i niezawodności, aby ułatwić wymianę informacji z podmiotami Unii. Przy rozpatrywaniu zgłoszeń CERT-UE może traktować zgłoszenia obowiązkowe priorytetowo względem zgłoszeń dobrowolnych. Bez uszczerbku dla art. 12 dobrowolne zgłoszenie nie może skutkować nałożeniem na zgłaszający podmiot Unii żadnych dodatkowych obowiązków, którym by nie podlegał, gdyby nie dokonał takiego zgłoszenia.

2. W celu realizacji swojej misji i zadań powierzonych na podstawie art. 13, CERT-UE może zwracać się do podmiotów Unii o przekazanie mu informacji z ich odpowiednich rejestrów zasobów systemów ICT, w tym informacji dotyczących cyberzagrożeń, potencjalnych zdarzeń dla cyberbezpieczeństwa, podatności, oznak naruszenia integralności systemu, ostrzeżeń dotyczących cyberbezpieczeństwa i zaleceń dotyczących konfiguracji narzędzi cyberbezpieczeństwa do celów wykrywania incydentów. Podmiot Unii, do którego się zwrócono, bez zbędnej zwłoki przekazuje wymagane informacje oraz ich wszelkie późniejsze aktualizacje.

3. CERT-UE może prowadzić z podmiotami Unii wymianę informacji dotyczących konkretnych incydentów ujawniających tożsamość podmiotu Unii, którego dotyczy incydent pod warunkiem, że podmiotu Unii, którego dotyczy incydent, wyrazi na to zgodę. Jeżeli podmiot Unii odmawia zgody, przedstawia CERT-UE uzasadnienie tej decyzji.

4. Podmioty Unii przekazują – na żądanie – Parlamentowi Europejskiemu i Radzie informacje na temat realizacji planów dotyczących cyberbezpieczeństwa.

5. IICB lub CERT-UE, stosownie do przypadku, udostępniają – na żądanie – Parlamentowi Europejskiemu i Radzie wytyczne, zalecenia i wezwania do działania.

6. Obowiązki w zakresie wymiany informacji określone w niniejszym artykule nie obejmują:

a) EUCI;

b) informacji, których dalsze rozpowszechnianie zostało wykluczone za pomocą widocznego oznakowania, chyba że wyraźnie zezwolono na ich wymianę z CERT-UE.

Artykuł 21

Obowiązki w zakresie zgłaszania incydentów

1. Incydent uznaje się za znaczący, jeżeli:

a) spowodował lub może spowodować dotkliwe zakłócenia operacyjne w funkcjonowaniu lub straty finansowe dla danego podmiotu Unii;

b) wpłynął lub może wpłynąć na inne osoby fizyczne lub prawne, powodując znaczne szkody majątkowe i niemajątkowe.

2. Podmioty Unii przedkładają CERT-UE:

a) bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od powzięcia wiedzy o znaczącym incydencie – wczesne ostrzeżenie, w którym w stosownych przypadkach wskazuje się, że znaczący incydent został przypuszczalnie wywołany działaniem bezprawnym lub działaniem w złym zamiarze lub że mógł wywrzeć wpływ międzyinstytucjonalny lub transgraniczny;

b) bez zbędnej zwłoki, a w każdym razie w ciągu 72 godzin od powzięcia wiedzy o znaczącym incydencie – zgłoszenie incydentu, w stosownych przypadkach wraz z aktualizacją informacji, o których mowa w lit. a), i ze wskazaniem wstępnej oceny znaczącego incydentu, w tym jego dotkliwości i skutków, a w stosownych przypadkach także oznak naruszenia integralności systemu;

c) na wniosek CERT-UE – sprawozdanie okresowe na temat odpowiednich aktualizacji statusu;

d) nie później niż miesiąc po zgłoszeniu incydentu na podstawie lit. b) – sprawozdanie końcowe zawierające następujące elementy:

(i) szczegółowy opis incydentu, w tym jego dotkliwości i skutków;

(ii) rodzaj zagrożenia lub pierwotną przyczynę, które prawdopodobnie były źródłem incydentu;

(iii) zastosowane i wdrażane środki ograniczające ryzyko;

(iv) w stosownych przypadkach – transgraniczne lub międzyinstytucjonalne skutki incydentu;

e) jeżeli incydent nie zakończył się w terminie składania sprawozdania końcowego, o którym mowa w lit. d) – sprawozdanie z postępu prac w danym momencie oraz sprawozdanie końcowe w terminie jednego miesiąca od zakończenia przez nie obsługi incydentu.

3. Podmiot Unii bez zbędnej zwłoki, a w każdym razie w ciągu 24 godzin od powzięcia wiedzy o znaczącym incydencie, informuje o wystąpieniu znaczącego incydentu wszelkie stosowne odpowiedniki krajowe, o których mowa w art. 17 ust. 1, w państwie członkowskim, w którym podmiot ten ma siedzibę.

4. Podmioty Unii zgłaszają między innymi wszelkie informacje umożliwiające CERT-UE określenie wszelkiego wpływu międzyinstytucjonalnego, wpływu na przyjmujące państwo członkowskie lub transgranicznego wpływu znaczącego incydentu. Bez uszczerbku dla art. 12 samo zgłoszenie nie nakłada na podmiot Unii zwiększonej odpowiedzialności.

5. W stosownych przypadkach podmioty Unii bez zbędnej zwłoki powiadamiają użytkowników sieci i systemów informatycznych, których dotyczy incydent, lub użytkowników innych elementów środowiska ICT, których potencjalnie dotyczy znaczący incydent lub poważne cyberzagrożenie, oraz którzy w stosownych przypadkach mają potrzebę podjęcia środków łagodzących, o wszelkich środkach lub środkach zaradczych, które użytkownicy ci mogą zastosować w reakcji na ten incydent lub to zagrożenie. w stosownych przypadkach podmioty Unii informują tych użytkowników o samym poważnym cyberzagrożeniu.

6. Jeżeli znaczący incydent lub poważne cyberzagrożenie mają wpływ na sieć i system informatyczny lub element środowiska ICT podmiotu Unii, które jest celowo powiązane ze środowiskiem ICT innego podmiotu Unii, CERT-UE wydaje stosowne ostrzeżenie dotyczące cyberbezpieczeństwa.

7. Podmioty Unii, na wniosek CERT-UE, przekazują mu bez zbędnej zwłoki informacje cyfrowe wygenerowane w wyniku korzystania z urządzeń elektronicznych uczestniczących w incydentach, które u nich wystąpiły. CERT-UE może dodatkowo sprecyzować, jakiego rodzaju informacji cyfrowych potrzebuje do celów orientacji sytuacyjnej i zareagowania na incydenty.

8. Co trzy miesiące CERT-UE przedkłada IICB, ENISA, EU INTCEN i sieci CSIRT sprawozdanie podsumowujące zawierające zanonimizowane i zagregowane dane dotyczące znaczących incydentów, incydentów, cyberzagrożeń, potencjalnych zdarzeń dla cyberbezpieczeństwa i podatności na podstawie art. 20 oraz znaczących incydentów zgłoszonych na podstawie ust. 2 niniejszego artykułu. To sprawozdanie podsumowujące stanowi wkład w przedstawiane co dwa lata sprawozdanie na temat stanu cyberbezpieczeństwa w Unii przyjmowane na podstawie art. 18 dyrektywy (UE) 2022/2555.

9. Do dnia 8 lipca 2024 r. IICB wyda wytyczne lub zalecenia doprecyzowujące zasady składania, format i treść zgłoszeń na podstawie niniejszego artykułu. Przygotowując takie wytyczne lub zalecenia, IICB uwzględnia wszelkie akty wykonawcze przyjęte na podstawie art. 23 ust. 11 dyrektywy (UE) 2022/2555 określające rodzaj informacji, format i procedurę zgłoszeń. CERT-UE rozpowszechnia odpowiednie szczegółowe informacje techniczne w celu umożliwienia proaktywnego wykrywania incydentów, reagowania na nie lub wprowadzania środków łagodzących ich skutki przez podmioty Unii.

10. Obowiązki w zakresie zgłaszania incydentów określone w niniejszym artykule nie obejmują:

a) EUCI;

b) informacji, których dalsze rozpowszechnianie zostało wykluczone za pomocą widocznego oznakowania, chyba że wyraźnie zezwolono na ich wymianę z CERT-UE.

Artykuł 22

Koordynacja reakcji na incydenty i współpraca

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

a) podmiotami Unii;

b) odpowiednikami, o których mowa w art. 17 i 18.

2. CERT-UE, w stosownych przypadkach w ścisłej współpracy w ENISA, ułatwia koordynację między podmiotami Unii w zakresie reagowania na incydenty, co obejmuje:

a) przyczynianie się do spójnej komunikacji zewnętrznej;

b) wzajemne wsparcie, takie jak wymiana informacji istotnych dla podmiotów Unii lub udzielanie pomocy, w stosownych przypadkach bezpośrednio na miejscu;

c) optymalne wykorzystanie zasobów operacyjnych;

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

3. CERT-UE, w ścisłej współpracy z ENISA, wspiera podmioty Unii w zakresie orientacji sytuacyjnej w odniesieniu do incydentów, cyberzagrożeń, podatności i potencjalnych zdarzeń dla cyberbezpieczeństwa, a także w dzieleniu się istotnymi postępami w dziedzinie cyberbezpieczeństwa.

4. Do dnia 8 stycznia 2025 r. IICB na podstawie propozycji CERT-UE przyjmie wytyczne lub zalecenia dotyczące koordynacji reagowania na incydenty i współpracy w tym zakresie w odniesieniu do znaczących incydentów. w przypadku podejrzenia, że incydent nosi znamiona przestępstwa, CERT-UE bez zbędnej zwłoki doradza, jak zgłosić incydent organom ścigania.

5. Na specjalny wniosek państwa członkowskiego i za zgodą zainteresowanych podmiotów Unii CERT-UE może zwrócić się do ekspertów z wykazu, o którym mowa w art. 23 ust. 4, o udział w reakcji na poważny incydent mający wpływ na to państwo członkowskie lub na incydent w cyberbezpieczeństwie na dużą skalę zgodnie z art. 15 ust. 3 lit. g) dyrektywy (UE) 2022/2555. Szczegółowe przepisy dotyczące dostępu podmiotów Unii do ekspertów technicznych oraz korzystania z ich usług są zatwierdzane przez IICB na wniosek CERT-UE.

Artykuł 23

Zarządzanie poważnymi incydentami

1. Aby wspierać na poziomie operacyjnym skoordynowane zarządzanie poważnymi incydentami mającymi wpływ na podmioty Unii oraz przyczyniać się do regularnej wymiany istotnych informacji między podmiotami Unii i z państwami członkowskimi, IICB ustanawia na podstawie art. 11 lit. q) plan zarządzania kryzysami w cyberprzestrzeni oparty o działania, o których mowa w art. 22 ust. 2, w ścisłej współpracy z CERT-UE i ENISA. Plan zarządzania kryzysami w cyberprzestrzeni obejmuje co najmniej następujące elementy:

a) ustalenia dotyczące koordynacji i przepływu informacji między podmiotami Unii na potrzeby zarządzania poważnymi incydentami na poziomie operacyjnym;

b) wspólne obowiązujące procedury działania (SOP);

c) wspólną taksonomię dotkliwości poważnych incydentów i punktów wywołujących kryzys;

d) regularne ćwiczenia;

e) kanały bezpiecznej komunikacji, które mają być używane.

2. Przedstawiciel Komisji w IICB, z zastrzeżeniem planu zarządzania kryzysami w cyberprzestrzeni ustanowionego na podstawie ust. 1 niniejszego artykułu i bez uszczerbku dla art. 16 ust. 2 akapit pierwszy dyrektywy (UE) 2022/2555, jest punktem kontaktowym do celów wymiany z EU-CyCLONe istotnych informacji dotyczących poważnych incydentów.

3. CERT-UE koordynuje pomiędzy podmiotami Unii zarządzanie poważnymi incydentami. Prowadzi rejestr dostępnej fachowej wiedzy technicznej, która może być potrzebna, aby zareagować na incydenty w przypadku poważnych incydentów, oraz wspiera IICB w koordynowaniu planów zarządzania kryzysami w cyberprzestrzeni opracowywanych przez podmioty Unii na wypadek poważnych incydentów, o których to planach mowa w art. 9 ust. 2.

4. Podmioty Unii wnoszą wkład w tworzenie rejestru fachowej wiedzy technicznej, udostępniając aktualizowany co roku wykaz ekspertów dostępnych w ich odpowiednich organizacjach, z wyszczególnieniem ich konkretnych umiejętności technicznych.

ROZDZIAŁ VI

PRZEPISY KOŃCOWE

Artykuł 24

Początkowa realokacja środków budżetowych

W celu zapewnienia sprawnego i stabilnego funkcjonowania CERT-UE Komisja może zaproponować realokację zasobów ludzkich i finansowych do budżetu Komisji na potrzeby operacji CERT-UE. Realokacja ta staje się skuteczna w tym samym czasie co pierwszy roczny budżet Unii przyjęty po wejściu w życie niniejszego rozporządzenia.

Artykuł 25

Przegląd

1. Do dnia 8 stycznia 2025 r., a następnie co roku IICB przy wsparciu CERT-UE składa Komisji sprawozdanie z wdrażania niniejszego rozporządzenia. IICB może kierować do Komisji zalecenia, aby dokonała przeglądu niniejszego rozporządzenia.

2. Do dnia 8 stycznia 2027 r., a następnie co dwa lata Komisja dokonuje oceny wdrożenia niniejszego rozporządzenia oraz składa Parlamentowi Europejskiemu i Radzie sprawozdanie z jego wykonania oraz z doświadczeń zdobytych na poziomie strategicznym i operacyjnym.

Sprawozdanie, o którym mowa w akapicie pierwszym niniejszego ustępu, obejmuje przegląd, o którym mowa w art. 16 ust. 1, dotyczący możliwości ustanowienia CERT-UE jako urzędu Unii.

3. Do dnia 8 stycznia 2029 r. Komisja dokona oceny funkcjonowania niniejszego rozporządzenia i złoży sprawozdanie Parlamentowi Europejskiemu, Radzie, Europejskiemu Komitetowi Ekonomiczno-Społecznemu i Komitetowi Regionów. Komisja oceni również stosowność włączenia sieci i systemów informatycznych przetwarzających EUCI do zakresu stosowania niniejszego rozporządzenia, z uwzględnieniem innych aktów ustawodawczych Unii mających zastosowanie do tych systemów. Sprawozdaniu towarzyszy w razie potrzeby wniosek ustawodawczy.

Artykuł 26

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 Strasburgu dnia 13 grudnia 2023 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*
R. METSOLA	P. NAVARRO RÍOS