

II

(Komunikaty)

POROZUMIENIA MIĘDZYINSTYTUCJONALNE

RADA

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)

(2018/C 12/01)

PARLAMENT EUROPEJSKI

RADA EUROPEJSKA, RADA UNII EUROPEJSKIEJ,

KOMISJA EUROPEJSKA,

TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ

EUROPEJSKI BANK CENTRALNY

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY,

EUROPEJSKA SŁUŻBA DZIAŁAŃ ZEWNĘTRZNYCH

EUROPEJSKI KOMITET EKONOMICZNO-SPOŁECZNY,

EUROPEJSKI KOMITET REGIONÓW

I EUROPEJSKI BANK INWESTYCYJNY

a także mając na uwadze, co następuje:

- (1) Zwiększenie możliwości wszystkich instytucji, organów i agencji Unii Europejskiej w zakresie radzenia sobie z zagrożeniami i słabościami cybernetycznymi oraz w zakresie zapobiegania atakom cybernetycznym wymierzonym w ich infrastrukturę technologii informacyjnych i komunikacyjnych (ICT), wykrywanie ich i reagowanie na nie jest nadal niezwykle istotne, ponieważ sprawne działanie sieci i systemów ICT jest kluczowe dla zdolności tych instytucji, organów i agencji do wypełniania ich misji;
- (2) W następstwie inicjatywy wiceprzewodniczących Komisji Neelie Kroes i Maroša Šefčoviča w maju 2011 r. sekretarze generalni instytucji i organów Unii postanowili utworzyć zespół ds. wstępnej konfiguracji zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach Unii (CERT-UE), pod nadzorem międzyinstytucjonalnej rady sterującej.
- (3) W lipcu 2012 r. sekretarze generalni potwierdzili ustalenia praktyczne i zgodzili się co do utrzymania CERT-UE jako stałego podmiotu, tak aby dalej wspomagać poprawę ogólnego poziomu bezpieczeństwa technologii informacyjnej (IT) w instytucjach, organach i agencjach Unii jako przykład dostrzegalnej współpracy międzyinstytucjonalnej w dziedzinie bezpieczeństwa cybernetycznego.

- (4) Przeglądy przeprowadzone w latach 2014 i 2016 wykazały, że CERT-UE w dalszym ciągu rozwijał się w kierunku dojrzałości i osiągnął już etap, na którym należy mu nadać charakter formalny, zapewniając mu bardziej zrównoważone i przejrzyste struktury zarządzania i finansowania.
- (5) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148⁽¹⁾ („dyrektywa w sprawie bezpieczeństwa sieci i informacji”) ustanawia sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), które składają się z przedstawicieli CSIRT państw członkowskich i z przedstawicieli CERT-UE, w celu przyczyniania się do rozwoju pewności i zaufania między państwami członkowskim oraz propagowania szybkiej i skutecznej współpracy operacyjnej.
- (6) Struktura zarządzania CERT-UE powinna określić rolę i zadania CERT-UE, zakres obowiązków jego szefa, rolę i zadania jej Rady Sterującej oraz zakres obowiązków instytucji, organów i agencji Unii we wspieraniu CERT-UE.
- (7) Należy zapewnić CERT-UE stabilne finansowanie i personel, przy jednoczesnym zapewnieniu odpowiedniego wykorzystania środków finansowych, oraz odpowiedni stały personel podstawowy, przy jednoczesnym utrzymaniu ogólnych kosztów administracyjnych CERT-UE na jak najniższym poziomie.
- (8) Niniejsze porozumienie zostaje podpisane przez uczestniczące instytucje i organy Unii po ukończeniu ich odpowiednich wewnętrznych procedur w tym zakresie; agencje Unii wymienione w załączniku I, które są odpowiedzialne za własną infrastrukturę ICT oficjalnie potwierdziły na piśmie przewodniczącemu rady sterującej CERT-UE, że będą je stosować,

ZAWARLI NINIEJSZE POROZUMIENIE:

Artykuł 1

Przedmiot i misja

1. Celem niniejszego porozumienia jest ustanowienie zasad funkcjonowania i organizacji międzyinstytucjonalnego zespołu reagowania na incydenty komputerowe w instytucjach, organach i agencjach Unii (CERT-UE).
2. Misja CERT-UE polega na wspomaganiu bezpieczeństwa infrastruktury ICT we wszystkich instytucjach, organach i agencjach Unii (zwanych dalej „podmiotami uczestniczącymi”), poprzez przyczynianie się do zapobiegania atakom cybernetycznym, wykrywania ich, łagodzenia ich skutków i reagowania na nie oraz poprzez służenie członkom jako punkt wymiany informacji na temat bezpieczeństwa cybernetycznego i punkt koordynacji reagowania na incydenty.

Artykuł 2

Zadania CERT-UE

1. CERT-UE gromadzi, analizuje i udostępnia podmiotom uczestniczącym informacje na temat zagrożeń, słabości i incydentów dotyczących jawnej infrastruktury ICT oraz zarządza tymi informacjami. Koordynuje reagowanie na incydenty na poziomie międzyinstytucjonalnym i na poziomie podmiotów uczestniczących, również poprzez świadczenie lub koordynowanie specjalistycznej pomocy operacyjnej.
2. CERT-UE oferuje wszystkim podmiotom uczestniczącym standardowe usługi CERT. Katalog określający szczegółową ofertę usług CERT-UE, oraz ewentualne aktualizacje, jest zatwierdzany przez Radę Sterującą. Dokonując przeglądu wykazu usług szef CERT-UE bierze pod uwagę przydzielone mu zasoby.
3. CERT-UE może, za zgodą danego podmiotu uczestniczącego, monitorować ruch w jego sieci.
4. CERT-UE może, na wyraźny wniosek danego podmiotu uczestniczącego, udzielić mu pomocy w zakresie incydentów w niejawnych sieciach i systemach informatycznych.
5. CERT-UE nie inicjuje działań ani nie interweniuje świadomie w żadnych sprawach, które należą do kompetencji krajowych służb bezpieczeństwa i wywiadu lub specjalistycznych wydziałów w organizacjach podmiotów uczestniczących. O wszelkich kontaktach z CERT-UE, które inicjują lub do których dążą krajowe służby bezpieczeństwa i wywiadu, bezzwłocznie informowane są: istniejąca w Komisji dyrekcja ds. bezpieczeństwa oraz przewodniczący Rady Sterującej CERT-UE.

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

6. CERT-UE informuje podmioty uczestniczące o swoich procedurach i procesach postępowania w razie incydentów.
7. CERT-UE może, na wyraźny wniosek jednostek politycznych podmiotów uczestniczących, zapewnić doradztwo techniczne lub wkład techniczny w zakresie odpowiednich spraw z dziedziny polityki.

Artykuł 3

Współpraca między podmiotami uczestniczącymi a CERT-UE

1. CERT-UE i podmioty uczestniczące współpracują zgodnie z zasadą „potrzeby wymiany” [*need-to-share*], z zastrzeżeniem ust. 3. CERT-UE zapewnia dostępność skutecznych środków łączności, aby ułatwić wymianę informacji z podmiotami uczestniczącymi.
2. Podmioty uczestniczące przekazują CERT-UE informacje na temat zagrożeń i słabości w dziedzinie bezpieczeństwa cybernetycznego, które mają na nich wpływ. Jeżeli CERT-UE dysponuje informacjami o zagrożeniu lub słabości, które wpływają lub mogą wpływać na dany podmiot uczestniczący, jak najszybciej powiadamia ten podmiot uczestniczący, dostarczając mu wszystkich odpowiednich informacji, w tym na temat poziomu krytyczności, tak aby można było wdrożyć środki ochronne lub zaradcze. CERT-UE może pomóc w zapewnieniu takich środków ochronnych lub zaradczych. Inne podmioty uczestniczące są informowane, o ile to zagrożenie lub ta słabość potencjalnie ich dotyczy.
3. Podmioty uczestniczące niezwłocznie informują CERT-UE, w przypadku gdy przydarzy się im istotny incydent cybernetyczny, udostępniając wszelkie odpowiednie szczegóły techniczne, chyba że mogłoby to zagrozić interesom bezpieczeństwa podmiotu uczestniczącego lub strony trzeciej. Za istotny uważa się każdy incydent, chyba że jest to incydent powtarzający się lub prosty, który najprawdopodobniej jest już dobrze zrozumiany pod względem metod i technologii. Informacje niemające charakteru technicznego mogą być udostępniane CERT-UE wedle uznania podmiotu uczestniczącego dotkniętego incydem. Informacje na temat incydemu, podane do wiadomości CERT-UE, nie są przekazywane na zewnątrz CERT-UE, nawet w formie anonimowej, chyba że podmiot uczestniczący dotknięty incydem wyraził na to zgodę. Aby przygotować się na sytuacje, w których należy szybko przekazać informacje w celu ochrony sieci i systemów członków, CERT-UE z wyprzedzeniem opracowuje z podmiotami uczestniczącymi metody służące realizacji tego celu.
4. CERT-UE, w porozumieniu z podmiotami uczestniczącymi, prowadzi bazę dostępnej im wspólnie wiedzy specjalistycznej, którą można potencjalnie wykorzystać, w granicach ich środków i zdolności, w przypadku poważnego incydemu cybernetycznego dotyczącego co najmniej jeden z tych podmiotów. W stosownych przypadkach, w celu zareagowania na incydem dotyczący bezpieczeństwa cybernetycznego, CERT-UE może zorganizować i koordynować wymianę informacji i wsparcie techniczne bezpośrednio między podmiotami uczestniczącymi.
5. W ramach swoich kompetencji CERT-UE współpracuje ściśle z Agencją Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz Europejskim Centrum ds. Walki z Cyberprzestępczością przy Europołu.
6. CERT-UE udostępnia organom ścigania informacje na temat konkretnych incydentów wyłącznie za uprzednią zgodą właściwych służb odpowiedniego podmiotu uczestniczącego lub odpowiednich podmiotów uczestniczących.
7. CERT-UE prowadzi ewidencję wszystkich informacji udostępnianych podmiotom uczestniczącym i wymienianych z innymi stronami. Podmioty uczestniczące mogą zwracać się do CERT-UE o podanie szczegółów dotyczących ich informacji udostępnianych innym stronom.
8. W razie potrzeby CERT-UE może z każdym podmiotem uczestniczącym zawrzeć porozumienie o gwarantowanym poziomie usług lub o współpracy w celu świadczenia usług CERT. CERT-UE może również zawrzeć porozumienie o gwarantowanym poziomie usług lub o współpracy dotyczącej odpłatnego świadczenia usług CERT dla potrzeb cywilnych unijnych operacji zarządzania kryzysowego na podstawie postanowień tytułu V rozdział 2 Traktatu o Unii Europejskiej. Niezależnie od przypadku takie porozumienia o gwarantowanym poziomie usług lub o współpracy musi zatwierdzić Rada Sterująca.

Artykuł 4

Współpraca CERT-UE z zespołami CERT państw członkowskich

1. CERT-UE współpracuje i wymienia z krajowymi lub rządowymi zespołami CERT lub CSIRT państw członkowskich informacje na temat zagrożeń dla bezpieczeństwa cybernetycznego, słabości i incydentów cybernetycznych, ewentualnych środków zaradczych, a także we wszystkich sprawach mających znaczenie dla poprawy ochrony infrastruktury ICT podmiotów uczestniczących, w tym za pośrednictwem sieci CSIRT, o której mowa w art. 12 dyrektywy NIS.

2. CERT-UE współpracuje z zespołami CERT państw członkowskich w celu zbierania informacji na temat ogólnych i szczegółowych zagrożeń dotyczących podmiotów uczestniczących oraz na temat narzędzi lub metod, w tym technik, taktyk i procedur, najlepszych praktyk i ogólnych słabości, pod kątem przekazywania tych informacji swoim podmiotom uczestniczącym. CERT-UE może wymieniać z takimi zespołami CERT informacje na temat narzędzi lub metod, w tym technik, taktyk i procedur, najlepszych praktyk oraz ogólnych zagrożeń i słabości.
3. Za zgodą dotkniętego incydem podmiotu uczestniczącego CERT-UE może wymieniać z tymi zespołami CERT informacje na temat tego konkretnego incydentu.

Artykuł 5

Współpraca z zespołami CERT podmiotów trzecich i z innymi partnerami

1. CERT-UE może współpracować z zespołami CERT działającymi w konkretnych sektorach przemysłu i z zespołami CERT spoza UE w zakresie narzędzi lub metod, takich jak techniki, taktyki i procedury, najlepsze praktyki oraz ogólne zagrożenia i słabości. Jeśli chodzi o współpracę z takimi zespołami CERT, również w takich konfiguracjach, w których zespoły CERT spoza UE współpracują z zespołami CERT z państw członkowskich, CERT-UE musi uzyskać uprzednią zgodę Rady Sterującej.
2. CERT-UE może współpracować z innymi partnerami, takimi jak podmioty komercyjne lub poszczególni eksperci, w celu zebrania informacji na temat ogólnych i szczegółowych zagrożeń, słabości i ewentualnych środków zaradczych. Jeśli chodzi o szerszą współpracę z takimi partnerami, CERT-UE musi uzyskać uprzednią zgodę Rady Sterującej.
3. Jeżeli z danym partnerem podpisano porozumienie lub umowę poufności, CERT-UE może za zgodą podmiotu uczestniczącego dotkniętego incydem udostępnić takim partnerom informacje na temat konkretnego incydentu w organizacji podmiotu uczestniczącego, o ile mogą one przyczynić się do analizy tego incydentu. Takie porozumienia lub umowy poufności podlegają weryfikacji prawnej zgodnie z odpowiednimi procedurami wewnętrznymi Komisji. Porozumienia czy umowy poufności nie wymagają uprzedniej zgody Rady Sterującej, ale o ich zawarciu informuje się przewodniczącego tego organu.
4. Za uprzednią zgodą Rady Sterującej CERT-UE może w drodze wyjątku zawierać porozumienia o gwarantowanym poziomie usług z podmiotami innymi niż podmioty uczestniczące.

Artykuł 6

Zadania szefa CERT-UE

1. Szef CERT-UE jest odpowiedzialny za sprawne funkcjonowanie zespołu, działając w ramach swoich kompetencji pod kierunkiem Rady Sterującej. Jest on odpowiedzialny za wprowadzanie w życie strategicznego kierunku, wytycznych, celów i priorytetów określonych przez Radę Sterującą i za należyte zarządzanie CERT-UE, w tym jego zasobami finansowymi i ludzkimi. Przedstawia on regularne sprawozdania przewodniczącemu Rady Sterującej.
2. Szefa CERT-UE obowiązują przepisy mające zastosowanie do Komisji i działa on jako subdelegowany urzędnik zatwierdzający w ramach wykonywania budżetu ogólnego Unii Europejskiej, zgodnie z właściwymi przepisami wewnętrznymi Komisji w sprawie delegowania uprawnień i ograniczeń w takich przypadkach. Działa on pod zwierzchnictwem Komisji wyłącznie dla potrzeb stosowania przepisów i procedur administracyjnych i finansowych.
3. Szef CERT-UE przedkłada Radzie Sterującej kwartalne sprawozdania dotyczące funkcjonowania CERT-UE, wykonania budżetu, zawartych umów lub innych porozumień i podróży służbowych personelu. Przedkłada on również roczne sprawozdanie Radzie Sterującej zgodnie z art. 8 ust. 1 lit. e).
4. 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. 66 ust. 9 rozporządzenia finansowego i regularnie składa mu sprawozdania z realizacji działań, co do których szefowi CERT-UE przekazano uprawnienia na zasadzie subdelegacji.
5. Szef CERT-UE opracowuje co roku plan finansowy w zakresie dochodów i wydatków administracyjnych w związku z działalnością zespołu, który ma zostać zatwierdzony przez Radę Sterującą zgodnie z art. 8 ust. 1 lit. c).

Artykuł 7

Rada Sterująca

1. Rada Sterująca zapewnia CERT-UE strategiczny kierunek i wytyczne oraz monitoruje realizację ogólnych priorytetów i celów zespołu. Jej członkami są przedstawiciele kierownictwa wyższego szczebla wyznaczeni przez każde z państw sygnatariuszy niniejszego porozumienia oraz przez ENISA, która reprezentuje interesy agencji wymienionych w załączniku I eksploatujących własną infrastrukturę ICT. Członkowie mogą być wspomagani przez zastępców. Inni przedstawiciele podmiotów uczestniczących mogą zostać zaproszeni przez przewodniczącego do obecności na posiedzeniach Rady Sterującej.
2. Spośród swoich członków Rada Sterująca wyznacza przewodniczącego na dwuletnią kadencję. Zastępca takiego członka staje się w tym samym okresie pełnoprawnym członkiem Rady.
3. Rada Sterująca zbiera się z inicjatywy przewodniczącego lub na wniosek któregośkolwiek z jej członków. Przyjmuje swój regulamin wewnętrzny.
4. Każdy sygnatariusz niniejszego porozumienia i ENISA dysponuje jednym głosem – prawo głosu jest wykonywane przez odpowiedniego członka lub członków. Decyzje Rady Sterującej podejmowane są zwykłą większością głosów, chyba że postanowiono inaczej. Przewodniczący nie bierze udziału w głosowaniu z wyjątkiem przypadków równej liczby głosów, kiedy to dysponuje on głosem rozstrzygającym.
5. Jeżeli konieczne będzie podjęcie pilnych decyzji ze względów operacyjnych, Rada Sterująca może w drodze wyjątku działać za zgodą przewodniczącego i podmiotów uczestniczących reprezentujących Komisję Europejską, Radę, Parlament Europejski oraz dotkniętego incydem podmiotu uczestniczącego lub dotkniętych incydem podmiotów uczestniczących.
6. Rada Sterująca może stanowić w drodze uproszczonej procedury pisemnej zainicjowanej przez przewodniczącego, zgodnie z którą odpowiednią decyzję uznaje się za przyjętą w terminie ustalonym przez przewodniczącego, chyba że któryś z członków wyrazi sprzeciw.
7. Szef CERT-UE uczestniczy w posiedzeniach Rady Sterującej, chyba że zadecyduje ona inaczej.
8. Sekretariat Rady Sterującej organizuje instytucja, której przedstawiciel kierownictwa wyższego szczebla jest przewodniczącym.
9. Sekretariat informuje agencje UE wymienione w załączniku I o decyzjach Rady Sterującej. Każda agencja UE jest uprawniona do przedkładania przewodniczącemu Rady Sterującej wszelkich kwestii, o których, jej zdaniem, należy powiadomić Radę Sterującą.

Artykuł 8

Zadania Rady Sterującej

1. W celu nadania CERT-UE strategicznego kierunku i wytycznych Rada Sterująca w szczególności:
 - (a) zatwierdza, na wniosek szefa CERT-UE, roczny program prac CERT-UE i monitoruje jego realizację;
 - (b) zatwierdza, na wniosek szefa CERT-UE, katalog usług CERT-UE;
 - (c) zatwierdza, na podstawie projektu sporządzonego przez szefa CERT-UE, plan finansowy w zakresie dochodów i wydatków, w tym dotyczących personelu, w związku z działalnością CERT-UE;
 - (d) zatwierdza co roku, na wniosek szefa CERT-UE, kwotę rocznych środków finansowych wypłacanych w zamian za usługi świadczone podmiotom uczestniczącym i stronom trzecim, które podpisały z CERT-UE porozumienia o gwarantowanym poziomie usług;
 - (e) analizuje i zatwierdza sprawozdanie roczne, sporządzone przez szefa CERT-UE, obejmujące działalność CERT-UE i zarządzanie środkami finansowymi przez ten zespół;

- (f) zatwierdza i monitoruje kluczowe wskaźniki skuteczności działania w odniesieniu do CERT-UE, określone na wniosek szefa zespołu;
 - (g) zatwierdza dokumenty CERT-UE określające ogólne polityki i wytyczne, w których znajdują się zalecenia w zakresie dobrych praktyk bezpieczeństwa ICT, których powinny przestrzegać podmioty uczestniczące;
 - (h) zatwierdza porozumienia o współpracy oraz porozumienia lub umowy o gwarantowanym poziomie usług między CERT-UE a innymi podmiotami na mocy art. 3 ust. 8 i art. 5 ust. 4;
 - (i) w razie potrzeby tworzy grupy doradztwa technicznego w celu wsparcia prac Rady Sterującej, zatwierdza ich zakresy uprawnień i wyznacza ich przewodniczących; oraz
 - (j) zmienia zawarty w załączniku I wykaz agencji Unii, które stosują niniejsze porozumienie.
2. Przewodniczący może reprezentować Radę Sterującą lub działać w jej imieniu, zgodnie z uzgodnieniami poczynionymi przez tę radę.

Artykuł 9

Sprawy dotyczące personelu i finansów

1. CERT-UE jest ustanowiony jako autonomiczny, międzyinstytucjonalny dostawca usług dla wszystkich instytucji, organów i agencji Unii, wchodzi jednak w skład struktury administracyjnej dyrekcji generalnej Komisji, aby korzystać z komisyjnych struktur wsparcia administracyjnego, finansowego, zarządczego i rachunkowego. Komisja informuje Radę Sterującą o umiejscowieniu CERT-UE w strukturze administracyjnej oraz o wszelkich zmianach w tym zakresie.
2. Komisja, po uzyskaniu jednomyślnej zgody Rady Sterującej, powołuje szefa CERT-UE. Na wszystkich etapach procedury poprzedzającej mianowanie szefa CERT-UE, w szczególności podczas przygotowywania ogłoszeń o naborze, rozpatrywania zgłoszeń oraz powoływania komisji selekcyjnych w odniesieniu do tego stanowiska zasięga się opinii Rady Sterującej.
3. Urzędnicy wszystkich instytucji i organów Unii są informowani o wszelkich ogłoszeniach o naborze na stanowiska w CERT-UE.
4. Z zastrzeżeniem prerogatyw władzy budżetowej Unii, instytucje i organy Unii uczestniczące w niniejszym porozumieniu, z wyjątkiem Europejskiego Trybunału Obrachunkowego, Europejskiego Banku Centralnego i Europejskiego Banku Inwestycyjnego, zobowiązują się do przeniesienia lub scedowania na rzecz CERT-UE, do roku budżetowego 2019 lub w innym terminie, ustalonym w załączniku II, liczby stanowisk określonej w załączniku II. Instytucje i organy Unii przenoszące lub cedujące określoną liczbę stanowisk otrzymują od CERT-UE obsługę w pełnym zakresie. Liczba stanowisk określona w załączniku II jest poddawana regularnemu przeglądowi co najmniej raz na pięć lat.
5. CERT-UE może porozumieć się z uczestniczącymi instytucjami i organami Unii w sprawie tymczasowego przydzielenia CERT-UE dodatkowego personelu.
6. Europejski Trybunał Obrachunkowy, Europejski Bank Centralny oraz Europejski Bank Inwestycyjny zawierają porozumienia o gwarantowanym poziomie usług w zakresie usług oferowanych przez CERT-UE zgodnie z jego katalogiem usług oraz z ich roczną rekompensatą finansową, którą każda z przedmiotowych instytucji jest zobowiązana wypłacić zgodnie z załącznikiem II na początku każdego roku obrachunkowego w zamian za usługi świadczone przez CERT-UE w ciągu poprzedniego roku budżetowego.
7. Rekompensata finansowa, która ma zostać wypłacona przez każdą agencję Unii w celu pokrycia kosztów oferty usług CERT-UE, jest uzgadniana z poszczególnymi agencjami Unii i uwzględniana w ogólnych ramach administracyjnych regulujących świadczenie przez Komisję usług na rzecz agencji Unii.
8. Szef CERT-UE co roku składa sprawozdanie na temat wysokości rocznej rekompensaty finansowej, którą mają wypłacić podmioty uczestniczące, które podpisały z CERT-UE porozumienia o gwarantowanym poziomie usług – zgodnie z ust. 6 oraz agencje Unii – zgodnie z ust. 7. Rada Sterująca co roku dokonuje przeglądu tej kwoty rocznej rekompensaty finansowej.

9. Zarządzaniem budżetem i finansami CERT-UE, w tym dochodami przeznaczonymi na określony cel z innych instytucji lub organów Unii, zajmuje się Komisja zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE, Euratom) nr 966/2012⁽¹⁾ w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii i innymi właściwymi zasadami i przepisami. Wszelkie środki lub dochody budżetowe przekazywane CERT-UE na mocy porozumień o gwarantowanym poziomie usług będą wyraźnie określone w planie finansowym.

Artykuł 10

Tajemnica zawodowa

CERT-UE i podmioty uczestniczące traktują wszelkie informacje otrzymane od innego podmiotu uczestniczącego lub strony trzeciej jako podlegające obowiązkowi zachowania tajemnicy zawodowej, zgodnie z art. 339 Traktatu o funkcjonowaniu Unii Europejskiej lub na mocy równoważnych, mających zastosowanie ram prawnych. Nie ujawniają żadnych takich informacji stronom trzecim, chyba że zostaną do tego wyraźnie upoważnieni przez dany podmiot uczestniczący lub daną stronę.

Artykuł 11

Ochrona danych osobowych

Przetwarzanie danych osobowych prowadzone na mocy niniejszego porozumienia podlega przepisom rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady⁽²⁾.

Artykuł 12

Audyt, pytania i publiczny dostęp do dokumentów

1. Funkcję audytora wewnętrznego pełni komisyjna Służba Audytu Wewnętrznego, przestrzegając postanowień art. 10. Rada Sterująca może sugerować służbie przeprowadzanie audytów.
2. Odpowiadanie na pytania Europejskiego Rzecznika Praw Obywatelskich i Europejskiego Inspektora Ochrony Danych należy, zgodnie z procedurami wewnętrznymi Komisji, do obowiązków szefa CERT-UE.
3. Procedury Komisji na podstawie rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady⁽³⁾ mają zastosowanie w odniesieniu do wniosków o publiczny dostęp do dokumentów będących w posiadaniu CERT-UE z uwzględnieniem zobowiązania do konsultowania się, w myśl tego rozporządzenia, z innymi podmiotami uczestniczącymi, w przypadku gdy wnioski dotyczą ich dokumentów.

Artykuł 13

Przegląd

Z uwagi na zmieniającą się sytuację w zakresie zagrożenia cybernetycznego i unijną reakcją na nią, w tym priorytety polityczne określone w strategii Unii Europejskiej w zakresie bezpieczeństwa cybernetycznego, Rada Sterująca regularnie dokonuje przeglądu organizacji i funkcjonowania CERT-UE. Może wydawać uczestniczącym instytucjom i organom zalecenia dotyczące przeglądu lub zmiany niniejszego porozumienia lub wszelkie inne zalecenia dotyczące skutecznego funkcjonowania CERT-UE.

Artykuł 14

Zakres stosowania i data rozpoczęcia stosowania

1. Niniejsze porozumienie ma zastosowanie do instytucji i organów Unii, które są jego sygnatariuszami, oraz do wymienionych w załączniku I agencji Unii, które eksploatują własną infrastrukturę ICT.
2. Niniejsze porozumienie stosuje się od dnia jego podpisania. Niniejszy tekst zostaje opublikowany w *Dzienniku Urzędowym Unii Europejskiej*.

⁽¹⁾ Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) nr 966/2012 z dnia 25 października 2012 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii oraz uchylające rozporządzenie Rady (WE, Euratom) nr 1605/2002 (Dz.U. L 298 z 26.10.2012, s. 1).

⁽²⁾ Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

⁽³⁾ 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).

Niniejsze porozumienie sporządzone jest w jednym oryginalnym egzemplarzu w językach: angielskim, bułgarskim, chorwackim, czeskim, duńskim, estońskim, fińskim, francuskim, greckim, hiszpańskim, litewskim, łotewskim, maltańskim, niderlandzkim, niemieckim, polskim, portugalskim, rumuńskim, słowackim, słoweńskim, szwedzkim, węgierskim i włoskim, i zostaje złożone do depozytu Sekretariatowi Generalnemu Rady Unii Europejskiej, który przekaże uwierzytelniony odpis każdemu z sygnatariuszy.

Sporządzono we Frankfurcie, w Luksemburgu i Brukseli dnia 20 grudnia 2017 r.

W imieniu Parlamentu Europejskiego

K. WELLE

Sekretarz Generalny

W imieniu Rady Europejskiej i Rady

J. TRANHOLM-MIKKELSEN

Sekretarz Generalny

W imieniu Komisji Europejskiej

A. ITALIANER

Sekretarz Generalny

W imieniu Trybunału Sprawiedliwości Unii Europejskiej

F. SCHAFF

Dyrektor Generalny DG ds. Infrastruktury

W imieniu Europejskiego Banku Centralnego

K. DE GEEST

Dyrektor Generalny ds. Systemów Informacyjnych

W imieniu Europejskiego Trybunału Obrachunkowego

E. RUIZ GARCÍA

Sekretarz Generalny

M. DIEMER

Dyrektor ds. administracyjnych

W imieniu Europejskiej Służby Działań Zewnętrznych

G. DI VITA

Dyrektor Generalny ds. Budżetu i Administracji

W imieniu Komitetu Ekonomiczno-Społecznego

L. PLANAS PUCHADES

Sekretarz Generalny

W imieniu Europejskiego Komitetu Regionów

J. BURIÁNEK

Sekretarz Generalny

W imieniu Europejskiego Banku Inwestycyjnego

P. KLAEDTKE

Dyrektor Generalny i Kontroler Finansowy

ZAŁĄCZNIK I

Wykaz agencji UE, o których mowa w art. 14 ust. 1

ACER	Agencja ds. Współpracy Organów Regulacji Energetyki
Urząd BEREC	Organ Europejskich Regulatorów Łączności Elektronicznej
CPVO	Wspólnotowy Urząd Ochrony Odmian Roślin
EU-OSHA	Europejska Agencja Bezpieczeństwa i Zdrowia w Pracy
Frontex	Europejska Agencja Straży Granicznej i Przybrzeżnej
eu-LISA	Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości
EASO	Europejski Urząd Wsparcia w dziedzinie Azylu
EASA	Europejska Agencja Bezpieczeństwa Lotniczego
EUNB	Europejski Urząd Nadzoru Bankowego
ECDC	Europejskie Centrum ds. Zapobiegania i Kontroli Chorób
Cedefop	Europejskie Centrum Rozwoju Kształcenia Zawodowego
ECHA	Europejska Agencja Chemikaliów
EEA	Europejska Agencja Środowiska
EFCA	Europejska Agencja Kontroli Rybołówstwa
EFSA	Europejski Urząd ds. Bezpieczeństwa Żywności
Eurofound	Europejska Fundacja na rzecz Poprawy Warunków Życia i Pracy
GSA	Agencja Europejskiego GNSS
EIGE	Europejski Instytut ds. Równości Kobiet i Mężczyzn
EIOPA	Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych
EMSA	Europejska Agencja Bezpieczeństwa Morskiego
EMA	Europejska Agencja Leków
EMCDDA	Europejskie Centrum Monitorowania Narkotyków i Narkomanii
ENISA	Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji
CEPOL	Agencja Unii Europejskiej ds. Szkolenia w Dziedzinie Ścigania
Europol	Agencja Unii Europejskiej ds. Współpracy Organów Ścigania
ERA	Agencja Kolejowa Unii Europejskiej
ESMA	Europejski Urząd Nadzoru Giełd i Papierów Wartościowych
ETF	Europejska Fundacja Kształcenia
FRA	Agencja Praw Podstawowych Unii Europejskiej
EUIPO	Urząd Unii Europejskiej ds. Własności Intelektualnej

Eurojust	Agencja Unii Europejskiej ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych
CdT	Centrum Tłumaczeń dla Organów Unii Europejskiej
EDA	Europejska Agencja Obrony
EIT	Europejski Instytut Innowacji i Technologii
IUESB	Instytut Unii Europejskiej Studiów nad Bezpieczeństwem
SATCEN	Centrum Satelitarne Unii Europejskiej
SRB	Jednolita Rada ds. Restrukturyzacji i Uporządkowanej Likwidacji

ZAŁĄCZNIK II

Stanowiska pełnoetatowe lub wkłady do budżetu wnoszone do CERT-UE przez członków

STANOWISKA PRZEWIDZIANE W PLANIE ZATRUDNIENIA

Institucja/organ	Względny udział personelu UE	Odpowiednie stanowiska pełnoetatowe, które mają być przeniesione lub sędowane do CERT-UE
Parlament Europejski	19,5 %	3 ⁽¹⁾
Rada Europejska / Rada	9 %	2
Komisja ⁽²⁾	55 %	8
Trybunał Sprawiedliwości	6 %	1 ⁽³⁾
Europejska Służba Działań Zewnętrznych	4,5 %	1 ⁽⁴⁾
Europejski Komitet Ekonomiczno-Społeczny/ Europejski Komitet Regionów	3,5 %	1 ⁽⁵⁾
Europejski Trybunał Obrachunkowy	2,5 %	0 ⁽⁶⁾
	OGÓŁEM:	16

Roczne zobowiązania finansowe na rzecz CERT-UE

Europejski Bank Centralny ⁽⁷⁾	120 000 EUR ⁽⁸⁾
Europejski Bank Inwestycyjny ⁽⁷⁾	120 000 EUR ⁽⁸⁾

⁽¹⁾ Parlament Europejski dokona przeniesienia dwóch pozostałych stanowisk najpóźniej w budżecie na rok 2021. W międzyczasie podejmuje się utrzymać obecny poziom zobowiązań: połowa etatu oddana do dyspozycji CERT-UE oraz coroczny wkład finansowy (120 000 EUR) przewidziany w porozumieniu o gwarantowanym poziomie usług.

⁽²⁾ W przypadku Komisji stanowiska będą wewnętrznie przekazywane na rzecz CERT-UE. Komisja zapewnia również CERT-UE wkład niepieniężny w formie lokali biurowych, logistyki i infrastruktury informatycznej. Względny udział w planie zatrudnienia personelu sędowanego przez Komisję nie uwzględnia stanowisk w urzędach Unii ani w poszczególnych europejskich agencjach wykonawczych Unii, w przypadku których Komisja zapewnia infrastrukturę informatyczną.

⁽³⁾ Trybunał Sprawiedliwości Unii Europejskiej nie jest w stanie zobowiązać się do przeniesienia stanowiska w terminie przewidzianym w art. 9 ust. 4. Dopóki nie będzie w stanie tego dokonać, podejmuje się utrzymać swój obecny poziom zobowiązań w postaci corocznego wkładu finansowego przewidzianego w porozumieniu o gwarantowanym poziomie usług.

⁽⁴⁾ Europejska Służba Działań Zewnętrznych nie jest w stanie zobowiązać się do przeniesienia stanowiska w terminie przewidzianym w art. 9 ust. 4. Dopóki nie będzie w stanie tego dokonać, podejmuje się utrzymać swój obecny poziom zobowiązań w postaci corocznego wkładu finansowego przewidzianego w porozumieniu o gwarantowanym poziomie usług.

⁽⁵⁾ Europejski Komitet Ekonomiczno-Społeczny i Europejski Komitet Regionów nie są w stanie zobowiązać się do przeniesienia stanowiska w terminie przewidzianym w art. 9 ust. 4. Dopóki nie będą w stanie tego dokonać, podejmują się utrzymać swój obecny poziom zobowiązań w postaci udostępnienia dwóch ekspertów na pół etatu.

⁽⁶⁾ Biorąc pod uwagę względną wielkość Europejskiego Trybunału Obrachunkowego, nie przeniesie on stanowiska, natomiast podejmie na rzecz CERT-UE zobowiązanie finansowe zgodnie z art. 9 ust. 6.

⁽⁷⁾ Jako że Europejski Bank Centralny i Europejski Bank Inwestycyjny nie działają na podstawie regulaminu pracowniczego UE, w związku z czym nie mogą przenosić stanowisk, oba podmioty będą nadal wnosić coroczny wkład finansowy do CERT-UE w ramach porozumienia o gwarantowanym poziomie usług, zgodnie z art. 9 ust. 6.

⁽⁸⁾ Powyższe kwoty mogą ulec zmianie, jak przewidziano w art. 9 ust. 8.