DECYZJA KOMISJI (UE, Euratom) 2018/559

z dnia 6 kwietnia 2018 r.

dotycząca ustanowienia przepisów wykonawczych do art. 6 decyzji (UE, Euratom) 2017/46 w sprawie bezpieczeństwa systemów teleinformatycznych w Komisji Europejskiej

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 249,

uwzględniając Traktat ustanawiający Europejską Wspólnotę Energii Atomowej,

uwzględniając decyzję Komisji (UE, Euratom) 2017/46 z dnia 10 stycznia 2017 r. w sprawie bezpieczeństwa systemów teleinformatycznych w Komisji Europejskiej ([1]), w szczególności jej art. 6,

a także mając na uwadze, co następuje:

(1) W związku z przyjęciem decyzji (UE, Euratom) 2017/46 istnieje potrzeba dokonania przez Komisję przeglądu, aktualizacji i konsolidacji przepisów wykonawczych związanych z uchyloną decyzją Komisji C(2006) 3602 w sprawie bezpieczeństwa systemów teleinformatycznych wykorzystywanych przez Komisję.

(2) Członek Komisji odpowiedzialny za kwestie bezpieczeństwa, w pełnej zgodności z regulaminem wewnętrznym, uprawniony został do ustanowienia przepisów wykonawczych zgodnie z art. 13 decyzji (UE, Euratom) 2017/46 ([2]).

(3) Przepisy wykonawcze zawarte w decyzji C(2006) 3602 powinny zatem zostać uchylone,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

ROZDZIAŁ 1

PRZEPISY OGÓLNE

Artykuł 1

Przedmiot i zakres stosowania

1. Przedmiot i zakres stosowania niniejszej decyzji określone są w art. 1 decyzji (UE, Euratom) 2017/46.

2. Przepisy niniejszej decyzji mają zastosowanie do wszystkich systemów teleinformatycznych (CIS). Obowiązki określone w niniejszej decyzji nie mają jednak zastosowania do systemów teleinformatycznych przetwarzających informacje niejawne UE. Stosowne obowiązki dotyczące tych systemów określane są zgodnie z decyzją Komisji (UE, Euratom) 2015/444 ([3]) przez właściciela systemu i organ ds. bezpieczeństwa Komisji.

3. W rozdziale 2 niniejszej decyzji przedstawiono praktyczne wdrażanie organizacji i obowiązków odnoszących się do bezpieczeństwa informatycznego. Rozdział 3 niniejszej decyzji zawiera przegląd procesów związanych z art. 6 decyzji (UE, Euratom) 2017/46.

Artykuł 2

Definicje

Definicje zawarte w art. 2 decyzji (UE, Euratom) 2017/46 mają zastosowanie do niniejszej decyzji. Na użytek niniejszej decyzji zastosowanie mają również następujące definicje:

1. „Organ ds. zatwierdzania produktów kryptograficznych" („CAA") jest funkcją pełnioną przez organ ds. bezpieczeństwa Komisji podlegający Dyrektorowi Generalnemu ds. Zasobów Ludzkich i Bezpieczeństwa;

([1]) Dz.U. L 6 z 11.1.2017, s. 40.
([2]) Decyzja Komisji C(2017) 7428 final z dnia 8 listopada 2017 r. przyznająca uprawnienia do przyjmowania przepisów wykonawczych, standardów i wytycznych dotyczących bezpieczeństwa systemów komunikacyjnych i informacyjnych w Komisji Europejskiej.
([3]) Decyzja Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 72 z 17.3.2015, s. 53).

2. „Łącze z siecią zewnętrzną” oznacza każde łącze między wewnętrzną siecią Komisji i innymi sieciami, w tym z internetem. Definicja ta wyklucza sieci należące do stron trzecich, udostępnione na podstawie umowy, aby pełnić funkcję części wewnętrznej sieci Komisji.

3. „Deponowanie klucza” oznacza procedurę przechowywania kopii kluczy kryptograficznych przez jedną lub więcej stron, w celu zapewnienia podziału obowiązków, aby umożliwić ich odzyskanie, w przypadku gdy utracona została kopia operacyjna. Klucze mogą zostać podzielone na dwie lub więcej części, z których każdą dysponuje inna osoba, aby zapewnić, że nikt nie ma dostępu do całego klucza.

4. „RASCI” jest skrótem od angielskiego terminu oznaczającego przypisanie odpowiedzialności w oparciu o następujące cechy:

a) R – „responsible” (odpowiedzialny) oznacza zobowiązany do działania i podejmowania decyzji w celu osiągnięcia wymaganych wyników;

b) A – „accountable” (rozliczalny) oznacza odpowiadający za działania, decyzje i wyniki;

c) S – „supports” (wspierający) oznacza zobowiązany do współpracy z osobą odpowiedzialną za wykonanie danego zadania;

d) C – „consulted” (konsultowany) oznacza dyspozycyjny w kwestii porad lub opinii;

e) I – „informed” (poinformowany) oznacza dysponujący na bieżąco odpowiednimi informacjami.

ROZDZIAŁ 2

ORGANIZACJA I ZAKRES OBOWIĄZKÓW

Artykuł 3

Role i obowiązki

Role i obowiązki odnoszące się do art. 4–8 niniejszej decyzji zdefiniowane są w załączniku zgodnie z modelem RASCI.

Artykuł 4

Dostosowanie do polityki Komisji w zakresie bezpieczeństwa informacji

1. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa dokonuje przeglądu polityki Komisji w zakresie bezpieczeństwa informatycznego, a także związanych z nim norm i wytycznych, aby zapewnić, że są one zgodne z ogólną polityką bezpieczeństwa Komisji, w szczególności z decyzją Komisji (UE, Euratom) 2015/443 [1] i decyzją (UE, Euratom) 2015/444.

2. Na wniosek innych służb Komisji Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa może dokonać przeglądu ich strategii w zakresie bezpieczeństwa IT lub innych dokumentów dotyczących tej kwestii, aby zapewnić ich spójność z polityką Komisji w zakresie bezpieczeństwa informacji. Szef odnośnego departamentu Komisji dopilnowuje, by wszelkie niezgodności zostały wyeliminowane.

3. Ponosząc odpowiedzialność za bezpieczeństwo informacji, Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa współpracuje z Dyrekcją Generalną ds. Informatyki w celu zapewnienia, że w procesach bezpieczeństwa IT będą w pełni stosowane klasyfikacja i zasady bezpieczeństwa określone w decyzji (UE, Euratom) 2015/443, w szczególności w jej art. 3 i 9.

ROZDZIAŁ 3

PROCESY BEZPIECZEŃSTWA IT

Artykuł 5

Technologie szyfrowania

1. Stosowanie technologii szyfrowania w celu ochrony niejawnych informacji UE (EUCI) musi być zgodne z decyzją (UE, Euratom) 2015/444.

2. Decyzje w sprawie stosowania technologii szyfrowania w celu ochrony danych niesklasyfikowanych jako niejawne informacje UE podejmowana jest przez właściciela każdego systemu komunikacyjno-informacyjnego, przy uwzględnieniu zarówno ryzyka, które ma zostać ograniczone dzięki zastosowaniu szyfrowania, jak i ryzyka, które się z nim wiąże.

3. W odniesieniu do wszystkich zastosowań technologii szyfrujących wymagane jest uprzednie zatwierdzenie przez organ ds. zatwierdzania produktów kryptograficznych (CAA), chyba że szyfrowanie jest wykorzystywane wyłącznie w celu ochrony poufności przekazywanych danych niebędących niejawnymi informacjami UE i stosowane są standardowe protokoły komunikacji sieciowej.

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

4. Z wyjątkiem przypadku opisanego w ust. 3 niniejszego artykułu departamenty Komisji zapewniają przechowywanie zapasowych kopii wszystkich kluczy deszyfrujących w depozycie do celów możliwego odzyskania przechowywanych danych, w przypadku gdy klucz deszyfrujący nie jest dostępny. Odzyskiwanie zaszyfrowanych danych z wykorzystaniem zapasowych kopii kluczy deszyfrujących przeprowadza się tylko wtedy, gdy jest to dozwolone zgodnie ze standardem określonym przez CAA.

5. Wnioski o udzielenie zgody na wykorzystanie technologii szyfrujących muszą być formalnie udokumentowane i zawierać szczegółowe informacje na temat systemu komunikacyjno-informacyjnego i danych, które mają być chronione, wykorzystywanych technologii oraz związanych z nimi procedur bezpieczeństwa operacyjnego. Takie wnioski o udzielenie zgody muszą być podpisane przez właściciela systemu.

6. Wnioski o udzielenie zgody na wykorzystanie technologii szyfrujących oceniane są przez CAA zgodnie z opublikowanymi normami i wymogami.

Artykuł 6

Kontrole bezpieczeństwa IT

1. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa przeprowadza kontrole bezpieczeństwa IT w celu sprawdzenia, czy środki bezpieczeństwa IT są zgodne z polityką Komisji w tym zakresie i sprawdzenia spójności tych środków kontroli.

2. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa może prowadzić inspekcję bezpieczeństwa IT:

a) z własnej inicjatywy;

b) na wniosek Rady Sterującej ds. Bezpieczeństwa Informacji;

c) na wniosek właściciela systemu;

d) w następstwie incydentu związanego z bezpieczeństwem; lub

e) po stwierdzeniu wysokiego poziomu ryzyka w danym systemie.

3. Właściciele danych mogą złożyć wniosek o przeprowadzenie kontroli bezpieczeństwa IT przed załadowaniem danych do systemu komunikacyjno-informacyjnego.

4. Wyniki kontroli powinny być udokumentowane w formalnym sprawozdaniu dla właściciela systemu, z kopią dla lokalnego pełnomocnika ds. bezpieczeństwa teleinformatycznego i zawierać wnioski i zalecenia mające na celu poprawę zgodności systemu komunikacyjno-informacyjnego z polityką w zakresie bezpieczeństwa IT; Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa zgłasza istotne problemy i przekazuje zalecenia Radzie Sterującej ds. Bezpieczeństwa Informacji.

5. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa monitoruje wdrażanie tych zaleceń.

6. W stosownych przypadkach kontrole bezpieczeństwa IT obejmują kontrolę usług, pomieszczeń i sprzętu dostarczonych właścicielowi systemu. Dotyczy to zarówno wewnętrznych, jak i zewnętrznych podmiotów świadczących dane usługi.

Artykuł 7

Dostęp przez sieci zewnętrzne

1. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa ustanawia zasady w odniesieniu do normy dotyczącej przyznania dostępu pomiędzy systemem komunikacyjno-informacyjnym Komisji a sieciami zewnętrznymi.

2. W przepisach musi być uwzględnione rozróżnienie pomiędzy różnymi rodzajami zewnętrznych połączeń sieciowych i muszą one zawierać odpowiednie zasady bezpieczeństwa w odniesieniu do każdego rodzaju połączenia, w tym również w przypadkach, kiedy wymagane jest uprzednie zezwolenie właściwego organu, jak to określono w ust. 4 niniejszego artykułu.

3. W razie potrzeby zezwolenie udzielane jest w odpowiednim procesie zatwierdzania na podstawie formalnego wniosku. Zezwolenie ważne jest przez określony czas i musi być uzyskane, zanim podłączenie będzie aktywne.

4. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa ponosi ogólną odpowiedzialność za zatwierdzanie wniosków, ale może też przekazać odpowiedzialność za zatwierdzanie niektórych rodzajów połączeń według własnego uznania, zgodnie z art. 17 ust. 3 decyzji (UE, Euratom) 2015/443 i z zastrzeżeniem warunków określonych w ust. 8.

5. Podmiot zatwierdzający może nałożyć dodatkowe wymogi bezpieczeństwa jako warunek zatwierdzenia w celu ochrony systemu komunikacyjno-informacyjnego Komisji i sieci przed zagrożeniami związanymi z nieuprawnionym dostępem lub innymi naruszeniami bezpieczeństwa.

6. Dyrekcja Generalna ds. Informatyki jest podstawowym dostawcą usług sieciowych dla Komisji. Jakikolwiek inny departament Komisji eksploatujący sieć, która nie jest udostępniona przez Dyrekcję Generalną ds. Informatyki, musi najpierw uzyskać zgodę Rady Sterującej ds. Bezpieczeństwa Informacji. Taki departament Komisji dokumentuje uzasadnienie biznesowe dla wniosku i wykazuje, że kontrole sieci są wystarczające do spełnienia odpowiednich wymogów w zakresie przepływu przychodzących i wychodzących informacji.

7. Właściciel systemu komunikacyjno-informacyjnego określa wymogi bezpieczeństwa dotyczące dostępu z zewnątrz do tego systemu i przy wsparciu lokalnego pełnomocnika ds. bezpieczeństwa teleinformatycznego zapewnia stosowanie odpowiednich środków w celu ochrony jego bezpieczeństwa.

8. Środki bezpieczeństwa stosowane w odniesieniu do zewnętrznych połączeń sieciowych oparte są na zasadach ograniczonego dostępu i minimalnego uprzywilejowania, które gwarantują, że określone osoby otrzymują wyłącznie informacje i prawa dostępu potrzebne im do pełnienia obowiązków służbowych na rzecz Komisji.

9. Wszystkie zewnętrzne połączenia sieciowe są filtrowane i monitorowane w celu wykrywania potencjalnych naruszeń bezpieczeństwa.

10. Tam gdzie połączenia zostały ustanowione, aby umożliwić outsourcing systemu komunikacyjno-informacyjnego, zezwolenie uzależnione jest od pomyślnego przeprowadzenia procedury opisanej w art. 8.

Artykuł 8

Outsourcing systemów komunikacyjno-informacyjnych

1. Do celów niniejszej decyzji system komunikacyjno-informacyjny uznaje się za objęty outsourcingiem, w sytuacji gdy jest on zapewniany na podstawie umowy z usługodawcą będącym osobą trzecią, na podstawie której to umowy przedmiotowy system komunikacyjno-informacyjny znajduje się poza lokalami Komisji. Dotyczy to outsourcingu jednego lub wielu systemów komunikacyjno-informacyjnych bądź innych usług informatycznych, ośrodków przetwarzania danych poza lokalami Komisji oraz przetwarzania zestawów danych Komisji przez służby zewnętrzne.

2. Outsourcing systemu komunikacyjno-informacyjnego musi w następujący sposób uwzględniać stopień wrażliwości lub klasyfikację przetwarzanych informacji:

a) akredytacja systemu komunikacyjno-informacyjnego przetwarzającego informacje niejawne UE dokonywana jest zgodnie z decyzją (UE, Euratom) 2015/444, po wcześniejszej konsultacji z organem Komisji ds. akredytacji bezpieczeństwa (SAA). Systemy, w których przetwarzane są informacje niejawne UE, nie mogą być poddane outsourcingowi;

b) właściciel systemu komunikacyjno-informacyjnego przetwarzającego informacje niebędące informacjami niejawnymi UE wdraża proporcjonalne środki w celu zabezpieczenia potrzeb w zakresie bezpieczeństwa, zgodnie z odpowiednimi zobowiązaniami prawnymi i współmiernie do wrażliwości informacji, biorąc pod uwagę ryzyko związane z outsourcingiem. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa może wprowadzić dodatkowe wymagania;

c) przy zlecaniu na zewnątrz projektów w dziedzinie opracowywania rozwiązań uwzględnia się wrażliwość opracowywanego kodu i wszelkich danych użytych do testowania.

3. Do poddanych outsourcingowi systemów komunikacyjno-informacyjnych poza wymogami ustanowionymi w art. 3 decyzji (UE, Euratom) 2017/46 mają zastosowanie następujące zasady:

a) warunki dotyczące outsourcingu muszą być ustalone w taki sposób, aby uniknąć uzależnienia od konkretnych dostawców;

b) warunki dotyczące bezpieczeństwa outsourcingu muszą być ustalone w taki sposób, aby zmniejszać do minimum możliwość dostępu do informacji Komisji lub ich modyfikowania przez personel strony trzeciej;

c) personel strony trzeciej mający dostęp do systemu komunikacyjno-informacyjnego podpisuje zobowiązanie do zachowania poufności;

d) informacja o outsourcingu systemów komunikacyjno-informacyjnych figuruje w dokumentacji tych systemów.

4. Właściciel systemu we współpracy z właścicielem danych:

a) ocenia i dokumentuje ryzyko związane z outsourcingiem;

b) ustanawia odpowiednie wymogi bezpieczeństwa;

c) konsultuje się z właścicielami wszystkich innych podłączonych systemów komunikacyjno-informacyjnych w celu zapewnienia, że ich wymogi bezpieczeństwa są uwzględnione;

d) dopilnowuje, by odpowiednie wymogi i uprawnienia w zakresie bezpieczeństwa były zawarte w umowach z wykonawcami zewnętrznymi;

e) spełnia wszelkie inne wymogi określone w szczegółowej procedurze, zgodnie z ust. 8 niniejszego artykułu.

Działania te zostają zakończone przed podpisaniem umowy lub innego porozumienia dotyczącego outsourcingu jednego lub wielu systemów komunikacyjno-informacyjnych.

5. Właściciele systemu zarządzają ryzykiem związanym z outsourcingiem podczas całego cyklu użytkowania systemu komunikacyjno-informacyjnego, tak aby spełnione były określone wymogi bezpieczeństwa.

6. Właściciele systemu dopilnowują, aby wykonawcy zewnętrzni będący stronami trzecimi byli zobowiązani do niezwłocznego powiadamiania Komisji o wszelkich związanych z bezpieczeństwem IT incydentach dotyczących objętego outsourcingiem systemu Komisji.

7. Właściciel systemu jest odpowiedzialny za zapewnienie zgodności systemu komunikacyjno-informacyjnego, umowy o outsourcingu i ustaleń w zakresie bezpieczeństwa z przepisami Komisji dotyczącymi bezpieczeństwa informacji i bezpieczeństwa informatycznego.

8. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa ustanawia szczegółowe normy związane z obowiązkami i działaniami określonymi w ust. 1–7, zgodnie z art. 10 poniżej.

ROZDZIAŁ 4

PRZEPISY RÓŻNE I KOŃCOWE

Artykuł 9

Przejrzystość

Niniejsza decyzja zostaje podana do wiadomości służb Komisji i wszystkich osób, których dotyczy, oraz zostaje opublikowana w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 10

Standardy

1. W razie potrzeby przepisy niniejszej decyzji mogą zostać szczegółowo określone w standardach lub wytycznych, które mają zostać przyjęte zgodnie z decyzją (UE, Euratom) 2017/46 i decyzją C(2017) 7428. Standardy i wytyczne dotyczące zabezpieczeń informatycznych dostarczą bardziej szczegółowych informacji na temat tych przepisów wykonawczych i decyzji (UE, Euratom) 2017/46 w odniesieniu do konkretnych dziedzin bezpieczeństwa, zgodnie z ISO 27001:2013, załącznik A. Te standardy i wytyczne oparte są na najlepszych praktykach branżowych i zostały wybrane w taki sposób, żeby pasowały do środowiska informatycznego Komisji.

2. W razie potrzeby, zgodnie z ISO 27001:2013, załącznik A, opracowywane są standardy w następujących dziedzinach:

1) organizacja bezpieczeństwa informacji;

2) bezpieczeństwo zasobów ludzkich;

3) zarządzanie aktywami;

4) kontrola dostępu;

5) kryptografia;

6) bezpieczeństwo fizyczne i bezpieczeństwo środowiska;

7) bezpieczeństwo pracy systemu;

8) bezpieczeństwo łączności;

9) zakup, rozwój i utrzymanie systemów;

10) relacje z dostawcami;

11) zarządzanie incydentami związanymi z bezpieczeństwem informacji;

12) aspekty bezpieczeństwa informacji w ramach zarządzania ciągłością działania;

13) zgodność.

3. Rada Sterująca ds. Bezpieczeństwa Informacji zatwierdza normy, o których mowa w ust. 1 i 2 niniejszego artykułu, przed ich przyjęciem.

4. Przepisy wykonawcze do decyzji C(2006) 3602 odnoszące się do zakresu stosowania niniejszej decyzji zostają niniejszym uchylone.

5. Standardy i wytyczne przyjęte na mocy decyzji C(2006) 3602 z dnia 16 sierpnia 2006 r. pozostają w mocy, o ile nie są sprzeczne z niniejszymi przepisami wykonawczymi, do chwili ich uchylenia lub zastąpienia standardami lub wytycznymi, które mają zostać przyjęte zgodnie z art. 13 decyzji (UE, Euratom) 2017/46.

Artykuł 11

Wejście w życie

Niniejsza decyzja wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 6 kwietnia 2018 r.

W imieniu Komisji,
za Przewodniczącego,
Günther OETTINGER
Członek Komisji

ZAŁĄCZNIK

ROLE I OBOWIĄZKI (RASCI)

W modelu RASCI przypisano podmiotom role z zastosowaniem następujących skrótów:

a) R – „responsible” (odpowiedzialny);

b) A – „accountable” (rozliczany);

c) S – „supporting” (wspierający);

d) C – „consulted” (konsultowany);

e) I – „informed” (poinformowany).

Proces: / Rola:	Rada Sterująca ds. Bezpieczeństwa Informacji	HR (DS – Dyrekcja ds. Bezpieczeństwa)	Departamenty Komisji	Właściciel systemu	Właściciel danych	Lokalny pełnomocnik ds. bezpieczeństwa teleinformatycznego	DIGIT	Wykonawcy
Dostosowanie do polityki Komisji w zakresie bezpieczeństwa informacji		**R/A**	**S**				**S**	
Technologie szyfrowania		**C**	**A**	**R**	**I**	**C**		
Kontrole bezpieczeństwa IT	**I**	**A/R**		**S**	**I**	**I**	**S**	
Dostęp przez sieci zewnętrzne	**C** [1]	**C**	**A**	**R**	**I**	**S**	**S**	
Outsourcing systemów komunikacyjno-informacyjnych		**S/C**	**A**	**R/C** [2]	**S**	**C**		**S**

[1] Rada Sterująca ds. Bezpieczeństwa Informacji konsultowana jest w odniesieniu do korzystania z wewnętrznych sieci przez wszystkie departamenty Komisji, inne niż Dyrekcja Generalna ds. Informatyki.

[2] Właściciel systemu komunikacyjno-informacyjnego poddanego outsourcingowi jest podmiotem odpowiedzialnym, a z właścicielem każdego innego systemu komunikacyjno-informacyjnego, z którymi objęty outsourcingiem system jest powiązany, należy się konsultować.