**Dokument ten służy wyłącznie do celów informacyjnych i nie ma mocy prawnej. Unijne instytucje nie ponoszą żadnej odpowiedzialności za jego treść. Autentyczne wersje odpowiednich aktów prawnych, włącznie z ich preambułami, zostały opublikowane w Dzienniku Urzędowym Unii Europejskiej i są dostępne na stronie EUR-Lex. Bezpośredni dostęp do tekstów urzędowych można uzyskać za pośrednictwem linków zawartych w dokumencie**

►**B**

# DECYZJA KOMISJI (UE, Euratom) 2017/46

## z dnia 10 stycznia 2017 r.

## w sprawie bezpieczeństwa systemów teleinformatycznych w Komisji Europejskiej

(Dz.U. L 6 z 11.1.2017, s. 40)

sprostowane przez:

►**C1** Sprostowanie, Dz.U. L 261 z 11.10.2017, s. 31 (2017/46)

▼B

# DECYZJA KOMISJI (UE, Euratom) 2017/46

## z dnia 10 stycznia 2017 r.

## w sprawie bezpieczeństwa systemów teleinformatycznych w Komisji Europejskiej

ROZDZIAŁ 1

## PRZEPISY OGÓLNE

*Artykuł 1*

### Przedmiot i zakres stosowania

1. Niniejsza decyzja ma zastosowanie do wszystkich systemów teleinformatycznych (CIS) posiadanych, zamawianych, zarządzanych i obsługiwanych przez Komisję lub w jej imieniu oraz do każdorazowego wykorzystania przedmiotowych CIS przez Komisję.

2. W niniejszej decyzji ustanawia się podstawowe zasady, cele, organizację i obowiązki dotyczące bezpieczeństwa wspomnianych CIS, w szczególności w odniesieniu do departamentów Komisji posiadających, zamawiających, zarządzających lub obsługujących CIS, w tym CIS zapewnianych przez wewnętrznego dostawcę usług informatycznych. Jeżeli CIS jest zapewniany, posiadany, zarządzany lub obsługiwany przez podmiot zewnętrzny na podstawie porozumienia dwustronnego lub umowy dwustronnej z Komisją, postanowienia tego rodzaju porozumienia lub umowy muszą być zgodne z niniejszą decyzją.

3. Niniejsza decyzja ma zastosowanie do wszystkich departamentów Komisji i agencji wykonawczych. Jeżeli z CIS Komisji korzystają inne organy i instytucje na podstawie porozumienia dwustronnego z Komisją, postanowienia tego porozumienia muszą być zgodne z niniejszą decyzją.

4. Bez uszczerbku dla jakichkolwiek konkretnych wskazań dotyczących poszczególnych grup pracowników, niniejsza decyzja ma zastosowanie do członków Komisji, pracowników Komisji objętych regulaminem pracowniczym urzędników Unii Europejskiej („regulamin pracowniczy”) i warunkami zatrudnienia innych pracowników Unii Europejskiej ([1]), ekspertów krajowych oddelegowanych do Komisji („oddelegowani eksperci krajowi”) ([2]), zewnętrznych dostawców usług i ich pracowników, stażystów oraz do wszystkich osób mających dostęp do CIS objętego zakresem niniejszej decyzji.

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

([2]) Decyzja Komisji z dnia 12 listopada 2008 r. dotycząca zasad mających zastosowanie do oddelegowanych ekspertów krajowych i ekspertów krajowych odbywających kształcenie zawodowe w ramach służb Komisji (C(2008) 6866 final).

▼B

5. Niniejsza decyzja ma zastosowanie do Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych (OLAF) w zakresie, w jakim jest zgodna z przepisami Unii i z decyzją Komisji 1999/352/WE, EWWiS, Euratom ([1]). W szczególności środków przewidzianych w niniejszej decyzji, w tym instrukcji, inspekcji, dochodzeń i środków równoważnych, nie można stosować w odniesieniu do CIS Urzędu, jeżeli narusza to niezależność funkcji dochodzeniowej Urzędu lub poufność informacji otrzymanych przez Urząd w ramach sprawowanej przez niego funkcji.

*Artykuł 2*

**Definicje**

Do celów niniejszej decyzji stosuje się następujące definicje:

1) „rozliczany” oznacza odpowiadający za działania, decyzje i wyniki;

2) „CERT–UE” oznacza zespół reagowania na incydenty komputerowe w instytucjach i agencjach UE. Jego zadaniem jest wspieranie instytucji europejskich w zakresie ochrony przed umyślnymi i złośliwymi atakami, które mogłyby naruszyć integralność ich aktywów IT i narazić na szkodę interesy UE. Zakres działań CERT–UE obejmuje zapobieganie, wykrywanie, reagowanie i przywracanie;

3) „departament Komisji” oznacza każdą dyrekcję generalną lub służbę Komisji lub każdy gabinet członka Komisji;

4) „organ ds. bezpieczeństwa Komisji” odnosi się do roli ustanowionej w decyzji (UE, Euratom) 2015/444;

5) „system teleinformatyczny” lub „CIS” oznacza każdy system umożliwiający przetwarzanie informacji w formie elektronicznej, w tym wszystkie zasoby niezbędne do jego działania, a także infrastrukturę, organizację, pracowników i zasoby informatyczne. Definicja ta obejmuje aplikacje biznesowe, wspólne usługi IT, systemy obsługiwane na zewnątrz oraz urządzenia użytkownika końcowego;

6) „Rada Zarządzania Korporacyjnego” zapewnia najwyższy poziom nadzoru zarządzania korporacyjnego w zakresie kwestii operacyjnych i administracyjnych w Komisji;

7) „właściciel danych” oznacza osobę odpowiedzialną za zapewnienie ochrony i wykorzystania konkretnych danych przetwarzanych przez CIS;

8) „zbiór danych” oznacza zbiór informacji przeznaczony do celów konkretnego procesu biznesowego lub działania Komisji;

9) „procedura awaryjna” oznacza uprzednio określony zbiór metod i obowiązków na potrzeby reagowania na nagłe sytuacje, mających zapobiec istotnemu oddziaływaniu na Komisję;

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

▼B

10) „polityka w zakresie bezpieczeństwa informacji” oznacza zbiór celów związanych z bezpieczeństwem informacji, które są lub mają zostać ustanowione, wdrożone i sprawdzone. Obejmuje ona między innymi decyzje (UE, Euratom) 2015/444 i (UE, Euratom) 2015/443;

11) „Rada Sterująca ds. Bezpieczeństwa Informacji” oznacza organ zarządzający, który wspiera Radę Zarządzania Korporacyjnego w jej zadaniach związanych z bezpieczeństwem IT;

12) „wewnętrzny dostawca usług IT” oznacza departament Komisji świadczący wspólne usługi IT;

13) „bezpieczeństwo IT” lub „bezpieczeństwo CIS” oznacza zachowanie poufności, integralności i dostępności CIS oraz zbiorów danych, które są w nich przetwarzane;

14) „wytyczne w sprawie bezpieczeństwa IT” obejmują zalecane, ale dobrowolne środki, które mają na celu wsparcie norm bezpieczeństwa IT lub służą jako odniesienie w przypadku, w którym nie została wprowadzona żadna norma;

15) „incydent związany z bezpieczeństwem IT” oznacza każde zdarzenie, które mogłyby negatywnie wpłynąć na poufność, integralność lub dostępność CIS;

16) „środek bezpieczeństwa IT” oznacza środek techniczny lub organizacyjny mający na celu ograniczanie ryzyka związanego z bezpieczeństwem IT;

17) „potrzeba w zakresie bezpieczeństwa IT” oznacza dokładną i jednoznaczną definicję poziomów poufności, integralności i dostępności związanych z informacją lub systemem IT w celu określenia wymaganego poziomu ochrony;

18) „cel związany z bezpieczeństwem IT” oznacza oświadczenie o zamiarze przeciwdziałania określonym zagrożeniom lub spełnienia określonych organizacyjnych wymogów lub założeń związanych z bezpieczeństwem;

19) „plan bezpieczeństwa IT” oznacza dokumentację środków bezpieczeństwa IT, które są wymagane, by spełnić potrzeby CIS w zakresie bezpieczeństwa IT;

20) „polityka w zakresie bezpieczeństwa IT” oznacza zbiór celów związanych z bezpieczeństwem IT, które są lub mają zostać ustanowione, wdrożone i sprawdzone. Obejmuje ona niniejszą decyzję i jej przepisy wykonawcze;

21) „wymóg bezpieczeństwa IT” oznacza potrzebę w zakresie bezpieczeństwa IT sformalizowaną za pośrednictwem uprzednio zdefiniowanego procesu;

22) „ryzyko związane z bezpieczeństwem IT” oznacza wpływ, jaki zagrożenie dla bezpieczeństwa IT może wywrzeć na CIS, wykorzystując jego podatność; ryzyko związane z bezpieczeństwem IT jako takie charakteryzują dwa czynniki: 1) niepewność, tj. prawdopodobieństwo, że zagrożenie związane z bezpieczeństwem IT spowoduje niepożądane zdarzenie; oraz 2) wpływ, tj. konsekwencje, jakie tego rodzaju niepożądane zdarzenie może mieć dla CIS;

▼B

23) „normy bezpieczeństwa IT” oznaczają szczególne obowiązkowe środki bezpieczeństwa IT, które ułatwiają egzekwowanie i wspieranie polityki w zakresie bezpieczeństwa IT;

24) „strategia bezpieczeństwa IT” oznacza zbiór projektów i działań, które mają ułatwić realizację celów Komisji i które muszą zostać ustanowione, wdrożone i sprawdzone;

25) „zagrożenie związane z bezpieczeństwem IT” oznacza czynnik mogący potencjalnie doprowadzić do niepożądanego zdarzenia, które może zaszkodzić CIS; tego rodzaju zagrożenia mogą być przypadkowe lub zamierzone i obejmują elementy zagrażające, potencjalne cele i metody ataku;

26) „lokalny pełnomocnik ds. bezpieczeństwa teleinformatycznego” oznacza urzędnika odpowiedzialnego za kontakty w zakresie bezpieczeństwa IT w danym departamencie Komisji;

27) „dane osobowe”, „przetwarzanie danych osobowych”, „administrator danych” i „zbiór danych osobowych” mają takie samo znaczenie jak w rozporządzeniu (WE) nr 45/2001, w szczególności w jego art. 2;

28) „przetwarzanie informacji” oznacza wszystkie funkcje CIS w odniesieniu do zbiorów danych, w tym tworzenie, modyfikację, wyświetlanie, przechowywanie, przesyłanie, usuwanie i archiwizowanie informacji; CIS może zapewniać przetwarzanie informacji jako zbiór funkcji na potrzeby użytkowników i jako usługi IT w stosunku do innych CIS;

29) „tajemnica zawodowa” oznacza ochronę informacji związanych z danymi biznesowymi objętych ze względu na swój charakter tajemnicą zawodową, a zwłaszcza informacji dotyczących przedsiębiorstw i ich stosunków handlowych lub kosztów własnych zgodnie z art. 339 TFUE;

30) „odpowiedzialny” oznacza zobowiązany do działania i podejmowania decyzji w celu osiągnięcia wymaganych wyników;

31) „bezpieczeństwo w Komisji” oznacza bezpieczeństwo osób, mienia i informacji w Komisji, a w szczególności integralność fizyczną osób i mienia, integralność, poufność i dostępność informacji i systemów teleinformatycznych, jak również swobodne funkcjonowanie działań Komisji;

32) „wspólna usługa IT” oznacza usługę świadczoną przez CIS na rzecz innych CIS w zakresie przetwarzania informacji;

33) „właściciel systemu” oznacza jednostkę odpowiedzialną w ogólnym ujęciu za udzielenie zamówienia na CIS, jego opracowywanie, integrację, modyfikację, działanie, utrzymywanie i wycofanie;

34) „użytkownik” oznacza każdą osobę wykorzystującą funkcję zapewnianą przez CIS zarówno w samej Komisji, jak i poza nią.

*Artykuł 3*

**Zasady bezpieczeństwa IT w Komisji**

1. Bezpieczeństwo IT w Komisji opiera się na zasadach legalności, przejrzystości, proporcjonalności i odpowiedzialności.

▼B

2. Kwestie związane z bezpieczeństwem IT uwzględnia się od początku procesu opracowywania i wdrażania CIS Komisji. W tym celu zaangażowane są Dyrekcja Generalna ds. Informatyki i Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa w ramach ich odpowiednich zakresów odpowiedzialności.

3. Skuteczne bezpieczeństwo IT zapewnia odpowiednie poziomy:

a) autentyczności: gwarancja, że informacje są prawdziwe i pochodzą z rzetelnych źródeł;

b) dostępności: cecha polegająca na tym, że informacje są dostępne i gotowe do wykorzystania na wniosek uprawnionego podmiotu;

c) poufności: cecha polegająca na tym, że informacje nie są ujawniane nieupoważnionym osobom lub podmiotom ani do celów nieuprawnionego przetwarzania;

d) integralności: cecha polegająca na zachowywaniu dokładności i kompletności zasobów i informacji;

e) niezaprzeczalności: możliwość udowodnienia, że działanie lub zdarzenie miało miejsce, aby następnie nie można było zaprzeczyć wystąpieniu tego działania lub zdarzenia.

f) ochrony danych osobowych: zapewnianie odpowiednich zabezpieczeń w odniesieniu do danych osobowych jest w pełni zgodne z rozporządzeniem (WE) nr 45/2001;

g) tajemnicy zawodowej: ochrona informacji objętych ze względu na swój charakter tajemnicą zawodową, a zwłaszcza informacji dotyczących przedsiębiorstw i ich stosunków handlowych lub kosztów własnych zgodnie z art. 339 TFUE.

4. Bezpieczeństwo IT opiera się na procesie zarządzania ryzykiem. Celem tego procesu jest określenie poziomów rodzajów ryzyka związanego z bezpieczeństwem IT i określenie środków bezpieczeństwa mających na celu ograniczenie takich rodzajów ryzyka do określonego poziomu przy zachowaniu proporcjonalnych kosztów.

5. Każdy CIS musi zostać zidentyfikowany, przypisany do właściciela systemu i zapisany w wykazie.

6. Wymogi dotyczące bezpieczeństwa wszystkich CIS określa się na podstawie ich potrzeb w zakresie bezpieczeństwa oraz potrzeb w zakresie bezpieczeństwa informacji, które przetwarzają. CIS, które świadczą usługi na rzecz innych CIS, mogą być projektowane w taki sposób, aby wspierać określone poziomy potrzeb w zakresie bezpieczeństwa.

7. Plany bezpieczeństwa IT i środki bezpieczeństwa IT są proporcjonalne do potrzeb w zakresie bezpieczeństwa CIS.

▼C1

8. Procesy związane z zasadami i działaniami określonymi w ust. 1–7 zostają szczegółowo opisane w przepisach wykonawczych zgodnie z art. 13.

▼B

ROZDZIAŁ 2

**ORGANIZACJA I ZAKRES OBOWIĄZKÓW**

*Artykuł 4*

**Rada Zarządzania Korporacyjnego**

Rada Zarządzania Korporacyjnego ponosi ogólną odpowiedzialność za zarządzanie całym bezpieczeństwem IT w Komisji.

*Artykuł 5*

**Rada Sterująca ds. Bezpieczeństwa Informacji**

1. Radzie Sterującej ds. Bezpieczeństwa Informacji przewodniczy Zastępca Sekretarza Generalnego odpowiedzialny za zarządzaniem bezpieczeństwem IT w Komisji. Jej członkowie reprezentują interesy związane z biznesem, technologią i bezpieczeństwem w departamentach Komisji oraz obejmują przedstawicieli Dyrekcji Generalnej ds. Informatyki, Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa, Dyrekcji Generalnej ds. Budżetu oraz zmieniających się co dwa lata na zasadzie rotacji przedstawicieli czterech innych zaangażowanych departamentów Komisji, w których bezpieczeństwo IT stanowi ważny aspekt w kontekście ich działań. Członkami są osoby należące do kadry kierowniczej wyższego szczebla.

2. Rada Sterująca ds. Bezpieczeństwa Informacji wspiera Radę Zarządzania Korporacyjnego w wykonywaniu jej zadań związanych z bezpieczeństwem IT. Rada Sterująca ds. Bezpieczeństwa Informacji ponosi odpowiedzialność operacyjną za zarządzanie całością bezpieczeństwa IT w Komisji.

3. Rada Sterująca ds. Bezpieczeństwa Informacji zaleca politykę Komisji w zakresie bezpieczeństwa IT, którą Komisja powinna przyjąć.

4. Dwa razy w roku Rada Sterująca ds. Bezpieczeństwa Informacji dokonuje przeglądu kwestii związanych z zarządzaniem, jak również kwestii związanych z bezpieczeństwem IT, w tym poważnych incydentów związanych z bezpieczeństwem IT, i składa sprawozdania na ten temat Radzie Zarządzania.

5. Rada Sterująca ds. Bezpieczeństwa Informacji monitoruje ogólne wdrożenie niniejszej decyzji oraz przeprowadza jego przegląd i składa Radzie Zarządzania Korporacyjnego sprawozdania na ten temat.

6. Na wniosek Dyrekcji Generalnej ds. Informatyki Rada Sterująca ds. Bezpieczeństwa Informacji dokonuje przeglądu wdrożenia aktualnej strategii bezpieczeństwa IT oraz zatwierdza i monitoruje jej wdrażanie. Rada Sterująca ds. Bezpieczeństwa Informacji składa Radzie Zarządzania Korporacyjnego sprawozdania na ten temat.

7. Rada Sterująca ds. Bezpieczeństwa Informacji monitoruje, ocenia i kontroluje sytuację w zakresie postępowania z ryzykiem, na które narażone są informacje korporacyjne, oraz posiada uprawnienie do wydawania w stosownych przypadkach formalnych wymogów w zakresie poprawy sytuacji.

▼C1

8. Procesy związane z obowiązkami i działaniami określonymi w ust. 1–7 zostają szczegółowo opisane w przepisach wykonawczych zgodnie z art. 13.

▼B

*Artykuł 6*

**Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa**

W odniesieniu do bezpieczeństwa IT na Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa ciążą poniższe obowiązki. Dyrekcja ta:

▼B

1) zapewnia dostosowanie polityki w zakresie bezpieczeństwa IT i polityki Komisji w zakresie bezpieczeństwa informacji;

2) ustanawia ramy na potrzeby upoważnienia do stosowania technologii szyfrujących w zakresie przechowywania i przekazywania informacji za pośrednictwem CIS;

3) informuje Dyrekcję Generalną ds. Informatyki o konkretnych zagrożeniach, które mogą mieć istotny wpływ na bezpieczeństwo CIS i zbiorów danych, które są w nich przetwarzane;

4) przeprowadza kontrole bezpieczeństwa IT, aby ocenić zgodność CIS Komisji z polityką w zakresie bezpieczeństwa, oraz przedstawia ich wyniki Radzie Sterującej ds. Bezpieczeństwa Informacji;

5) ustanawia ramy w zakresie upoważnienia dostępu do CIS Komisji z sieci zewnętrznych oraz powiązanych odpowiednich przepisów bezpieczeństwa, a także opracowuje odpowiednie normy bezpieczeństwa IT i wytyczne w sprawie bezpieczeństwa IT w ścisłej współpracy z Dyrekcją Generalną ds. Informatyki;

6) proponuje zasady i przepisy dotyczące outsourcingu CIS, aby utrzymać właściwą kontrolę bezpieczeństwa informacji;

▼C1

7) opracowuje odpowiednie normy bezpieczeństwa IT oraz wytyczne określone w pkt 1–6 w ścisłej współpracy z Dyrekcją Generalną ds. Informatyki;

8) procesy związane z obowiązkami i działaniami określonymi w pkt 1–7 zostają szczegółowo opisane w przepisach wykonawczych zgodnie z art. 13.

▼B

*Artykuł 7*

**Dyrekcja Generalna ds. Informatyki**

W odniesieniu do ogólnego bezpieczeństwa IT Komisji na Dyrekcji Generalnej ds. Informatyki ciążą poniższe obowiązki. Dyrekcja ta:

1) opracowuje normy bezpieczeństwa IT oraz wytyczne w sprawie bezpieczeństwa IT, z wyjątkiem przewidzianych w art. 6, w ścisłej współpracy z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa w celu zapewnienia spójności między polityką w zakresie bezpieczeństwa IT a polityką Komisji w zakresie bezpieczeństwa informacji oraz przedstawia je Radzie Sterującej ds. Bezpieczeństwa Informacji;

2) ocenia metody, procesy i wyniki zarządzania rodzajami ryzyka związanego z bezpieczeństwem IT w odniesieniu do wszystkich departamentów Komisji i składa regularnie sprawozdania na ten temat Radzie Sterującej ds. Bezpieczeństwa Informacji;

3) przedstawia bieżącą strategię bezpieczeństwa IT Radzie Sterującej ds. Bezpieczeństwa Informacji do przeglądu i zatwierdzenia, a następnie przyjęcia przez Radę Zarządzania Korporacyjnego, oraz przedstawia program, w tym planowanie projektów i działań mających na celu wdrożenie strategii bezpieczeństwa IT;

4) monitoruje realizację strategii bezpieczeństwa IT Komisji i składa regularnie sprawozdania na ten temat Radzie Sterującej ds. Bezpieczeństwa Informacji;

5) monitoruje rodzaje ryzyka związanego z bezpieczeństwem IT i środki bezpieczeństwa IT wdrożone w CIS oraz składa regularnie sprawozdania na ten temat Radzie Sterującej ds. Bezpieczeństwa Informacji;

▼B

6) składa regularnie Radzie Sterującej ds. Bezpieczeństwa Informacji sprawozdania na temat ogólnego wykonania i przestrzegania niniejszej decyzji;

7) po konsultacjach z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa wymaga od właścicieli systemów podjęcia określonych środków bezpieczeństwa IT w celu ograniczenia rodzajów ryzyka związanego z bezpieczeństwem IT, na jakie narażone są CIS Komisji;

8) zapewnia, aby właściciele systemów i właściciele danych mieli dostęp do odpowiedniego katalogu usług w zakresie bezpieczeństwa IT Dyrekcji Generalnej ds. Informatyki, dzięki któremu będą mogli wywiązać się ze swoich obowiązków związanych z bezpieczeństwem IT oraz stosować się do polityki w zakresie bezpieczeństwa IT i norm bezpieczeństwa IT;

9) zapewnia właścicielom systemu i właścicielom danych odpowiednią dokumentację oraz konsultuje się z nimi, w stosownych przypadkach, w sprawie środków bezpieczeństwa IT wdrażanych na potrzeby ich usług IT w celu ułatwienia im zachowania zgodności z polityką w zakresie bezpieczeństwa IT oraz wspierania właścicieli systemów w zarządzaniu ryzykiem w obszarze IT;

10) organizuje regularne spotkania sieci lokalnych pełnomocników ds. bezpieczeństwa teleinformatycznego (LISO) i wspiera ich w wykonywaniu ich obowiązków;

11) określa potrzeby szkoleniowe i koordynuje programy szkoleniowe w zakresie bezpieczeństwa IT we współpracy z departamentami Komisji oraz opracowuje, wdraża i koordynuje kampanie na rzecz poszerzania wiedzy w obszarze bezpieczeństwa IT w ścisłej współpracy z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa;

12) zapewnia, aby właściciele systemów, właściciele danych oraz inne podmioty pełniące funkcje związane z bezpieczeństwem IT w departamentach Komisji zapoznali się z polityką w zakresie bezpieczeństwa IT;

13) powiadamia Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa o określonych zagrożeniach związanych z bezpieczeństwem IT, incydentach i wyjątkach dotyczących polityki Komisji w zakresie bezpieczeństwa IT zgłoszonych przez właścicieli systemów, które mogły znacząco wpłynąć na bezpieczeństwo w Komisji;

14) w związku ze swoją rolą wewnętrznego dostawcy usług IT przekazuje Komisji katalog wspólnych usług IT, które zapewniają określone poziomy bezpieczeństwa. Odbywa się to poprzez systematyczne ocenianie rodzajów ryzyka związanego z bezpieczeństwem IT, zarządzanie nim i monitorowanie w celu wdrożenia środków bezpieczeństwa dla osiągnięcia określonego poziomu bezpieczeństwa;

▼C1

15) procesy związane z obowiązkami i działaniami określonymi w pkt 1–14 zostają szczegółowo opisane w przepisach wykonawczych zgodnie z art. 13.

▼B

*Artykuł 8*

**Departamenty Komisji**

W odniesieniu do bezpieczeństwa IT w swoim departamencie każdy szef departamentu Komisji:

1) w odniesieniu do każdego CIS – formalnie wyznacza właściciela systemu, będącego urzędnikiem lub pracownikiem zatrudnionym na czas określony, który będzie odpowiadał za bezpieczeństwo IT tego systemu, a także w odniesieniu do każdego zbioru danych przechowywanego w CIS – formalnie wyznacza właściciela danych, który powinien należeć do tej samej jednostki administracyjnej będącej administratorem danych w odniesieniu do zbiorów danych podlegających rozporządzeniu (WE) nr 45/2001;

2) formalnie wyznacza lokalnego pełnomocnika ds. bezpieczeństwa teleinformatycznego, który może pełnić obowiązki niezależnie od właścicieli systemów i właścicieli danych. Lokalnego pełnomocnika ds. bezpieczeństwa teleinformatycznego można przypisać do jednego lub kilku departamentów Komisji;

3) zapewnia, aby opracowane i wdrożone zostały odpowiednie oceny rodzajów ryzyka związanego z bezpieczeństwem IT oraz plany bezpieczeństwa IT;

4) zapewnia regularne przekazywanie Dyrekcji Generalnej ds. Informatyki podsumowania rodzajów ryzyka i środków związanych z bezpieczeństwem IT;

5) zapewnia, przy wsparciu Dyrekcji Generalnej ds. Informatyki, wprowadzanie odpowiednich procesów, procedur i rozwiązań celem zapewnienia efektywnego wykrywania, zgłaszania i rozwiązywania incydentów związanych z bezpieczeństwem IT ich systemów teleinformatycznych;

6) uruchamia procedury awaryjne w przypadku zagrożenia bezpieczeństwa IT;

7) spoczywa na nim ostateczna odpowiedzialność za bezpieczeństwo IT, co obejmuje obowiązki właściciela systemu i właściciela danych;

8) jest właściwy w odniesieniu do rodzajów ryzyka dotyczącego jego systemów teleinformatycznych i zbiorów danych;

9) rozstrzyga wszystkie spory między właścicielami danych a właścicielami systemów, a w przypadku utrzymywania się sporu przekazuje sprawę Radzie Sterującej ds. Bezpieczeństwa Informacji do rozstrzygnięcia;

10) zapewnia wdrożenie planów bezpieczeństwa IT i środków bezpieczeństwa IT oraz odpowiednie uwzględnienie zagrożeń;

▼C1

11) procesy związane z obowiązkami i działaniami określonymi w pkt 1–10 zostają szczegółowo opisane w przepisach wykonawczych zgodnie z art. 13.

▼B

*Artykuł 9*

**Właściciele systemów**

1. Właściciel systemu jest odpowiedzialny za bezpieczeństwo IT systemu teleinformatycznego i składa sprawozdania szefowi departamentu Komisji.

▼B

2. W odniesieniu do bezpieczeństwa IT właściciel systemu:

a) zapewnia zgodność CIS z polityką w zakresie bezpieczeństwa IT;

b) zapewnia dokładne zarejestrowanie CIS w stosownym wykazie;

c) ocenia rodzaje ryzyka związanego z bezpieczeństwem IT i określa potrzeby w zakresie bezpieczeństwa IT w odniesieniu do każdego CIS, we współpracy z właścicielami danych i w porozumieniu z Dyrekcją Generalną ds. Informatyki;

d) przygotowuje plan bezpieczeństwa, w tym, w stosownych przypadkach, szczegółowe informacje na temat ocenionych rodzajów ryzyka oraz wszelkich dodatkowych wymaganych środków bezpieczeństwa;

e) wdraża odpowiednie środki bezpieczeństwa IT, proporcjonalne do zidentyfikowanych rodzajów ryzyka związanego z bezpieczeństwem IT, i postępuje zgodnie z zaleceniami zatwierdzonymi przez Radę Sterującą ds. Bezpieczeństwa Informacji;

f) określa wszelkie zależności od innych systemów teleinformatycznych lub wspólnych usług IT oraz, w stosownych przypadkach, wdraża środki bezpieczeństwa na podstawie poziomów bezpieczeństwa zaproponowanych przez te systemy teleinformatyczne lub wspólne usługi IT;

g) zarządza rodzajami ryzyka związanego z bezpieczeństwem IT i je monitoruje;

h) regularnie zgłasza szefowi departamentu Komisji profil ryzyka związanego z bezpieczeństwem IT swojego CIS oraz powiadamia Dyrekcję Generalną ds. Informatyki o powiązanych rodzajach ryzyka, działaniach z zakresu zarządzania ryzykiem oraz podjętych środkach bezpieczeństwa;

i) konsultuje z lokalnym pełnomocnikiem ds. bezpieczeństwa teleinformatycznego z odpowiedniego departamentu Komisji kwestie związane z bezpieczeństwem IT;

j) wydaje instrukcje dla użytkowników dotyczące korzystania z CIS i powiązanych danych oraz dotyczące obowiązków użytkowników związanych z CIS;

k) działając jako organ ds. kryptograficznych, wymaga od Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa upoważnienia w odniesieniu do każdego CIS korzystającego z technologii szyfrowania;

l) z wyprzedzeniem konsultuje się z organem ds. bezpieczeństwa Komisji w sprawie każdego systemu przetwarzania informacji niejawnych UE;

m) zapewnia przechowywanie kopii zapasowych wszystkich kluczy deszyfrujących w depozycie. Odzyskiwanie zaszyfrowanych danych przeprowadza się tylko wtedy, gdy jest to dozwolone zgodnie z ramami określonymi przez Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa;

n) przestrzega przekazanych przez odpowiedniego administratora danych instrukcji, które dotyczą ochrony danych osobowych oraz stosowania przepisów o ochronie danych na temat bezpieczeństwa przetwarzania danych;

o) powiadamia Dyrekcję Generalną ds. Informatyki o wszelkich odstępstwach od polityki Komisji w zakresie bezpieczeństwa IT, w tym o odpowiednich uzasadnieniach;

▼B

p) zgłasza szefowi departamentu Komisji wszelkie nierozwiązywalne spory między właścicielem danych a właścicielem systemu oraz, stosownie do przypadku, powiadamia w odpowiednim czasie odpowiednie zainteresowane strony o incydentach związanych z bezpieczeństwem IT w zależności od ich stopnia zagrożenia zgodnie z art. 15;

q) w odniesieniu do systemów zewnętrznych zapewnia uwzględnienie odpowiednich przepisów dotyczących bezpieczeństwa IT w umowach outsourcingowych oraz zgłoszenie incydentów związanych z bezpieczeństwem IT występujących w zewnętrznym CIS zgodnie z art. 15;

r) w odniesieniu do CIS zapewniającego wspólne usługi IT zapewnia i jasno dokumentuje określony poziom bezpieczeństwa oraz zapewnia wdrożenie środków bezpieczeństwa w odniesieniu do tego CIS w celu osiągnięcia określonego poziomu bezpieczeństwa.

3. Właściciele systemów mogą formalnie przekazywać część lub całość swoich zadań związanych z bezpieczeństwem IT, nadal jednak pozostają odpowiedzialni za bezpieczeństwo IT swojego CIS.

▼C1

4. Procesy związane z obowiązkami i działaniami określonymi w ust. 1–3 zostają szczegółowo opisane w przepisach wykonawczych zgodnie z art. 13.

▼B

*Artykuł 10*

**Właściciele danych**

1. Właściciel danych jest odpowiedzialny za bezpieczeństwo IT określonego zbioru danych przed szefem departamentu Komisji oraz jest rozliczany z kwestii poufności, integralności i dostępności zbioru danych.

2. W odniesieniu do tego zbioru danych właściciel danych:

a) zapewnia właściwą klasyfikację wszystkich zbiorów danych, za które odpowiada, zgodnie z decyzjami (UE, Euratom) 2015/443 i (UE, Euratom) 2015/444;

b) określa potrzeby w zakresie bezpieczeństwa informacji i informuje odpowiednich właścicieli systemów o tych potrzebach;

c) uczestniczy w ocenie ryzyka dotyczącej CIS;

d) zgłasza szefowi departamentu Komisji wszelkie nierozwiązywalne spory między właścicielem danych a właścicielem systemu;

e) zgłasza incydenty związane z bezpieczeństwem IT, jak przewidziano w art. 15.

3. Właściciele danych mogą formalnie przekazywać część lub całość swoich zadań związanych z bezpieczeństwem IT, nadal jednak zachowują zakres odpowiedzialności określony w niniejszym artykule.

▼C1

4. Procesy związane z obowiązkami i działaniami określonymi w ust. 1–3 zostają szczegółowo opisane w przepisach wykonawczych zgodnie z art. 13.

▼B

*Artykuł 11*

**Lokalni pełnomocnicy ds. bezpieczeństwa teleinformatycznego**

▼C1

1. W odniesieniu do bezpieczeństwa IT lokalny pełnomocnik ds. bezpieczeństwa teleinformatycznego:

a) aktywnie identyfikuje właścicieli systemów, właścicieli danych i inne podmioty pełniące funkcje związane z bezpieczeństwem IT w departamentach Komisji oraz informuje ich o polityce w zakresie bezpieczeństwa IT;

b) w ramach sieci lokalnych pełnomocników ds. bezpieczeństwa teleinformatycznego kontaktuje się z Dyrekcją Generalną ds. Informatyki w sprawach dotyczących bezpieczeństwa IT w departamentach Komisji;

c) uczestniczy w organizowanych regularnie spotkaniach lokalnych pełnomocników ds. bezpieczeństwa teleinformatycznego;

d) prowadzi przegląd procesu zarządzania ryzykiem związanym z bezpieczeństwem informacji oraz przegląd procesu opracowywania i wdrażania planów bezpieczeństwa w odniesieniu do systemów informatycznych;

e) doradza właścicielom danych, właścicielom systemów i szefom departamentów Komisji w kwestiach związanych z bezpieczeństwem IT;

f) wspólnie z Dyrekcją Generalną ds. Informatyki rozpowszechnia dobre praktyki w zakresie bezpieczeństwa IT oraz proponuje określone programy uświadamiające i szkoleniowe;

g) przedkłada szefowi departamentu Komisji sprawozdania dotyczące bezpieczeństwa IT oraz określa braki i usprawnienia.

2. Procesy związane z obowiązkami i działaniami określonymi w ust. 1 zostają szczegółowo opisane w przepisach wykonawczych zgodnie z art. 13.

▼B

*Artykuł 12*

**Użytkownicy**

1. W odniesieniu do bezpieczeństwa IT użytkownicy:

a) postępują zgodnie z polityką w zakresie bezpieczeństwa IT i wydanymi przez właściciela systemu instrukcjami dotyczącymi korzystania z danego CIS;

b) zgłaszają incydenty związane z bezpieczeństwem IT, jak przewidziano w art. 15.

2. Korzystanie z CIS Komisji z naruszeniem polityki w zakresie bezpieczeństwa IT lub instrukcji wydanych przez właściciela systemu może stanowić podstawę do wszczęcia postępowania dyscyplinarnego.

▼C1

3. Procesy związane z obowiązkami i działaniami określonymi w ust. 1 i 2 zostają szczegółowo opisane w przepisach wykonawczych zgodnie z art. 13.

▼B

ROZDZIAŁ 3

## WYMOGI I OBOWIĄZKI ZWIĄZANE Z BEZPIECZEŃSTWEM

*Artykuł 13*

### Wykonanie niniejszej decyzji

1. ►C1 Przyjęcie przepisów wykonawczych dotyczących art. 6 pkt 2, a także związanych z nimi norm i wytycznych, może być przedmiotem decyzji Komisji w sprawie uprawnień przysługujących członkowi Komisji odpowiedzialnemu za kwestie bezpieczeństwa. ◄

2. ►C1 Przyjęcie wszystkich pozostałych przepisów wykonawczych do niniejszej decyzji, a także związanych z nimi norm bezpieczeństwa IT i wytycznych w sprawie bezpieczeństwa IT, może być przedmiotem decyzji Komisji w sprawie uprawnień przysługujących członkowi Komisji odpowiedzialnemu za kwestie informatyczne. ◄

3. Rada Sterująca ds. Bezpieczeństwa Informacji zatwierdza przepisy wykonawcze, normy i wytyczne wspomniane w ust. 1 i 2 powyżej przed ich przyjęciem.

*Artykuł 14*

### Obowiązek przestrzegania

1. Przestrzeganie przepisów opisanych w polityce w zakresie bezpieczeństwa IT i norm bezpieczeństwa IT jest obowiązkowe.

2. Nieprzestrzeganie polityki w zakresie bezpieczeństwa IT i norm bezpieczeństwa IT może pociągać za sobą odpowiedzialność dyscyplinarną zgodnie z traktatami, regulaminem pracowniczym i warunkami zatrudnienia innych pracowników Wspólnot Europejskich oraz sankcje umowne lub czynności prawne wynikające z krajowych przepisów ustawowych i wykonawczych.

3. Dyrekcję Generalną ds. Informatyki powiadamia się o wszelkich odstępstwach od polityki w zakresie bezpieczeństwa IT.

4. Jeżeli Rada Sterująca ds. Bezpieczeństwa Informacji stwierdza, że istnieje stałe niedopuszczalne ryzyko związane z CIS Komisji, Dyrekcja Generalna ds. Informatyki we współpracy z właścicielem systemu proponuje środki ograniczające ryzyko, które podlegają zatwierdzeniu przez Radę Sterującą ds. Bezpieczeństwa Informacji. Środki te mogą, między innymi, obejmować wzmocnione monitorowanie i sprawozdawczość, ograniczenia usług i odłączenie.

5. W razie potrzeby Rada Sterująca ds. Bezpieczeństwa Informacji nakłada obowiązek wdrożenia zatwierdzonych środków ograniczających ryzyko. Rada Sterująca ds. Bezpieczeństwa Informacji może również zalecić Dyrektorowi Generalnemu Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa wszczęcie postępowania administracyjnego. Dyrekcja Generalna ds. Informatyki informuje Radę Sterującą ds. Bezpieczeństwa Informacji o każdej sytuacji, w której zastosowano środki ograniczające ryzyko.

▼C1

6. Procesy związane z obowiązkami i działaniami określonymi w ust. 1–5 zostają szczegółowo opisane w przepisach wykonawczych zgodnie z art. 13.

▼B

*Artykuł 15*

**Reagowanie na incydenty związane z bezpieczeństwem IT**

1. Dyrekcja Generalna ds. Informatyki jest odpowiedzialna za zapewnienie głównej operacyjnej zdolności reagowania na incydenty związane z bezpieczeństwem IT w Komisji Europejskiej.

2. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa, jako zainteresowana strona mająca swój udział w reagowaniu na incydenty związane z bezpieczeństwem IT:

a) ma prawo dostępu do informacji zbiorczych zawartych we wszystkich rejestrach incydentów i pełnych rejestrów po złożeniu stosownego wniosku;

b) uczestniczy w działaniach grup ds. zarządzania sytuacjami kryzysowymi obejmującymi incydenty związane z bezpieczeństwem IT oraz w procedurach awaryjnych związanych z bezpieczeństwem IT;

c) odpowiada za kontakty z organami ścigania i służbami wywiadowczymi;

d) wykonuje analizę kryminalistyczną dotyczącą bezpieczeństwa cybernetycznego zgodnie z art. 11 decyzji (UE, Euratom) 2015/443;

e) podejmuje decyzje w sprawie wszczęcia formalnego postępowania;

f) powiadamia Dyrekcję Generalną ds. Informatyki o wszelkich incydentach związanych z bezpieczeństwem IT, które mogą zagrażać innym CIS.

3. Dyrekcja Generalna ds. Informatyki regularnie komunikuje się z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa w celu wymiany informacji i koordynowania reakcji na incydenty związane z bezpieczeństwem IT, które mogą wymagać wszczęcia formalnego postępowania.

4. W stosownych przypadkach usługi w zakresie koordynowania reakcji na incydenty – oferowane instytucjom, organom i agencjom UE przez zespół reagowania na incydenty komputerowe („CERT–UE”) – mogą być wykorzystywane do wspierania procesu reagowania na incydenty oraz wymiany wiedzy z innymi zagrożonymi instytucjami i agencjami UE.

5. Właściciele systemów uczestniczący w incydencie związanym z bezpieczeństwem IT:

a) niezwłocznie powiadamiają swoich szefów departamentów Komisji, Dyrekcję Generalną ds. Informatyki, Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa, lokalnego pełnomocnika ds. bezpieczeństwa teleinformatycznego oraz, w stosownych przypadkach, właściciela danych o wszelkich poważnych incydentach związanych z bezpieczeństwem IT, w szczególności tych, które dotyczą naruszenia poufności danych;

b) współpracują z odpowiednimi organami Komisji i przestrzegają ich instrukcji dotyczących zgłaszania incydentów, reagowania na nie i stosowania środków zaradczych.

▼B

6. Użytkownicy powiadamiają w stosownym czasie odpowiedni helpdesk IT o wszystkich rzeczywistych lub podejrzewanych incydentach związanych z bezpieczeństwem IT.

7. Właściciele danych powiadamiają w stosownym czasie zespół reagowania na incydenty związane z bezpieczeństwem IT o wszystkich rzeczywistych lub podejrzewanych incydentach związanych z bezpieczeństwem IT.

8. Dyrekcja Generalna ds. Informatyki, przy wsparciu innych uczestniczących zainteresowanych stron, jest odpowiedzialna za reagowanie na wszelkie incydenty związane z bezpieczeństwem IT wykryte w odniesieniu do CIS Komisji, które nie są systemami obsługiwanymi przez firmy zewnętrzne.

9. Dyrekcja Generalna ds. Informatyki powiadamia o incydentach związanych z bezpieczeństwem IT zagrożone departamenty Komisji, odpowiednich lokalnych pełnomocników ds. bezpieczeństwa teleinformatycznego oraz, w stosownych przypadkach, CERT–UE na zasadzie wiedzy koniecznej.

10. Dyrekcja Generalna ds. Informatyki składa regularnie Radzie Sterującej ds. Bezpieczeństwa Informacji sprawozdania na temat poważnych incydentów związanych z bezpieczeństwem IT, które zagrażają CIS Komisji.

11. Odpowiedni lokalny pełnomocnik ds. bezpieczeństwa teleinformatycznego uzyskuje, na wniosek, dostęp do rejestrów incydentów związanych z bezpieczeństwem IT dotyczących CIS departamentu Komisji.

12. W przypadku poważnego incydentu związanego z bezpieczeństwem IT Dyrekcja Generalna ds. Informatyki pełni rolę punktu kontaktowego na potrzeby zarządzania sytuacjami kryzysowymi poprzez koordynowanie działań grup ds. zarządzania kryzysowego na wypadek incydentów związanych z bezpieczeństwem IT.

13. W przypadku sytuacji wyjątkowej Dyrektor Generalny Dyrekcji Generalnej ds. Informatyki może zdecydować o wszczęciu procedury awaryjnej dotyczącej bezpieczeństwa IT. Dyrekcja Generalna ds. Informatyki opracowuje procedury awaryjne, które mają zostać zatwierdzone przez Radę Sterującą ds. Bezpieczeństwa Informacji.

14. Dyrekcja Generalna ds. Informatyki składa sprawozdania na temat wykonania procedur awaryjnych Radzie Sterującej ds. Bezpieczeństwa Informacji i szefom zagrożonych departamentów Komisji.

▼C1

15. Procesy związane z obowiązkami i działaniami określonymi w ust. 1–14 zostają szczegółowo opisane w przepisach wykonawczych zgodnie z art. 13.

▼B

ROZDZIAŁ 4

**PRZEPISY KOŃCOWE**

*Artykuł 16*

**Przejrzystość**

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

▼B

*Artykuł 17*

**Odniesienia do innych aktów**

Przepisy niniejszej decyzji pozostają bez uszczerbku dla decyzji (UE, Euratom) 2015/443, decyzji (UE, Euratom) 2015/444, rozporządzenia (WE) nr 45/2001, rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady ([1]), decyzji 2002/47/ WE, EWWiS, Euratom ([2]), rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 ([3]) oraz decyzji 1999/352/WE, EWWiS, Euratom.

*Artykuł 18*

**Uchylenie i środki przejściowe**

Decyzja C(2006) 3602 z dnia 16 sierpnia 2006 r. traci moc.

Przepisy wykonawcze i normy bezpieczeństwa IT przyjęte zgodnie z art. 10 decyzji C(2006) 3602 pozostają w mocy, o ile nie są sprzeczne z niniejszą decyzją, do czasu zastąpienia ich przepisami wykonawczymi i normami, które zostaną przyjęte zgodnie z art. 13 niniejszej decyzji. Każde odniesienie do art. 10 decyzji C(2006) 3602 należy rozumieć jako odniesienie do art. 13 niniejszej decyzji.

*Artykuł 19*

**Wejście w życie**

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

([1]) 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).

([2]) Decyzja Komisji 2002/47/WE, EWWiS, Euratom z dnia 23 stycznia 2002 r. zmieniająca jej regulamin (Dz.U. L 21 z 24.1.2002, s. 23).

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