# DECYZJA KOMISJI (UE, Euratom) 2015/443

## z dnia 13 marca 2015 r.

## w sprawie bezpieczeństwa w Komisji

KOMISJA EUROPEJSKA,

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

uwzględniając Traktat ustanawiający Europejską Wspólnotę Energii Atomowej,

uwzględniając Protokół nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej załączony do traktatów, w szczególności jego art. 18,

a także mając na uwadze, co następuje:

(1) Zapewnienie bezpieczeństwa w obrębie Komisji ma umożliwić jej funkcjonowanie w bezpiecznym i zabezpieczonym środowisku dzięki ustanowieniu spójnego i zintegrowanego podejścia do bezpieczeństwa, utrzymaniu odpowiedniego poziomu ochrony osób, mienia i informacji współmiernie do rozpoznanego ryzyka oraz zapewnieniu bezpieczeństwa szybko i skutecznie.

(2) Komisja, podobnie jak inne organy międzynarodowe, stoi w obliczu poważnych zagrożeń i wyzwań w dziedzinie bezpieczeństwa, w szczególności, w związku z terroryzmem, atakami cybernetycznymi, szpiegostwem politycznym i handlowym.

(3) Komisja Europejska zawarła z rządami Belgii, Luksemburga i Włoch porozumienia w sprawie bezpieczeństwa swoich głównych siedzib ([1]). Porozumienia te stanowią potwierdzenie, że Komisja jest odpowiedzialna za swoje bezpieczeństwo.

(4) Aby zapewnić bezpieczeństwo osób, mienia i informacji, Komisja może być zmuszona do podjęcia działań w obszarach chronionych prawami podstawowymi sformułowanymi w Karcie praw podstawowych i w europejskiej konwencji praw człowieka i uznawanymi przez Trybunał Sprawiedliwości.

(5) Wszelkie tego typu działania powinny być zatem uzasadnione znaczeniem interesu, jaki mają za zadanie chronić, powinny być proporcjonalne i zapewniać pełne poszanowanie praw podstawowych, w tym w szczególności prawa do prywatności i ochrony danych.

(6) W ramach systemu nastawionego na praworządność i poszanowanie praw podstawowych Komisja musi dążyć do zapewnienia odpowiedniego poziomu bezpieczeństwa swoich pracowników, mienia i informacji, dzięki czemu zapewnione będzie prowadzenia działalności bez ograniczania przy tym praw podstawowych w stopniu większym niż to ściśle konieczne.

(7) Bezpieczeństwo w Komisji opiera się na zasadach legalności, przejrzystości, proporcjonalności i odpowiedzialności.

(8) Pracowników upoważnionych do podejmowania środków bezpieczeństwa nie należy stawiać w niekorzystnej sytuacji ze względu na ich działania, chyba że działania te wykraczały poza zakres ich uprawnień lub spowodowały naruszenie prawa, więc niniejszą decyzję należy uznać za instrukcję postępowania w rozumieniu regulaminu pracowniczego.

(9) Komisja powinna podjąć właściwe inicjatywy, aby promować i wzmacniać swoją kulturę bezpieczeństwa, efektywniej zapewniając bezpieczeństwo, poprawiając zarządzanie bezpieczeństwem, dalej zacieśniając sieci i współpracę z odpowiednimi organami na szczeblu międzynarodowym, europejskim i krajowym oraz poprawiając monitorowanie i kontrolę procesu wdrażania środków bezpieczeństwa.

(10) Utworzenie Europejskiej Służby Działań Zewnętrznych (ESDZ) jako funkcjonalnie autonomicznego organu Unii miało znaczący wpływ na interesy Komisji w zakresie bezpieczeństwa, w związku z tym konieczne jest, aby ESDZ i Komisja ustanowiły zasady i procedury dotyczące współpracy w zakresie bezpieczeństwa i zabezpieczenia, w szczególności w odniesieniu do wywiązywania się przez Komisję z obowiązku dochowania należytej staranności wobec własnych pracowników w delegaturach Unii.

([1]) Por. „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité" z dnia 31 grudnia 2004 r., „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois" z dnia 20 stycznia 2007 r. i „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale" z dnia 22 lipca 1959 r.

(11) Polityka bezpieczeństwa prowadzona przez Komisję powinna być realizowana w sposób zgodny z innymi procesami i procedurami wewnętrznymi, które mogą obejmować kwestię bezpieczeństwa. Należą do nich w szczególności zarządzanie ciągłością działania, które ma na celu zachowanie funkcji krytycznych Komisji w przypadku zakłócenia działania, oraz proces ARGUS wykorzystywany do koordynacji sytuacji kryzysowych o charakterze wielosektorowym.

(12) Niezależnie od środków istniejących już w momencie przyjęcia niniejszej decyzji i zgłoszonych Europejskiemu Inspektorowi Ochrony Danych ([1]), wszelkie środki wprowadzone w ramach niniejszej decyzji i związane z przetwarzaniem danych osobowych podlegają przepisom wykonawczym zgodnie z art. 21, w którym określono odpowiednie gwarancje dla podmiotów danych.

(13) W związku z tym istnieje potrzeba dokonania przez Komisję przeglądu, aktualizacji i konsolidacji istniejącej podstawy prawnej dotyczącej bezpieczeństwa w Komisji.

(14) Należy zatem uchylić decyzję Komisji C(94) 2129 ([2]),

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

ROZDZIAŁ 1

**PRZEPISY OGÓLNE**

*Artykuł 1*

**Definicje**

Do celów niniejszej decyzji stosuje się następujące definicje:

1) „mienie" oznacza wszystkie ruchomości i nieruchomości oraz posiadłości Komisji;

2) „departament Komisji" oznacza dyrekcję generalną lub służbę Komisji lub gabinet członka Komisji;

3) „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;

4) „kontrola ryzyka" oznacza wszelkie środki bezpieczeństwa, co do których można przypuszczać, że pozwolą skutecznie kontrolować ryzyko związane z bezpieczeństwem dzięki zapobieganiu ryzyku, jego ograniczaniu, unikaniu lub przenoszeniu.

5) „sytuacja kryzysowa" oznacza okoliczność, zdarzenie, incydent lub sytuację wyjątkową (lub ich serię bądź połączenie) prowadzące do poważnego lub bezpośredniego zagrożenia dla bezpieczeństwa Komisji, niezależnie od źródła zagrożenia;

6) „dane" oznaczają informacje w formie, która pozwala na ich przekazanie, zapisanie lub przetworzenie;

7) „członek Komisji odpowiedzialny za bezpieczeństwo" oznacza członka Komisji odpowiedzialnego za Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa;

8) „dane osobowe" oznaczają dane osobowe w rozumieniu art. 2 lit. a) rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady ([3]);

9) „obiekty" oznaczają dowolną nieruchomość lub inną własność i mienie Komisji;

10) „zapobieganie ryzyku" oznacza wszelkie środki bezpieczeństwa, co do których można przypuszczać, że będą utrudniać, opóźniać lub powstrzymywać występowanie ryzyka związanego z bezpieczeństwa.

11) „ryzyko związane z bezpieczeństwem" oznacza połączenie stopnia zagrożenia, stopnia podatności na zagrożenia i ewentualnych skutków zdarzenia;

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

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

([2]) Decyzja Komisji C(94) 2129 z dnia 8 września 1994 r. w sprawie zadań Biura Bezpieczeństwa.

([3]) 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).

13) „środek bezpieczeństwa" oznacza każdy środek podejmowany zgodnie z niniejszą decyzją na potrzeby skontrolowania ryzyka związanego z bezpieczeństwem;

14) „regulamin pracowniczy" oznacza Regulamin pracowniczy urzędników Unii Europejskiej ustanowiony rozporządzeniem Rady (EWG, Euratom, EWWiS) nr 259/68 ([1]) i aktami go zmieniającymi;

15) „zagrożenie dla bezpieczeństwa" oznacza każde zdarzenie lub czynnik, co do których można przypuszczać, że negatywnie wpłyną na bezpieczeństwo, jeżeli nie spotkają się z odpowiednią reakcją i nie zostaną skontrolowane;

16) „bezpośrednie zagrożenie dla bezpieczeństwa" oznacza zagrożenie dla bezpieczeństwa, które ma miejsce bez wcześniejszego ostrzeżenia lub z wcześniejszym ostrzeżeniem wysłanym na krótko przed wystąpieniem zagrożenia, oraz

17) „poważne zagrożenie dla bezpieczeństwa" oznacza zagrożenie dla bezpieczeństwa, co do którego można przypuszczać, że doprowadzi do utraty życia, poważnego urazu lub szkody, znacznego uszkodzenia mienia, narazi na szwank bezpieczeństwo danych szczególnie chronionych, zakłóci działanie systemów IT lub istotnych zdolności operacyjnych Komisji;

18) „podatność" oznacza dowolny słaby punkt, co do którego można przypuszczać, że negatywnie wpłynie na bezpieczeństwo w Komisji, jeżeli zostanie wykorzystany przez jedno zagrożenie lub większą ich liczbę.

*Artykuł 2*

**Przedmiot**

1. W niniejszej decyzji określa się cele, podstawowe zasady, organizację i obowiązki w zakresie bezpieczeństwa w Komisji.

2. Niniejszą decyzję stosuje się do wszystkich departamentów Komisji i do wszystkich jej obiektów.Personel Komisji zatrudniony w delegaturach Unii podlegają przepisom bezpieczeństwa obowiązującym w przypadku Europejskiej Służby Działań Zewnętrznych ([2]).

3. Nie naruszając żadnych konkretnych wskazań dotyczących poszczególnych grup pracowników, niniejsza decyzja ma zastosowanie do członków Komisji, pracowników Komisji objętych regulaminem pracowniczym i warunkami zatrudnienia innych pracowników Unii Europejskiej, ekspertów krajowych oddelegowanych do Komisji, dostawców usług i ich pracowników, stażystów oraz do wszystkich osób mających dostęp do budynków lub innego mienia Komisji lub do informacji znajdujących się w posiadaniu Komisji.

4. Przepisy niniejszej decyzji nie naruszają decyzji Komisji 2002/47/WE, EWWiS, Euratom ([3]) i decyzji Komisji 2004/563/WE, Euratom ([4]), decyzji Komisji C(2006) 1623 ([5]) i decyzji Komisji C(2006) 3602 ([6]).

ROZDZIAŁ 2

**ZASADY**

*Artykuł 3*

**Zasady dotyczące bezpieczeństwa w Komisji**

1. W ramach wdrażania niniejszej decyzji Komisja postępuje zgodnie z traktatami, a w szczególności z Kartą praw podstawowych i Protokołem nr 7 w sprawie przywilejów i immunitetów Unii Europejskiej oraz instrumentami, o których mowa w motywie 2, i wszelkimi obowiązującymi przepisami prawa krajowego, a także warunkami określonymi w niniejszej decyzji. W stosownych przypadkach wydaje się instrukcje bezpieczeństwa w rozumieniu art. 21 ust. 2 zawierające wytyczne w tym zakresie.

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

3. Zasada legalności wskazuje na konieczność ścisłego przestrzegania ram prawnych przy wdrażaniu niniejszej decyzji oraz stosowania się do wymogów prawnych.

---

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

([2]) Decyzja Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 19 kwietnia 2013 r. w sprawie przepisów bezpieczeństwa mających zastosowanie do Europejskiej Służby Działań Zewnętrznych (Dz.U. C 190 z 29.6.2013, s. 1).

([3]) 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) z załączonymi przepisami dotyczącymi zarządzania dokumentami.

([4]) Decyzja Komisji 2004/563/WE, Euratom z dnia 7 lipca 2004 r. zmieniająca jej regulamin wewnętrzny (Dz.U. L 251 z 27.7.2004, s. 9) z załączonymi przepisami dotyczącymi dokumentów elektronicznych i cyfrowych.

([5]) Decyzja C(2006) 1623 z dnia 21 kwietnia 2006 r. ustanawiająca zharmonizowaną politykę bezpieczeństwa i higieny pracy dla wszystkich pracowników Komisji Europejskiej.

([6]) Decyzja C(2006) 3602 z dnia 16 sierpnia 2006 r. dotycząca bezpieczeństwa systemów informacyjnych wykorzystywanych przez Komisję Europejską.

4. Wszelkie środki bezpieczeństwa podejmuje się jawnie, chyba że istnieje uzasadnione przekonanie, że takie działanie może osłabić ich skutek. Adresatów środka bezpieczeństwa powiadamia się z wyprzedzeniem o przyczynach zastosowania środka i jego skutkach, chyba że istnieje uzasadnione przekonanie, że jego działanie zostanie osłabione w wyniku przekazania takiej informacji. W takim przypadku adresata środka bezpieczeństwa powiadamia się po wyeliminowaniu ryzyka osłabienia działania środka bezpieczeństwa.

5. Departamenty Komisji zapewniają uwzględnianie kwestii bezpieczeństwa od początku opracowywania i realizacji polityki, decyzji, programów, projektów i działań Komisji, za które są odpowiedzialne. W tym celu, od najwcześniejszych etapów przygotowań, departamenty angażują Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa w ogólnym zakresie i głównego inspektora ds. bezpieczeństwa informacji w Komisji w odniesieniu do systemów IT.

6. W stosownych przypadkach Komisja dąży do nawiązania współpracy z właściwymi organami państwa przyjmującego, innych państw członkowskich i innych instytucji, agencji lub organów UE uwzględniając, w miarę możliwości, środki podejmowane lub planowane przez te organy w celu ograniczenia ryzyka związanego z bezpieczeństwem.

*Artykuł 4*

**Obowiązek przestrzegania**

1. Przestrzeganie niniejszej decyzji i jej przepisów wykonawczych oraz środków bezpieczeństwa i instrukcji udzielonych przez upoważnionych pracowników jest obowiązkowe.

2. Nieprzestrzeganie przepisów bezpieczeństwa może pociągać za sobą odpowiedzialność dyscyplinarną zgodnie z traktatami i regulaminem pracowniczym oraz sankcje umowne lub czynności prawne na mocy krajowych przepisów ustawowych i wykonawczych.

ROZDZIAŁ 3

**ZAPEWNIENIE BEZPIECZEŃSTWA**

*Artykuł 5*

**Upoważnieni pracownicy**

1. Jedynie pracownikom upoważnionym na podstawie imiennego uprawnień przyznanych im przez Dyrektora Generalnego ds. Zasobów Ludzkich i Bezpieczeństwa, z uwagi na ich bieżące obowiązki, można przyznać prawo do stosowania jednego lub kilku z następujących środków:

1) noszenie broni bocznej;

2) prowadzenie dochodzeń w sprawie bezpieczeństwa, o których mowa w art. 13;

3) podejmowanie środków bezpieczeństwa, o których mowa w art. 12, określonych w uprawnieniu.

2. Uprawnienia, o których mowa w ust. 1, przyznaje się na okres nie dłuższy niż okres zajmowania przez daną osobę stanowiska lub pełnienia przez nią określonej funkcji, w odniesieniu do której przyznano dane uprawnienie. Uprawnienia przyznaje się zgodnie z obowiązującymi przepisami określonymi w art. 3 ust. 1.

3. Jeżeli chodzi o upoważnionych pracowników, niniejsza decyzja stanowi instrukcję postępowania w rozumieniu art. 21 regulaminu pracowniczego.

*Artykuł 6*

**Przepisy ogólne dotyczące środków bezpieczeństwa**

1. Podejmując środki bezpieczeństwa Komisja przede wszystkim, na ile to możliwe, zapewnia:

a) poszukiwanie wsparcia lub pomocy ze strony danego państwa, pod warunkiem że państwo to jest państwem członkowskim Unii Europejskiej, a jeżeli nie, to jest stroną europejskiej konwencji praw człowieka lub gwarantuje prawa, które są co najmniej równorzędne prawom zagwarantowanym w tej konwencji;

b) przekazanie informacji na temat danej osoby jedynie odbiorcom innym niż instytucje i organy wspólnotowe niepodlegające prawu krajowemu przyjętemu zgodnie z dyrektywą 95/46/WE Parlamentu Europejskiego i Rady ([1]), zgodnie z art. 9 rozporządzenia (WE) nr 45/2001;

([1]) Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).

c) jeżeli dana osoba stanowi zagrożenie dla bezpieczeństwa, wobec tej osoby stosuje się wszelkie środki bezpieczeństwa oraz można ją obciążyć poniesionymi kosztami. Wymienione środki bezpieczeństwa można zastosować wobec innych osób tylko wówczas, jeżeli bezpośrednie lub poważne zagrożenie dla bezpieczeństwa jest kontrolowane i spełnione zostały następujące warunki:

   a) nie można podjąć przewidzianych środków wobec osoby stwarzającej zagrożenie dla bezpieczeństwa lub istnieje prawdopodobieństwo, że dane środki będą nieskuteczne;

   b) Komisja nie może kontrolować zagrożenia dla bezpieczeństwa w ramach swoich działań, ani nie może tego dokonać w odpowiednim czasie;

   c) środek nie stanowi nieproporcjonalnego zagrożenia dla innej osoby i jej praw.

2. Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa ustanawia przegląd środków bezpieczeństwa, w przypadku których konieczne może być orzeczenie sądu zgodne z przepisami ustawowymi i wykonawczymi państw członkowskich, w których znajdują się obiekty Komisji.

3. Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa może zwrócić się do wykonawcy o wykonanie, pod kierownictwem i nadzorem Dyrekcji ds. Bezpieczeństwa, zadań związanych z bezpieczeństwem.

*Artykuł 7*

**Środki bezpieczeństwa w odniesieniu do osób**

1. Uwzględniając wymogi w zakresie bezpieczeństwa, osobom przebywającym w obiektach Komisji przysługuje odpowiedni poziom ochrony.

2. W przypadku poważnego ryzyka związanego z bezpieczeństwem Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa zapewnia ścisłą ochronę członkom Komisji lub innym pracownikom, w sytuacji, gdy z oceny zagrożenia wynika, że taka ochrona jest potrzebna, aby zapewnić im bezpieczeństwo.

3. W przypadku poważnego ryzyka związanego z bezpieczeństwem Komisja może zarządzić ewakuację swoich obiektów.

4. Ofiary wypadków lub ataków na terenie obiektów Komisji otrzymają pomoc.

5. Aby zapobiegać ryzyku związanemu z bezpieczeństwem i kontrolować je, upoważnieni pracownicy mogą dokonać kontroli przeszłości osób objętych zakresem niniejszej decyzji w celu ustalenia, czy przyznanie takim osobom dostępu do obiektów Komisji lub jej informacji nie stanowi zagrożenia dla bezpieczeństwa. W tym celu oraz zgodnie z rozporządzeniem (WE) nr 45/2001 i przepisami, o których mowa w art. 3 ust. 1, upoważnieni pracownicy mogą:

a) korzystać z wszelkich dostępnych Komisji źródeł informacji, uwzględniając wiarygodność źródła informacji;

b) uzyskać dostęp do akt personalnych lub danych Komisji na temat osób, które zatrudnia lub planuje zatrudnić, lub na temat pracowników wykonawców, gdy jest to należycie uzasadnione.

*Artykuł 8*

**Środki bezpieczeństwa w odniesieniu do bezpieczeństwa fizycznego i mienia**

1. Bezpieczeństwo mienia zapewnia się w wyniku zastosowania odpowiednich fizycznych i technicznych środków ochronnych i odpowiednich procedur, zwanych dalej „bezpieczeństwem fizycznym", tworzących wielowarstwowy system.

2. Środki można przyjąć zgodnie z niniejszym artykułem w celu ochrony osób lub informacji w Komisji oraz ochrony mienia.

3. Cele bezpieczeństwa fizycznego obejmują:

— zapobieganie aktom przemocy wymierzonym w członków Komisji lub osoby objęte zakresem niniejszej decyzji,

— zapobieganie szpiegostwu i stosowaniu podsłuchu w celu zdobycia danych szczególnie chronionych lub informacji niejawnych,

— zapobieganie kradzieżom, aktom wandalizmu, sabotażowi i innym aktom przemocy zmierzającym do uszkodzenia lub zniszczenia budynków i mienia Komisji,

— umożliwienie prowadzenia dochodzenia wyjaśniającego i dochodzenia w sprawie bezpieczeństwa w zakresie incydentów związanych z bezpieczeństwem, w tym w drodze sprawdzenia plików dziennika kontroli wejść i wyjść, nagrań w systemie CCTV, zapisów rozmów telefonicznych i podobnych danych, o których mowa w art. 22 ust. 2 poniżej i innych źródłach informacji.

4. Bezpieczeństwo fizyczne obejmuje:

— politykę dostępu mającą zastosowanie do wszystkich osób lub pojazdów potrzebujących dostępu do obiektów Komisji, w tym parkingów,

— system kontroli dostępu, który tworzą strażnicy, urządzenia i środki techniczne, systemy informacyjne lub połączenie wszystkich tych elementów.

5. W celu zapewnienia bezpieczeństwa fizycznego mogą zostać podjęte następujące działania:

— rejestrowanie wejść i wjazdów na teren obiektów Komisji oraz wyjść i wyjazdów z terenu Komisji w odniesieniu do osób, pojazdów, towarów i urządzeń,

— kontrole tożsamości w obiektach,

— kontrole pojazdów, towarów i urządzeń za pomocą środków wizualnych lub technicznych,

— zapobieganie wejścia, wjazdu i wwozu nieupoważnionych osób, pojazdów i towarów na teren obiektów Komisji.

*Artykuł 9*

**Środki bezpieczeństwa w odniesieniu do informacji**

1. Bezpieczeństwo informacji obejmuje wszystkie informacje będące w posiadaniu Komisji.

2. Bezpieczeństwo informacji, niezależnie od swojej formy, utrzymuje równowagę między przejrzystością, proporcjonalnością, odpowiedzialnością i skutecznością a koniecznością ochrony informacji przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, zniszczeniem lub nieuprawnioną zmianą.

3. Bezpieczeństwo informacji ma na celu ochronę poufności, integralności i dostępności.

4. W związku z tym stosuje się procesy zarządzania ryzykiem w celu sklasyfikowania zasobów informacyjnych i opracowania proporcjonalnych środków bezpieczeństwa, procedur i norm, w tym środków zmniejszających ryzyko.

5. Te ogólne zasady dotyczące bezpieczeństwa informacji stosuje się w szczególności w odniesieniu do:

a) „informacji niejawnych UE" (zwanych dalej „EUCI"), a mianowicie wszelkich informacji lub materiałów objętych klauzulą tajności UE, których nieuprawnione ujawnienie mogłoby w różnym stopniu zaszkodzić interesom Unii Europejskiej lub interesom co najmniej jednego państwa członkowskiego;

b) „szczególnie chronionych informacji jawnych", tj. informacji lub materiałów, które Komisja musi chronić z powodu zobowiązań prawnych określonych w traktatach lub aktach przyjętych w celu ich wykonania lub ze względu na ich szczególną ochronę. Szczególnie chronione informacje jawne obejmują między innymi informacje lub materiały objęte ze względu na swój charakter tajemnicą służbową, o czym jest mowa w art. 339 TFUE, informacje objęte interesami chronionymi na mocy art. 4 rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiej i Rady ([1]) w związku z odpowiednim orzecznictwem Trybunału Sprawiedliwości lub dane osobowe objęte zakresem rozporządzenia (WE) nr 45/2001.

6. Szczególnie chronione informacje jawne podlegają zasadom dotyczącym przetwarzania tych informacji i ich przechowywania. Informacje te ujawnia się tylko tym osobom, które muszą je znać. W razie konieczności zapewnienia skutecznej ochrony poufności informacji, stosuje się oznaczenie identyfikujące dokument niejawny i odpowiednie instrukcje przetwarzania zatwierdzone przez Dyrektora Generalnego ds. Zasobów Ludzkich i Bezpieczeństwa. Jeżeli informacje tego rodzaju przetwarza się lub przechowuje w systemach teleinformatycznych, wówczas chroni się je także zgodnie z decyzją C(2006) 3602, jej przepisami wykonawczymi i odpowiednimi normami.

7. Wobec każdej osoby odpowiedzialnej za narażenie na szwank bezpieczeństwa lub utratę EUCI lub szczególnie chronionych informacji jawnych, które są określone jako takie w zasadach dotyczących ich przetwarzanie i przechowywanie, może zostać wszczęte postępowanie dyscyplinarne zgodnie z regulaminem pracowniczym. Postępowanie dyscyplinarne nie wpływa na wszelkie dalsze postępowania sądowe lub karne prowadzone przez właściwe organy krajowe państw członkowskich zgodnie z ich przepisami ustawowymi i wykonawczymi oraz na umowne środki odwoławcze.

([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).

*Artykuł 10*

**Środki bezpieczeństwa w odniesieniu do systemów teleinformatycznych**

1. Wszystkie systemy teleinformatyczne („CIS") wykorzystywane przez Komisję są zgodne z polityką Komisji w dziedzinie bezpieczeństwa systemów informatycznych określoną w decyzji C(2006) 3602, jej przepisach wykonawczych i odpowiednich normach bezpieczeństwa.

2. Służby Komisji posiadające system teleinformatyczny, zarządzające nim lub obsługujące go zezwalają na dostęp do tych systemów wyłącznie innym instytucjom, agencjom, organom UE lub innym organizacjom, pod warunkiem że wspomniane instytucje, agencje, organy UE lub inne organizacje mogą zagwarantować wystarczającą pewność, że ich systemy IT są chronione na poziomie równorzędnym polityce Komisji w dziedzinie bezpieczeństwa systemów informatycznych określonej w decyzji C(2006) 3602, jej przepisach wykonawczych i odpowiednich normach bezpieczeństwa. Komisja monitoruje przestrzeganie polityki, a w przypadku poważnego naruszenia lub utrzymującego się nieprzestrzegania jest uprawniona do zakazania dostępu.

*Artykuł 11*

**Analiza kryminalistyczna dotycząca bezpieczeństwa cybernetycznego**

Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa jest przede wszystkim odpowiedzialna za przeprowadzenia technicznej analizy kryminalistycznej we współpracy z właściwymi departamentami Komisji w celu wsparcia dochodzeń w sprawie bezpieczeństwa, o których mowa w art. 13, związanych z kontrwywiadem, przeciekiem danych, atakami cybernetycznymi i bezpieczeństwem systemów informatycznych.

*Artykuł 12*

**Środki bezpieczeństwa w odniesieniu do osób i przedmiotów**

1. W celu zapewnienia bezpieczeństwa w Komisji oraz zapobiegania ryzyku i jego kontroli upoważnieni pracownicy mogą, zgodnie z art. 5 oraz przestrzegając zasad określonych w art. 3, zastosować m.in. jeden lub kilka środków bezpieczeństwa, takich jak:

a) zabezpieczenie miejsca i dowodów, w tym plików dziennika kontroli wyjść i wejść, nagrań w systemie CCTV, w przypadku incydentów lub zachowań, które mogą prowadzić do wszczęcia postępowania administracyjnego, dyscyplinarnego, cywilnego lub karnego;

b) ograniczone środki dotyczące osób stwarzających zagrożenie dla bezpieczeństwa, w tym nakazanie opuszczenia obiektów Komisji, eskortowanie podczas opuszczania obiektów Komisji, zakazanie wstępu do obiektów Komisji przez określony czas; przy czym ten ostatni środek określa się zgodnie z kryteriami, które mają zostać zdefiniowane w przepisach wykonawczych;

c) ograniczone środki dotyczące przedmiotów stwarzających zagrożenie dla bezpieczeństwa, w tym usunięcie, zajęcie lub unieszkodliwienie przedmiotów;

d) przeszukanie obiektów Komisji, w tym biur, na terenie tych obiektów;

e) przeszukanie CIS i urządzeń, przesyłu danych telefonicznych i telekomunikacyjnych, plików dzienników, kont użytkowników itd.;

f) inne szczególne środki bezpieczeństwa o podobnych skutkach, mające na celu zapobieganie ryzyku związanemu z bezpieczeństwem lub kontrolę takiego ryzyka, w szczególności w kontekście praw Komisji jako właściciela lub pracodawcy zgodnie z mającym zastosowanie prawem krajowym.

2. W wyjątkowych okolicznościach pracownicy Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa upoważnieni zgodnie z art. 5 mogą podjąć wszelkie środki ochronne, ściśle przestrzegając zasad określonych w art. 3. Jak najszybciej po zastosowaniu środków, pracownicy powiadamiają dyrektora Dyrekcji ds. Bezpieczeństwa, który występuje o odpowiednie upoważnienie do Dyrektora Generalnego ds. Zasobów Ludzkich i Bezpieczeństwa potwierdzające zastosowane środki i zezwalające na podjęcie dalszych niezbędnych działań oraz kontaktuje się w stosownych przypadkach z właściwymi organami krajowymi.

3. Zgodnie z niniejszym artykułem środki bezpieczeństwa należy udokumentować w czasie ich stosowania lub, w przypadku bezpośredniego zagrożenia lub sytuacji kryzysowej, w rozsądnym terminie po ich podjęciu. W tym ostatnim przypadku dokumentacja musi także zawierać elementy, na których opierała się ocena dotycząca zaistnienia bezpośredniego zagrożenia lub sytuacji kryzysowej. Dokumentacja może być zwięzła, ale powinna być tworzona w taki sposób, aby osoba objęta środkiem mogła skorzystać z prawa do obrony i ochrony danych osobowych zgodnie z rozporządzeniem (WE) nr 45/2001 oraz, aby możliwa była kontrola legalności danego środka. Akta personalne osoby nie zawierają żadnych informacji na temat szczególnych środków bezpieczeństwa zastosowanych wobec pracownika.

4. Stosując środki bezpieczeństwa zgodnie z lit. b), Komisja gwarantuje także, że dana osoba będzie miała możliwość skontaktowania się z prawnikiem lub zaufaną osobą oraz zostanie poinformowana o przysługującym jej prawie do odwołania się do Europejskiego Inspektora Ochrony Danych.

*Artykuł 13*

**Dochodzenia**

1. 1. Bez uszczerbku dla art. 86 i załącznika IX do regulaminu pracowniczego i dla wszelkich szczególnych ustaleń między Komisją a ESDZ, takich jak szczególne ustalenia podpisane w dniu 28 maja 2014 r. między Dyrekcją Generalną Zasobów Ludzkich i Bezpieczeństwa Komisji Europejskiej a Europejską Służbą Działań Zewnętrznych w sprawie obowiązku dochowania należytej staranności wobec personelu Komisji oddelegowanego do delegatur Unii, można prowadzić dochodzenia w sprawie bezpieczeństwa:

a) w przypadku incydentów mających wpływ na bezpieczeństwo w Komisji, w tym podejrzeń o popełnienie przestępstwa;

b) w przypadku potencjalnego wycieku szczególnie chronionych informacji jawnych, EUCI lub informacji niejawnych Euratom, nieostrożnego obchodzenia się z tymi informacjami lub narażenia ich na szwank;

c) w kontekście kontrwywiadu i walki z terroryzmem;

d) w przypadku poważnych incydentów cybernetycznych.

2. Decyzję o przeprowadzeniu dochodzenia w sprawie bezpieczeństwa podejmuje Dyrektor Generalny ds. Zasobów Ludzkich i Bezpieczeństwa, który będzie jednocześnie odbiorcą sprawozdania z dochodzenia.

3. Dochodzenia w sprawie bezpieczeństwa prowadzone są jedynie przez wyznaczonych i należycie upoważnionych zgodnie z art. 5 pracowników Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa.

4. Upoważnieni pracownicy korzystają w sposób niezależny ze swoich uprawnień w zakresie prowadzenia dochodzenia w sprawie bezpieczeństwa zgodnie z upoważnieniem i posiadają uprawnienia wymienione w art. 12.

5. Upoważnieni pracownicy posiadający uprawnienia do prowadzenia dochodzeni w sprawie bezpieczeństwa mogą gromadzić informacje pochodzące ze wszystkich dostępnych źródeł na temat wszelkich przestępstw administracyjnych lub kryminalnych popełnionych na terenie obiektu Komisji lub z udziałem osób wymienionych w art. 2 ust. 3 w roli ofiary lub sprawcy tych przestępstw.

6. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa powiadamia właściwe organy przyjmującego państwa członkowskiego lub w stosownych przypadkach innego państwa członkowskiego, w szczególności gdy z dochodzenia wynika, że doszło do popełnienia przestępstwa. W tym kontekście Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa może w stosownych przypadkach, lub gdy jest to wymagane, zapewnić wsparcie organom przyjmującego państwa członkowskiego lub innego państwa członkowskiego.

7. W przypadku poważnych incydentów cybernetycznych Dyrekcja Generalna ds. Informatyki współpracuje ściśle z Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa w celu zapewnienia wsparcia we wszystkich kwestiach technicznych. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa podejmuje w porozumieniu z Dyrekcją Generalną ds. Informatyki decyzję, kiedy należy powiadomić właściwe organy państwa przyjmującego lub innego państwa członkowskiego. Służby koordynacji incydentów zespołu reagowania na incydenty komputerowe obsługującego instytucje, organy i agencje europejskie („CERT-EU") będzie wykorzystywana w celu zapewnienia wsparcia pozostałym narażonym instytucjom i agencjom UE.

8. Dochodzenia w sprawie bezpieczeństwa należy udokumentować.

*Artykuł 14*

**Wyznaczenie kompetencji w odniesieniu do postępowania sprawdzającego/dochodzenia w sprawie bezpieczeństwa i innych rodzajów dochodzeń**

1. Jeżeli Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa prowadzi dochodzenia w sprawie bezpieczeństwa, o których mowa w art. 13, i jeżeli przedmiotowe dochodzenia wchodzą w zakres kompetencji Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych (OLAF) lub Biura Dochodzeń i Postępowań Dyscyplinarnych Komisji (IDOC), wówczas bezzwłocznie kontaktuje się z tymi organami, w szczególności aby nie narazić na szwank późniejszych działań podejmowanych przez OLAF lub IDOC. W stosownych przypadkach Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa zwraca się do OLAF-u i IDOC-u o przystąpienie do udziału w dochodzeniu.

2. Dochodzenia w sprawie bezpieczeństwa, o których mowa w art. 13, pozostają bez uszczerbku dla kompetencji OLAF-u i IDOC-u określonych w przepisach dotyczących tych organów. Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa może zostać poproszona o udzielenie pomocy technicznej w prowadzeniu dochodzeń wszczętych przez OLAF lub IDOC.

3. Dyrekcja ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa może zostać poproszona o udzielenie pomocy pracownikom OLAF-u, gdy wchodzą na teren obiektów Komisji zgodnie z art. 3 ust. 5 i art. 4 ust. 4 Rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) nr 883/2013 ([1]), aby ułatwić im

([1]) 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).

wykonanie zadań. Dyrekcja ds. Bezpieczeństwa powiadamia o takich wnioskach o udzielenie pomocy Sekretarza Generalnego i Dyrektora Generalnego Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa lub, jeżeli takie dochodzenie prowadzone jest w obiektach Komisji zajmowanych przez jej członków lub przez sekretarza generalnego, przewodniczącego Komisji i komisarza ds. zasobów ludzkich.

4. Bez uszczerbku dla art. 22 lit. a) regulaminu pracowniczego, jeżeli sprawa może wchodzić w zakres kompetencji zarówno Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa, jak i IDOC-u, Dyrekcja ds. Bezpieczeństwa doradza Dyrektorowi Generalnemu ds. Zasobów Ludzkich i Bezpieczeństwa na jak najwcześniejszym etapie w momencie przekazania przez nią informacji zgodnie z art. 13, czy istnieją podstawy, które uzasadniają udział IDOC w tej sprawie. Etap ten zostaje w szczególności uznany za zrealizowany, gdy bezpośrednie zagrożenie dla bezpieczeństwa zostanie zażegnane. Decyzję w tej sprawie podejmuje Dyrektor Generalny ds. Zasobów Ludzkich i Bezpieczeństwa.

5. W przypadku gdy sprawa może wchodzić w zakres kompetencji zarówno Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa, jak i OLAF-u, Dyrekcja ds. Bezpieczeństwa niezwłocznie przekazuje informacje Dyrektorowi Generalnemu ds. Zasobów Ludzkich i Bezpieczeństwa oraz na jak najwcześniejszym etapie powiadamia Dyrektora Generalnego OLAF-u. Etap ten zostaje w szczególności uznany za zrealizowany, gdy bezpośrednie zagrożenie dla bezpieczeństwa zostanie zażegnane.

*Artykuł 15*

**Kontrole bezpieczeństwa**

1. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa przeprowadza kontrole bezpieczeństwa, aby sprawdzić, czy służby Komisji i poszczególne osoby przestrzegają postanowień niniejszej decyzji i jej przepisów wykonawczych, oraz aby sformułować zalecenia, gdy uzna to za konieczne.

2. W stosownych przypadkach Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa przeprowadza kontrole bezpieczeństwa lub wizyty monitorujące lub oceniające, aby sprawdzić, czy bezpieczeństwo służb Komisji, jej mienia i informacji, za które odpowiedzialność ponoszą inne instytucje, agencje lub organy unijne, państwa członkowskie, państwa trzecie lub organizacje międzynarodowe, jest odpowiednio chronione zgodnie z przepisami bezpieczeństwa, regulacjami i normami, które są co najmniej równorzędne przepisom, regulacjom i normom Komisji. W stosownych przypadkach i w duchu dobrej współpracy między administracjami, wspomniane kontrole bezpieczeństwa obejmują także kontrole prowadzone w kontekście wymiany informacji niejawnych z innymi instytucjami, organami i agencjami unijnymi, państwami członkowskimi lub państwami trzecimi lub organizacjami międzynarodowymi.

3. Niniejszy artykuł jest wykonywany odpowiednio w odniesieniu do personelu Komisji w delegaturach Unii, bez uszczerbku dla wszelkich szczególnych ustaleń między Komisją a ESDZ, takich jak szczególne ustalenia podpisane w dniu 28 maja 2014 r. między Dyrekcją Generalną Zasobów Ludzkich i Bezpieczeństwa Komisji Europejskiej a Europejską Służbą Działań Zewnętrznych w sprawie obowiązku dochowania należytej staranności wobec personelu Komisji oddelegowanego do delegatur Unii.

*Artykuł 16*

**Stopnie alarmowe i zarządzanie sytuacjami kryzysowymi**

1. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa jest odpowiedzialna za wdrożenie odpowiednich środków w zakresie stopni alarmowych w przewidywaniu zagrożeń i incydentów mających wpływ na bezpieczeństwo w Komisji lub w odpowiedzi na takie zagrożenia i incydenty oraz jest odpowiedzialna za środki wymagane do zarządzania sytuacjami kryzysowymi.

2. Środki w zakresie stopni alarmowych, o których mowa w ust. 1, są współmierne do poziomu zagrożenia dla bezpieczeństwa. Poziomy stopni alarmowych określa się w ścisłej współpracy z właściwymi służbami innych instytucji, agencji i organów unijnych oraz służbami państwa członkowskiego lub państw członkowskich, w których znajdują się obiekty Komisji.

3. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa jest punktem kontaktowym, jeżeli chodzi o stopnie alarmowe i zarządzanie sytuacjami kryzysowymi.

ROZDZIAŁ 4

**ORGANIZACJA**

*Artykuł 17*

**Ogólne obowiązki służb Komisji**

1. Obowiązki Komisji, o których mowa w niniejszej decyzji, są wykonywane przez Dyrekcję Generalną ds. Zasobów Ludzkich i Bezpieczeństwa z upoważnienia członka Komisji odpowiedzialnego za bezpieczeństwo i na jego odpowiedzialność.

2. Szczególne ustalenia dotyczące bezpieczeństwa cybernetycznego określono w decyzji C(2006) 3602.

3. Obowiązki w zakresie wykonania niniejszej decyzji i jej przepisów wykonawczych oraz zachowania bieżącej zgodności można przekazać innym departamentom Komisji, gdy zdecentralizowany system zapewniania bezpieczeństwa przynosi znaczące oszczędności wynikające z poprawy efektywności oraz oszczędności zasobów i czasu np. ze względu na lokalizację geograficzną danych usług.

4. W przypadkach, w których zastosowanie ma ust. 3, Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa, a w stosownym przypadku Dyrektor Generalny ds. Informatyki zawierają porozumienia z poszczególnymi departamentami Komisji, ustanawiając wyraźne role i obowiązki w zakresie wdrażania i monitorowania polityki bezpieczeństwa.

*Artykuł 18*

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

1. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa odpowiada w szczególności za:

1) opracowywanie polityki bezpieczeństwa Komisji, przepisów wykonawczych i instrukcji bezpieczeństwa;

2) gromadzenie informacji, biorąc pod uwagę ocenę zagrożeń i ryzyka związanego z bezpieczeństwem oraz informacji na temat wszystkich kwestii, które mogą wpłynąć na bezpieczeństwo w Komisji;

3) zapewnienie ochrony przed inwigilacją elektroniczną i ochrony wszystkich obiektów Komisji, z należytym uwzględnieniem ocen zagrożeń i dowodów na prowadzenie nielegalnych działań wobec interesów Komisji;

4) zapewnienie służby ratunkowej w służbach Komisji działającej 7 dni w tygodniu i 24 godziny na dobę oraz pracowników odpowiedzialnych za wszelkie kwestie związane z bezpieczeństwem;

5) wdrażanie środków bezpieczeństwa służących ograniczeniu ryzyka dla bezpieczeństwa oraz opracowywanie i prowadzenie odpowiedniego CIS w celu zaspokojenia swoich potrzeb operacyjnych, w szczególności w dziedzinach kontroli dostępu fizycznego, zarządzania upoważnieniami w zakresie bezpieczeństwa i zarządzania informacjami szczególnie chronionymi i niejawnymi UE;

6) podnoszenie świadomości, organizowanie ćwiczeń oraz zapewnianie szkoleń i doradztwa w zakresie wszystkich kwestii związanych z bezpieczeństwem w Komisji w celu promowania kultury bezpieczeństwa i utworzenia grupy pracowników odpowiednio przeszkolonych w sprawach bezpieczeństwa.

2. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa, bez uszczerbku dla kompetencji i obowiązków służb Komisji, zapewnia zewnętrzne kontakty:

1) z departamentami bezpieczeństwa innych instytucji, agencji i organów UE w sprawach związanych z bezpieczeństwem osób, mienia i informacji w Komisji;

2) ze służbami bezpieczeństwa, służbami wywiadowczymi i służbami odpowiedzialnymi za ocenę zagrożeń, w tym krajowymi organami bezpieczeństwa, służbami państw członkowskich, państw trzecich oraz organizacji i organów międzynarodowych w sprawach mających wpływ na bezpieczeństwo osób, mienia i informacji w Komisji;

3) z policją i innymi służbami ratowniczymi we wszystkich rutynowych i nadzwyczajnych sprawach mających wpływ na bezpieczeństwo Komisji;

4) z organami bezpieczeństwa innych instytucji, agencji i organów UE, państw członkowskich i państw trzecich w zakresie reagowania na ataki cybernetyczne mające potencjalny wpływ na bezpieczeństwo w Komisji;

5) w zakresie przyjmowania, oceniania i przekazywania danych wywiadowczych na temat zagrożeń stwarzanych przez działalność terrorystyczną i szpiegowską mającą wpływ na bezpieczeństwo w Komisji;

6) w zakresie kwestii związanych z informacjami niejawnymi określonymi w decyzji Komisji (UE, Euratom) 2015/444 ([1]).

3. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa odpowiada w szczególności za bezpieczne przekazanie informacji zgodnie z niniejszym artykułem, w tym przekazywanie danych osobowych.

*Artykuł 19*

**Grupa Ekspertów ds. Bezpieczeństwa Komisji**

Powołuje się Grupę Ekspertów ds. Bezpieczeństwa Komisji upoważnioną do doradzania Komisji w stosownych przypadkach w sprawach związanych z polityką bezpieczeństwa wewnętrznego Komisji, a zwłaszcza w celu ochrony informacji niejawnych UE.

([1]) Decyzja Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (zob. s. 53 niniejszego Dziennika Urzędowego).

*Artykuł 20*

**Lokalni pełnomocnicy ochrony (LSO)**

1. Każdy departament Komisji lub Gabinet wyznacza lokalnego pełnomocnika ochrony (LSO), który pełni funkcję głównego punktu kontaktowego między ich służbami a Dyrekcją Generalną ds. Zasobów Ludzkich i Bezpieczeństwa we wszystkich sprawach związanych z bezpieczeństwem w Komisji. W stosownych przypadkach można wyznaczyć jednego lub kilku zastępców LSO. LSO jest urzędnikiem lub pracownikiem zatrudnionym na czas określony.

2. Jako główny punkt kontaktowy ds. bezpieczeństwa w swoim departamencie Komisji lub gabinecie, LSO przekazuje, w regularnych odstępach czasu, Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa i swoim zwierzchnikom sprawozdanie na temat kwestii bezpieczeństwa dotyczących jego departamentu Komisji oraz przekazuje niezwłocznie sprawozdanie na temat wszelkich incydentów związanych z bezpieczeństwem, w tym incydentów dotyczących naruszenia EUCI lub szczególnie chronionych informacji jawnych.

3. W sprawach związanych z bezpieczeństwem systemów teleinformatycznych, LSO kontaktuje z lokalnym pełnomocnikiem bezpieczeństwa teleinformatycznego (LISO) ze swojego departamentu Komisji, którego rolę i obowiązki określono w decyzji C(2006) 3602.

4. LSO uczestniczy w szkoleniach w zakresie bezpieczeństwa i działaniach uświadamiających mających na celu zaspokojenie określonych potrzeb pracowników, wykonawców i innych osób pracujących pod zwierzchnictwem jego departamentu Komisji.

5. Na wniosek Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa LSO mogą zostać przypisane konkretne zadania w przypadku poważnego lub bezpośredniego zagrożenia dla bezpieczeństwa lub w sytuacjach wyjątkowych. Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa powiadamia o tych konkretnych zadaniach Dyrektora Generalnego lub Dyrektora ds. Zasobów Ludzkich lokalnej dyrekcji generalnej LSO.

6. Obowiązki LSO pozostają bez uszczerbku dla roli i obowiązków przypisanych lokalnym pełnomocnikom bezpieczeństwa teleinformatycznego (LISO), kierownikom ds. bezpieczeństwa i higieny pracy, urzędnikom kontroli kancelarii lub wszelkim innym pracownikom pełniącym funkcje powiązane z odpowiedzialnością w zakresie bezpieczeństwa. LSO kontaktuje z nimi w celu zapewnienia spójnego i konsekwentnego podejścia do bezpieczeństwa i efektywnego przepływu informacji w sprawach związanych z bezpieczeństwem w Komisji.

7. LSO ma bezpośredni dostęp do swojego dyrektora generalnego lub szefa służby podczas informowania swojego bezpośredniego przełożonego. LSO posiada upoważnienie w zakresie bezpieczeństwa umożliwiające mu dostęp do EUCI, co najmniej do poziomu SECRET UE/EU SECRET.

8. Aby promować wymianę informacji i najlepszych praktyk Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa organizuje co najmniej dwa razy w roku konferencję LSO. Obecność osób pełniących funkcję LSO na tych konferencjach jest obowiązkowa.

ROZDZIAŁ 5

**WDRAŻANIE**

*Artykuł 21*

**Przepisy wykonawcze i instrukcje bezpieczeństwa**

1. W stosownych przypadkach przyjęcie przepisów wykonawczych do niniejszej decyzji w pełnej zgodności z regulaminem wewnętrznym będzie przedmiotem odrębnej decyzji Komisji w sprawie uprawnień przysługujących członkowi Komisji odpowiedzialnemu za kwestie bezpieczeństwa.

2. Po uzyskaniu uprawnień w następstwie wyżej wspomnianej decyzji Komisji członek Komisji odpowiedzialny za kwestie bezpieczeństwa może opracowywać instrukcje bezpieczeństwa, w których określi wytyczne dotyczące bezpieczeństwa i najlepsze praktyki w zakresie niniejszej decyzji i jej przepisów wykonawczych.

3. Komisja może przekazać zadania wspomniane w ust. 1 i 2 niniejszego artykułu Dyrektorowi Generalnemu ds. Zasobów Ludzkich i Bezpieczeństwa w ramach osobnej decyzji w sprawie przekazywania zadań w pełnej zgodności z regulaminem wewnętrznym.

ROZDZIAŁ 6

**PRZEPISY RÓŻNE I KOŃCOWE**

*Artykuł 22*

**Przetwarzanie danych osobowych**

1. Komisja przetwarza dane osobowe niezbędne do wykonania niniejszej decyzji zgodnie z rozporządzeniem (WE) nr 45/2001.

2. Niezależnie od środków istniejących już w momencie przyjęcia niniejszej decyzji i zgłoszonych Europejskiemu Inspektorowi Ochrony Danych ([1]) wszelkie środki wprowadzone w ramach niniejszej decyzji i związane z przetwarzaniem danych osobowych, takich jak pliki dziennika wejść i wyjść, nagrania w systemie CCTV, zapisy połączeń telefonicznych z biurem lub centralami wysyłkowymi i innych podobnych danych, które są wymagane ze względów bezpieczeństwa lub reagowania kryzysowego, podlegają przepisom wykonawczym zgodnie z art. 21, w którym określono odpowiednie gwarancje dla podmiotów danych.

3. Dyrektor Generalny ds. Zasobów Ludzkich i Bezpieczeństwa odpowiada za bezpieczne przetwarzanie danych osobowych prowadzone w kontekście niniejszej decyzji.

4. Powyższe przepisy i procedury wykonawcze przyjmuje się po konsultacji z inspektorem ochrony danych i Europejskim Inspektorem Ochrony Danych zgodnie z rozporządzeniem (WE) nr 45/2001.

*Artykuł 23*

**Przejrzystość**

Niniejsza decyzja i jej przepisy wykonawcze są podawane do wiadomości pracowników Komisji i wszystkich osób, do których się odnoszą.

*Artykuł 24*

**Uchylenie poprzednich decyzji**

Uchyla się decyzję C(94) 2129.

*Artykuł 25*

**Wejście w życie**

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

Sporządzono w Brukseli dnia 13 marca 2015 r.

*W imieniu Komisji*
Jean-Claude JUNCKER
*Przewodniczący*

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.