IV

(Informacje)

INFORMACJE INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ

PARLAMENT EUROPEJSKI

DECYZJA PREZYDIUM PARLAMENTU EUROPEJSKIEGO

z dnia 6 czerwca 2011 r.

w sprawie przepisów regulujących postępowanie z informacjami poufnymi w Parlamencie Europejskim

(2011/C 190/02)

PREZYDIUM PARLAMENTU EUROPEJSKIEGO,

uwzględniając art. 23 ust. 12 Regulaminu Parlamentu Europejskiego,

mając na uwadze, że:

(1) W świetle porozumienia ramowego w sprawie stosunków między Parlamentem Europejskim i Komisją Europejską [1] podpisanego dnia 20 października 2010 r. konieczne jest wprowadzenie zmian do decyzji Prezydium z dnia 13 listopada 2006 r. w sprawie administracyjnego postępowania z dokumentami poufnymi.

(2) Traktat z Lizbony wyznacza Parlamentowi Europejskiemu nowe zadania, a w celu rozwinięcia działań Parlamentu w tych obszarach, które wymagają pewnego stopnia poufności, konieczne jest określenie podstawowych reguł, minimalnych standardów bezpieczeństwa i odpowiednich procedur postępowania przez Parlament Europejski z informacjami poufnymi, w tym niejawnymi.

(3) Przepisy decyzji mają na celu zapewnienie równoważnych standardów ochrony i zgodności z przepisami przyjętymi przez inne instytucje, organy, urzędy i agencje powołane na mocy lub na podstawie traktatów lub też przez państwa członkowskie, tak aby ułatwić sprawne funkcjonowanie procesu decyzyjnego Unii Europejskiej.

(4) Przepisy niniejszej decyzji nie naruszają postanowień art. 15 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) ani rozporządzenia (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 [2].

(5) Przepisy niniejszej decyzji nie naruszają art. 16 TFUE ani rozporządzenia (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 [3],

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Cel

Niniejsza decyzja reguluje tworzenie, przyjmowanie, przesyłanie i przechowywanie informacji poufnych przez Parlament Europejski w celu odpowiedniej ochrony ich poufnego charakteru. Wdraża ona w szczególności postanowienia załącznika 2 do porozumienia ramowego.

[1] Dz.U. L 304 z 20.11.2010, s. 47.

[2] Dz.U. L 145 z 31.5.2001, s. 43.

[3] Dz.U. L 8 z 12.1.2001, s. 1.

Artykuł 2

Definicje

Na użytek niniejszej decyzji:

a) „informacja" oznacza każdą informację pisemną lub ustną, niezależnie od jej nośnika i autora;

b) „informacja poufna" oznacza „informację niejawną UE" (EUCI) oraz „inne informacje poufne" nieoznaczone klauzulą tajności;

c) „informacja niejawna UE" (EUCI) oznacza każdą informację i materiał opatrzone klauzulą „TRES SECRET UE/UE TOP SECRET" (ściśle tajne UE), „SECRET UE/UE SECRET" (tajne UE), „CONFIDENTIEL UE/UE CONFIDENTIAL" (poufne UE) lub „RESTREINT UE/UE RESTRICTED" (zastrzeżone UE), których nieuprawnione ujawnienie mogłoby spowodować różnego stopnia szkody dla interesów UE lub co najmniej jednego z jej państw członkowskich, niezależnie od tego, czy taka informacja pochodzi z instytucji, organów, urzędów i agencji ustanowionych na mocy lub na podstawie traktatów, czy została otrzymana od państw członkowskich, państw trzecich lub organizacji międzynarodowych. W związku z tym:

— TRÈS SECRET UE/TOP SECRET EU (ściśle tajne UE) stanowi klauzulę dla informacji lub materiałów, których nieupoważnione ujawnienie spowodowałoby wyjątkowo duże szkody dla podstawowych interesów Unii albo co najmniej jednego z jej państw członkowskich,

— SECRET UE/UE SECRET (tajne UE) stanowi klauzulę dla informacji lub materiałów, których nieupoważnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom Unii lub co najmniej jednego z jej państw członkowskich,

— CONFIDENTIEL UE/UE CONFIDENTIAL (poufne UE) stanowi klauzulę dla informacji lub materiałów, których nieupoważnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii lub co najmniej jednego z jej państw członkowskich;

— RESTREINT UE/UE RESTRICTED (zastrzeżone UE) stanowi klauzulę dla informacji lub materiałów, których nieupoważnione ujawnienie byłoby niekorzystne z punktu widzenia interesów Unii lub co najmniej jednego z jej państw członkowskich.

d) „inne informacje poufne" oznaczają wszelkie inne nieoznaczone klauzulą tajności informacje poufne, w tym informacje objęte przepisami o ochronie danych lub obowiązkiem tajemnicy służbowej, których autorem jest Parlament Europejski lub przekazane Parlamentowi Europejskiemu przez inne instytucje, organy urzędy i agencje utworzone na mocy traktatów lub przez państwa członkowskie;

e) „dokument" oznacza każdą utrwaloną informację, bez względu na jej formę fizyczną i cechy charakterystyczne;

f) „materiały" oznaczają jakikolwiek dokument lub dowolny mechanizm lub sprzęt, już wytworzony lub będący w trakcie wytwarzania;

g) „ograniczony dostęp" oznacza, że w przypadku danej osoby występuje potrzeba dostępu do informacji poufnych w związku z oficjalnym pełnieniem stanowiska lub wykonywaniem zadania;

h) „upoważnienie" oznacza decyzję przyjętą przez Przewodniczącego (w przypadku posłów do Parlamentu Europejskiego) lub Sekretarza Generalnego (w przypadku urzędników Parlamentu Europejskiego i innych pracowników Parlamentu zatrudnionych w grupach politycznych) o przyznaniu indywidualnego dostępu do EUCI do określonego poziomu tajności, w oparciu o pomyślny wynik postępowania sprawdzającego przeprowadzonego przez organ krajowy na podstawie przepisów danego państwa i zgodnie z postanowieniami określonymi w załączniku I część 2;

i) „obniżenie klasyfikacji" oznacza obniżenie poziomu klauzuli tajności;

j) „odtajnienie" oznacza zniesienie klauzuli tajności;

k) „autor" oznacza należycie upoważnionego autora EUCI lub każdej innej informacji poufnej;

l) „instrukcje bezpieczeństwa" oznaczają środki wykonawcze o charakterze technicznym określone w załączniku II [1].

Artykuł 3

Podstawowe zasady i minimalne standardy

1. Postępowanie Parlamentu Europejskiego względem informacji poufnych opiera się na podstawowych zasadach i minimalnych standardach określonych w załączniku I część 1.

2. Parlament Europejski ustanawia – zgodnie z podstawowymi zasadami i minimalnymi standardami – system zarządzania bezpieczeństwem informacji (ISMS), którego celem jest ułatwienie działań parlamentarnych administracyjnych, przy jednoczesnym zapewnieniu ochrony każdej informacji poufnej przetwarzanej przez Parlament Europejski, przy pełnym poszanowaniu zasad określonych przez autora takiej informacji zapisanych w instrukcjach bezpieczeństwa.

Przetwarzanie informacji poufnych za pomocą zautomatyzowanego systemu informacyjnego Parlamentu Europejskiego odbywa się zgodnie z zasadą gwarancji bezpieczeństwa informacji i jest określone w instrukcjach bezpieczeństwa.

[1] Załącznik do przyjęcia.

3. Posłowie do Parlamentu Europejskiego mogą zapoznawać się z informacjami niejawnymi, do poziomu klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL włącznie, bez poświadczenia bezpieczeństwa. W przypadku informacji oznaczonych klauzulą CONFIDENTIEL UE/EU CONFIDENTIAL posłowie podpisują uroczyste oświadczenie, że nie ujawnią oni treści przedmiotowych informacji osobom trzecim. Informacje opatrzone klauzulą na poziomie wyższym niż CONFIDENTIEL UE/EU CONFIDENTIAL są udostępniane jedynie tym posłom, którzy posiadają poświadczenie bezpieczeństwa na odpowiednim poziomie.

4. Urzędnicy Parlamentu Europejskiego i inni pracownicy Parlamentu zatrudnieni w grupach politycznych mogą zapoznawać się z informacjami poufnymi pod warunkiem ustanowienia zasady ograniczonego dostępu oraz z informacjami niejawnymi powyżej poziomu RESTREINT UE/EU RESTRICTED, jeżeli posiadają poświadczenie bezpieczeństwa na odpowiednim poziomie.

Artykuł 4

Tworzenie informacji poufnych oraz postępowanie administracyjne z tymi informacjami przez Parlament Europejski

1. Przewodniczący Parlamentu Europejskiego, przewodniczący zainteresowanych komisji parlamentarnych i Sekretarz Generalny i/lub wszelkie inne osoby należycie przez niego upoważnione na piśmie mogą być autorami informacji poufnych lub nadawać im charakter niejawny zgodnie z zapisami w instrukcjach bezpieczeństwa.

2. Tworząc informacje niejawne, autor stosuje odpowiednią klauzulę tajności zgodnie z międzynarodowymi standardami i definicjami określonymi w załączniku I. Autor określa również, z reguły, adresatów, którzy mają zostać upoważnieni do zapoznania się z danymi informacjami na poszczególnych poziomach tajności. Informacje te należy przekazać wydziałowi ds. informacji poufnych w momencie złożenia dokumentu w tym wydziale.

3. Informacje poufne objęte tajemnicą zawodową podlegają zasadom postępowania określonym w instrukcjach bezpieczeństwa.

Artykuł 5

Przyjmowanie informacji poufnych przez Parlament Europejski

1. Informacje poufne przyjmowane przez Parlament Europejski są przekazywane w sposób następujący:

— EUCI oznaczone klauzulą tajności RESTREINT UE/UE RESTRICTED i inne informacje poufne do sekretariatu organu parlamentarnego/osoby sprawującej urząd, który/która o nie wnioskuje,

— EUCI opatrzone klauzulą CONFIDENTIEL UE/UE CONFIDENTIAL lub wyższą do wydziału ds. informacji poufnych.

2. Rejestracja, przechowywanie i śledzenie drogi informacji poufnych są zapewniane albo przez sekretariat organu parlamentarnego/osoby sprawującej urząd, który/która otrzymał/otrzymała informacje, albo przez wydział ds. informacji poufnych.

3. W przypadku informacji poufnych przekazanych przez Komisję zgodnie z porozumieniem ramowym uzgodnienia w rozumieniu pkt 3.2 załącznika 2 do porozumienia ramowego (poczynione wspólnie i dotyczące adresatów, procedury zapoznawania się z dokumentami, np. zabezpieczonej czytelni i posiedzeń przy drzwiach zamkniętych lub innych kwestii), których celem jest zachowanie poufności informacji, są składane razem z informacją poufną w sekretariacie organu parlamentarnego/osoby sprawującej urząd lub w wydziale ds. informacji poufnych, jeżeli informacje oznaczone są klauzulą CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą.

4. Uzgodnienia, o których mowa w ust. 3, mogą również być stosowane przez analogię do przekazywania informacji poufnych przez inne instytucje, organy, urzędy i agencje ustanowione na mocy lub na podstawie traktatów lub przez państwa członkowskie.

5. EUCI opatrzone klauzulą TRÈS SECRET UE/EU TOP SECRET są przekazywane Parlamentowi Europejskiemu zgodnie z dodatkowymi ustaleniami, które zostaną uzgodnione między organem parlamentarnym/osobą sprawującą urząd, który/która wnioskuje o informacje, a instytucjami unijnymi lub państwami członkowskimi, przez które są one przekazywane. Konferencja Przewodniczących ustanawia komisję nadzoru. Zapewnia ona poziom ochrony adekwatny do klauzuli tajności.

Artykuł 6

Przekazywanie informacji niejawnych UE przez Parlament Europejski stronom trzecim

Parlament Europejski może, za zgodą autora informacji, przekazywać EUCI innym instytucjom, organom, urzędom czy agencjom ustanowionym na mocy lub na podstawie traktatów lub państwom członkowskim, pod warunkiem że zapewnią one przestrzeganie w toku pracy z EUCI zasad ściśle odpowiadających przepisom zawartym w decyzji, w ramach ich służb i obiektów.

Artykuł 7

Przechowywanie i zapoznawanie się z informacjami poufnymi w pomieszczeniach zabezpieczonych (zabezpieczona czytelnia)

1. Zabezpieczone czytelnie dysponują zabezpieczonym magazynem i pozbawione są kserokopiarek, telefonów, faksów, skanerów lub innego sprzętu technicznego służącego do powielania lub przekazywania dokumentów.

2. Dostęp do zabezpieczonej czytelni podlega następującym warunkom:

a) dostęp do zabezpieczonej czytelni mają wyłącznie następujące osoby:

— posłowie do Parlamentu Europejskiego, urzędnicy Parlamentu Europejskiego i inni pracownicy Parlamentu zatrudnieni w grupach politycznych, wyraźnie wskazani zgodnie z ustaleniami, o których mowa w art. 4 ust. 2 i art. 5 ust. 3 i 4,

— urzędnicy Parlamentu Europejskiego odpowiedzialni za zarządzanie wydziałem ds. informacji poufnych,

— jeżeli to konieczne – urzędnicy Parlamentu Europejskiego odpowiedzialni za bezpieczeństwo i bezpieczeństwo pożarowe.

Sprzątanie pomieszczeń zabezpieczonych następuje wyłącznie w obecności i pod ścisłym nadzorem pracownika wydziału ds. informacji poufnych;

b) każda osoba ubiegająca się o dostęp do informacji poufnych podaje uprzednio swoje nazwisko wydziałowi ds. informacji. Wydział ds. informacji kontroluje tożsamość każdej osoby, która składa wniosek o zapoznanie się z tymi informacjami oraz w razie potrzeby sprawdza, czy osoba ta posiada poświadczenie bezpieczeństwa na odpowiednim poziomie oraz jest faktycznie upoważniona do wglądu w nie w świetle ustaleń, o których mowa w art. 4 ust. 2 lub art. 5 ust. 3 i 4;

c) wydział ds. informacji poufnych może odmówić dostępu do czytelni każdej osobie nieupoważnionej na mocy powyższych lit. a) i b). Wszelkie sprzeciwy wobec decyzji wydziału ds. informacji poufnych przedstawiane są Przewodniczącemu w przypadku posłów do Parlamentu Europejskiego lub Sekretarzowi Generalnemu w innych przypadkach.

3. Zapoznawanie się z informacjami poufnymi w zabezpieczonej czytelni podlega następującym warunkom:

a) osoby upoważnione do zapoznania się z informacjami, które złożyły wniosek, o którym mowa w ust. 2 lit. b), stawiają się osobiście w wydziale ds. informacji poufnych.

Z wyjątkiem sytuacji nadzwyczajnych (np. przy dużej liczbie wniosków złożonych w krótkim czasie) możliwość zapoznania się z informacjami poufnymi w zabezpieczonej czytelni ma każdorazowo tylko jedna osoba, w obecności urzędnika wydziału ds. informacji poufnych.

Urzędnik ten informuje osobę upoważnioną o spoczywających na niej obowiązkach, a w szczególności zwraca się do niej o podpisanie uroczystego oświadczenia, że nie ujawni ona treści tych informacji osobie trzeciej;

b) w trakcie zapoznawania się z informacjami zakazane są kontakty zewnętrzne (w tym przy użyciu telefonu lub innych technologii), sporządzanie notatek i reprodukowanie czy fotografowanie informacji poufnych;

c) przed umożliwieniem danej osobie opuszczenia zabezpieczonej czytelni odpowiedzialny urzędnik z wydziału ds. informacji poufnych, o którym mowa w lit. a), upewnia się, że informacje poufne, do których osoba miała wgląd, są nadal na swoim miejscu oraz są w stanie nienaruszonym i kompletnym.

4. W przypadku uchybienia wspomnianym zasadom odpowiedzialny urzędnik z wydziału ds. informacji poufnych informuje o tym Sekretarza Generalnego, który przekazuje sprawę Przewodniczącemu, jeżeli sprawcą uchybienia jest poseł do Parlamentu Europejskiego.

Artykuł 8

Minimalne standardy dotyczące innych przypadków zapoznawania się z informacjami poufnymi

1. W odniesieniu do administracyjnego postępowania z informacjami poufnymi podczas posiedzenia przy drzwiach zamkniętych, sekretariat organu parlamentarnego/osoby sprawującej urząd odpowiedzialnego/odpowiedzialnej za to posiedzenie dopilnowuje, aby:

— wejście na salę posiedzenia było dozwolone jedynie dla wskazanych uczestników posiadających poświadczenie bezpieczeństwa na wymaganym poziomie,

— wszystkie dokumenty zostały ponumerowane, rozdane na początku posiedzenia i ponownie zebrane w momencie jego zakończenia oraz aby nie sporządzano notatek z tych dokumentów ani nie wykonywano ich fotokopii czy zdjęć,

— protokół posiedzenia nie zawierał żadnych odniesień do treści dyskusji nad informacją, która była rozpatrywana w trybie poufnym,

— informacje poufne przekazywane odbiorcom w Parlamencie Europejskim ustnie podlegały równorzędnym poziomom ochrony jak informacje w formie pisemnej. Może to obejmować uroczyste oświadczenie składane przez odbiorcę tych wiadomości, że nie ujawni ich treści żadnej osobie trzeciej.

2. Do administracyjnego postępowania z informacjami poufnymi poza posiedzeniami przy drzwiach zamkniętych przez sekretariat organu parlamentarnego/osoby sprawującej urząd mają zastosowanie następujące zasady:

— papierowa kopia dokumentów przekazywana jest osobiście kierownikowi sekretariatu, który rejestruje dokumenty i wydaje poświadczenie odbioru,

— takie dokumenty, w czasie kiedy nikt z nich nie korzysta, przechowywane są w zamkniętym pomieszczeniu, na odpowiedzialność sekretariatu,

— bez uszczerbku dla administracyjnego postępowania z informacjami poufnymi na posiedzeniu przy drzwiach zamkniętych, jak określono w ust. 1, w żadnym wypadku nie mogą one być powielane, zapisywane na innym nośniku czy też przekazywane jakiejkolwiek osobie,

— dostęp do takich dokumentów jest ograniczony do jego adresatów i pozostaje, zgodnie z ustaleniami, o których mowa w art. 4 ust. 2 lub art. 5 ust. 3 lub 4, pod nadzorem sekretariatu,

— sekretariat prowadzi rejestr osób, które zapoznały się z dokumentami, oraz dat i czasu tych konsultacji. Rejestr ten jest przekazywany wydziałowi ds. informacji poufnych w celu sporządzenia rocznego sprawozdania, o którym mowa w art. 12.

Artykuł 9

Archiwizowanie informacji poufnych

1. W pomieszczeniach Parlamentu Europejskiego zapewnia się bezpieczny system archiwizacji.

Informacje poufne złożone ostatecznie w wydziale ds. informacji poufnych lub w sekretariacie organu parlamentarnego/osoby sprawującej urząd są przenoszone do zabezpieczonego archiwum w wydziale ds. informacji poufnych w terminie 6 miesięcy po ostatnim wglądzie do nich i najpóźniej w terminie 1 roku od dnia ich złożenia.

2. Za zarządzanie zabezpieczonymi archiwami zgodnie ze standardowymi kryteriami archiwizacji odpowiada wydział ds. informacji poufnych.

3. Zapoznawanie się z informacjami poufnymi znajdującymi się w zabezpieczonych archiwach jest możliwe po spełnieniu następujących warunków:

— wyłącznie osoby określone imiennie lub przez zajmowane stanowisko w karcie towarzyszącej, wypełnionej przy składaniu informacji poufnych, upoważnione są do zapoznawania się z tymi informacjami,

— wniosek o zapoznanie się z informacjami poufnymi musi zostać przedstawiony wydziałowi ds. informacji poufnych, który przekazuje dany dokument do zabezpieczonej czytelni,

— stosuje się procedury i warunki odnoszące się do zapoznawania się z informacjami poufnymi, określone w art. 7.

Artykuł 10

Obniżanie klasyfikacji i odtajnianie informacji niejawnych UE

1. Klasyfikacja EUCI może być obniżona lub informacje te mogą być odtajnione wyłącznie za pozwoleniem autora oraz, gdy istnieje taka potrzeba, w uzgodnieniu z innymi zainteresowanymi stronami. Decyzję o obniżeniu klasyfikacji lub odtajnieniu potwierdza się na piśmie. Autor jest zobowiązany do informowania adresatów informacji o zmianie, a adresaci są z kolei odpowiedzialni za poinformowanie kolejnych adresatów, do których przesłali dokument lub dla których wykonali jego kopię, o zmianie. Autor w miarę możliwości określa na dokumencie niejawnym datę, okres lub wydarzenie, po którym klasyfikacja tego dokumentu może zostać obniżona lub dokument ten może zostać odtajniony. W przeciwnym razie autor przeprowadza przynajmniej raz na pięć lat przegląd dokumentów w celu dokonania oceny, czy nadana klauzula tajności nadal jest konieczna.

2. Odtajnienie dokumentów przechowywanych w zabezpieczonych archiwach odbywa się najpóźniej po upływie 30 lat, zgodnie z przepisami rozporządzenia Rady (EWG, Euratom) nr 354/83 z dnia 1 lutego 1983 r. dotyczącego udostępnienia do wglądu publicznego historycznych materiałów archiwalnych Europejskiej Wspólnoty Gospodarczej i Europejskiej Wspólnoty Energii Atomowej [1]. Odtajnienia dokonuje autor informacji niejawnej lub służba aktualnie za nią odpowiedzialna, zgodnie z przepisami załącznika I część 1 sekcja 10.

Artykuł 11

Naruszenie poufności

1. Naruszenie poufności ogólnie, a w niniejszej niniejszej decyzji w szczególności, skutkuje w przypadku posłów do Parlamentu Europejskiego zastosowaniem odnośnych przepisów dotyczących kar, przewidzianych w Regulaminie Parlamentu Europejskiego.

2. Naruszenie poufności przez pracowników skutkuje zastosowaniem procedur i kar przewidzianych odpowiednio w regulaminie pracowniczym i warunkach zatrudnienia innych pracowników Unii Europejskiej, zawartych w rozporządzeniu (EWG, Euratom) nr 259/68 [2] „Regulamin pracowniczy".

3. Przewodniczący i Sekretarz Generalny organizują wszelkie niezbędne dochodzenia.

Artykuł 12

Dostosowanie niniejszej decyzji oraz przepisy wykonawcze do niej i coroczne sprawozdania ze stosowania niniejszej decyzji

1. Sekretarz Generalny wnioskuje o wszelkie niezbędne dostosowania niniejszej decyzji i załączników do niej zawierających postanowienia wykonawcze oraz przekazuje te wnioski Prezydium w celu podjęcia decyzji.

2. Sekretarz Generalny przedstawia Prezydium roczne sprawozdanie ze stosowania niniejszej decyzji.

[1] Dz.U. L 43 z 15.2.1983, s. 1.
[2] Dz.U. L 56 z 4.3.1968, s. 1.

Artykuł 13

Przepisy przejściowe i końcowe

1. Informacje poufne, które przed rozpoczęciem stosowania niniejszej decyzji były w posiadaniu wydziału ds. informacji poufnych lub zostały zgromadzone w archiwum, są automatycznie opatrywane klauzulą RESTREINT UE/EU RESTRICTED (zastrzeżone UE), chyba że w ciągu jednego roku od wejścia w życie niniejszej decyzji autor tych informacji podejmie decyzję o nienadawaniu im klauzuli tajności lub o podwyższeniu ich klauzuli tajności albo też o opatrzeniu ich oznaczeniem.

2. Jeśli autor podejmie decyzję o podwyższeniu klauzuli tajności takich informacji poufnych, są one klasyfikowane na najniższym możliwym poziomie przez autora lub osoby przez niego wyznaczone, w porozumieniu z wydziałem ds. informacji poufnych i zgodnie z kryteriami zawartymi w załączniku I.

3. Uchyla się decyzję Prezydium z dnia 13 listopada 2006 r. w sprawie administracyjnego postępowania z dokumentami poufnymi.

4. Uchyla się decyzję Prezydium z dnia 24 października 2005 r. upoważniającą Sekretarza Generalnego do ustanowienia komisji ds. odtajnienia oraz do podejmowania decyzji w kwestii odtajnienia.

Artykuł 14

Wejście w życie

1. Niniejsza decyzja wchodzi w życie w dniu jej publikacji w *Dzienniku Urzędowym Unii Europejskiej*.

2. Decyzja zaczyna obowiązywać od dnia 1 lipca 2011 r.

ZAŁĄCZNIK I

CZĘŚĆ 1

PODSTAWOWE ZASADY I MINIMALNE NORMY BEZPIECZEŃSTWA W ZAKRESIE OCHRONY INFORMACJI POUFNYCH

1. **Wstęp**

Niniejsze przepisy ustanawiają podstawowe zasady i minimalne normy bezpieczeństwa, które muszą być przestrzegane przez Parlament Europejski we wszystkich miejscach, w których zatrudnia on pracowników, a także przez wszystkich odbiorców informacji niejawnych UE i innych informacji poufnych w celu zapewnienia bezpieczeństwa oraz zagwarantowania wszystkim osobom zainteresowanym, że została ustanowiona wspólna norma ochrony. Uzupełnieniem niniejszych przepisów są przepisy regulujące postępowanie z informacjami poufnymi w komisjach parlamentarnych i innych organach parlamentarnych przez osoby sprawujące urząd.

2. **Zasady ogólne**

Polityka bezpieczeństwa Parlamentu Europejskiego stanowi integralną część jego całościowej polityki wewnętrznego zarządzania i z tego względu jest oparta na zasadach rządzących tą całościową polityką. Zasady te obejmują legalność, przejrzystość, odpowiedzialność oraz pomocniczość i proporcjonalność.

Zasada legalności oznacza potrzebę pozostawania w ramach prawnych przy wykonywaniu zadań związanych z bezpieczeństwem oraz stosowania się do mających zastosowanie wymogów prawnych. Oznacza to także, że zakresy odpowiedzialności w sferze bezpieczeństwa muszą być oparte na odpowiednich przepisach prawa. Pełne zastosowanie mają tu przepisy regulaminu pracowniczego, w szczególności jego art. 17 dotyczący obowiązku powstrzymywania się przez personel od jakiegokolwiek niedozwolonego ujawniania informacji uzyskanych zgodnie z wykonywanymi zadaniami oraz tytuł VI określający środki dyscyplinarne. Oznacza to także, że pociąganie do odpowiedzialności za przypadki nieprzestrzegania przepisów bezpieczeństwa w ramach obszaru odpowiedzialności Parlamentu Europejskiego odbywa się zgodnie z polityką Parlamentu Europejskiego w zakresie środków dyscyplinarnych.

Zasada przejrzystości oznacza potrzebę zapewnienia jasności wszelkich zasad i przepisów w zakresie bezpieczeństwa, zachowania równowagi pomiędzy różnymi służbami i dziedzinami (bezpieczeństwo fizyczne w porównaniu z ochroną informacji itp.) oraz prowadzenia spójnej i odpowiednio ukierunkowanej polityki mającej na celu edukację w zakresie bezpieczeństwa. Oznacza ona także potrzebę opracowania zrozumiałych pisemnych wytycznych w celu wdrażania środków bezpieczeństwa.

Zasada odpowiedzialności oznacza, że w sferze bezpieczeństwa muszą być jasno określone zakresy odpowiedzialności. Ponadto wiąże się to z potrzebą regularnego sprawdzania, czy odpowiedzialność ta jest właściwie wypełniana.

Zasada pomocniczości oznacza, że struktury bezpieczeństwa są organizowane na najniższym możliwym poziomie organizacji i są jak najściślej związane z dyrekcjami generalnymi i służbami Parlamentu Europejskiego. Zasada proporcjonalności oznacza, że działania w zakresie bezpieczeństwa są ściśle ograniczone do tego, co jest bezwzględnie konieczne oraz że środki ochrony są proporcjonalne do chronionych interesów oraz do faktycznych lub potencjalnych zagrożeń tych interesów, tak aby zapewnić im obronę przy jak najmniejszym poziomie utrudnień.

3. **Podstawy bezpieczeństwa informacji**

Podstawy bezpieczeństwa informacji tworzą:

a) w ramach Parlamentu Europejskiego, organ INFOSEC (służba ds. bezpieczeństwa informacji), odpowiedzialny za współpracę z właściwymi władzami bezpieczeństwa w zakresie przekazywania informacji i wskazówek na temat zagrożeń natury technicznej dla bezpieczeństwa i wskazywania środków przeciwdziałania im;

b) ścisłą współpracę pomiędzy właściwymi służbami Parlamentu Europejskiego a służbami innych instytucji unijnych odpowiedzialnymi za bezpieczeństwo.

4. **Zasady bezpieczeństwa informacji**

4.1. *Cele*

Podstawowe cele bezpieczeństwa informacji to:

a) ochrona EUCI przed szpiegostwem, narażeniem na szwank ich bezpieczeństwa lub nieupoważnionym ujawnieniem;

b) ochrona EUCI przetwarzanych w systemach i sieciach teleinformatycznych przed zagrożeniami dla ich poufności, integralności i dostępności;

c) ochrona pomieszczeń Parlamentu Europejskiego, w których znajdują się EUCI, przed sabotażem i celowym złośliwym uszkodzeniem;

d) w przypadku gdyby zastosowane środki ochrony zawiodły, zapewnienie możliwości oceny wyrządzonych szkód, ograniczenia ich konsekwencji, przeprowadzenia dochodzenia w sprawie naruszenia bezpieczeństwa oraz zastosowania niezbędnych środków zaradczych.

4.2. *Nadawanie klauzuli tajności*

4.2.1. W przypadkach wymagających zachowania poufności niezbędne jest dokonanie rozważnej i opartej na doświadczeniu oceny, które informacje i materiały wymagają ochrony, i określenie zakresu tej ochrony. Najistotniejsze jest dostosowanie stopnia ochrony do znaczenia z punktu widzenia bezpieczeństwa danej informacji lub materiału, które mają zostać objęte ochroną. W celu zapewnienia swobodnego przepływu informacji należy unikać zarówno zawyżania, jak i zaniżania klauzuli tajności.

4.2.2. System nadawania klauzul tajności stanowi instrument zapewniający wdrażanie powyższych zasad określonych w niniejszej sekcji; podobny system nadawania klauzul tajności jest stosowany w toku planowania i organizowania działań mających na celu przeciwdziałanie szpiegostwu, aktom sabotażu, terroryzmowi i innym zagrożeniom, tak aby najwyższą ochroną były objęte najważniejsze obiekty, w których znajdują się EUCI, oraz ich najbardziej newralgiczne punkty.

4.2.3. Wyłącznie autor informacji odpowiada za nadanie jej klauzuli tajności.

4.2.4. Poziom klauzuli tajności może być określony wyłącznie na podstawie treści informacji.

4.2.5. W przypadku łączenia elementów różnych informacji całości nadaje się klauzulę tajności odpowiadającą co najmniej najwyższej klauzuli nadawanej poszczególnym informacjom. Zbiorowi informacji można jednak nadać klauzulę wyższą niż jego poszczególnym częściom.

4.2.6. Klauzulę tajności nadaje się wyłącznie wtedy, gdy jest to konieczne, i na niezbędny okres.

4.3. *Cele stosowania środków bezpieczeństwa*

Środki bezpieczeństwa:

a) obejmują wszystkie osoby, które mają dostęp do informacji niejawnych, nośników EUCI i innych informacji poufnych, a także wszystkie obiekty, w których takie informacje się znajdują, oraz ważne instalacje;

b) są zaprojektowane w sposób zapewniający wykrycie osób, które z racji umiejscowienia mogłyby stanowić zagrożenie dla takich informacji lub ważnych instalacji, w których znajdują się te informacje, oraz pozwalający na uniemożliwienie tym osobom dostępu lub ich usunięcie;

c) zapobiegają uzyskiwaniu przez osoby nieupoważnione dostępu do takich informacji lub zawierających je instalacji;

d) zapewniają udostępnianie takich informacji wyłącznie zgodnie z zasadą ograniczonego dostępu, która stanowi podstawę wszystkich aspektów bezpieczeństwa;

e) zapewniają integralność (tzn. zapobieganie zniekształcaniu treści, dokonywaniu zmian w sposób nieupoważniony lub niszczeniu informacji w sposób nieupoważniony) i dostępność (tzn. dla osób, które powinny zapoznać się z informacją i zostały do tego upoważnione) wszystkich informacji poufnych, zarówno objętych klauzulą tajności, jak i jawnych, w szczególności jeżeli są one przechowywane, przetwarzane lub przesyłane w postaci elektromagnetycznej.

5. **Wspólne minimalne normy**

Parlament Europejski jest zobowiązany do zagwarantowania przestrzegania wspólnych minimalnych norm bezpieczeństwa przez wszystkich odbiorców EUCI, zarówno w ramach instytucji, jak i w zakresie jej właściwości, tj. przez wszystkie jego departamenty i kontrahentów, tak aby przekazywaniu tych informacji towarzyszyła pewność, że będą one wykorzystywane z zachowaniem takiej samej staranności. Takie minimalne normy obejmują kryteria poświadczenia bezpieczeństwa mające zastosowanie do urzędników Parlamentu Europejskiego i innych pracowników Parlamentu zatrudnionych w grupach politycznych oraz procedury ochrony informacji poufnych.

Parlament Europejski zezwala na udostępnienie tych informacji podmiotom zewnętrznym wyłącznie wtedy, gdy zapewnią one, że w toku wykorzystywania tych informacji przestrzegane są przepisy co najmniej ściśle odpowiadające niniejszym wspólnym minimalnym normom.

Takie minimalne normy mają również zastosowanie w przypadkach, gdy Parlament Europejski powierza podmiotom prowadzącym działalność przemysłową lub innym zadania wymagające informacji poufnych.

6. **Bezpieczeństwo urzędników Parlamentu Europejskiego i innych pracowników Parlamentu zatrudnionych w grupach politycznych**

6.1. *Instrukcje dotyczące bezpieczeństwa skierowane do urzędników Parlamentu Europejskiego i innych pracowników Parlamentu zatrudnionych w grupach politycznych*

Urzędnicy Parlamentu Europejskiego i inni pracownicy Parlamentu zatrudnieni w grupach politycznych na stanowiskach, na których mogą mieć dostęp do EUCI, otrzymują dokładne instrukcje zarówno w momencie podejmowania pracy, jak i później w regularnych odstępach czasu o wymogach bezpieczeństwa oraz procedurach mających na celu ich spełnienie. Wymagane jest, by osoby te potwierdziły na piśmie, że przeczytały i w pełni rozumieją mające zastosowanie przepisy bezpieczeństwa.

6.2. *Obowiązki przełożonych*

Przełożeni mają obowiązek wiedzieć, którzy z podlegających im pracowników zajmują się informacjami niejawnymi lub mają dostęp do zabezpieczonych systemów komunikacyjnych lub informacyjnych oraz odnotowywać i zgłaszać wszelkie incydenty oraz stwierdzone słabości, które mogą mieć wpływ na bezpieczeństwo.

6.3. *Status bezpieczeństwa urzędników Parlamentu Europejskiego i innych pracowników Parlamentu zatrudnionych w grupach politycznych*

Ustanawia się procedury gwarantujące, że w przypadku uzyskania niekorzystnych informacji na temat urzędnika Parlamentu Europejskiego lub innego pracownika Parlamentu zatrudnionego w grupie politycznej podejmowane są kroki w celu ustalenia, czy osoba ta wykonuje pracę związaną z dostępem do informacji niejawnych lub czy ma ona dostęp do zabezpieczonych systemów komunikacyjnych lub informatycznych, oraz że została powiadomiona właściwa służba Parlamentu Europejskiego. W przypadku stwierdzenia, że osoba ta zagraża bezpieczeństwu, odmawia się jej dostępu do zadań, przy wykonywaniu których może zagrażać bezpieczeństwu, lub zostaje ona odsunięta od takich zadań.

7. **Bezpieczeństwo fizyczne**

Bezpieczeństwo fizyczne oznacza stosowanie środków ochrony fizycznej i technicznej, aby zapobiec nieuprawnionemu dostępowi do EUCI.

7.1. *Potrzeba ochrony*

Stopień środków bezpieczeństwa fizycznego stosowanych w celu zapewnienia ochrony EUCI jest proporcjonalny do klauzuli tajności, ilości oraz zagrożenia przechowywanych informacji i materiałów. Wszyscy posiadacze EUCI przestrzegają jednolitych praktyk dotyczących klauzuli tajności tych informacji i muszą przestrzegać wspólnych norm ochrony dotyczących nadzoru, przekazywania oraz dysponowania informacjami i materiałami wymagającymi ochrony.

7.2. *Kontrola*

Przed opuszczeniem obszaru, na którym znajdują się EUCI, do osób sprawujących nad nimi nadzór należy zapewnienie, aby były one bezpiecznie przechowywane oraz aby uruchomiono wszystkie urządzenia zabezpieczające (zamki, systemy alarmowe itp.). Po godzinach pracy prowadzone są kolejne, niezależne kontrole.

7.3. *Bezpieczeństwo budynków*

Budynki, w których znajdują się EUCI lub zabezpieczone systemy komunikacyjne i informacyjne, są chronione przed możliwością dostępu do nich osób nieupoważnionych.

Charakter środków ochrony przyznanych EUCI, na przykład: okratowanie okien, zamki w drzwiach, strażnicy przy wejściach, zautomatyzowane systemy kontroli dostępu, kontrole zabezpieczeń i patrole, systemy alarmowe, systemy wykrywające intruzów i psy stróżujące, zależą od:

a) klauzuli tajności i ilości informacji i materiałów podlegających ochronie oraz usytuowania pomieszczeń, w których są przechowywane;

b) jakości zabezpieczonych pojemników wykorzystywanych do przechowywania danych informacji i materiałów;

c) struktury fizycznej i lokalizacji budynku.

Sposób ochrony systemów komunikacyjnych i informatycznych zależy od oceny wartości odnośnych zasobów i stopnia szkód wynikających z potencjalnego narażenia bezpieczeństwa, od struktury fizycznej i lokalizacji budynku, w którym znajdują się te systemy oraz od umiejscowienia systemów w budynku.

7.4. *Plany ochrony na wypadek sytuacji nadzwyczajnych*

Szczegółowe plany ochrony informacji niejawnych na wypadek wystąpienia zagrożenia są przygotowywane z wyprzedzeniem.

8. **Zastrzeżenia, oznaczenia, nanoszenie klauzul tajności i zarządzanie nimi**

8.1. *Zastrzeżenia*

Nie dopuszcza się stosowania innych klauzul tajności niż określone w art. 2 lit. c) niniejszej decyzji.

W celu określenia terminu obowiązywania klauzuli tajności (co w przypadku informacji niejawnych oznacza automatyczne obniżenie klasyfikacji lub odtajnienie) dopuszczalne jest stosowanie uzgodnionych zastrzeżeń. Zastrzeżenie może mieć formę „OBOWIĄZUJE DO … (czas/data)" lub „OBOWIĄZUJE DO … (wydarzenie)".

W przypadkach gdy istnieje potrzeba ograniczenia kręgu odbiorców lub wskazania na szczególne zasady postępowania z dokumentem, stanowiące uzupełnienie środków określonych na podstawie klauzuli tajności, należy stosować dodatkowe zastrzeżenia, takie jak CRYPTO lub inne uznawane w ramach UE.

Zastrzeżeń używa się wyłącznie w połączeniu z klauzulą tajności.

8.2. *Oznaczenia*

Możliwe jest stosowanie dodatkowych oznaczeń w celu określenia dziedziny, do której odnosi się dany dokument, lub szczególnego kręgu odbiorców, zgodnie z zasadą ograniczonego dostępu, lub (w przypadku informacji innych niż niejawne) czasu obowiązywania embarga.

Oznaczenie nie jest klauzulą tajności i nie może być stosowane zamiast niej.

8.3. *Nanoszenie klauzul i zastrzeżeń*

Klauzule nanosi się w następujący sposób:

a) na dokumentach oznaczonych jako RESTREINT UE/EU RESTRICTED za pomocą środków mechanicznych lub elektronicznych;

b) na dokumentach oznaczonych jako CONFIDENTIEL UE/EU CONFIDENTIAL za pomocą środków mechanicznych i ręcznie, możliwe jest także drukowanie ich na wcześniej oznakowanych i zarejestrowanych arkuszach;

c) na dokumentach oznaczonych jako SECRET UE/EU SECRET i TRÈS SECRET EU/EU TOP SECRET – przy pomocy urządzeń mechanicznych lub ręcznie.

Zastrzeżenia muszą być nanoszone tak samo, w taki sam sposób jak klauzule tajności, bezpośrednio pod nimi.

8.4. *Zarządzanie klauzulami*

8.4.1. Postanowienia ogólne

Klauzula niejawności nadawana jest informacjom tylko w razie konieczności. Klauzula musi być wyraźnie i prawidłowo naniesiona. Może ona być utrzymywana tylko przez niezbędny okres.

Wyłącznie autor odpowiada za nadanie klauzuli oraz, następnie, za obniżenie klasyfikacji lub odtajnienie.

Urzędnicy Parlamentu Europejskiego nadają informacjom klauzule, obniżają klasyfikację lub odtajniają informacje zgodnie z instrukcją lub z upoważnienia Sekretarza Generalnego.

Szczegółowe procedury postępowania z dokumentami niejawnymi określa się w sposób zapewniający, że są one chronione w sposób odpowiedni dla zawartych w nich informacji.

Liczba osób upoważnionych do tworzenia dokumentów opatrzonych klauzulą TRÈS SECRET UE/EU TOP SECRET musi być ograniczona do niezbędnego minimum, a ich nazwiska umieszczone w wykazie prowadzonym przez wydział ds. informacji poufnych.

8.4.2. Stosowanie klauzuli

Klauzula danego dokumentu jest określana na podstawie stopnia sensytywności zawartych w nim informacji, zgodnie z definicjami zamieszczonymi w art. 2 lit. c). Ważne jest, by klauzule były stosowane prawidłowo i oszczędnie, w szczególności w odniesieniu do klauzuli TRÈS SECRET UE/EU TOP SECRET.

Klauzula pisma lub noty zawierających załączniki ma taki poziom jak najwyższa klauzula nadana jednemu z załączników do nich. Autor wyraźnie wskazuje poziom, na który powinno się klasyfikować pismo lub notę po oddzieleniu od załączników.

Autor dokumentu, który zamierza nadać mu klauzulę tajności, musi pamiętać o powyższych przepisach i opanować wszelkie tendencje zarówno do zawyżania, jak i zaniżania klauzuli.

Poszczególne strony, ustępy, części, aneksy, dodatki, załączniki lub uzupełnienia do danego dokumentu mogą wymagać objęcia ich inną klauzulą tajności; z tego względu wymagane jest ich odpowiednie oznakowanie. Klauzula całego dokumentu musi odpowiadać klauzuli jego najwyżej zaklasyfikowanej części.

9. **Inspekcje**

Okresowe kontrole uzgodnień w dziedzinie bezpieczeństwa dotyczących ochrony EUCI są przeprowadzane przez dyrekcję Parlamentu Europejskiego ds. bezpieczeństwa, którą może wspierać w tym zadaniu wydział ds. informacji poufnych.

Dyrekcja Parlamentu Europejskiego ds. bezpieczeństwa i służby bezpieczeństwa innych instytucji, organów, urzędów i agencji ustanowionych na mocy lub na podstawie traktatów dysponujących EUCI mogą również zgodzić się na przeprowadzenie wzajemnej oceny uzgodnień w dziedzinie bezpieczeństwa dotyczących ochrony EUCI.

10. **Procedura odtajnienia**

10.1. Wydział ds. informacji poufnych zbada EUCI i przedstawi autorowi dokumentu propozycje odtajnienia, w każdym wypadku nie później niż w 25. roku od dnia jego utworzenia. Dokumenty nieodtajnione podczas pierwszego badania są ponownie badane okresowo, a przynajmniej co pięć lat.

10.2. Oprócz dokumentów znajdujących się faktycznie w zabezpieczonych archiwach i należycie opatrzonych klauzulą tajności proces odtajnienia może też obejmować inne poufne informacje istniejące w zabezpieczonych archiwach lub w Centrum Archiwów i Dokumentacji Parlamentu Europejskiego (CARDOC).

10.3. Wydział ds. informacji poufnych będzie odpowiadał w imieniu autora za poinformowanie adresatów dokumentu o zmianie klauzuli, a ci są z kolei odpowiedzialni za poinformowanie o zmianie dalszych adresatów, do których przesłali dokument lub dla których wykonali jego kopię.

10.4. Odtajnienie nie wpływa na jakiekolwiek oznaczenia, które mogą figurować na dokumencie.

10.5. Pierwotna klauzula naniesiona u góry i na dole każdej strony zostaje przekreślona. Pierwsza (tytułowa) strona dokumentu zostaje opatrzona pieczęcią i odnośnikiem wydziału ds. informacji poufnych.

10.6. Tekst odtajnionego dokumentu zostaje załączony do elektronicznej karty lub równoważnego systemu, w którym został on zarejestrowany.

10.7. W przypadku dokumentów objętych wyjątkiem z powodów dotyczących prywatności i uczciwości osoby fizycznej lub interesów handlowych osoby fizycznej lub prawnej oraz w przypadku dokumentów sensytywnych zastosowanie ma art. 2 rozporządzenia (EWG, Euratom) nr 354/83.

10.8. Oprócz postanowień pkt 10.1 do 10.7, zastosowanie mają następujące zasady:

a) w odniesieniu do dokumentów stron trzecich wydział ds. informacji poufnych skonsultuje się z zainteresowaną stroną trzecią przed przeprowadzeniem odtajnienia. Strona trzecia będzie miała osiem tygodni na przedstawienie uwag;

b) w odniesieniu do wyjątku z powodów dotyczących prywatności i uczciwości osoby fizycznej procedura odtajnienia uwzględni w szczególności zgodę osoby zainteresowanej, niemożność identyfikacji osoby zainteresowanej oraz fakt, że osoba ta już nie żyje;

c) w odniesieniu do wyjątku z powodów dotyczących interesów handlowych osoby fizycznej lub prawnej osoba zainteresowana może zostać powiadomiona za pomocą publikacji w *Dzienniku Urzędowym Unii Europejskiej*, z terminem czterech tygodni od daty tej publikacji na ewentualne uwagi.

CZĘŚĆ 2

PROCEDURA SPRAWDZAJĄCA W ZAKRESIE BEZPIECZEŃSTWA

11. **Procedura sprawdzająca w zakresie poświadczenia bezpieczeństwa dla posłów do Parlamentu Europejskiego**

11.1. W związku z uprawnieniami i kompetencjami Parlamentu Europejskiego posłom do niego można udzielić dostępu do EUCI do poziomu klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL włącznie, bez poświadczenia bezpieczeństwa. W przypadku informacji o klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL podpisują oni uroczyste oświadczenie, że nie ujawnią treści tych informacji żadnej osobie trzeciej.

11.2. Warunkiem uzyskania dostępu do informacji o klauzulach TRÈS SECRET UE/EU TOP SECRET lub SECRET UE/EU SECRET przez posłów do Parlamentu Europejskiego jest otrzymanie upoważnienia, zgodnie z procedurą określoną w pkt 11.3 i 11.4.

11.3. Upoważnienie udzielane jest wyłącznie posłom do Parlamentu Europejskiego, w stosunku do których właściwe organy krajowe państw członkowskich przeprowadziły postępowania sprawdzające, zgodnie z procedurą określoną w pkt 11.9 do 11.14. Przewodniczący odpowiada za udzielanie upoważnienia posłom.

11.4. Przewodniczący może udzielić upoważnienia po otrzymaniu opinii właściwych organów krajowych państw członkowskich, wydawanej na podstawie postępowania sprawdzającego zgodnie z procedurą określoną w pkt 11.8 do 11.13.

11.5. Dyrekcja Parlamentu Europejskiego ds. bezpieczeństwa prowadzi aktualny wykaz wszystkich posłów do Parlamentu Europejskiego, którzy uzyskali upoważnienie, w tym tymczasowe upoważnienie w rozumieniu pkt 11.15.

11.6. Upoważnienie jest wydawane na okres pięciu lat lub na okres wykonywania obowiązków, w odniesieniu do których zostało przyznane, zależnie od tego, który okres jest krótszy. Może natomiast zostać przedłużone zgodnie z procedurą określoną w pkt 11.4.

11.7. Przewodniczący cofa upoważnienie gdy uzna, że istnieją ku temu uzasadnione przesłanki. Decyzja o cofnięciu upoważnienia jest przekazywana zainteresowanemu posłowi do Parlamentu Europejskiego, który może ubiegać się o wysłuchanie przez Przewodniczącego zanim cofnięcie wejdzie w życie, oraz właściwemu organowi krajowemu.

11.8. Postępowanie sprawdzające jest przeprowadzane przy udziale zainteresowanego posła do Parlamentu Europejskiego na wniosek Przewodniczącego. Postępowanie sprawdzające przeprowadza właściwy organ krajowy państwa członkowskiego, którego obywatelem jest zainteresowany poseł.

11.9. Jednym z wymogów postępowania sprawdzającego jest wypełnienie formularza osobowego przez posła do Parlamentu Europejskiego.

11.10. Przewodniczący określa w swoim wniosku do właściwych organów krajowych poziom klauzuli tajności niejawnych informacji, które mają być udostępnione zainteresowanemu posłowi do Parlamentu Europejskiego, tak aby mogły one przeprowadzić postępowanie sprawdzające w zakresie poświadczenia bezpieczeństwa.

11.11. Całe postępowanie sprawdzające w zakresie poświadczenia bezpieczeństwa prowadzone przez właściwe organy krajowe, wraz z uzyskanymi wynikami, powinno być zgodne z właściwymi regułami i przepisami obowiązującymi w danym państwie członkowskim, włączając te dotyczące odwołań.

11.12. W przypadku wydania pozytywnej opinii przez właściwe organy krajowe państwa członkowskiego Przewodniczący może udzielić upoważnienia zainteresowanemu posłowi do Parlamentu Europejskiego.

11.13. Negatywna opinia właściwych organów krajowych jest przekazywana zainteresowanemu posłowi do Parlamentu Europejskiego, który może ubiegać się o wysłuchanie przez Przewodniczącego. Przewodniczący, jeśli uzna to za konieczne, może zwrócić się do właściwych organów krajowych z wnioskiem o udzielenie dodatkowych wyjaśnień. W przypadku potwierdzenia negatywnej opinii nie udziela się upoważnienia.

11.14. Wszyscy posłowie do Parlamentu Europejskiego, którym przyznano upoważnienie w rozumieniu pkt 11.3, w chwili przyznania upoważnienia, a następnie w regularnych odstępach czasu, otrzymują wszelkie niezbędne instrukcje dotyczące ochrony informacji niejawnych i środków zapewniających taką ochronę. Posłowie ci podpisują oświadczenie stwierdzające otrzymanie tych instrukcji.

11.15. W wyjątkowych okolicznościach Przewodniczący może udzielić posłowi do Parlamentu Europejskiego tymczasowego upoważnienia na okres nieprzekraczający sześciu miesięcy, obowiązującego do czasu zakończenia postępowania sprawdzającego określonego w pkt 11.11, pod warunkiem że poinformował o takim zamiarze właściwe organy krajowe i że nie zgłosiły one sprzeciwu w ciągu miesiąca. Przyznane w ten sposób tymczasowe upoważnienia nie dają prawa dostępu do informacji opatrzonych klauzulą TRÈS SECRET UE/EU TOP SECRET.

12. **Procedura sprawdzająca w zakresie poświadczenia bezpieczeństwa dla urzędników Parlamentu Europejskiego i innych pracowników Parlamentu zatrudnionych w grupach politycznych**

12.1. Dostęp do informacji niejawnych mogą posiadać wyłącznie urzędnicy Parlamentu Europejskiego i inni pracownicy Parlamentu zatrudnieni w grupach politycznych, którzy ze względu na swoje obowiązki oraz z uwagi na wymogi służbowe muszą posiadać wiedzę zawartą w takich informacjach.

12.2. Warunkiem uzyskania dostępu do informacji o klauzulach TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET oraz CONFIDENTIEL UE/EU CONFIDENTIAL przez osoby określone w pkt 12.1 jest otrzymanie upoważnienia, zgodnie z procedurą określoną w pkt 12.3 i 12.4.

12.3. Upoważnienie może być udzielone wyłącznie osobom, o których mowa w pkt 12.1, w stosunku do których właściwe organy krajowe państw członkowskich (krajowe władze bezpieczeństwa) przeprowadziły postępowania sprawdzające, zgodnie z procedurą określoną w pkt 12.9 do 12.14. Sekretarz Generalny odpowiada za udzielanie upoważnienia urzędnikom Parlamentu Europejskiego i innym pracownikom Parlamentu zatrudnionym w grupach politycznych.

12.4. Sekretarz Generalny może udzielić upoważnienia po otrzymaniu opinii właściwych organów krajowych państw członkowskich, wydawanej na podstawie postępowania sprawdzającego zgodnie z pkt 12.8 do 12.13.

12.5. Dyrekcja Parlamentu Europejskiego ds. bezpieczeństwa prowadzi aktualny wykaz wszystkich stanowisk wymagających poświadczenia bezpieczeństwa, na podstawie informacji przekazywanych przez poszczególne departamenty Parlamentu Europejskiego, oraz wszystkich osób, które uzyskały upoważnienia, włącznie z upoważnieniami tymczasowymi w rozumieniu pkt 12.15.

12.6. Upoważnienie jest wydawane na okres pięciu lat lub na okres wykonywania obowiązków, w związku z którymi zostało przyznane, zależnie od tego, który z nich jest krótszy. Może ono zostać przedłużone zgodnie z procedurą określoną w pkt 12.4.

12.7. Sekretarz Generalny cofa upoważnienie gdy uzna, że istnieją ku temu uzasadnione przesłanki. Decyzja o cofnięciu upoważnienia jest przekazywana zainteresowanemu urzędnikowi Parlamentu Europejskiego lub innemu pracownikowi Parlamentu zatrudnionemu w grupach politycznych, który może ubiegać się o wysłuchanie przez Sekretarza Generalnego, zanim cofnięcie to wejdzie w życie, oraz właściwemu organowi krajowemu.

12.8. Postępowanie sprawdzające w zakresie poświadczenia bezpieczeństwa jest przeprowadzane przy udziale zainteresowanej osoby na wniosek Sekretarza Generalnego. Postępowanie sprawdzające przeprowadza właściwy organ krajowy państwa członkowskiego, którego obywatelem jest osoba zainteresowana. Jeżeli krajowe przepisy ustawowe i wykonawcze dopuszczają taką możliwość, właściwe organy krajowe mogą przeprowadzać postępowania sprawdzające w odniesieniu do osób niebędących obywatelami ich kraju, którym potrzebny jest dostęp do informacji opatrzonej klauzulą CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej.

12.9. Jednym z wymogów postępowania sprawdzającego jest wypełnienie formularza osobowego przez zainteresowanego urzędnika Parlamentu Europejskiego lub innego pracownika Parlamentu zatrudnionego w zainteresowanej grupie politycznej.

12.10. Sekretarz Generalny określa w swoim wniosku do właściwych organów krajowych poziom klauzuli tajności informacji niejawnych, które mają być udostępnione zainteresowanej osobie, tak aby mogły one przeprowadzić postępowanie sprawdzające w zakresie poświadczenia bezpieczeństwa i wydać opinię dotyczącą stopnia upoważnienia, który mógłby zostać przyznany tej osobie.

12.11. Całe postępowanie sprawdzające w zakresie poświadczenia bezpieczeństwa prowadzone przez właściwe organy krajowe podlega, wraz z uzyskanymi wynikami, właściwym regułom i przepisom obowiązującym w danym państwie członkowskim, włączając te dotyczące odwołań.

12.12. W przypadku wydania pozytywnej opinii przez właściwe organy krajowe państwa członkowskiego Przewodniczący może udzielić upoważnienia zainteresowanej osobie.

12.13. Negatywna opinia właściwych organów krajowych jest przekazywana zainteresowanemu urzędnikowi Parlamentu Europejskiego lub innemu pracownikowi Parlamentu zatrudnionemu w zainteresowanej grupie politycznej, który może ubiegać się o wysłuchanie przez Sekretarza Generalnego. Sekretarz Generalny, jeśli uzna to za konieczne, może zwrócić się do właściwych organów krajowych z wnioskiem o udzielenie dodatkowych wyjaśnień. W przypadku potwierdzenia negatywnej opinii nie można udzielić upoważnienia.

12.14. Wszyscy urzędnicy Parlamentu Europejskiego i inni pracownicy Parlamentu zatrudnieni w grupach politycznych, którym przyznano upoważnienie w rozumieniu pkt 12.4 i 12.5, w chwili przyznania upoważnienia, a następnie w regularnych odstępach czasu, otrzymują wszelkie niezbędne instrukcje dotyczące ochrony informacji niejawnych i środków zapewniających taką ochronę. Ci urzędnicy i pracownicy podpisują oświadczenie stwierdzające otrzymanie tych instrukcji i zobowiązują się do ich przestrzegania.

12.15. W wyjątkowych okolicznościach Sekretarz Generalny może udzielić urzędnikowi Parlamentu Europejskiemu lub innemu pracownikowi Parlamentu zatrudnionemu w grupie politycznej tymczasowego upoważnienia na okres nieprzekraczający sześciu miesięcy, obowiązującego do czasu zakończenia postępowania sprawdzającego określonego w pkt 12.11 niniejszej sekcji, pod warunkiem że poinformował o takim zamiarze właściwe organy krajowe i że nie zgłosiły one sprzeciwu w ciągu miesiąca. Przyznane w ten sposób tymczasowe upoważnienia nie dają prawa dostępu do informacji opatrzonych klauzulą TRÈS SECRET UE/EU TOP SECRET.