II

(Komunikaty)

KOMUNIKATY INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH UNII EUROPEJSKIEJ

PARLAMENT EUROPEJSKI

DECYZJA PREZYDIUM PARLAMENTU EUROPEJSKIEGO

z dnia 15 kwietnia 2013 r.

dotycząca przepisów regulujących postępowanie z informacjami poufnymi w Parlamencie Europejskim

(2014/C 96/01)

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. (porozumienie ramowe) oraz porozumienia międzyinstytucjonalnego między Parlamentem Europejskim a Radą w sprawie przekazywania Parlamentowi Europejskiemu i wykorzystywania przez Parlament Europejski posiadanych przez Radę informacji niejawnych dotyczących spraw innych niż z dziedziny wspólnej polityki zagranicznej i bezpieczeństwa [2], podpisanego w dniu 12 marca 2014 r. (porozumienie międzyinstytucjonalne), konieczne jest ustanowienie szczegółowych przepisów regulujących postępowanie z informacjami poufnymi w Parlamencie Europejskim.

(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 obecnych i przyszłych przepisów o dostępie do dokumentów, przyjętych zgodnie z art. 15 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE).

[1] Dz.U. L 304 z 20.11.2010, s. 47.
[2] Dz.U. C 95, 1.4.2014, s. 1.

(5) Przepisy niniejszej decyzji nie naruszają obecnych i przyszłych przepisów o ochronie danych osobowych, przyjętych zgodnie z art. 16 TFUE

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Cel

Niniejsza decyzja reguluje zarządzanie informacjami poufnymi przez Parlament Europejski i postępowanie z nimi, w tym tworzenie, przyjmowanie, przesyłanie i przechowywanie takich informacji w celu odpowiedniej ochrony ich poufnego charakteru. Wdraża ona porozumienie międzyinstytucjonalne oraz porozumienie ramowe, w szczególności załącznik II do tego porozumienia.

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" oraz „inne informacje poufne" nieoznaczone klauzulą tajności.

c) „informacja niejawna" oznacza „informację niejawną UE" oraz „równoważne informacje niejawne";

d) „informacja niejawna UE" (EUCI) oznacza każdą informację i materiał opatrzone klauzulą tajności „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 Unii lub co najmniej jednego z jej państw członkowskich, niezależnie od tego, czy taka informacja pochodzi z instytucji, organów, urzędów lub agencji ustanowionych na mocy lub na podstawie traktatów. W związku z tym informacje i materiały niejawne opatrzone klauzulą tajności na poziomie:

— TRÈS SECRET UE/ TOP SECRET EU (ściśle tajne UE) stanowią informacje lub materiały, 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) stanowią informacje lub materiały, których nieupoważnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom Unii lub co najmniej jednego z jej państw członkowskich;

— CONFIDENTIEL UE/ UE CONFIDENTIAL (poufne UE) stanowią informacje lub materiały, których nieupoważnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii lub co najmniej jednego z jej państw członkowskich;

— RESTREINT UE/ UE RESTRICTED (zastrzeżone UE) stanowią informacje lub materiały, których nieupoważnione ujawnienie byłoby niekorzystne z punktu widzenia interesów Unii lub co najmniej jednego z jej państw członkowskich;

e) „równoważna informacja niejawna" oznacza informację niejawną wydaną przez państwa członkowskie, państwa trzecie lub organizacje międzynarodowe, która jest opatrzona oznaczeniami klauzul tajności równoważnymi z jednym z oznaczeń klauzul tajności stosowanych w przypadku EUCI i która została przekazana Parlamentowi Europejskiemu przez Radę lub Komisję;

f) „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;

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

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

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

j) „upoważnienie" oznacza decyzję przyjętą przez przewodniczącego (w przypadku posłów do Parlamentu Europejskiego) lub sekretarza generalnego (w przypadku urzędników Parlamentu Europejskiego i innych pracowników Parlamentu Europejskiego zatrudnionych w grupach politycznych), o przyznaniu indywidualnego dostępu do informacji niejawnych 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;

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

l) „odtajnienie" oznacza zniesienie klauzuli tajności;

m) „oznaczenie" oznacza znak naniesiony na „inne informacje poufne" w celu rozpoznania określonych uprzednio szczególnych instrukcji dotyczących postępowania z tymi informacjami lub dziedziny, której dany dokument dotyczy. Może ono być również naniesione na informacje niejawne w celu nałożenia dodatkowych wymogów dotyczących postępowania z tymi informacjami;

n) „likwidacja oznaczenia" oznacza zniesienie wszelkich oznaczeń;

o) „autor" oznacza należycie upoważnionego autora informacji poufnej;

p) „instrukcje bezpieczeństwa" oznaczają środki wykonawcze określone w załączniku II;

q) „zasady postępowania" oznaczają techniczne instrukcje wydane służbom Parlamentu Europejskiego, dotyczące zarządzania informacjami poufnymi.

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). ISMS składa się z instrukcji bezpieczeństwa, zasad postępowania oraz w właściwego regulaminu. ISMS ma na celu ułatwienie działań parlamentarnych i 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 komunikacyjnego i informacyjnego (CIS) Parlamentu Europejskiego odbywa się zgodnie z zasadą gwarancji bezpieczeństwa informacji, określoną w instrukcji bezpieczeństwa 3.

3. Posłowie do Parlamentu Europejskiego mogą zapoznawać się z informacjami niejawnymi, do poziomu klauzuli tajności RESTREINT UE/ UE RESTRICTED włącznie, bez poświadczenia bezpieczeństwa.

4. Informacje opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/ EU CONFIDENTIAL lub równoważną są udostępniane tym posłom do Parlamentu Europejskiego, którzy zostali do tego upoważnieni przez przewodniczącego na mocy ust. 5, lub którzy podpisali uroczyste oświadczenie, że nie ujawnią tych informacji osobom trzecim, oświadczenie o wypełnieniu obowiązku ochrony informacji opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/ EU CONFIDENTIAL, a także oświadczenie stwierdzające, że są świadomi skutków naruszenia tych reguł.

5. Informacje opatrzone klauzulą tajności na poziomie SECRET UE/ EU SECRET lub TRÈS SECRET/ EU TOP SECRET lub równoważną są udostępniane tym posłom do Parlamentu Europejskiego, którzy zostali do tego upoważnieni przez przewodniczącego, po tym, jak:

a) uzyskali poświadczenie bezpieczeństwa zgodnie z załącznikiem II część druga niniejszej decyzji, lub

b) otrzymano powiadomienie od właściwych organów krajowych, że ze względu na pełnione przez nich funkcje danym posłom przyznano odpowiednie upoważnienie zgodnie z krajowymi przepisami ustawowymi.

6. Przed uzyskaniem dostępu do informacji niejawnych posłowie do Parlamentu Europejskiego informowani są o spoczywającym na nich obowiązku ochrony takich informacji i potwierdzają przyjęcie do wiadomości tego obowiązku, zgodnie z załącznikiem I. Są oni również informowani o środkach zapewniających taką ochronę.

7. 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. Dostęp do informacji niejawnych jest przyznawany wyłącznie wtedy, jeżeli zostali oni poinformowani oraz otrzymali pisemne wskazówki dotyczące spoczywającego na nich obowiązku ochrony takich informacji i środków zapewniających taką ochronę oraz podpisali oświadczenie, w którym potwierdzili otrzymanie tych wskazówek oraz zobowiązanie do stosowania się do nich zgodnie z niniejszymi przepisami.

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 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 Działowi ds. Informacji Niejawnych (CIU) w momencie złożenia dokumentu w tym dziale.

3. „Inne informacje poufne" objęte tajemnicą zawodową podlegają postępowaniu zgodnie z załącznikiem II i II oraz zasadom postępowania.

Artykuł 5

Przyjmowanie informacji poufnych przez Parlament Europejski

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

a) informacje oznaczone klauzulą tajności na poziomie RESTREINT UE/ UE RESTRICTED lub równoważną i inne informacje poufne do sekretariatu organu parlamentarnego/ osoby sprawującej urząd, który/ która o nie wnioskuje;

b) informacje opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/ EU CONFIDENTIAL, SECRET UE/ EU SECRET lub TRÈS SECRET/ EU TOP SECRET lub równoważną dla CIU.

2. Rejestracją, przechowywaniem i śledzeniem drogi informacji poufnych zajmuje się, zależnie od przypadku, sekretariat organu parlamentarnego/ osoby sprawującej urząd, który/ która otrzymał/ otrzymała informacje lub CIU.

3. Poczynione wspólnie uzgodnienia, których celem jest zachowanie poufności informacji, w przypadku informacji poufnych przekazanych przez Komisję zgodnie z pkt. 3.2 załącznika II do porozumienia ramowego lub, w przypadku informacji niejawnych przekazanych przez Radę, zgodnie z art. 5 ust. 4 porozumienia międzyinstytucjonalnego, są składane razem z informacją poufną w sekretariacie organu parlamentarnego/ osoby sprawującej urząd lub w CIU, zależnie od przypadku.

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. W celu zapewnienia poziomu ochrony adekwatnego do klauzuli tajności na poziomie TRÈS SECRET UE/ EU TOP SECRET lub równoważnej Konferencja Przewodniczących powołuje komisję nadzoru. Informacje opatrzone klauzulą tajności na poziomie TRÈS SECRET UE/ EU TOP SECRET lub równoważną są przekazywane Parlamentowi Europejskiemu zgodnie z dodatkowymi ustaleniami, które zostaną uzgodnione między Parlamentem Europejskim a instytucją unijną, od której informacje zostały otrzymane.

Artykuł 6

Przekazywanie przez Parlament Europejski informacji niejawnych stronom trzecim

Parlament Europejski może, pod warunkiem uzyskania uprzedniej pisemnej zgody autora lub instytucji unijnej, która przekazała informacje niejawne Parlamentowi Europejskiemu, zależnie od przypadku, przekazywać takie informacje niejawne stronom trzecim, pod warunkiem, że w toku pracy z takimi informacjami zapewnią one przestrzeganie zasad ściśle odpowiadających przepisom zawartym w niniejszej decyzji, w ramach ich służb i obiektów.

Artykuł 7

Bezpieczna infrastruktura

1. Dla celów zarządzania informacjami poufnymi Parlament Europejski przygotowuje strefę bezpieczeństwa i zabezpieczone czytelnie.

2. Strefa bezpieczeństwa zapewnia infrastrukturę służącą rejestracji, archiwizacji i przekazywaniu informacji poufnych oraz zapoznawaniu się i postępowaniu z nimi. Zawiera ona między innymi czytelnię i salę spotkań na potrzeby zapoznawania się z informacjami poufnymi oraz podlega zarządzaniu CIU.

3. Możliwe jest tworzenie zabezpieczonych czytelni poza strefą bezpieczeństwa, w celu umożliwienia zapoznania się z informacjami opatrzonymi klauzulą tajności na poziomie RESTREINT UE/ EU RESTRICTED lub równoważną, oraz „innymi informacjami poufnymi". Wspomnianymi zabezpieczonymi czytelniami zarządzają właściwe służby sekretariatu organu parlamentarnego/ osoby sprawującej urząd lub CIU, zależnie od przypadku. Pozbawione są one kserokopiarek, telefonów, faksów, skanerów lub innego sprzętu technicznego służącego do powielania lub przekazywania dokumentów.

Artykuł 8

Rejestracja i przechowywanie informacji poufnych oraz postępowanie z nimi

1. Informacje opatrzone klauzulą tajności na poziomie RESTREINT UE/ EU RESTRICTED lub równoważną oraz „inne informacje poufne" są rejestrowane i przechowywane przez właściwe służby sekretariatów organu parlamentarnego/ osoby sprawującej urząd lub CIU, w zależności od tego, kto otrzymał rzeczone informacje.

2. Do postępowania z informacjami opatrzonymi klauzulą tajności na poziomie RESTREINT UE/ EU RESTRICTED lub równoważną oraz „innymi informacjami poufnymi" zastosowanie mają następujące warunki:

a) dokumenty przekazywane są osobiście kierownikowi sekretariatu, który rejestruje dokumenty i wydaje poświadczenie odbioru;

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

c) informacja nie może być w żadnym wypadku zapisana na innym nośniku ani przekazana jakiejkolwiek osobie. Dokumenty takie mogą być powielane przy pomocy należycie zatwierdzonego sprzętu, jak określono w instrukcjach bezpieczeństwa;

d) dostęp do takich informacji jest ograniczony do informacji wyznaczonych przez autora lub przez instytucję unijną, która przekazała informację Parlamentowi Europejskiemu, zgodnie z ustaleniami, o których mowa w art. 4 ust. 2 lub art. 5 ust. 3, 4 i 5;

e) sekretariat organu parlamentarnego/ osoby sprawującej urząd prowadzi rejestr osób, które zapoznały się z informacją, oraz dat i czasu tych konsultacji i przekazuje rejestr CIU w chwili złożenia informacji w CIU.

3. Informacje opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/ EU CONFIDENTIAL, SECRET UE/ EU SECRET lub TRÈS SECRET/ EU TOP SECRET lub równoważną są rejestrowane, wykorzystywane i przechowywane przez CIU w strefie bezpieczeństwa, zgodnie z właściwym poziomem klauzuli tajności określonym w instrukcjach bezpieczeństwa.

4. W przypadku uchybienia zasadom określonym w ust. 1-3 odpowiedzialny urzędnik z sekretariatu organu parlamentarnego/ osoby sprawującej urząd lub CIU, zależnie od przypadku, informuje o tym sekretarza generalnego, który przekazuje sprawę przewodniczącemu, jeżeli jest w nią zaangażowany poseł do Parlamentu Europejskiego.

Artykuł 9

Dostęp do zabezpieczonej infrastruktury

1. Dostęp do strefy bezpieczeństwa mają wyłącznie następujące osoby:

a) osoby, które zgodnie z art. 3 ust. od 4 do 7 są upoważnione do zapoznawawania się z informacjami przechowywanymi w tej strefie i złożyły odnośny wniosek zgodnie z art. 10 ust. 1;

b) osoby, które zgodnie z art. 4 ust. 1 są upoważnione do tworzenia informacji niejawnych i złożyły odnośny wniosek zgodnie z art. 10 ust. 1;

c) urzędnicy CIU zatrudnieni w Parlamencie Europejskim;

d) urzędnicy Parlamentu Europejskiego odpowiedzialni za zarządzanie wydziałem ds. informacji poufnych;

e) urzędnicy Parlamentu Europejskiego odpowiedzialni za bezpieczeństwo i bezpieczeństwo pożarowe, jeżeli to konieczne;

f) personel sprzątający, ale wyłącznie w obecności i pod ścisłym nadzorem pracownika CIU.

2. CIU może odmówić dostępu do strefy bezpieczeństwa każdej osobie nieupoważnionej do wejścia. Wszelkie sprzeciwy wobec takiej odmowy dostępu przedstawiane są przewodniczącemu w przypadku wniosków o dostęp złożonych przez posłów do Parlamentu Europejskiego lub sekretarzowi generalnemu w innych przypadkach.

3. Sekretarz generalny może zatwierdzić posiedzenie ograniczonej liczby osób w sali posiedzeń położonej w strefie bezpieczeństwa.

4. Dostęp do zabezpieczonej czytelni mają wyłącznie następujące osoby:

a) posłowie do Parlamentu Europejskiego, urzędnicy Parlamentu Europejskiego i inni pracownicy Parlamentu Europejskiego zatrudnieni w grupach politycznych, wyraźnie wskazani do celów zapoznawania się z informacjami poufnymi lub tworzenia informacji poufnych;

b) urzędnicy Parlamentu Europejskiego odpowiedzialni za zarządzanie wydziałem ds. informacji poufnych, urzędnicy sekretariatu organu parlamentarnego/ osoby sprawującej urząd, który/ która otrzymał/ otrzymała informacje, oraz urzędnicy CIU;

c) jeżeli to konieczne — urzędnicy Parlamentu Europejskiego odpowiedzialni za bezpieczeństwo i bezpieczeństwo pożarowe;

d) personel sprzątający, ale wyłącznie w obecności i pod ścisłym nadzorem urzędnika sekretariatu organu parlamentarnego/ osoby sprawującej urząd lub pracownika CIU, zależnie od przypadku.

5. Właściwy sekretariat organu parlamentarnego/ osoby sprawującej urząd lub CIU, zależnie od przypadku, może odmówić dostępu do zabezpieczonej czytelni każdej osobie nieupoważnionej. Wszelkie sprzeciwy wobec takiej odmowy przedstawiane są przewodniczącemu w przypadku wniosków o dostęp złożonych przez posłów do Parlamentu Europejskiego lub sekretarzowi generalnemu w innych przypadkach.

Artykuł 10

Zapoznawanie się z informacjami poufnymi w zabezpieczonych pomieszczeniach lub tworzenie w nich informacji poufnych

1. Osoba ubiegająca się o dostęp do informacji poufnych lub pragnące stworzyć informację poufną w strefie bezpieczeństwa podaje uprzednio swoje nazwisko CIU. CIU kontroluje tożsamość takiej osoby oraz sprawdza, czy osoba ta jest upoważniona zgodnie z art. 3 ust. 3 — 7, art. 4 ust. 1 lub art. 5 ust. 3, 4 i 5, do zapoznawania się z informacjami poufnymi lub tworzenia ich.

2. Osoba pragnąca, zgodnie z art. 3 ust. 3 i 7, zapoznać się z informacjami poufnymi opatrzonymi klauzulą tajności na poziomie RESTREINT UE/ EU RESTRICTED lub równoważną oraz „innymi informacjami poufnymi" w zabezpieczonej czytelni podaje z wyprzedzeniem swoje nazwisko właściwym służbom sekretariatów organu parlamentarnego/ osoby sprawującej urząd lub CIU.

3. Z wyjątkiem sytuacji nadzwyczajnych (np. przy dużej liczbie wniosków złożonych w krótkim czasie) możliwość zapoznania się z informacjami poufnymi w zabezpieczonym pomieszczeniu ma każdorazowo tylko jedna osoba, w obecności urzędnika sekretariatu organu parlamentarnego/ osoby sprawującej urząd lub CIU.

4. W trakcie zapoznawania się z informacjami zakazane są kontakty zewnętrzne (w tym przy użyciu telefonu lub innych urządzeń technicznych), sporządzanie notatek i reprodukowanie czy fotografowanie informacji poufnych.

5. Przed umożliwieniem danej osobie opuszczenia zabezpieczonego pomieszczenia urzędnik sekretariatu organu parlamentarnego/ osoby sprawującej urząd lub CIU upewnia się, że informacje poufne, do których osoba miała wgląd, są nadal na swoim miejscu oraz są w stanie nienaruszonym i kompletnym.

6. W przypadku uchybienia wspomnianym zasadom urzędnik sekretariatu organu parlamentarnego/ osoby sprawującej urząd lub CIU informuje o tym sekretarza generalnego, który przekazuje sprawę przewodniczącemu w przypadku gdy jest w nią zaangażowany poseł do Parlamentu Europejskiego.

Artykuł 11

Minimalne standardy dotyczące zapoznawania się z informacjami poufnymi na posiedzeniu przy drzwiach zamkniętych poza zabezpieczonym pomieszczeniem

1. Z informacjami opatrzonymi klauzulą tajności na poziomie RESTREINT UE/ EU RESTRICTED lub równoważną oraz „innymi informacjami poufnymi" mogą zapoznawać się członkowie komisji parlamentarnych lub innych organów politycznych i administracyjnych Parlamentu Europejskiego podczas posiedzeń przy drzwiach zamkniętych odbywających się poza zabezpieczonymi pomieszczeniami.

2. W sytuacji określonej w ust. 1 sekretariat organu parlamentarnego/ osoby sprawującej urząd odpowiedzialnego/ odpowiedzialnej za to posiedzenie dopilnowuje, by następujące warunki zostały spełnione:

a) wstęp do sali posiedzenia jest dozwolony jedynie uczestnikom wskazanym przez przewodniczącego właściwej komisji lub organu;

b) 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;

c) protokół posiedzenia nie zawiera żadnych odniesień do treści dyskusji nad rozpatrywaną informacją. W protokole może znaleźć się jedynie odnośna decyzja, o ile została podjęta;

d) informacje poufne przekazywane odbiorcom w Parlamencie Europejskim ustnie podlegały równorzędnym poziomom ochrony jak informacje w formie pisemnej;

e) żaden dodatkowy zapas dokumentów nie jest przechowywany w salach posiedzeń;

f) na początku posiedzenia uczestnikom i tłumaczom ustnym rozdaje się wyłącznie niezbędną ilość kopii dokumentów;

g) klauzula tajności/ oznaczenie dokumentów są jasno określane przez przewodniczącego posiedzenia na samym początku posiedzenia;

h) uczestnicy nie wynoszą dokumentów z sali posiedzeń;

i) z końcem posiedzenia wszystkie kopie dokumentów są zbierane i przeliczane przez sekretariat organu parlamentarnego/ osoby sprawującej urząd; i

j) do sali posiedzeń, w której następuje zapoznawanie się z rzeczonymi informacjami poufnymi i ich omówienie, nie można wnosić żadnych urządzeń komunikacji elektronicznej ani innych urządzeń elektronicznych.

3. W przypadku gdy zgodnie z wyjątkami określonymi w pkt. 3.2.2. załącznika II do porozumienia ramowego oraz w art. 6 ust. 5 porozumienia międzyinstytucjonalnego informacja opatrzona klauzulą tajności na poziomie CONFIDENTIEL UE/ EU CONFIDENTIAL lub równoważną jest omawiana na posiedzeniu przy drzwiach zamkniętych, sekretariat organu parlamentarnego/ osoby sprawującej urząd odpowiedzialnego/ odpowiedzialnej za to posiedzenie dopilnowuje, by dodatkowo oprócz spełnienia wymogów przepisów określonych w ust. 2 osoby wyznaczone do uczestnictwa w posiedzeniu spełniały wymogi art. 3 ust. 4 i 7.

4. W przypadku przewidzianym w ust. 3 CIU udostępnia sekretariatowi organu parlamentarnego/ osoby sprawującej urząd odpowiedzialnego/ odpowiedzialnej za to posiedzenie przy drzwiach zamkniętych wymaganą ilość kopii dokumentów do omówienia, które po zakończeniu posiedzenia są zwracane CIU.

Artykuł 12

Archiwizowanie informacji poufnych

1. Zapewnia się bezpieczny system archiwizacji w strefie bezpieczeństwa. Za zarządzanie zabezpieczonymi archiwami zgodnie ze standardowymi kryteriami archiwizacji odpowiada CIU.

2. Informacje niejawne złożone ostatecznie w CIU oraz informacje opatrzone klauzulą tajności na poziomie RESTREINT UE/ EU RESTRICTED lub równoważną złożone w sekretariacie organu parlamentarnego/ osoby sprawującej urząd są przenoszone do zabezpieczonego archiwum w strefie bezpieczeństwa w terminie 6 miesięcy po ostatnim wglądzie do nich i najpóźniej w terminie 1 roku od dnia ich złożenia. „Inne informacje poufne" są archiwizowane, chyba że zostały przekazane CIU przez sekretariat danego organu parlamentarnego/ osoby sprawującej urząd, zgodnie z ogólnymi przepisami dotyczącymi zarządzania dokumentami.

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

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

b) wniosek o zapoznanie się z informacjami poufnymi jest przedstawiany CIU, który przekazuje dany dokument do zabezpieczonej czytelni; i

c) stosuje się procedury i warunki odnoszące się do zapoznawania się z informacjami poufnymi, określone w art. 10.

Artykuł 13

Obniżenie klasyfikacji, odtajnienie i likwidacja oznaczenia informacji poufnych

1. Informacje poufne mogą być obniżone, odtajnione lub może zostać zlikwidowane ich oznaczenie wyłącznie za uprzednią pisemną zgodą autora oraz, gdy istnieje taka potrzeba, w uzgodnieniu z innymi zainteresowanymi stronami.

2. 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.

3. Informacje poufne przechowywane w zabezpieczonych archiwach są analizowane w odpowiednim czasie, ale nie później niż w 25. rocznicę ich utworzenia, w celu podjęcia decyzji dotyczącej ich odtajnienia, obniżenia ich klasyfikacji lub likwidacji ich oznaczenia. Analiza i publikacja takich informacji odbywa się 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.

4. Wskutek odtajnienia informacje uprzednio niejawne przechowywane w zabezpieczonych archiwach są przekazywane historycznym archiwom Parlamentu Europejskiego w celu ich zachowania i dalszego przetwarzania na mocy obowiązujących przepisów.

5. Wskutek likwidacji oznaczenia uprzednie „inne informacje poufne" zaczynają podlegać przepisom Parlamentu Europejskiego dotyczącym zarządzania dokumentami.

Artykuł 14

Naruszenie bezpieczeństwa oraz utrata lub zagrożenie bezpieczeństwa informacji poufnych

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

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

3. Przewodniczący ilub sekretarz generalny, zależnie od przypadku, organizują wszelkie niezbędne dochodzenia w przypadku naruszenia określonego w instrukcji bezpieczeństwa 6.

4. Jeżeli informacja poufna została przekazana Parlamentowi Europejskiemu przez inną instytucję unijną lub państwo członkowskie, przewodniczący lub sekretarz generalny, zależnie od przypadku, informują daną instytucję unijną lub państwo członkowskie o wszelkiej udowodnionej lub podejrzewanej utracie informacji niejawnej lub zagrożeniu jej bezpieczeństwa, a także o wynikach dochodzenia i środkach przyjętych w celu niedopuszczenia do ponownego wystąpienia takiego zdarzenia.

Artykuł 15

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. Za wykonanie niniejszej decyzji przez służby Parlamentu Europejskiego odpowiada sekretarz generalny, który wydaje zasady postępowania dotyczące kwestii objętych ISMS zgodnie z zasadami określonymi w niniejszej decyzji.

3. Sekretarz generalny przedstawia Prezydium roczne sprawozdanie ze stosowania niniejszej decyzji.

Artykuł 16

Przepisy przejściowe i końcowe

1. Informacje niebędące informacjami niejawnymi, będące w posiadaniu CIU lub jakiegokolwiek innego archiwum Parlamentu Europejskiego jako poufne i datowane przed dniem 1 kwietnia 2014 r., są uważane do celów niniejszej decyzji za „inne informacje poufne". Autor tych informacji może w każdej chwili zmienić ich stopień poufności.

2. W drodze odstępstwa od art. 5 ust. 1 lit. a) oraz art. 8 ust. 1 niniejszej decyzji, przez okres dwunastu miesięcy od dnia 1 kwietnia 2014 r. informacje udostępniane przez Radę na mocy porozumienia międzyinstytucjonalnego i opatrzone klauzulą tajności na poziomie RESTREINT UE/ EU RESTRICTED lub równoważną są składane do CIU i przez CIU rejestrowane oraz przechowywane. Z takimi informacjami można zapoznawać się zgodnie z art. 4 ust. 2 lit. a) i c) oraz art. 5 ust. 4 porozumienia międzyinstytucjonalnego.

3. Uchyla się decyzję Prezydium z dnia 6 czerwca 2011 r. w sprawie przepisów regulujących postępowanie z informacjami poufnymi w Parlamencie Europejskim.

Artykuł 17

Wejście w życie

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

ZAŁĄCZNIK I

Część I

PODSTAWOWE ZASADY I MINIMALNE NORMY BEZPIECZEŃSTWA W ZAKRESIE OCHRONY INFORMACJI POUFNYCH

1. **WPROWADZENIE**

Niniejsze przepisy ustanawiają podstawowe zasady i minimalne normy bezpieczeństwa w zakresie ochrony informacji poufnych, które muszą być przestrzegane lub spełniane przez Parlament Europejski we wszystkich miejscach, w których zatrudnia on pracowników, w tym przez wszystkich odbiorców informacji niejawnych i innych informacji poufnych w celu zapewnienia bezpieczeństwa oraz zagwarantowania wszystkich osobom zainteresowanym, że została ustanowiona wspólna norma ochrony. Uzupełnieniem tych przepisów są instrukcje bezpieczeństwa zawarte w załączniku II i inne przepisy regulujące postępowanie z informacjami poufnymi w komisjach parlamentarnych i innych organach parlamentarnych/ przez osoby sprawujące urząd.

2. **PODSTAWOWE ZASADY**

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.

Legalność oznacza potrzebę pozostawania w ramach prawnych przy wykonywaniu zadań związanych z bezpieczeństwem oraz stosowania się do mających zastosowanie wymogów prawnych. Dodatkowo 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 zadania oraz tytuł VI określający środki dyscyplinarne. Pociąganie do odpowiedzialności za przypadki nieprzestrzegania przepisów bezpieczeństwa w ramach obszaru odpowiedzialności Parlamentu Europejskiego odbywa się zgodnie z Regulaminem oraz jego polityką w zakresie środków dyscyplinarnych.

Przejrzystość 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. Potrzeba też opracowania zrozumiałych pisemnych wytycznych w celu wdrażania środków bezpieczeństwa.

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

Pomocniczość oznacza, że struktury bezpieczeństwa muszą być organizowane na najniższym możliwym poziomie organizacji i są jak najściślej związane z dyrekcjami generalnymi i służbami Parlamentu Europejskiego.

Proporcjonalność oznacza, że działania w zakresie bezpieczeństwa muszą być ściśle ograniczone do tego, co jest bezwzględnie konieczne oraz że środki ochrony muszą być proporcjonalne do chronionych interesów oraz do faktycznych lub potencjalnych zagrożeń tych interesów, tak aby zapewnić tym interesom obronę w sposób zapewniający jak najmniejszy poziom utrudnień.

3. **PODSTAWY BEZPIECZEŃSTWA INFORMACJI**

Podstawy bezpieczeństwa informacji tworzą:

a) właściwe systemy komunikacyjno-informacyjne (CIS). Wchodzą one w zakres odpowiedzialności organu bezpieczeństwa Parlamentu Europejskiego (określonego w instrukcji bezpieczeństwa 1);

b) w ramach Parlamentu Europejskiego, Organ ds. zabezpieczania informacji (określony w instrukcji bezpieczeństwa 1), odpowiedzialny za współpracę z właściwym organem bezpieczeństwa w zakresie przekazywania informacji i wskazówek na temat zagrożeń natury technicznej dla CIS i wskazywania środków przeciwdziałania tym zagrożeniom;

c) ścisła współpraca 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 informacji poufnych przed szpiegostwem, zagrożeniem ich bezpieczeństwa lub nieupoważnionym ujawnieniem;

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

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

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

4.2. ***Nadawanie klauzuli tajności***

4.2.1. W przypadkach wymagających zachowania poufności niezbędna jest rozważność i oparcie na doświadczeniu, by dokonać oceny, które informacje i materiały wymagają ochrony, oraz ocenić zakres wymaganej 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 zasad określonych w niniejszej sekcji. Podobny system nadawania klauzul powinien być stosowany w toku planowania i realizacji działań mających na celu przeciwdziałanie szpiegostwu, aktom sabotażu, terroryzmowi i innym zagrożeniom, tak aby zapewnić najściślejszą ochronę najważniejszym obiektom, w których znajdują się informacje niejawne, oraz najbardziej newralgicznym punktom tych obiektów.

4.2.3. Autor informacji jest wyłącznie odpowiedzialny za nadanie danej informacji klauzuli tajności.

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

4.2.5. W przypadku łączenia kilku elementów różnych informacji całości nadaje się klauzulę tajności odpowiadającą co najmniej najwyższej klauzuli nadanej jednemu z elementów informacji. 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 zawierających informacje niejawne i innych informacji poufnych, a także wszystkie obiekty, w których takie informacje się znajdują, oraz ważne instalacje;

b) są zaprojektowane w sposób zapewniający identyfikację osób, które z racji umiejscowienia (w kontekście dostępu, więzi personalnych lub z innych przyczyn) 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 (przez. 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) informacji poufnych, 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 informacji niejawnych, 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 stronom trzecim wyłącznie wtedy, gdy zagwarantują 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 informacji niejawnych, otrzymują dokładne instrukcje zarówno w momencie podejmowania pracy, jak i później w regularnych odstępach czasu, dotyczące zarówno wymogów bezpieczeństwa, jak i stosowanych procedur. Wymagane jest, by osoby te potwierdziły na piśmie, że przeczytały i w pełni rozumieją mające zastosowanie przepisy bezpieczeństwa.

6.2. ***Obowiązki przełożonych***

Częścią obowiązków przełożonych jest posiadanie wiedzy, 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 przez właściwy krajowy organ bezpieczeństwa, 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 informacji niejawnych.

7.1. ***Potrzeba ochrony***

Stopień środków bezpieczeństwa fizycznego stosowanych w celu zapewnienia ochrony informacji niejawnych jest proporcjonalny do klauzuli tajności, ilości oraz zagrożenia przechowywanych informacji i materiałów. Wszyscy posiadacze informacji niejawnych 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. ***Kontrole***

Przed opuszczeniem stref, w których znajdują się informacje poufne, osoby sprawujące nad nimi pieczę są zobowiązane do zapewnienia, że informacje są przechowywane w bezpieczny sposób oraz że zostały zamknięte zamki i uaktywnione systemy alarmowe. Po godzinach pracy prowadzone są kolejne, niezależne kontrole.

7.3. ***Bezpieczeństwo budynków***

Budynki, w których znajdują się informacje poufne lub zabezpieczone systemy i sieci teleinformatyczne, są chronione przed możliwością uzyskania do nich nieupoważnionego dostępu.

Sposób ochrony informacji poufnych, np. przez zastosowanie krat w oknach, zamków, straży przy wejściach, automatycznych systemów kontroli dostępu, kontroli bezpieczeństwa i patroli, systemów alarmowych, systemów wykrywania wtargnięcia i psów strażniczych, musi być określony na podstawie:

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; oraz

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 zapewniające ochronę informacji niejawnych w przypadku 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. d) 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.

Zastrzeżeń używa się wyłącznie w połączeniu z klauzulą tajności.

Zastrzeżenia są szczegółowo uregulowane w instrukcji bezpieczeństwa 2 oraz określone w zasadach postępowania.

8.2. ***Oznaczenia***

Oznaczenie jest stosowane w celu zidentyfikowania określonych uprzednio szczególnych instrukcji dotyczących postępowania z informacjami poufnymi. Oznaczenie może też wskazywać dziedzinę, do której odnosi się dany dokument, szczególny krąg 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.

Oznaczenia są szczegółowo uregulowane w instrukcji bezpieczeństwa 2 oraz określone w zasadach postępowania.

8.3. ***Nanoszenie klauzul i zastrzeżeń***

Nanoszenie klauzul, zastrzeżeń i oznaczeń jest dokonywane zgodnie z instrukcją bezpieczeństwa 2 sekcja E oraz zgodnie z zasadami postępowania.

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 informacji niejawnych opatrzonych klauzulą tajności na poziomie TRÈS SECRET UE/ EU TOP SECRET musi być ograniczona do niezbędnego minimum, a ich nazwiska zapisane w wykazie prowadzonym przez CIU.

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. d). Ważne jest, by klauzule były stosowane prawidłowo i oszczędnie.

Klauzula pisma lub noty zawierających załączniki ma co najmniej 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 przestrzegać powyższych przepisów i unikać 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 wewnętrzne kontrole uzgodnień w dziedzinie bezpieczeństwa informacji niejawnych są przeprowadzane przez Dyrekcję Parlamentu Europejskiego ds. Bezpieczeństwa i Oceny Ryzyka, która może zwrócić się o wsparcie ze strony organów bezpieczeństwa Rady lub Komisji.

Organy bezpieczeństwa i właściwe służby instytucji Unii mogą prowadzić, w ramach uzgodnionego procesu zapoczątkowanego przez którąkolwiek ze stron, wzajemne oceny uzgodnień w dziedzinie bezpieczeństwa dotyczących ochrony informacji niejawnych, wymienianych na mocy odnośnych porozumień międzyinstytucjonalnych.

10. **ODTAJNIENIE I PROCEDURY LIKWIDACJI OZNACZENIA**

10.1. CIU bada informacje poufne zawarte w swoim rejestrze i zwraca się do autora z propozycją udzielenia zgody na odtajnienie lub likwidację oznaczenia dokumentu, w każdym wypadku nie później niż w 25 rocznicę jego utworzenia. Dokumenty nieodtajnione lub wobec których nie zlikwidowano oznaczenia podczas pierwszego badania są ponownie badane okresowo, a przynajmniej co pięć lat. Oprócz dokumentów znajdujących się faktycznie w zabezpieczonych archiwach w strefie bezpieczeństwa i należycie opatrzonych klauzulą tajności, proces likwidacji oznaczenia może obejmować też inne poufne informacje będące w posiadaniu służb Parlamentu lub działu odpowiedzialnego za archiwa historyczne Parlamentu.

10.2 Decyzja dotycząca odtajnienia lub likwidacji oznaczenia dokumentu jest zasadniczo podejmowana wyłącznie przez jego autora, lub — wyjątkowo — we współpracy z organem parlamentarnym/ osobą sprawującą urząd, będącym w posiadaniu takiej informacji, zanim zawarta w dokumencie informacja zostanie przekazana działowi odpowiedzialnemu za archiwa historyczne Parlamentu. Informacja poufna może zostać odtajniona lub odznaczona wyłącznie za uprzednią pisemną zgodą autora. W przypadku „innych informacji poufnych" sekretariat organu parlamentarnego/osoby sprawującej urząd, będącym w posiadaniu takiej informacji we współpracy z autorem decyduje o tym, czy oznaczenie dokumentu może zostać zlikwidowane.

10.3. CIU będzie odpowiadał w imieniu autora za poinformowanie adresatów dokumentu o zmianie klauzuli lub oznaczeniu, 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 zastrzeżenia lub oznaczenia, które mogą figurować na dokumencie.

10.5. W przypadku odtajnienia pierwotna klauzula naniesiona u góry i na dole każdej strony zostaje przekreślona. Pierwsza (tytułowa) strona dokumentu zostaje opatrzona pieczęcią i odnośnikiem CIU. W przypadku likwidacji oznaczenia pierwotne oznaczenie naniesione u góry na każdej stronie zostaje przekreślone.

10.6. Tekst odtajnionego dokumentu lub dokumentu ze zlikwidowanym oznaczeniem 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 CIU konsultuje się z zainteresowaną stroną trzecią przed przeprowadzeniem odtajnienia lub likwidacji oznaczenia;

b) w odniesieniu do wyjątku z powodów dotyczących prywatności i uczciwości osoby fizycznej procedura odtajnienia lub likwidacji oznaczenia uwzględni w szczególności zgodę osoby zainteresowanej, lub — o ile ma to zastosowanie — niemożność identyfikacji osoby zainteresowanej;

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. Warunkiem uzyskania dostępu do informacji opatrzonych klauzulą tajności na poziomie „CONFIDENTIEL UE/ EU CONFIDENTIAL" lub równoważnych przez posłów do Parlamentu Europejskiego jest otrzymanie upoważnienia zgodnie z procedurą określoną w pkt. 11.3 i 11.4, lub złożenie przez tych posłów, zgodnie z art. 3 ust. 4 niniejszej decyzji, uroczystego oświadczenia, że informacje te nie zostaną ujawnione.

11.2 Warunkiem uzyskania dostępu do informacji opatrzonych klauzulą tajności na poziomie SECRET UE/ EU SECRET lub TRÈS SECRET UE/ EU TOP SECRET lub równoważnych przez posłów do Parlamentu Europejskiego jest otrzymanie upoważnienia, zgodnie z procedurą określoną w pkt. 11.3 i 11.14.

11.3. Upoważnienie udzielne 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 na piśmie 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 i Oceny Ryzyka 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 związku z którymi zostało przyznane, zależnie od tego, który z nich jest krótszy. Może natomiast zostać przedłużone zgodnie z procedurą określoną w pkt. 11.4.

11.7. Przewodniczący cofa upoważnienie, gdy uzna, że istnieją uzasadnione przesłanki dla takiego cofnięcia. Decyzja o cofnięciu upoważnienia jest przekazywana zainteresowanemu posłowi do Parlamentu Europejskiego, który może ubiegać się o wysłuchanie przez przewodniczącego zanim cofnięcie upoważnienia 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 właściwego organu krajowego poziom klauzuli tajności niejawnych informacji, które mają być udostępnione zainteresowanemu posłowi do Parlamentu Europejskiego, tak aby mógł on przeprowadzić postępowanie sprawdzające w zakresie poświadczenia bezpieczeństwa.

11.11 Całe postępowanie sprawdzające w zakresie poświadczenia bezpieczeństwa prowadzone przez właściwy organ krajowy, 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 właściwy organ krajowy 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 właściwego organu krajowego z wnioskiem o udzielenie dodatkowych wyjaśnień. W przypadku potwierdzenia negatywnej opinii nie można udzielić 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 potwierdzające 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 właściwy organ krajowy i że organ ten nie zgłosił sprzeciwu w ciągu miesiąca. Przyznane w ten sposób tymczasowe upoważnienia nie dają prawa dostępu do informacji opatrzonych klauzulą tajności na poziomie TRÈS SECRET UE/ EU TOP SECRET lub równoważną.

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 opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/ EU CONFIDENTIAL, SECRET UE/ EU SECRET lub TRÈS SECRET UE/ EU TOP SECRET, lub równoważnych przez zainteresowanych urzędników Parlamentu Europejskiego i innych pracowników Parlamentu zatrudnionych w grupach politycznych 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 pisemnego 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 i Oceny Ryzyka 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 uzasadnione przesłanki dla takiego cofnięcia. Decyzja o cofnięciu upoważnienia jest przekazywana zainteresowanemu urzędnikowi Parlamentu Europejskiego lub innemu pracownikowi Parlamentu zatrudnionemu w grupie politycznej, który może ubiegać się o wysłuchanie przez sekretarza generalnego, zanim cofnięcie upoważnienia wejdzie w życie, oraz właściwemu organowi krajowemu.

12.8. Postępowanie sprawdzające jest przeprowadzane przy udziale zainteresowanego urzędnika Parlamentu Europejskiego lub innego pracownika Parlamentu zatrudnionego w grupie politycznej, 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 tajności na poziomie CONFIDENTIEL UE/ EU CONFIDENTIAL SECRET UE/ EU SECRET lub TRÈS SECRET UE/ EU TOP SECRET.

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

12.10. Sekretarz generalny określa w swoim wniosku do właściwego organu krajowego poziom klauzuli tajności informacji niejawnych, które mają być udostępnione zainteresowanemu urzędnikowi Parlamentu Europejskiego lub innemu pracownikowi Parlamentu zatrudnionemu w grupie politycznej, tak aby mógł on przeprowadzić postępowanie sprawdzające w zakresie poświadczenia bezpieczeństwa i wydać opinię dotyczącą stopnia upoważnienia ewentualnie przyznanego tej osobie.

12.11. Całe postępowanie sprawdzające w zakresie poświadczenia bezpieczeństwa prowadzone przez właściwy organ krajowy, wraz z uzyskanymi wynikami, powinno być zgodne z właściwymi regułami i przepisami obowiązującymi w danym państwie członkowskim, włączając te dotyczące odwołań.

12.12. W przypadku wydania pozytywnej opinii przez właściwy organ krajowy sekretarz generalny może udzielić upoważnienia zainteresowanemu urzędnikowi Parlamentu Europejskiego lub innemu pracownikowi Parlamentu zatrudnionemu w grupie politycznej.

12.13. Negatywna opinia właściwych organów krajowych jest przekazywana zainteresowanemu urzędnikowi Parlamentu Europejskiego lub innemu pracownikowi Parlamentu zatrudnionemu w 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. Tacy urzędnicy i pracownicy podpisują oświadczenie potwierdzające 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, pod warunkiem że poinformował o takim zamiarze właściwy organ krajowy i że organ ten nie zgłosiła sprzeciwu w ciągu miesiąca. Przyznane w ten sposób tymczasowe upoważnienia nie dają prawa dostępu do informacji opatrzonych klauzulą tajności na poziomie TRÈS SECRET UE/ EU TOP SECRET lub równoważnej.

ZAŁĄCZNIK II

WPROWADZENIE

Niniejsze przepisy określają instrukcje bezpieczeństwa regulujące i zapewniające bezpieczne przetwarzanie informacji poufnych i zarządzanie nimi przez Parlament Europejski. Te instrukcje bezpieczeństwa wraz z zasadami postępowania tworzą system zarządzania bezpieczeństwem informacji (ISMS) Parlamentu Europejskiego, o którym mowa w art. 3 ust. 2 niniejszej decyzji:

INSTRUKCJA BEZPIECZEŃSTWA 1

Organizacja bezpieczeństwa w Parlamencie Europejskim w zakresie ochrony informacji poufnych

INSTRUKCJA BEZPIECZEŃSTWA 2

Zarządzanie informacjami poufnymi

INSTRUKCJA BEZPIECZEŃSTWA 3

Przetwarzanie informacji poufnych za pomocą zautomatyzowanych systemów komunikacyjno-informacyjnych (CIS)

INSTRUKCJA BEZPIECZEŃSTWA 4

Bezpieczeństwo fizyczne

INSTRUKCJA BEZPIECZEŃSTWA 5

Bezpieczeństwo przemysłowe

INSTRUKCJA BEZPIECZEŃSTWA 6

Naruszenie bezpieczeństwa, utrata lub zagrożenie bezpieczeństwa informacji poufnych

INSTRUKCJA BEZPIECZEŃSTWA 1

ORGANIZACJA BEZPIECZEŃSTWA W PARLAMENCIE EUROPEJSKIM W ZAKRESIE OCHRONY INFORMACJI POUFNYCH

1. Sekretarz generalny odpowiada za kompleksowe i spójne wdrożenie niniejszej decyzji.

Sekretarz generalny podejmuje wszelkie niezbędne środki, aby zadbać o stosowanie niniejszej decyzji do celów przetwarzania lub przechowywania informacji poufnych w budynkach Parlamentu przez posłów do Parlamentu Europejskiego, urzędników Parlamentu Europejskiego, pozostałych pracowników Parlamentu pracujących dla grup politycznych oraz kontrahentów.

2. Sekretarz generalny pełni rolę organu bezpieczeństwa (SA). Wykonując tę funkcję, odpowiada za:

2.1. koordynację wszelkich kwestii bezpieczeństwa związanych z działalnością Parlamentu w zakresie ochrony informacji poufnych;

2.2. zatwierdzenie utworzenia strefy bezpieczeństwa, zabezpieczonych czytelni oraz bezpiecznego wyposażenia;

2.3. wdrożenie decyzji zezwalających zgodnie z art. 6 niniejszej decyzji na przekazywanie przez Parlament informacji niejawnych stronom trzecim;

2.4. prowadzenie lub zlecanie dochodzenia w sprawie wszelkich wycieków informacji, do których prima facie doszło w Parlamencie, we współpracy z przewodniczącym Parlamentu Europejskiego, jeżeli dotyczy to posła do Parlamentu Europejskiego;

2.5. utrzymywanie ścisłego kontaktu z organami bezpieczeństwa pozostałych instytucji unijnych oraz z krajowymi organami bezpieczeństwa w państwach członkowskich w celu zapewnienia optymalnej koordynacji polityki bezpieczeństwa w zakresie informacji poufnych;

2.6. dokonywanie nieustannego przeglądu polityki i procedur bezpieczeństwa Parlamentu oraz wydawanie odpowiednich zaleceń w jego wyniku;

2.7. zdawanie sprawozdań krajowemu organowi bezpieczeństwa (NSA), który wykonał procedurę postępowania sprawdzającego zgodnie z załącznikiem I część 2 pkt 11.3, w przypadkach obejmujących jakiekolwiek niekorzystneh informacje, które mogą wpłynąć na ten organ.

3. Jeżeli sprawa dotyczy posła do Parlamentu Europejskiego, sekretarz generalny wykonuje swoje obowiązki w ścisłej współpracy z przewodniczącym Parlamentu Europejskiego.

4. Wykonując swoje obowiązki określone w pkt 2 i 3, sekretarz generalny otrzymuje wsparcie ze strony zastępcy sekretarza generalnego, Dyrekcji ds. Bezpieczeństwa i Oceny Ryzyka, Dyrekcji ds. Technologii Informacyjnych (DIT) oraz Działu ds. Informacji Niejawnych (CIU).

4.1. Dyrekcja ds. Bezpieczeństwa i Oceny Ryzyka odpowiada za środki bezpieczeństwa osobistego oraz w szczególności za procedurę poświadczenia bezpieczeństwa, określoną w załączniku 1 część 2. Dyrekcja ds. Bezpieczeństwa i Oceny Ryzyka powinnarównież:

a) stanowić punkt kontaktowy dla organów bezpieczeństwa pozostałych instytucji unijnych oraz dla krajowych organów bezpieczeństwa w sprawach związanych z procedurami poświadczenia bezpieczeństwa dotyczących posłów do Parlamentu Europejskiego, urzędników Parlamentu Europejskiego i pozostałych pracowników Parlamentu pracujących dla grup politycznych;

b) udzielać niezbędnych informacji ogólnych na temat bezpieczeństwa, dotyczących obowiązków ochrony informacji niejawnych oraz skutków zaniechania tego obowiązku;

c) monitorować funkcjonowanie strefy bezpieczeństwa i zabezpieczonych czytelni w budynkach Parlamentu, w odpowiednich przypadkach we współpracy ze służbami bezpieczeństwa pozostałych instytucji unijnych i krajowych organów bezpieczeństwa;

d) kontrolować we współpracy z organami bezpieczeństwa pozostałych instytucji unijnych i państw członkowskich procedury zarządzania informacjami niejawnymi i ich przechowywania, strefę bezpieczeństwa oraz zabezpieczone czytelnie w budynkach Parlamentu, w których przetwarzane są informacje niejawne;

e) przedstawiać sekretarzowi generalnemu odpowiednie zasady postępowania.

4.2. DIT odpowiada za bezpieczne systemy informatyczne, w których Parlament Europejski przetwarza informacje poufne.

4.3. CIU odpowiada za:

a) rozpoznanie potrzeb w zakresie bezpieczeństwa w celu skutecznej ochrony informacji poufnych, w ścisłej współpracy z Dyrekcją ds. Bezpieczeństwa i Oceny Ryzyka, DIT oraz organami bezpieczeństwa pozostałych instytucji unijnych;

b) identyfikację wszystkich aspektów zarządzania informacjami poufnymi i ich przechowywania w Parlamencie, określonych w zasadach postępowania;

c) funkcjonowanie strefy bezpieczeństwa;

d) zarządzanie informacjami poufnymi lub zapoznawanie się z nimi w strefie bezpieczeństwa lub w zabezpieczonej czytelni CIU zgodnie z art. 7 ust. 2 i art. 7 ust. 3 niniejszej decyzji;

e) zarządzanie rejestrem CIU;

f) zgłaszanie organowi bezpieczeństwa wszelkich dowiedzionych lub podejrzewanych naruszeń zasad bezpieczeństwa, utraty lub zagrożenia bezpieczeństwa informacji poufnych złożonych w CIU oraz przechowywanych w strefie bezpieczeństwa lub w zabezpieczonej czytelni CIU.

5. Pełniąc rolę organu bezpieczeństwa, sekretarz generalny wyznacza ponadto następujące organy:

a) organ ds. akredytacji bezpieczeństwa (SAA);

b) operacyjny organ ds. zabezpieczania informacji (IAOA);

c) organ ds. dystrybucji produktów kryptograficznych (CDA);

d) organ ds. TEMPEST (TA);

e) organ ds. zabezpieczania informacji (IAA).

Wykonywanie powyższych funkcji nie wymaga odrębnych jednostek organizacyjnych. Są one objęte oddzielnymi mandatami. Funkcje te oraz towarzyszące im obowiązki mogą być jednak połączone lub zintegrowane w tej samej jednostce organizacyjnej lub też podzielone na różne jednostki organizacyjne pod warunkiem, że nie prowadzi to do konfliktów interesów i powielania zadań.

6. SAA doradza we wszystkich kwestiach bezpieczeństwa związanych z akredytacją każdego systemu i każdej sieci technologii informacyjnej w Parlamencie przez:

6.1. dopilnowywanie, by CIS był zgodny z odnośnymi strategiami oraz wytycznymi w dziedzinie bezpieczeństwa, wydawanie poświadczenia dopuszczenia CIS do przetwarzania informacji niejawnych objętych określoną klauzulą tajności w jego środowisku operacyjnym oraz określanie warunków akredytacji i kryteriów, które muszą być spełnione, by konieczne było ponowne zatwierdzenie;

6.2. opracowanie procedury akredytacji bezpieczeństwa zgodnie z odnośnymi strategiami, która wyraźnie określi warunki zatwierdzenia CIS pod nadzorem SAA;

6.3. opracowanie strategii akredytacji bezpieczeństwa określającej stopień szczegółowości procedury akredytacji, który jest proporcjonalny do wymaganego poziomu zabezpieczenia;

6.4. analizowanie i zatwierdzanie dokumentacji związanej z bezpieczeństwem, w tym oświadczeń o zarządzaniu ryzykiem i o ryzyku szczątkowym, dokumentacji związanej z weryfikacją zapewnienia bezpieczeństwa oraz procedur bezpiecznej eksploatacji systemu, jak również zapewnianie zgodności tej dokumentacji ze strategiami i przepisami Parlamentu w zakresie bezpieczeństwa;

6.5. sprawdzanie wdrażania środków bezpieczeństwa w odniesieniu do CIS przez dokonywanie lub inicjowanie ocen, inspekcji lub przeglądów bezpieczeństwa czy też wspieranie takich działań;

6.6. określanie wymogów bezpieczeństwa (np. stopnie poświadczenia bezpieczeństwa osobowego) w przypadku stanowisk o szczególnie wrażliwym charakterze w odniesieniu do CIS;

6.7. zatwierdzanie lub w odpowiednich przypadkach uczestniczenie we wspólnym zatwierdzaniu międzysystemowego połączenia danego CIS z innymi CIS;

6.8. zatwierdzanie standardów bezpieczeństwa wyposażenia technicznego przeznaczonego do bezpiecznego przetwarzania informacji niejawnych oraz ich ochrony;

6.9. dopilnowanie, by produkty kryptograficzne stosowane w Parlamencie znalazły się na wykazie produktów zatwierdzonych przez UE; oraz

6.10. konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w związku z zarządzaniem ryzykiem dla bezpieczeństwa, w szczególności ryzykiem szczątkowym, jak również z warunkami i okolicznościami poświadczenia zatwierdzenia.

7. operacyjny organ ds. zabezpieczania informacji (IAOA) odpowiada za:

7.1. opracowanie dokumentacji bezpieczeństwa zgodnie ze strategiami oraz wytycznymi w dziedzinie bezpieczeństwa, w tym zwłaszcza oświadczenia o ryzyku szczątkowym, procedur bezpiecznej eksploatacji systemu i planu kryptograficznego w ramach procedury akredytacji CIS;

7.2. uczestnictwo w wyborze i testowaniu technicznych środków bezpieczeństwa, urządzeń i oprogramowania dla poszczególnych systemów w celu nadzorowania ich wdrażania oraz w celu dopilnowania, by były one w bezpieczny sposób instalowane, konfigurowane i konserwowane zgodnie z odpowiednią dokumentacją bezpieczeństwa;

7.3. monitorowanie wdrażania i stosowania procedur bezpiecznej eksploatacji systemu oraz — w stosownych przypadkach — przekazywanie obowiązków związanych z bezpieczeństwem operacyjnym właścicielowi systemu, czyli CIU;

7.4. zarządzanie produktami kryptograficznymi i ich wykorzystywanie, zapewnianie nadzoru nad obiektami kryptograficznymi i kontrolowanymi oraz, jeżeli jest to wymagane, zapewnienie wytwarzania zmiennych kryptograficznych;

7.5. przeprowadzanie przeglądów i testów analizy bezpieczeństwa, w szczególności w celu sporządzenia odpowiednich sprawozdań o ryzyku, zgodnie z wymogami SAA;

7.6. zapewnienie szkoleń na temat zabezpieczania informacji w odniesieniu do poszczególnych CIS;

7.7. wdrażanie i stosowanie środków bezpieczeństwa w odniesieniu do poszczególnych CIS.

8. Do zadań organu ds. dystrybucji produktów kryptograficznych (CDA) należą:

8.1. zarządzanie materiałami kryptograficznymi UE i odpowiedzialność za nie;

8.2. dopilnowanie w ścisłej współpracy z SAA, by wprowadzono odpowiednie procedury oraz aby istniały plany dotyczące bezpiecznego postępowania z wszystkimi materiałami kryptograficznymi UE oraz odpowiedzialności za nie, ich przechowywania i dystrybucji; oraz

8.3. zapewnianie przekazywania materiałów kryptograficznych UE między osobami lub służbami korzystającymi z tych materiałów.

9. Organ ds. TEMPEST (TA) odpowiada za zapewnienie zgodności CIS ze strategiami TEMPEST oraz zasadami postępowania. Zatwierdza on środki zaradcze TEMPEST dla instalacji i produktów, które służą ochronie informacji niejawnych do określonego poziomu klauzuli tajności w jego środowisku operacyjnym.

10. Organ ds. zabezpieczania informacji (IAA) odpowiada za wszystkie aspekty zarządzania informacjami poufnymi i postępowania z nimi w Parlamencie, a w szczególności za:

10.1 opracowanie wytycznych dotyczących bezpieczeństwa zabezpieczania informacji oraz bezpieczeństwa własnego, a także monitorowanie ich skuteczności i stosowności;

10.2. zabezpieczanie informacji technicznych związanych z produktami kryptograficznymi i zarządzanie tymi informacjami;

10.3. dopilnowanie, by środki zabezpieczania informacji wybrane do ochrony informacji niejawnych były zgodne z odpowiednimi strategiami dotyczącymi kryteriów ich przydatności i wyboru;

10.4. dopilnowanie, by wybór produktów kryptograficznych następował zgodnie ze strategiami dotyczącymi kryteriów ich przydatności i wyboru;

10.5. konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w związku z bezpieczeństwem zabezpieczania informacji;

INSTRUKCJA BEZPIECZEŃSTWA 2

ZARZĄDZANIE INFORMACJAMI POUFNYMI

A. **WPROWADZENIE**

1. Niniejsza instrukcja bezpieczeństwa określa przepisy dotyczące zarządzania przez Parlament informacjami poufnymi.

2. Tworząc informacje poufne, autor ocenia stopień poufności oraz podejmuje decyzję w oparciu o zasady określone w niniejszej instrukcji bezpieczeństwa, które dotyczą nadawania klauzuli tajności lub oznaczania takich informacji.

B. **NADAWANIE EUCI KLAUZULI TAJNOŚCI**

3. Decyzja o utajnieniu dokumentu zapada przed jego sporządzeniem. W tym celu opatrzenie informacji klauzulą EUCI wymaga wcześniejszej oceny stopnia jej poufności oraz decyzji autora, że nieupoważnione ujawnienie takich informacji mogłoby spowodować pewne szkody dla interesów Unii Europejskiej lub co najmniej jednego z jej państw członkowskich lub też osób fizycznych.

4. Po podjęciu decyzji o utajnieniu informacji należy dokonać drugiej wcześniejszej oceny w celu określenia stosownej klauzuli tajności. Klauzula tajności dokumentu jest określana na podstawie stopnia sensytywności zawartych w nim informacji.

5. Wyłącznie autor informacji odpowiada za nadanie jej klauzuli tajności. Urzędnicy Parlamentu nadają informacjom klauzule zgodnie z instrukcjami lub z upoważnienia sekretarza generalnego.

6. Z możliwości nadawania klauzul należy korzystać prawidłowo i oszczędnie. Autor dokumentu, który zamierza nadać mu klauzulę tajności, stara się uniknąć zarówno zawyżania, jak i zaniżania klauzuli.

7. Klauzula tajności przypisana danej informacji określa poziom ochrony przyznany jej w obszarze bezpieczeństwa osobowego, fizycznego, proceduralnego oraz zabezpieczenia informacji.

8. Informację, w przypadku której uzasadnione jest nadanie klauzuli tajności, należy oznaczać i przetwarzać jako taką niezależnie od jej formy fizycznej. Jej niejawny charakter należy wyraźnie zakomunikować odbiorcom albo przez oznaczenie klauzuli tajności (jeżeli informacja jest przekazywana w formie pisemnej, niezależnie od tego, czy na papierze, czy w CIS), albo w drodze komunikatu (jeżeli jest przekazywana ustnie, np. w trakcie rozmowy lub posiedzenia przy drzwiach zamkniętych). Materiał niejawny należy oznaczyć fizycznie, aby umożliwić łatwą identyfikację jego klauzuli tajności.

9. EUCI w formie elektronicznej można utworzyć jedynie w akredytowanym CIS. Same informacje niejawne, a także nazwa pliku i urządzenie do przechowywania (jeżeli zewnętrzne, takie jak CD-ROM lub pamięć USB) powinny być opatrzone odpowiednią klauzulą tajności.

10. Informacjom należy nadawać klauzulę tajności, gdy tylko nadana zostanie im forma. Na przykład osobiste notatki, robocze wersje lub wiadomości elektroniczne zawierające informacje, w przypadku których uzasadnione jest nadanie klauzuli tajności, należy od początku oznaczać jako EUCI oraz tworzyć i przetwarzać je zgodnie z niniejszą decyzją oraz odnośnymi zasadami postępowania pod względem fizycznym i technicznym. Z takich informacji może następnie powstać oficjalny dokument, który z kolei zostanie odpowiednio oznaczony i przetworzony. Być może podczas sporządzania oficjalny dokument trzeba poddać ponownej ocenie i nadać mu wyższą lub niższą klauzulę tajności w miarę jego opracowywania.

11. Autor może podjąć decyzję o nadaniu standardowej klauzuli tajności kategoriom informacji, które regularnie wytwarza. Musi jednak dopilnować, aby podczas tej czynności systematycznie nie zawyżać ani nie zaniżać klauzul tajności poszczególnych informacji.

12. EUCI jest zawsze opatrzona oznaczeniem klauzuli tajności odpowiadającym poziomowi jej klauzuli tajności.

B.1. ***Klauzule tajności***

13. EUCI otrzymują jedną z następujących klauzul tajności:

— „TRÈS SECRET UE/EU TOP SECRET", zgodnie z definicją zawartą w art. 2 lit. d) niniejszej decyzji, jeżeli zagrożenie bezpieczeństwa informacji mogłoby:

a) bezpośrednio zagrażać wewnętrznej stabilności Unii lub co najmniej jednego z jej państw członkowskich, państw trzecich lub organizacji międzynarodowych,

b) spowodować wyjątkowo poważną szkodę w stosunkach z państwami trzecimi lub organizacjami międzynarodowymi,

c) bezpośrednio prowadzić do znacznych strat w ludziach,

d) spowodować wyjątkowo poważną szkodę w bezpieczeństwie lub skuteczności operacyjnej personelu państw członkowskich lub innych stron uczestniczących, lub utrzymaniu skuteczności niezwykle istotnych działań organów bezpieczeństwa lub wywiadu, lub

e) spowodować dotkliwe długoterminowe straty w gospodarce Unii lub państw członkowskich;

— „SECRET UE/EU SECRET", zgodnie z definicją zawartą w art. 2 lit. d) niniejszej decyzji, jeżeli zagrożenie bezpieczeństwa informacji mogłoby:

a) doprowadzić do poważnych napięć międzynarodowych,

b) wyrządzić poważną szkodę w stosunkach z państwami trzecimi lub organizacjami międzynarodowymi,

c) bezpośrednio zagrażać życiu lub poważnie zaszkodzić w utrzymywaniu porządku publicznego lub bezpieczeństwa osobistego lub swobód,

d) zaszkodzić istotnym negocjacjom politycznym bądź handlowym, powodując znaczne problemy operacyjne dla Unii lub państw członkowskich,

e) spowodować poważną szkodę w bezpieczeństwie operacyjnym państw członkowskich lub skuteczności niezwykle istotnych działań organów bezpieczeństwa lub wywiadu,

f) spowodować poważne straty materialne w interesach finansowych, monetarnych, gospodarczych i handlowych Unii lub państw członkowskich,

g) poważnie osłabić zdolność finansową najważniejszych organizacji lub podmiotów, lub

h) poważnie utrudniać rozwój lub realizację działań Unii mających istotne skutki gospodarcze, handlowe lub finansowe;

— „CONFIDENTIEL UE/EU", zgodnie z definicją zawartą w art. 2 lit. d) niniejszej decyzji, jeżeli zagrożenie bezpieczeństwa informacji mogłoby:

a) poważnie zaszkodzić stosunkom dyplomatycznym, np. w przypadkach, w których spowodowałoby to oficjalny protest lub inne sankcje,

b) narazić na szwank osobiste bezpieczeństwo lub swobody,

c) poważnie zagrażać wynikowi negocjacji handlowych lub politycznych, powodując problemy operacyjne dla Unii lub państw członkowskich,

d) spowodować szkodę w bezpieczeństwie operacyjnym jednego lub kilku z państw członkowskich lub skuteczności działań organów bezpieczeństwa lub wywiadu,

e) poważnie osłabić zdolność finansową najważniejszych organizacji lub podmiotów,

f) utrudniać prowadzenie dochodzeń lub ułatwiać popełnianie przestępstw lub działalność terrorystyczną,

g) działać zasadniczo na niekorzyść finansowych, monetarnych, gospodarczych i handlowych interesów Unii lub państw członkowskich, lub

h) poważnie utrudniać rozwój lub realizację działań Unii mających istotne skutki gospodarcze, handlowe lub finansowe;

— „RESTREINT UE/EU RESTRICTED", zgodnie z definicją zawartą w art. 2 lit. d) niniejszej decyzji, jeżeli zagrożenie bezpieczeństwa informacji mogłoby:

a) niekorzystnie wpłynąć na ogólne interesy Unii,

b) niekorzystnie wpłynąć na stosunki dyplomatyczne,

c) spowodować bardzo trudną sytuację pojedynczych osób lub spółek,

d) niekorzystnie wpłynąć na negocjacje handlowe lub polityczne Unii lub państw członkowskich,

e) utrudnić skuteczne zachowanie bezpieczeństwa w Unii lub w państwach członkowskich,

f) utrudniać skuteczny rozwój lub realizację polityki Unii,

g) osłabić właściwe zarządzanie Unii i jej działaniami,

h) naruszać zobowiązania Parlamentu dotyczące utrzymania poufności informacji dostarczanych przez strony trzecie,

i) naruszać ograniczenia ustawowe dotyczące ujawniania informacji,

j) spowodować straty finansowe lub ułatwiać osiąganie nienależnego zysku bądź korzyści przez osoby lub spółki, lub

k) utrudniać prowadzenie dochodzeń lub ułatwiać popełnianie przestępstw.

B.2. ***Nadawanie klauzuli tajności zestawieniom, stronom tytułowym i fragmentom***

14. 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. Jeżeli pismo przewodnie lub pismo nie wymaga utajnienia, zawiera następujące sformułowanie: „Po oddzieleniu od załączników klauzula poufności niniejszej noty/niniejszego pisma zostaje zniesiona.".

15. Dokumenty lub pliki zawierające elementy, których częściom nadaje się różne klauzule tajności, są w miarę możliwości sporządzane w taki sposób, aby części oznaczone różnymi klauzulami można było łatwo zidentyfikować i w razie konieczności rozdzielić. Ogólna klauzula tajności dokumentu lub pliku jest co najmniej tak wysoka jak klauzula tajności tej części dokumentu, która została oznaczona najwyższą klauzulą tajności.

16 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. W celu wskazania poziomu klauzuli tajności sekcji lub ciągłych fragmentów tekstu krótszych niż jedna strona w dokumentach zawierających EUCI można stosować standardowe skróty.

17. W przypadku zebrania informacji pochodzących z różnych źródeł sprawdza się ostateczną wersję dokumentu w celu określenia jego ogólnej klauzuli tajności, gdyż może istnieć konieczność nadania mu klauzuli tajności wyższej niż klauzule jego poszczególnych części.

C. **INNE INFORMACJE POUFNE**

18. „Inne informacje poufne" oznacza się zgodnie z pkt E niniejszej instrukcji bezpieczeństwa i z zasadami postępowania.

D. **TWORZENIE INFORMACJI POUFNYCH**

19. Jedynie osoby uprawnione na mocy niniejszej decyzji lub upoważnione przez organ bezpieczeństwa mogą tworzyć informacje poufne.

20. Informacji poufnych nie dodaje się do internetowych lub intranetowych systemów zarządzania dokumentami.

D.1. ***Tworzenie EUCI***

21. Aby stworzyć EUCI opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET lub TRÈS SECRET UE/EU TOP SECRET, dana osoba jest uprawniona na mocy niniejszej decyzji lub uprzednio otrzymała upoważnienie, o którym mowa w art. 4 ust. 1 niniejszej decyzji.

22. EUCI opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET lub TRÈS SECRET UE/EU TOP SECRET są tworzone jedynie w strefie bezpieczeństwa.

23. Tworzenie EUCI podlega następującym zasadom:

a) każdą stronę wyraźnie oznacza się klauzulą tajności, która ma zastosowanie;

b) na każdej stronie widnieje numer strony oraz wskazanie całkowitej liczby stron;

c) pierwsza strona dokumentu zawiera numer referencyjny oraz opis przedmiotu dokumentu, które to informacje same w sobie nie mają charakteru poufnego, chyba że są załączone jako takie;

d) na pierwszej stronie dokumentu podaje się datę;

e) pierwsza strona dokumentu opatrzonego klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET lub TRÈS SECRET UE/EU TOP SECRET zawiera wykaz wszystkich aneksów i załączników;

f) na każdej stronie dokumentów opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET lub TRÈS SECRET UE/EU TOP SECRET widnieje liczba kopii, jeżeli mają one zostać udostępnione w wielu kopiach. Na pierwszej stronie każdej kopii również widnieje całkowita liczba kopii i stron, oraz

g) jeżeli dokument zawiera odniesienie do innych dokumentów zawierających informacje niejawne otrzymane od innych instytucji unijnych, lub jeżeli zawiera informacje niejawne wyodrębnione z takich dokumentów, jest opatrzony taką samą klauzulą tajności co te dokumenty i nie może bez wcześniejszej pisemnej zgody autora informacji zostać udostępniony żadnym innym osobom niż wymienione w liście dystrybucyjnej dotyczącej oryginalnego dokumentu lub dokumentów zawierających informacje niejawne.

24. Autor informacji zachowuje kontrolę nad EUCI, którą stworzył. Jego wcześniejsza pisemna zgoda jest konieczna, zanim EUCI zostanie:

a) odtajniona lub obniżona zostanie jej klauzula tajności;

b) wykorzystana do celów innych niż określone przez autora;

c) ujawniona państwu trzeciemu lub organizacji międzynarodowej;

d) ujawniona jakiejkolwiek osobie, instytucji, państwu lub organizacji międzynarodowej innej niż adresaci pierwotnie upoważnieni przez autora do zapoznania się z przedmiotową informacją;

e) ujawniona kontrahentowi lub potencjalnemu kontrahentowi mającemu siedzibę w państwie trzecim;

f) skopiowana lub przetłumaczona, jeżeli informacja jest opatrzona klauzulą tajności na poziomie TRÈS SECRET UE/EU TOP SECRET;

g) zniszczona.

D.2. ***Tworzenie innych informacji poufnych***

25. Pełniąc rolę organu bezpieczeństwa (SA), sekretarz generalny może podjąć decyzję o wyrażeniu zgody na stworzenie „innej informacji poufnej" przez dany podmiot, jednostkę i/lub osobę.

26. „Inne informacje poufne" są opatrzone jednym z oznaczeń określonych w zasadach postępowania.

27. Tworzenie „innych informacji poufnych" podlega następującym zasadom:

a) oznaczenie zostaje naniesione u góry pierwszej strony dokumentu;

b) na każdej stronie widnieje numer strony oraz całkowita liczba stron;

c) pierwsza strona dokumentu zawiera numer referencyjny oraz opis przedmiotu dokumentu;

d) na pierwszej stronie dokumentu podaje się datę; oraz

e) ostatnia strona dokumentu zawiera wykaz wszystkich aneksów i załączników.

28. Tworzenie „innych informacji poufnych" podlega szczegółowym przepisom i procedurom określonym w zasadach postępowania.

E. **ZASTRZEŻENIA I OZNACZENIA**

29. Zastrzeżenia i oznaczenia na dokumentach mają na celu kontrolę przepływu informacji oraz ograniczenie dostępu do informacji poufnych w oparciu o zasadę ograniczonego dostępu.

30. Przy stosowaniu lub załączaniu zastrzeżeń i/lub oznaczeń należy dopilnować, aby uniknąć pomylenia z klauzulami tajności dla EUCI: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET.

31. Zasady postępowania określają szczegółowe przepisy dotyczące stosowania zastrzeżeń i oznaczeń wraz z wykazem oznaczeń bezpieczeństwa zatwierdzonych przez Parlament Europejski.

E.1. ***Zastrzeżenia***

32. Zastrzeżeń można dokonywać jedynie w połączeniu z klauzulą tajności i nie można ich oddzielnie stosować do dokumentów. Zastrzeżenie można zastosować w odniesieniu do EUCI w celu:

a) ograniczenia ważności klauzuli tajności (co w przypadku informacji niejawnych oznacza automatyczne obniżenie klauzuli tajności lub odtajnienie);

b) ograniczenia dystrybucji danego EUCI;

c) wprowadzenia szczególnych zasad postępowania w uzupełnieniu do zasad odpowiadających klauzuli tajności.

33. Dodatkowe kontrole stosowane w odniesieniu do postępowania z dokumentami zawierającymi EUCI oraz przechowywania takich dokumentów stanowią dodatkowe obciążenie dla wszystkich zainteresowanych. Aby ograniczyć do minimum wymagany nakład pracy, przy tworzeniu takiego dokumentu należy określić termin lub wydarzenie, po zakończeniu którego klauzula tajności automatycznie wygaśnie, a informacja zawarta w dokumencie zostanie odtajniona lub jej klauzula tajności zostanie zniesiona.

34. Jeżeli dokument dotyczy szczególnego zakresu działalności, a jego dystrybucja musi zostać ograniczona i/lub powinna podlegać szczególnym zasadom postępowania, można w tym celu dodać do jego klauzuli tajności stosowne oświadczenie, aby umożliwić ustalenie jego docelowych odbiorców.

E.2. ***Oznaczenia***

35. Oznaczenia nie stanowią klauzuli tajności. Mają one w zamierzeniu jedynie dostarczać konkretnych instrukcji dotyczących postępowania z dokumentem i nie należy ich stosować do opisywania treści takiego dokumentu.

36. Oznaczenia można wprowadzać oddzielnie do dokumentów lub w połączeniu z klauzulą tajności.

37. Oznaczenia stosuje się z reguły do informacji objętych tajemnicą zawodową (o której mowa w art. 339 TFUE i art. 17 regulaminu pracowniczego, lub informacji wymagających ochrony Parlamentu ze względów prawnych), jednak nie muszą one (lub nie mogą) być utajnione.

E.3. ***Stosowanie oznaczeń w CIS***

38. Zasady dotyczące stosowania oznaczeń mają również zastosowanie do akredytowanych CIS.

39. SAA ustanawia szczegółowe zasady dotyczące stosowania oznaczeń w akredytowanych CIS.

F. **PRZYJMOWANIE INFORMACJI**

40. W Parlamencie jedynie CIU jest upoważniony do przyjmowania od stron trzecich informacji opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET lub TRÈS SECRET UE/EU TOP SECRET (lub równoważną).

41. W przypadku informacji opatrzonych klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED lub równoważną oraz „innych informacji poufnych", zarówno CIU, jak i właściwy organ parlamentarny/osoba sprawująca urząd mogą być odpowiedzialne za przyjmowanie informacji od stron trzecich, a także za stosowanie zasad określonych w niniejszej instrukcji bezpieczeństwa.

G. **REJESTRACJA**

42. Rejestracja oznacza stosowanie procedur rejestrowania etapów cyklu życia informacji poufnych, w tym ich rozpowszechniania, zapoznawania się z nimi i ich niszczenia.

43. Do celów niniejszej instrukcji bezpieczeństwa „dziennik" oznacza rejestr, w którym zapisywana jest w szczególności data i godzina:

a) wpłynięcia informacji do właściwego sekretariatu organu parlamentarnego/osoby sprawującej urząd lub — w zależności od przypadku — do CIU, oraz ich opuszczenia;

b) skorzystania z informacji przez osobę posiadającą poświadczenie bezpieczeństwa lub przekazania jej informacji; oraz

c) zniszczenia informacji.

44. W momencie tworzenia dokumentu zawierającego informacje niejawne autor takich informacji ma obowiązek zaznaczyć to po raz pierwszy. To oświadczenie zostaje przekazane CIU po stworzeniu dokumentu.

45. Informacje opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET lub TRÈS SECRET UE/EU TOP SECRET lub równoważną mogą zostać zarejestrowane do celów bezpieczeństwa tylko przez CIU. Informacje opatrzone klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED lub równoważną oraz „inne informacje poufne" otrzymane od stron trzecich są rejestrowane do celów administracyjnych przez służbę odpowiedzialną za oficjalne przyjmowanie dokumentów, którą może być CIU lub sekretariat organu parlamentarnego/osoby sprawującej urząd. „Inne informacje poufne" wytwarzane w Parlamencie są rejestrowane do celów administracyjnych przez autora.

46. Informacje opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET lub TRÈS SECRET UE/EU TOP SECRET lub równoważną są rejestrowane w szczególności, gdy:

a) są wytwarzane;

b) wpływają do CIU lub opuszczają go oraz

c) wpływają do CIS lub opuszczają go.

47. Informacje opatrzone klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED lub równoważną są rejestrowane w szczególności, gdy:

a) są wytwarzane;

b) wpływają do właściwego sekretariatu organu parlamentarnego/osoby sprawującej urząd lub do CIU bądź opuszczają je oraz

c) wpływają do CIS lub opuszczają go.

48. Rejestracji informacji poufnych można dokonywać na papierze lub w dziennikach elektronicznych/CIS.

49. W przypadku informacji opatrzonych klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED lub równoważną oraz „innych informacji poufnych" należy zapisać przynajmniej następujące dane:

a) datę i godzinę wpłynięcia do właściwego sekretariatu organu parlamentarnego/osoby sprawującej urząd lub do CIU bądź datę i godzinę opuszczenia ich, zależnie od przypadku;

b) tytuł dokumentu, poziom klauzuli tajności lub oznaczenia, datę wygaśnięcia klauzuli tajności/oznaczenia oraz każdy numer referencyjny, jakim opatrzono dokument.

50. W przypadku informacji opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET lub TRÈS SECRET UE/EU TOP SECRET lub równoważną należy zapisać przynajmniej następujące dane:

a) datę i godzinę wpłynięcia do CIU bądź opuszczenia go;

b) tytuł dokumentu, poziom klauzuli tajności lub oznaczenia, każdy numer referencyjny, jakim opatrzono dokument, oraz datę wygaśnięcia klauzuli tajności/oznaczenia;

c) szczegółowe dane dotyczące wytwórcy;

d) zapis tożsamości osoby (osób), które uzyskały dostęp do dokumentu, oraz daty tego, kiedydana osoba z niego skorzystała;

e) zapis wykonanych kopii lub tłumaczeń dokumentu;

f) datę i godzinę, kiedy kopie lub tłumaczenia dokumentu opuszczają CIU lub są zwracane do niego, oraz szczegółowe dane dotyczące miejsca docelowego, do którego je wysłano, i tego, kto je zwrócił;

g) datę i godzinę zniszczenia dokumentu oraz informację, kto tego dokonał, zgodnie z przepisami bezpieczeństwa Parlamentu dotyczącymi niszczenia dokumentów oraz

h) odtajnienie lub obniżenie klauzuli tajności dokumentu.

51. Dzienniki są opatrywane klauzulą tajności lub odpowiednio oznaczane. Dzienniki informacyjne opatrzone klauzulą tajnościna poziomie TRES SECRET UE/EU TOP SECRET lub równoważną są rejestrowane na tym samym poziomie.

52. Informacje niejawne mogą być rejestrowane:

a) w jednym dzienniku lub

b) w oddzielnych dziennikach według poziomu klauzuli tajności, statusu z podziałem na informacje przychodzące i wychodzące lub według pochodzenia i przeznaczenia informacji.

53. W przypadku elektronicznej obsługi w ramach CIS, procedury rejestracji mogą być prowadzone z wykorzystaniem środków z samego CIS spełniających wymogi równoważne powyższym. Gdy EUCI opuszczają obręb CIS, obowiązuje procedura rejestracji określona powyżej.

54. CIU prowadzi zapis wszystkich informacji niejawnych udostępnianych przez Parlament stronom trzecim oraz informacji niejawnych otrzymywanych przez Parlament od stron trzecich.

55. Po zakończeniu rejestracji informacji opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET lub TRES SECRET UE/EU TOP SECRET lub równoważną CIU sprawdza, czy adresaci posiadają ważne zezwolenie bezpieczeństwa. Jeżeli tak jest, CIU informuje adresata. Zapoznanie się z informacjami niejawnymi może nastąpić wyłącznie po zarejestrowaniu dokumentu zawierającego te informacje.

H. **UDOSTĘPNIANIE**

56. Autor informacji sporządza pierwotną listę dystrybucyjną dla EUCI, które wytworzył.

57. Informacje opatrzone klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED i inne informacje wytwarzane przez Parlament są udostępnianie przez autora wewnątrz Parlamentu, zgodnie z odnośnymi zasadami postępowania i zasadą ograniczonego dostępu. W przypadku informacji opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET lub TRES SECRET UE/EU TOP SECRET wytworzonych przez Parlament w strefie bezpieczeństwa lista dystrybucyjna (i wszelkie dalsze instrukcje dotyczące udostępniania) są przekazywane CIU, który jest odpowiedzialny za zarządzanie nią.

58. EUCI wytworzone przez Parlament mogą być udostępniane stronom trzecim jedynie przez CIU zgodnie z zasadą ograniczonego dostępu.

59. Informacje poufne otrzymywane przez CIU lub organ parlamentarny/ osobę sprawującą urząd, która o nie wnioskuje, są udostępniane zgodnie z instrukcjami otrzymanymi od autora informacji.

I. **POSTĘPOWANIE, PRZECHOWYWANIE I ZAPOZNAWANIE SIĘ**

60. Postępowanie z informacjami poufnymi, przechowywanie ich i zapoznawanie się z nimi odbywa się zgodnie z instrukcją bezpieczeństwa 2 i z zasadami postępowania.

J. **KOPIOWANIE/ TŁUMACZENIE PISEMNE/ TŁUMACZENIE USTNE INFORMACJI NIEJAWNYCH**

61. Dokumenty zawierające informacje opatrzone klauzulą tajności na poziomie TRES SECRET UE/EU TOP SECRET lub równoważną nie mogą być kopiowane ani tłumaczone bez wcześniejszej pisemnej zgody autora informacji. Dokumenty zawierające informacje opatrzone klauzulą na poziomie SECRET UE/EU SECRET lub równoważną bądź opatrzone klauzulą na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL lub równoważną mogą być kopiowane lub tłumaczone na polecenie ich posiadacza, o ile autor tego nie zabronił.

62. Dla celów bezpieczeństwa należy rejestrować każdy dokument zawierający informacje opatrzone klauzulą tajności na poziomie TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET lub CONFIDENTIEL UE/EU CONFIDENTIAL lub równoważną.

63. Środki bezpieczeństwa stosowane do oryginału dokumentu zawierającego informacje niejawne mają zastosowanie do jego kopii i tłumaczeń.

64. Dokumenty otrzymane z Rady powinny być sporządzone we wszystkich językach urzędowych.

65. Wytwórca lub posiadacz kopii może zwrócić się o otrzymanie kopii i/lub tłumaczeń dokumentów zawierających informacje niejawne. Kopie dokumentów zawierających informacje opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET lub TRES SECRET UE/EU TOP SECRET lub równoważną można tworzyć wyłącznie w zabezpieczonym miejscu i na kopiarkach będących częścią akredytowanego CIS. Kopie dokumentów zawierających informacje opatrzone klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED lub równoważną oraz inne informacje poufne tworzy się z wykorzystaniem akredytowanego urządzenia powielającego w budynkach Parlamentu.

66. Wszystkie kopie i tłumaczenia wszelkich dokumentów lub część kopii dokumentów zawierających informacje poufne są odpowiednio oznaczane, numerowane i rejestrowane.

67. Wykonuje się jedynie niezbędną liczbę kopii. Wszystkie kopie są niszczone po upłynięciu okresu konsultacji zgodnie z zasadami postępowania.

68. Wyłącznie tłumacze ustni i pisemni, którzy są urzędnikami Parlamentu, otrzymują dostęp do informacji niejawnych.

69. Tłumacze ustni i pisemni mający dostęp do dokumentów zawierających informacje opatrzone klauzulą tajności na poziomie , SECRET UE/EU SECRET lub TRES SECRET UE/EU TOP SECRET lub równoważną posiadają odpowiednie poświadczenie bezpieczeństwa.

70. Tłumacze ustni i pisemni pracują w strefie bezpieczeństwa nad dokumentami zawierającymi informacje opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET lub TRES SECRET UE/EU TOP SECRET lub równoważną.

K. **OBNIŻENIE, ODTAJNIENIE I LIKWIDACJA OZNACZENIA INFORMACJI POUFNYCH**

K.1. ***Zasady ogólne***

71. Odtajnia się informacje poufne, obniża się ich klauzulę tajności bądź likwiduje ich oznaczenie wówczas, gdy ich ochrona nie jest już konieczna lub nie jest już wymagana na pierwotnym poziomie.

72. Podjęcie decyzji o obniżeniu klauzuli tajności, odtajnieniu lub likwidacji oznaczenia informacji zawartych w dokumentach wytworzonych w Parlamencie może również być konieczne w trybie ad hoc, na przykład w odpowiedzi na wniosek o przyznanie dostępu złożony przez obywateli bądź inną instytucję UE lub z inicjatywy CIU bądź organu parlamentarnego/ osoby sprawującej urząd.

73. W chwili wytwarzania informacji wytwórca EUCI wskazuje, o ile jest to możliwe, czy w danym terminie lub w następstwie konkretnych okoliczności klauzula tajności EUCI może zostać obniżona lub zniesiona. Gdy takich wskazówek nie da się uzyskać, wytwórca, CIU lub organ parlamentarny/ osoba sprawująca urząd posiadający informacje dokonują przeglądu poziomu klasyfikacji EUCI przynajmniej raz na pięć lat. We wszystkich przypadkach klauzula tajności EUCI może zostać obniżona lub zniesiona jedynie po uzyskaniu pisemnej zgody wytwórcy.

74. Jeżeli wytwórcy EUCI nie można ustalić ani zlokalizować w przypadku dokumentów wytworzonych w Parlamencie, organ bezpieczeństwa dokonuje przeglądu poziomu klasyfikacji danych EUCI na podstawie wniosku organu parlamentarnego/ osoby sprawującej urząd posiadających informacje, którzy mogą w związku z tym przeprowadzić konsultacje z CIU.

75. CIU lub organ parlamentarny/ osoba sprawująca urząd posiadające informacje odpowiadają za informowanie adresata(adresatów) o obniżeniu lub zniesieniu klauzuli tajności informacji, a adresat(adresaci) odpowiadają ze swej strony za informowanie dalszego adresata (dalszych adresatów), którym przesłali dokument bądź jego kopię.

76. Odtajnienie informacji zawartych w dokumencie, obniżenie lub zniesienie ich klauzuli tajności jest odnotowywane.

K.2. ***Odtajnienie***

77. EUCI mogą zostać odtajnione w całości lub w części. Mogą onezostać odtajnione w części, jeżeli uznano, że dalsza ochrona nie jest konieczna w odniesieniu do konkretnej części dokumentu zawierającego te informacje, lecz nadal jest uzasadniona w przypadku pozostałej części dokumentu.

78. Jeżeli w wyniku przeglądu EUCI zawartych w dokumencie wytworzonym w Parlamencie podjęto decyzję od odtajnieniu ich, należy rozważyć, czy dokument może zostać upubliczniony lub oznaczony jako możliwy do udostępnienia (tj. nieupubliczniony).

79. Gdy EUCI zostają odtajnione, należy zapisać to w dzienniku wraz z następującymi danymi: datą odtajnienia, nazwiskami osób, które wnioskowały o odtajnienie, i osób, które zezwoliły na nie, numerem referencyjnym odtajnionego dokumentu oraz jego ostatecznym przeznaczeniem.

80. Na odtajnionym dokumencie i na wszystkich jego kopiach przekreśla się poprzednie oznaczenia klauzuli tajności. Dokumenty i wszystkie ich kopie muszą być odpowiednio przechowywane.

81. Po częściowym odtajnieniu informacji niejawnych część, którą odtajniono, jest sporządzana w formie wypisu i odpowiednio przechowywana. Właściwe służby rejestrują:

a) datę częściowego odtajnienia;

b) nazwiska osób, które wnioskowały o odtajnienie i które zezwoliły na nie oraz

c) numer referencyjny odtajnionego wypisu.

K.3. ***Obniżenie klauzuli tajności***

82. Po obniżeniu klauzuli tajności informacji niejawnych odpowiedni dokument, który je obejmuje, jest zarejestrowany w dziennikach odpowiadających zarówno poprzedniemu jak i nowemu poziomowi klauzuli tajności. Zapisuje się datę obniżenia klauzuli tajności oraz nazwisko osoby, która je zatwierdziła.

83. Dokument zawierający informację o obniżonej klauzuli i wszystkie jego kopie są oznaczane nową klauzulą i odpowiednio przechowywane.

L. **NISZCZENIE INFORMACJI POUFNYCH**

84. Informacje poufne (kopia papierowa lub w formie elektronicznej), które nie są już potrzebne, są niszczone lub usuwane zgodnie z zasadami postępowania i odpowiednimi przepisami dotyczącymi archiwizacji.

85. Informacje opatrzone klauzulą tajności na poziomie TRES SECRET UE/EU TOP SECRET lub SECRET UE/EU SECRET lub równoważną są niszczone przez CIU. Ich zniszczenie odbywa się w obecności osoby posiadającej poświadczenie bezpieczeństwa odpowiadające co najmniej poziomowi klauzuli niszczonej informacji.

86. Informacje opatrzone klauzulą na poziomie TRES SECRET UE/EU TOP SECRET lub równoważną są niszczone jedynie po uzyskaniu wcześniejszej pisemnej zgody autora informacji.

87. Informacje opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET lub TRES SECRET UE/EU TOP SECRET lub równoważną są niszczone i usuwane przez CIU na polecenie autora lub właściwego organu. Dzienniki i inne rejestry są odpowiednio aktualizowane. Informacje opatrzone klauzulą na poziomie RESTREINT UE/EU RESTRICTED lub równoważną są niszczone i usuwane przez CIU lub właściwy organ parlamentarny/ osobę sprawującą urząd.

88. Urzędnik odpowiedzialny za niszczenie oraz osoba obecna przy niszczeniu podpisują protokół zniszczenia, który jest załączany do dokumentacji i archiwizowany w CIU. CIU zachowuje — wraz z formularzami dotyczącymi udostępniania — protokoły zniszczenia informacji opatrzonych klauzulą na poziomie TRES SECRET UE/EU TOP SECRET lub równoważną przez okres przynajmniej dziesięciu lat oraz, w odniesieniu do protokołów zniszczenia informacji opatrzonych klauzulą na poziomie SECRET UE/EU SECRET lub równoważną i CONFIDENTIEL UE/EU CONFIDENTIAL lub równoważną — przez okres co najmniej pięciu lat.

89. Dokumenty zawierające informacje niejawne są niszczone w sposób spełniający właściwe normy UE lub normy równoważne, aby zapobiec ich odtworzeniu w całości lub w części.

90. Niszczenie komputerowego nośnika informacji wykorzystanego do przechowywania informacji niejawnych przeprowadza się zgodnie z właściwymi zasadami postępowania.

91. Niszczenie informacji niejawnych zapisuje się w odnośnym dzienniku wraz z następującymi danymi:

a) datą i godziną zniszczenia;

b) nazwiskiem urzędnika odpowiedzialnego za zniszczenie;

c) określeniem zniszczonego dokumentu lub jego kopii;

d) pierwotną formą fizyczną niszczonych EUCI;

e) sposobem zniszczenia oraz

f) miejscem zniszczenia.

M. **ARCHIWIZACJA**

92. Informacje niejawne, w tym nota/pismo przewodnie, załączniki, odcinek potwierdzający złożenie informacji lub inne elementy dokumentacji, są przenoszone do zabezpieczonego archiwum w strefie bezpieczeństwa w terminie 6 miesięcy po ostatnim wglądzie do nich i najpóźniej w terminie 1 roku od dnia ich złożenia. Szczegółowe przepisy dotyczące archiwizacji informacji niejawnych zostały określone w zasadach postępowania.

93. W przypadku „innych informacji poufnych" zastosowanie mają ogólne przepisy dotyczące zarządzania dokumentami bez szkody dla innych szczególnych przepisów dotyczących postępowania z tymi informacjami.

INSTRUKCJA BEZPIECZEŃSTWA 3

PRZETWARZANIE INFORMACJI POUFNYCH ZA POMOCĄ ZAUTOMATYZOWANYCH SYSTEMÓW KOMUNIKACYJNYCH I INFORMACYJNYCH (CIS)

A. **ZABEZPIECZANIE INFORMACJI W PRZYPADKU INFORMACJI NIEJAWNYCH PRZETWARZANYCH W SYSTEMIE INFORMACYJNYM**

1. „Zabezpieczanie informacji" w ramach systemów informacyjnych oznacza pewność, że systemy te będą chronić informacje niejawne, które są przez nie przetwarzane, i będą działać zgodnie z przeznaczeniem, w razie potrzeby pod kontrolą uprawnionych użytkowników. Skuteczne zabezpieczanie informacji gwarantuje odpowiednie poziomy poufności, integralności, dostępności, niezaprzeczalności i autentyczności. Zabezpieczanie informacji opiera się na procesie zarządzania ryzykiem.

2. „Systemy komunikacyjno-informacyjne" (CIS) do przetwarzania informacji niejawnych oznaczają systemy umożliwiające przetwarzanie informacji w formie elektronicznej. System informacyjny obejmuje wszystkie zasoby niezbędne do jego funkcjonowania, w tym infrastrukturę, organizację, personel oraz zasoby informacyjne.

3. CIS przetwarzają informacje niejawne zgodnie z zasadą gwarancji bezpieczeństwa informacji.

4. CIS poddawane są procedurze akredytacji. Celem akredytacji jest upewnienie się, że zastosowano wszystkie odpowiednie środki bezpieczeństwa i że osiągnięto wystarczający poziom ochrony informacji niejawnych i CIS zgodnie z niniejszą instrukcją bezpieczeństwa. W świadectwie akredytacji określa się najwyższą klauzulę tajności informacji, które mogą być przetwarzane w ramach danego CIS, oraz odpowiednie warunki.

5. Następujące cechy i koncepcje zabezpieczania informacji są niezbędne dla bezpieczeństwa i prawidłowego funkcjonowania operacji dokonywanych w ramach CIS:

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

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

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

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

e) niezaprzeczalność: możliwość udowodnienia, że działanie lub wydarzenie miało miejsce, aby wykluczyć możliwość zaprzeczenia wystąpieniu tego działania lub wydarzenia.

B. **ZASADY ZABEZPIECZANIA INFORMACJI**

6. Przedstawione poniżej przepisy stanowią podstawę bezpieczeństwa wszelkich systemów CIS, w ramach których przetwarzane są informacje niejawne. Szczegółowe wymogi dotyczące wdrażania tych przepisów zostały zdefiniowane w ramach polityki bezpieczeństwa w zakresie zabezpieczania informacji oraz w wytycznych dotyczących bezpieczeństwa.

B.1. ***Zarządzanie ryzykiem dla bezpieczeństwa***

7. Zarządzanie ryzykiem dla bezpieczeństwa stanowi integralną część definiowania, rozwijania, obsługiwania i konserwacji CIS. Zarządzanie ryzykiem (ocena, zmniejszanie ryzyka, akceptacja i powiadamianie) jest prowadzone jako interaktywny proces wspólnie przez przedstawicieli właścicieli systemu, organy odpowiedzialne za projekt, organy operacyjne oraz organy zatwierdzające bezpieczeństwo, o których mowa w instrukcji bezpieczeństwa 1, w ramach sprawdzonego, przejrzystego i zrozumiałego procesu oceny ryzyka. Zakres stosowania CIS oraz ich zasobów jest jasno definiowany na początku procesu zarządzania ryzykiem.

8. Właściwe organy, o których mowa w instrukcji bezpieczeństwa 1, dokonują przeglądu potencjalnych zagrożeń dla CIS i posiadają aktualne i dokładne oceny zagrożeń, odzwierciedlające aktualne środowisko operacyjne. Stale uaktualniają swoją wiedzę na temat podatności na zagrożenia i dokonują okresowych przeglądów oceny podatności, aby dostosować się do zmieniających się technologii informacyjnych (IT).

9. Celem zmniejszania ryzyka naruszenia zasad bezpieczeństwa jest zastosowanie zestawu środków bezpieczeństwa prowadzących do osiągnięcia zadowalającej równowagi między wymaganiami użytkownika, kosztami a szczątkowym ryzykiem naruszenia zasad bezpieczeństwa.

10. Akredytacja CIS obejmuje oficjalne oświadczenie o ryzyku szczątkowym oraz akceptację ryzyka szczątkowego przez odpowiedzialny organ. Szczególne wymogi, skala i stopień szczegółowości określone przez odpowiednie SAA do celów przyznania akredytacji CIS są proporcjonalne do szacowanego ryzyka z uwzględnieniem wszystkich odpowiednich czynników, w tym poziomu klauzuli tajności informacji niejawnych przetwarzanych w danym CIS.

B.2. ***Bezpieczeństwo w całym cyklu życia CIS***

11. **Zapewnianie bezpieczeństwa jest wymogiem obowiązującym w** całym **cyklu życia** CIS, od ich uruchomienia do wycofania z użytkowania.

12. Dla każdego etapu cyklu życia CIS określana jest rola i interakcja każdego z podmiotów związanych z CIS w odniesieniu do jego bezpieczeństwa.

13. CIS wraz z technicznymi i innymi środkami bezpieczeństwa są podczas procedury akredytacji poddawane testom bezpieczeństwa, aby zapewnić osiągnięcie odpowiedniego stopnia zabezpieczenia oraz sprawdzić, czy CIS, wraz z technicznymi i innymi środkami bezpieczeństwa, są prawidłowo wdrożone, zintegrowane i skonfigurowane.

14. Oceny bezpieczeństwa, inspekcje i przeglądy przeprowadzane są okresowo w fazie operacyjnej oraz podczas konserwacji CIS, jak również przy pojawieniu się nadzwyczajnych okoliczności.

15. Dokumentacja bezpieczeństwa CIS ewoluuje podczas wszystkich etapów jego cyklu życia na zasadzie integralnej części procesu zarządzania zmianami.

16. Procedury rejestracji stosowane w razie konieczności w ramach CIS sprawdzane są jako element procedury akredytacji.

B.3. ***Dobre praktyki***

17. IAA rozwija dobre praktyki na rzecz ochrony informacji niejawnych przetwarzanych w ramach CIS. Wytyczne w zakresie dobrych praktyk zawierają techniczne, fizyczne, organizacyjne i proceduralne środki bezpieczeństwa dotyczące CIS o sprawdzonej skuteczności w zapobieganiu danym zagrożeniom i podatności.

18. Ochrona informacji niejawnych przetwarzanych w ramach CIS wykorzystuje doświadczenia podmiotów zaangażowanych w zabezpieczanie informacji.

19. Rozpowszechnianie, a następnie wdrażanie dobrych praktyk pomaga w osiągnięciu równoważnego poziomu zabezpieczenia CIS eksploatowanych przez Sekretariat Parlamentu, które przetwarzają informacje niejawne.

B.4. ***Ochrona w głąb***

20. Aby zmniejszyć ryzyko zagrażające CIS, wdrażany jest pakiet technicznych i innych środków bezpieczeństwa o strukturze różnych poziomów ochrony. Poziomy te obejmują:

a) powstrzymywanie: środki bezpieczeństwa ukierunkowane na zniechęcenie osób planujących atak na CIS;

b) zapobieganie: środki bezpieczeństwa ukierunkowane na udaremnienie lub powstrzymanie ataku na CIS;

c) wykrywanie: środki bezpieczeństwa ukierunkowane na ujawnienie ataku na CIS;

d) odporność: środki bezpieczeństwa ukierunkowane na ograniczenie skutków ataku, tak by dotknęły one jak najmniejszą ilość informacji lub zasobów CIS, oraz na zapobieżenie dalszym szkodom; oraz

e) usuwanie skutków: środki bezpieczeństwa ukierunkowane na odzyskanie bezpiecznego statusu CIS.

Stopień rygorystyczności takich środków bezpieczeństwa ustalany jest na podstawie oceny ryzyka.

21. Właściwe organy, określone w instrukcji bezpieczeństwa 1, dbają o to, by były w stanie reagować na incydenty, które mogą przekraczać granice poszczególnych organizacji, w taki sposób, aby koordynować reakcje i dzielić się informacjami o tych incydentach i związanym z nimi ryzyku (zdolności do reagowania na sytuacje nadzwyczajne w ramach systemów komputerowych).

B.5. ***Zasada minimalistycznych i najmniejszych uprawnień***

22. Aby zapobiec niepotrzebnemu ryzyku, stosowane są wyłącznie funkcje, urządzenia i usługi niezbędne do spełnienia wymogów operacyjnych.

23. Aby ograniczyć szkody wynikające z wypadków, błędów lub nieuprawnionego korzystania z zasobów CIS, użytkownicy CIS oraz procesy zautomatyzowane otrzymują wyłącznie taki dostęp i takie przywileje i upoważnienia, jakie są im niezbędne do wykonywania ich zadań.

B.6. ***Świadomość zabezpieczania informacji***

24. Świadomość ryzyka i dostępnych środków bezpieczeństwa stanowi pierwszą linię obrony bezpieczeństwa CIS. W szczególności wszyscy członkowie personelu związani z CIS na poszczególnych etapach jego cyklu życia, w tym użytkownicy, powinni zrozumieć:

a) że niedopatrzenia w dziedzinie bezpieczeństwa mogą w sposób znaczący uszkodzić CIS przetwarzające informacje niejawne;

b) potencjalne szkody, jakie mogą ponieść inne podmioty w związku z podłączeniem do systemów lub sieci i współzależnością, oraz

c) że osobiście ponoszą odpowiedzialność i są rozliczani za bezpieczeństwo CIS zgodnie z pełnionymi przez siebie funkcjami w tych systemach i procesach.

25. Aby zapewnić zrozumienie obowiązków związanych z bezpieczeństwem, wszyscy członkowie personelu związani z CIS, w tym wyższe kierownictwo, posłowie do Parlamentu Europejskiego i użytkownicy CIS, przechodzą obowiązkowe szkolenia mające na celu edukację i zdobycie wiedzy w zakresie zabezpieczania informacji.

B.7. ***Ocena i zatwierdzanie produktów służących bezpieczeństwu systemów informatycznych***

26. CIS przetwarzające informacje niejawne opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL z technicznymi i innymi środkami bezpieczeństwa lub równoważną są chronione w taki sposób, by bezpieczeństwo informacji nie mogło być zagrożone z powodu niezamierzonych emisji elektromagnetycznych („środki bezpieczeństwa TEMPEST").

27. Jeżeli ochronę informacji niejawnych zapewniają produkty kryptograficzne, produkty takie posiadają certyfikat SAA jako należące do produktów kryptograficznych zatwierdzonych na poziomie UE.

28. Podczas transmisji informacji niejawnych drogą elektroniczną używa się produktów kryptograficznych zatwierdzonych na poziomie UE. Niezależnie od tego wymogu w wyjątkowych okolicznościach mogą mieć zastosowanie szczególne procedury lub szczególne konfiguracje techniczne określone w pkt 41-44.

29. Wymagany stopień zabezpieczenia, jaki zapewniają środki bezpieczeństwa, określony jako poziom zabezpieczenia, określa się zgodnie z wynikami procesu zarządzania ryzykiem i zgodnie z odpowiednimi politykami i wytycznymi dotyczącymi bezpieczeństwa.

30. Poziom zabezpieczenia sprawdzany jest przy użyciu uznanych na szczeblu międzynarodowym lub zatwierdzonych na szczeblu krajowym procesów i metod. Obejmują one przede wszystkim ocenę, kontrole i audyt.

31. SAA zatwierdza wytyczne dotyczące bezpieczeństwa *odnoszące się do kwalifikowania i zatwierdzania niekryptograficznych produktów służących bezpieczeństwu systemów informatycznych*.

B.8. ***Transmisja w strefie bezpieczeństwa***

32. Jeżeli transmisja informacji niejawnych odbywa się w obrębie strefy bezpieczeństwa, można stosować niezaszyfrowane udostępnianie lub szyfrowanie na niższym stopniu w oparciu o wyniki procesu zarządzania ryzykiem i po zatwierdzeniu przez SAA.

B.9. ***Bezpieczne połączenia międzysystemowe CIS***

33. Połączenia międzysystemowe oznaczają bezpośrednie połączenie co najmniej dwóch systemów IT do celów wymiany danych i innych źródeł informacji w sposób jednokierunkowy lub wielokierunkowy.

34. CIS traktuje każdy system informatyczny przyłączony połączeniem międzysystemowym jako niewiarygodny i stosuje środki ochrony, aby kontrolować wymianę informacji niejawnych z innym CIS.

35. Wszystkie połączenia międzysystemowe CIS z innym systemem informatycznym spełniają następujące podstawowe wymogi:

a) właściwe organy określają i zatwierdzają wymogi — biznesowe i operacyjne — dla takich połączeń;

b) dane połączenie międzysystemowe przechodzi procedurę zarządzania ryzykiem i akredytacji oraz wymaga zatwierdzenia przez właściwe SAA;

c) na granicach CIS stosowane są usługi ochrony systemów (PS).

36. Pomiędzy CIS posiadającym akredytację a siecią niezabezpieczoną lub publiczną brak jest połączeń międzysystemowych z wyjątkiem sytuacji, w których w ramach CIS zainstalowano w tym celu zatwierdzone PS między CIS a siecią niezabezpieczoną lub publiczną. Środki bezpieczeństwa dotyczące takich połączeń międzysystemowych są poddawane przeglądowi przez właściwy organ ds. zabezpieczania informacji i zatwierdzane przez właściwy SAA.

37. Gdy sieć niezabezpieczona lub publiczna wykorzystywana jest wyłącznie jako nośnik, a dane zostały zaszyfrowane przy wykorzystaniu produktu kryptograficznego zatwierdzonego na poziomie UE zgodnie z ust. 27, takiego połączenia nie uznaje się za połączenie międzysystemowe.

38. Niedozwolone jest bezpośrednie lub kaskadowe połączenie międzysystemowe z siecią niezabezpieczoną lub publiczną CIS akredytowanego do przetwarzania informacji opatrzonych klauzulą tajności na poziomie TRES SECRET UE/EU TOP SECRET lub równoważną lub SECRET UE/EU SECRET lub równoważną.

B.10. ***Komputerowe nośniki informacji***

39. Komputerowe nośniki informacji są niszczone zgodnie z procedurami zatwierdzonymi przez właściwy organ bezpieczeństwa.

40. Komputerowe nośniki informacji są ponownie wykorzystywane, odtajniane lub obniża się ich klauzulę tajności zgodnie z zasadami postępowania.

B.11. ***Okoliczności nadzwyczajne***

41. Szczególne procedury opisane poniżej mogą mieć zastosowanie w okolicznościach nadzwyczajnych, na przykład w sytuacjach nieuchronnego lub istniejącego kryzysu, konfliktu, wojny lub w wyjątkowych okolicznościach operacyjnych.

42. Informacje niejawne można przekazywać z wykorzystaniem produktów kryptograficznych zatwierdzonych dla niższego poziomu klauzuli tajności lub w postaci niezaszyfrowanej za zgodą właściwego organu, jeżeli wszelka zwłoka spowodowałaby szkody wyraźnie większe od szkód, które mogłoby spowodować ujawnienie materiałów niejawnych, oraz jeżeli:

a) nadawca i odbiorca nie posiadają wymaganego urządzenia szyfrującego lub też nie posiadają żadnego urządzenia szyfrującego oraz

b) materiały niejawne nie mogą być dostarczone w wystarczającym czasie w inny sposób.

43. Informacje niejawne przekazywane w okolicznościach przedstawionych w pkt 41 nie są opatrzone żadnymi oznaczeniami ani wskazaniami odróżniającymi je od informacji jawnych lub informacji, które mogą być chronione przy pomocy dostępnego urządzenia szyfrującego. Odbiorcy są bezzwłocznie powiadamiani o poziomie klauzuli tajności za pomocą innych środków.

44. W razie zastosowania przepisów ust. 41 lub 42 należy następnie przedłożyć raport właściwemu organowi.

INSTRUKCJA BEZPIECZEŃSTWA 4

BEZPIECZEŃSTWO FIZYCZNE

A. **WPROWADZENIE**

Niniejsza instrukcja bezpieczeństwa ustala zasady bezpieczeństwa dotyczące tworzenia bezpiecznego otoczenia dla zapewnienia właściwego przetwarzania informacji poufnych w Parlamencie Europejskim. Zasady te, w tym dotyczące bezpieczeństwa technicznego, zostaną uzupełnione zasadami postępowania.

B. **ZARZĄDZANIE RYZYKIEM DLA BEZPIECZEŃSTWA**

1. Ryzyko dotyczące informacji niejawnych zarządzane jest jako proces. Proces ten ma na celu określenie znanego ryzyka dla bezpieczeństwa, określenie środków bezpieczeństwa na rzecz zmniejszenia tego rodzaju ryzyka do poziomu możliwego do zaakceptowania, zgodnie z podstawowymi zasadami i minimalnymi normami określonymi w niniejszej instrukcji bezpieczeństwa, oraz zastosowanie tych środków zgodnie z koncepcją ochrony w głąb określonej w instrukcji bezpieczeństwa 3. Skuteczność takich środków jest stale oceniana.

2. Środki bezpieczeństwa służące ochronie informacji niejawnych na wszystkich etapach ich cyklu życia są proporcjonalne w szczególności do ich klauzuli tajności, formy, ilości danych informacji lub materiałów, lokalizacji i konstrukcji obiektów, w których przechowywane są informacje niejawne, oraz oceny zagrożenia wystąpieniem w tym miejscu działań realizowanych w złych zamiarach lub działalności przestępczej, w tym działalności szpiegowskiej, sabotażowej lub terrorystycznej.

3. Plany awaryjne uwzględniają potrzebę ochrony informacji niejawnych podczas sytuacji nadzwyczajnych w celu zapobieżenia nieuprawnionemu dostępowi do informacji, ich ujawnieniu lub utracie ich integralności lub dostępności.

4. W planach ciągłości działania zamieszczane są środki zapobiegawcze i naprawcze służące zminimalizowaniu skutków poważnych niedopatrzeń lub incydentów związanych z wykorzystywaniem i przechowywaniem informacji niejawnych.

C. **ZASADY OGÓLNE**

5. Poziom niejawności lub tajności danej informacji określa poziom ochrony nadany jej w obszarze bezpieczeństwa fizycznego.

6. Informacja wymagająca utajnienia jest oznaczana i wykorzystywana jako taka niezależnie od jej formy fizycznej. Jej niejawny charakter należy wyraźnie zakomunikować odbiorcom albo przez oznaczenie klauzuli tajności (jeżeli informacja jest przekazywana w formie pisemnej, niezależnie od tego, czy na papierze, czy w CIS), albo w drodze komunikatu (jeżeli jest przekazywana ustnie, np. w trakcie rozmowy lub prezentacji). Materiał opatrzony klauzulą poufności jest fizycznie oznaczony, aby umożliwić łatwą identyfikację jego klauzuli tajności.

7. Informacje poufne nie są w żadnych okolicznościach dostępne w miejscach publicznych, gdzie może je zauważyć ktoś nieupoważniony do zaznajomienia się z nimi, np. w pociągach, samolotach, kawiarniach, barach itp. Nie wolno zostawiać ich w hotelowych sejfach lub pokojach. Nie należy zostawiać ich bez nadzoru w miejscach publicznych.

D. **ZAKRES OBOWIĄZKÓW**

8. CIU jest odpowiedzialny za fizyczne bezpieczeństwo w postępowaniu z informacjami poufnymi przechowywanymi w jego bezpiecznej infrastrukturze. CIU jest również odpowiedzialny za zarządzanie swoją bezpieczną infrastrukturą.

9. Fizyczne bezpieczeństwo w postępowaniu z informacją opatrzoną klauzulą tajności na poziomie RESTREINT UE/ EU RESTRICTED lub równoważną, a także z „innymi informacjami poufnymi" należy do obowiązków odpowiedniego organu Parlamentu lub osoby pełniącej odnośną funkcję.

10. Dyrekcja ds. Bezpieczeństwa i Oceny Ryzyka zapewnia osobiste bezpieczeństwo oraz poświadczenie bezpieczeństwa wymagane do zagwarantowania bezpiecznego postępowania z informacjami poufnymi w Parlamencie Europejskim.

11. DIT udziela porad oraz zapewnia, żeby każdy utworzony lub wykorzystywany CIS był w pełni zgodny z instrukcją bezpieczeństwa 3 oraz z odnośnymi zasadami postępowania.

E. **BEZPIECZNA INFRASTRUKTURA**

12. Można zainstalować bezpieczną infrastrukturę w oparciu o techniczne normy bezpieczeństwa i według poziomu poufności nadanego informacjom zgodnie z art. 7.

13. Bezpieczna infrastruktura jest certyfikowana przez SAA i zatwierdzana przez SA.

F. **ZAPOZNAWANIE SIĘ Z INFORMACJAMI POUFNYMI**

14. Jeżeli informacja opatrzona klauzulą tajności na poziomie RESTREINT UE/ EU RESTRICTED lub równoważną, a także „inne informacje poufne" są przechowywane w CIU i mają być udostępnione poza strefą bezpieczeństwa, CIU przekazuje kopię do właściwej upoważnionej służby, która gwarantuje, że zapoznawanie się i postępowanie z taką informacją jest zgodne z art. 8 ust. 2 oraz art. 10 niniejszej decyzji, a także z odpowiednimi zasadami postępowania.

15. Jeżeli informacja opatrzona klauzulą tajności na poziomie RESTREINT UE/ EU RESTRICTED lub równoważną, a także „inne informacje poufne" są przechowywane w organie/biurze parlamentarnym innym niż CIU, sekretariat tego organu/biura parlamentarnego gwarantuje, że zapoznawanie się i postępowanie z taką informacją jest zgodne z art. 7 ust. 3, art. 8 ust. 1, 2 i 4, art. 9 ust. 3, 4 i 5, art. 10 ust. 2 — 6 oraz art. 11 niniejszej decyzji, a także z odpowiednimi zasadami postępowania.

16. Jeżeli informacja opatrzona klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET lub TRES SECRET UE/EU TOP SECRET lub równoważną ma być udostępniona w strefie bezpieczeństwa, CIU gwarantuje, że zapoznawanie się i postępowanie z taką informacją jest zgodne z art. 9 i 10 niniejszej decyzji, a także z odpowiednimi zasadami postępowania.

G. **BEZPIECZEŃSTWO TECHNICZNE**

17. Środki bezpieczeństwa technicznego należą do obowiązków SAA, który określa konkretne środki bezpieczeństwa technicznego, które mają być stosowane w odpowiednich zasadach postępowania.

18. Zabezpieczone czytelnie, w których można zapoznać się z informacjami niejawnymi opatrzonymi klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED lub klauzulą jej równoważną lub z innymi informacjami poufnymi spełniają szczególne techniczne środki bezpieczeństwa, określone w zasadach postępowania.

19. Strefa bezpieczeństwa zawiera następujące wyposażenie:

a) pomieszczenie do sprawdzania bezpiecznego dostępu (SAS), zainstalowane zgodnie z technicznymi środkami bezpieczeństwa, określonymi w zasadach postępowania. Dostęp do tego pomieszczenia jest rejestrowany. SAS spełnia wysokie normy w zakresie identyfikacji osób i umożliwia rejestrację wejść, nadzór wideo, a także zapewnia bezpieczne miejsce do deponowania przedmiotów osobistych niedozwolonych w bezpiecznych czytelniach (telefony, długopisy itp.);

b) pomieszczenie do komunikacji, służące do przekazywania i otrzymywania informacji niejawnych, w tym zaszyfrowanych informacji niejawnych, zgodnie z instrukcją bezpieczeństwa 3 i odnośnymi zasadami postępowania;

c) bezpieczne archiwum, w którym zatwierdzone i certyfikowane pojemniki są używane osobno dla informacji opatrzonych klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET EU/EU SECRET lub równoważną. Informacje opatrzone klauzulą tajności na poziomie TRES SECRET UE/EU TOP SECRET lub równoważną są przechowywane w oddzielnym pomieszczeniu w specjalnym certyfikowanym pojemniku. Jedynym dodatkowym wyposażeniem w tym oddzielnym pomieszczeniu jest pomocnicze biurko do obsługi archiwum przez CIU;

d) pomieszczenie do rejestracji, wyposażone w narzędzia niezbędne do zapewnienia rejestracji na papierze lub elektronicznie, a zatem wyposażone w niezbędny bezpieczny sprzęt do instalacji odpowiedniego CIS. Jedynie w pomieszczeniu do rejestracji może znajdować się zatwierdzony i akredytowany sprzęt kopiujący (do robienia kopii w formie papierowej lub elektronicznej). Zasady postępowania określają, jaki sprzęt kopiujący jest zatwierdzony i akredytowany. Pomieszczenie do rejestracji umożliwia także niezbędne przechowywanie i wykorzystywanie akredytowanego wyposażenia koniecznego do oznaczania, kopiowania i rozsyłania informacji niejawnych w formie fizycznej, według poziomu niejawności. CIU określa całe akredytowane wyposażenie, które jest następnie akredytowane przez SAA, zgodnie z opinią otrzymaną od IAOA. W pomieszczeniu do rejestracji znajduje się także akredytowana niszczarka, zatwierdzona dla najwyższego poziomu niejawności, opisana w zasadach postępowania. Tłumaczenie pisemne informacji niejawnych opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL SECRET EU/EU SECRET lub TRES SECRETUE/EU TOP SECRET lub równoważnej jest dokonywane w pomieszczeniu do rejestracji przy użyciu odpowiedniego akredytowanego systemu. W pomieszczeniu do rejestracji znajdują się stanowiska pracy dla maksymalnie dwóch tłumaczy pisemnych jednocześnie dla tego samego dokumentu. Obecny jest pracownik CIU.

e) czytelnia, służąca indywidualnemu zapoznaniu się z informacjami niejawnymi przez należycie uprawnioną osobę. Czytelnia jest wystarczająco duża dla dwóch osób, łącznie z pracownikiem CIU obecnym przez cały czas zapoznawania się z treścią dokumentu. Poziom bezpieczeństwa tego pomieszczenia jest odpowiedni dla zapoznawania się z informacjami opatrzonymi klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL SECRET EU/EU SECRET lub TRES SECRETUE/EU TOP SECRET lub równoważnej. Czytelnia może być wyposażona w urządzenie TEMPEST umożliwiające w miarę potrzeby zapoznanie się z informacjami drogą elektroniczną, zgodnie z poziomem niejawności danych informacji.

f) sala posiedzeń, mogąca pomieścić do 25 osób w celu omówienia informacji opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL oraz SECRET EU/EU SECRET lub równoważną. Sala posiedzeń jest wyposażona w niezbędną bezpieczną i certyfikowaną infrastrukturę techniczną do tłumaczenia ustnego na i z maksymalnie dwóch języków. Salę posiedzeń można wykorzystywać także na dodatkową czytelnię do indywidualnego zapoznawania się z informacjami. W wyjątkowych przypadkach CIU może zezwolić więcej niż jednej upoważnionej osobie na zapoznanie się z informacjami niejawnymi, o ile poziom upoważnienia i konieczność zaznajomienia się z informacjami są takie same dla wszystkich osób w pomieszczeniu. Nie zezwala się więcej niż czterem osobom jednocześnie na zapoznawanie się z informacjami niejawnymi. Liczba obecnych pracowników CIU jest zwiększona.

g) bezpieczne pomieszczenia techniczne zawierające całe wyposażenie techniczne, związane z bezpieczeństwem całej strefy bezpieczeństwa, a także bezpieczne serwery IT.

20. Strefa bezpieczeństwa odpowiada mającym zastosowanie międzynarodowym normom bezpieczeństwa i jest certyfikowana przez Dyrekcję ds. Bezpieczeństwa i Oceny Ryzyka. Strefa bezpieczeństwa jest wyposażona w następujące minimalne techniczne urządzenia bezpieczeństwa:

a) alarmowe i monitorujące systemy bezpieczeństwa;

b) wyposażenie w środki bezpieczeństwa i systemy ostrzegania (dwukierunkowy system ostrzegania)

c) system CCTV;

d) systemy wykrywania włamania;

e) kontrola dostępu (łącznie z biometrycznym systemem bezpieczeństwa);

f) pojemniki;

g) schowki;

h) ochrona przed polem elektromagnetycznym.

21. SAA może dodać niezbędne dodatkowe techniczne środki bezpieczeństwa, działając w ścisłej współpracy z CIU i po zatwierdzeniu przez SA.

22. Infrastruktura ta może być połączona z ogólnymi systemami zarządzania w budynku, w którym znajduje się strefa bezpieczeństwa. Jednakże sprzęt związany z bezpieczeństwem przeznaczony do kontroli dostępu i dla CIS jest niezależny od jakiegokolwiek już istniejącego systemu tego rodzaju w Parlamencie Europejskim.

H. **INSPEKCJE STREFY BEZPIECZEŃSTWA**

23. Inspekcji strefy bezpieczeństwa dokonuje regularnie SAA na wniosek CIU.

24. SAA opracowuje i aktualizuje wykaz elementów, jakie należy sprawdzić podczas inspekcji bezpieczeństwa zgodnie z zasadami postępowania.

I. **TRANSPORT INFORMACJI POUFNYCH**

25. Informacje poufne podczas transportu nie mogą być widoczne i nic nie może wskazywać na ich poufny charakter, zgodnie z zasadami postępowania.

26. Jedynie woźni lub pracownicy posiadający zezwolenie o odpowiednim poziomie bezpieczeństwa mogą transportować informacje niejawne opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL SECRET EU/EU SECRET lub TRES SECRETUE/EU TOP SECRET lub równoważnej.

27. Informacje niejawne mogą być wysyłane poza budynek jedynie przy użyciu zewnętrznej skrzynki poczty elektronicznej lub przez kuriera na warunkach określonych w zasadach postępowania.

28. Informacji niejawnych opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL SECRET EU/EU SECRET lub TRES SECRE UE/EU TOP SECRET lub równoważnej nie należy nigdy wysyłać pocztą elektroniczną lub faksem, nawet jeśli jest do dyspozycji bezpieczny system e-mail lub faks szyfrujący. Informacje niejawne opatrzone klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED lub wyższej, a także inne informacje poufne można wysłać pocztą elektroniczną przy użyciu akredytowanego systemu szyfrującego.

J. **PRZECHOWYWANIE INFORMACJI POUFNYCH**

29. Poziom niejawności lub oznaczenia przyznany informacji niejawnej określa poziom ochrony przyznany jej z myślą o przechowywaniu.,Przechowuje się ją w infrastrukturze certyfikowanej do tego celu zgodnie z zasadami postępowania.

30. Informacje niejawne opatrzone klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED lub równoważnej, a także inne informacje poufne:

a) są przechowywane w standardowej stalowej, zamkniętej na klucz szafie, w biurze lub w strefie pracy, gdy nie są rzeczywiście wykorzystywane;

b) nie są pozostawione bez nadzoru, chyba że prawidłowo zamknięte i przechowywane;

c) nie są pozostawione na biurku czy stole w sposób umożliwiający osobie nieupoważnionej, np. odwiedzającym, sprzątaczkom, personelowi konserwującemu itp., zapoznanie się z nimi lub usunięcie ich;

d) nie są pokazywane jakimkolwiek osobom nieupoważnionym ani dyskutowane z nimi;

31. Informacje niejawne opatrzone klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED lub równoważnej, a także inne informacje poufne są przechowywane jedynie w sekretariatach organów/biur parlamentarnych lub w CIU zgodnie z zasadami postępowania.

32. Informacje opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET EU/EU SECRET lub TRES SECRETUE/EU TOP SECRET lub równoważną:

a) są przechowywane w strefie bezpieczeństwa w zabezpieczonym pojemniku lub w zabezpieczonym pomieszczeniu. Wyjątkowo — np. gdy CIU jest zamknięty — mogą być przechowywane w zatwierdzonym i certyfikowanym sejfie na terenie służb bezpieczeństwa.

b) nie są nigdy pozostawione bez nadzoru w strefie bezpieczeństwa bez uprzedniego ich zamknięcia w zatwierdzonym sejfie (nawet na bardzo krótko);

c) nie są pozostawione na biurku czy stole w sposób umożliwiający osobie nieupoważnionej zapoznanie się z nimi lub usunięcie ich, nawet jeśli odpowiedzialny pracownik CIU pozostaje w pomieszczeniu.

Jeżeli w strefie bezpieczeństwa powstaje elektroniczna forma dokumentu zawierającego informacje niejawne, komputer należy zablokować, a ekran uczynić niedostępnym, jeżeli autor lub odpowiedzialny pracownik CIU opuszczają pomieszczenie (nawet na bardzo krótko). Automatyczny system blokujący po kilku minutach nie jest uważany za środek wystarczający.

INSTRUKCJA BEZPIECZEŃSTWA 5

BEZPIECZEŃSTWO PRZEMYSŁOWE

A. **WPROWADZENIE**

1. Niniejsza instrukcja bezpieczeństwa dotyczy jedynie informacji niejawnych.

2. Określa ona przepisy dotyczące stosowania wspólnych minimalnych norm części 1 załącznika I do niniejszej decyzji.

3. Bezpieczeństwo przemysłowe oznacza stosowanie środków mających zapewnić ochronę informacji niejawnych przez wykonawców lub podwykonawców podczas negocjacji poprzedzających zawarcie umów i na wszystkich etapach cyklu życia umów niejawnych. Umowy takie nie obejmują dostępu do informacji niejawnych opatrzonych klauzulą tajności na poziomie TRÈS SECRET UE/EU TOP SECRET.

4. Jako instytucja zamawiająca Parlament Europejski zapewnia, by w przypadku zawierania umów niejawnych z podmiotami prowadzącymi działalność gospodarczą lub inną spełnione były minimalne normy bezpieczeństwa przemysłowego określone w niniejszej decyzji i te, o których mowa w danej umowie.

B. **ELEMENTY DOTYCZĄCE BEZPIECZEŃSTWA W UMOWIE NIEJAWNEJ**

B.1. ***Przewodnik nadawania klauzul (SCG)***

5. Przed zamieszczeniem ogłoszenia o przetargu lub zawarciem umowy niejawnej, Parlament Europejski jako instytucja zamawiająca określa klauzulę tajności wszelkich informacji, które należy dostarczyć oferentom i wykonawcom, jak również klauzulę tajności wszelkich informacji, które mają być wytworzone przez wykonawcę. W tym przygotowuje on Przewodnik nadawania klauzul (SCG) do stosowania przy wykonywaniu umowy.

6. Do określania poziomu klauzuli tajności poszczególnych elementów umowy niejawnej zastosowanie mają następujące zasady:

a) podczas opracowywania SCG Parlament Europejski uwzględnia wszystkie odpowiednie aspekty bezpieczeństwa, w tym klauzulę tajności nadaną informacjom, które ich wytwórca przekazał i których wykorzystanie zatwierdził na użytek umowy;

b) ogólna klauzula tajności umowy nie może być niższa od najwyższej klauzuli tajności któregokolwiek z jej elementów.

B.2. ***Dokument określający aspekty bezpieczeństwa (SAL)***

7. Związane z umową wymogi bezpieczeństwa są opisane w Dokumencie określającym aspekty bezpieczeństwa (SAL). SAL w odpowiednich przypadkach zawiera SCG i stanowi integralną część umowy niejawnej lub niejawnej umowy o podwykonawstwo.

8. SAL zawiera przepisy zobowiązujące wykonawcę lub podwykonawcę do przestrzegania minimalnych norm określonych w niniejszej decyzji. Nieprzestrzeganie tych minimalnych norm może stanowić powód do rozwiązania umowy.

B.3. ***Instrukcje bezpieczeństwa programu/projektu (PSI)***

9. W zależności od zakresu programów lub projektów obejmujących dostęp do EUCI, ich wykorzystywanie lub przechowywanie, organ wyznaczony do zarządzania danym programem lub projektem może sporządzić specjalne instrukcje bezpieczeństwa danego programu/projektu (PSI).

C. **ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO (FSC)**

10. FSC wydawane jest przez NSA lub jakikolwiek inny właściwy organ bezpieczeństwa państwa członkowskiego w celu zaświadczenia zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, że dany podmiot prowadzący działalność gospodarczą lub inną jest w stanie zapewnić w swoich obiektach ochronę EUCI na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET lub równoważnym. Dowód wydania FSC przedstawiany jest Parlamentowi Europejskiemu, jako instytucji zamawiającej, przed dostarczeniem EUCI wykonawcy, podwykonawcy, potencjalnemu wykonawcy lub potencjalnemu podwykonawcy, lub umożliwieniem im dostępu do EUCI.

11. FSC:

a) ocenia uczciwość podmiotu prowadzącego działalność gospodarczą lub inną;

b) ocenia własność, kontrolę lub możliwość wystąpienia niewłaściwego wpływu, który można uznać za ryzyko naruszenia zasad bezpieczeństwa;

c) ocenia, czy podmiot prowadzący działalność gospodarczą lub inną stworzył w obiekcie system bezpieczeństwa, który obejmuje wszystkie odpowiednie środki bezpieczeństwa niezbędne do ochrony informacji lub materiałów niejawnych opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET zgodnie z wymogami określonymi w niniejszej decyzji;

d) ocenia, czy status bezpieczeństwa osobowego kadry zarządzającej, właścicieli i pracowników, którzy mają mieć dostęp do informacji niejawnych opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, został ustalony zgodnie z wymogami określonymi w niniejszej decyzji;

e) ocenia, czy podmiot prowadzący działalność gospodarczą lub inną powołał pełnomocnika ds. ochrony, który jest odpowiedzialny przed kadrą zarządzającą za egzekwowanie obowiązków dotyczących bezpieczeństwa w obrębie tego podmiotu.

12. W stosownych przypadkach Parlament Europejski, jako instytucja zamawiająca, powiadamia odpowiednią NSA lub jakikolwiek inny właściwy organ bezpieczeństwa o tym, że na etapie poprzedzającym zawarcie umowy lub do wykonywania umowy wymagane jest FSC. FSC lub Świadectwo Bezpieczeństwa Osobowego (PSC) są wymagane na etapie poprzedzającym zawarcie umowy, jeżeli podczas składania ofert mają być dostarczone informacje opatrzone klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET.

13. Instytucja zamawiająca nie zawiera umowy niejawnej z wybranym oferentem, zanim nie otrzyma od NSA lub jakiegokolwiek innego właściwego organu bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest ten wykonawca lub podwykonawca, potwierdzenia, że wydane zostało, jeśli istnieje taki wymóg, odpowiednie FSC.

14. Jakikolwiek właściwy organ bezpieczeństwa, który wydał FSC, powiadamia Parlament Europejski, jako instytucję zamawiającą, o wszelkich zmianach dotyczących FSC. W przypadku umowy o podwykonawstwo należy stosownie poinformować właściwy organ bezpieczeństwa.

15. Cofnięcie FSC przez odpowiednią NSA lub jakikolwiek inny właściwy organ bezpieczeństwa stanowią dla Parlamentu Europejskiego, jako instytucji zamawiającej, wystarczający powód do rozwiązania umowy niejawnej lub wykluczenia oferenta z postępowania.

D. **UMOWY NIEJAWNE I NIEJAWNE UMOWY O PODWYKONAWSTWO**

16. Jeżeli informacje niejawne przekazywane są potencjalnym oferentom na etapie poprzedzającym zawarcie umowy, ogłoszenie o przetargu zawiera przepis zobowiązujący tych oferentów, którzy nie złożą oferty lub którzy nie zostaną wybrani, do zwrotu wszystkich dokumentów niejawnych w określonym terminie.

17. Po zawarciu umowy niejawnej lub niejawnej umowy o podwykonawstwo Parlament Europejski, jako instytucja zamawiająca, powiadamia NSA wykonawcy lub podwykonawcy lub jakikolwiek inny właściwy organ bezpieczeństwa o zawartych w tej umowie przepisach bezpieczeństwa.

18. Po zakończenia takich umów Parlament Europejski, jako instytucja zamawiająca (lub, w odpowiednim przypadku, właściwy organ bezpieczeństwa w przypadku umowy o podwykonawstwo) niezwłocznie powiadamia o tym fakcie NSA lub jakikolwiek inny właściwy organ bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest wykonawca lub podwykonawca.

19. Z reguły od wykonawcy lub podwykonawcy wymaga się zwrotu do instytucji zamawiającej wszelkich posiadanych przez niego informacji niejawnych po zakończeniu obowiązywania umowy niejawnej lub niejawnej umowy o podwykonawstwo.

20. W SAL określa się szczególne przepisy dotyczące niszczenia informacji niejawnych podczas wykonywania umowy lub po zakończeniu jej obowiązywania.

21. Jeżeli wykonawca lub podwykonawca są upoważnieni do zachowania informacji niejawnych po zakończeniu obowiązywania umowy, nadal mają do nich zastosowanie minimalne normy zawarte w niniejszej decyzji i nadal chronią oni poufność EUCI.

22. Warunki, na których wykonawca może zlecić podwykonawstwo, są określone w ogłoszeniu o przetargu oraz w umowie.

23. Przed zleceniem podwykonawstwa jakiejkolwiek części umowy niejawnej wykonawca uzyskuje zgodę Parlamentu Europejskiego jako instytucji zamawiającej. Nie można zawrzeć umowy o podwykonawstwo z podmiotami prowadzącymi działalność gospodarczą lub inną zarejestrowanymi w państwie trzecim, które nie zawarło z Unią umowy o bezpieczeństwie informacji.

24. Wykonawca odpowiada za zapewnienie zgodności wszystkich podejmowanych czynności podwykonawczych z minimalnymi normami określonymi w niniejszej decyzji i nie dostarcza EUCI podwykonawcy bez uprzedniej pisemnej zgody instytucji zamawiającej.

25. W odniesieniu do informacji niejawnych wytworzonych lub wykorzystywanych przez wykonawcę lub podwykonawcę prawa przysługujące wytwórcy są wykonywane przez instytucję zamawiającą.

E. **WIZYTY ZWIĄZANE Z UMOWAMI NIEJAWNYMI**

26. Jeżeli Parlamentowi Europejskiemu, wykonawcy lub podwykonawcy niezbędny jest w związku z wykonaniem umowy niejawnej dostęp do informacji niejawnych opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET w swoich obiektach, organizowane są wizyty wraz z NSA lub jakimkolwiek innym właściwym organem bezpieczeństwa. Jednak w kontekście konkretnych projektów NSA mogą uzgodnić procedurę umożliwiającą bezpośrednie organizowanie wizyt.

27. Wszystkie osoby odwiedzające posiadają stosowne PSC oraz mają dostęp do informacji niejawnych dotyczących umowy Parlamentu Europejskiego zgodnie z zasadą ograniczonego dostępu.

28. Odwiedzający uzyskują dostęp jedynie do informacji niejawnych związanych z celem wizyty.

F. **PRZEKAZYWANIE I TRANSPORT INFORMACJI NIEJAWNYCH**

29. W przypadku transportu informacji niejawnych drogą elektroniczną zastosowanie mają odnośne przepisy określone w instrukcji bezpieczeństwa 3.

30. W przypadku transportu informacji niejawnych zastosowanie mają odnośne przepisy określone w instrukcji bezpieczeństwa 4 oraz odpowiednie zasady postępowania.

31. Podczas transportu materiału niejawnego jako ładunku do określania zabezpieczeń stosuje się następujące zasady:

a) bezpieczeństwo zapewnia się na wszystkich etapach przewozu, począwszy od miejsca wyjazdu do ostatecznego miejsca przeznaczenia;

b) stopień ochrony, którym objęto przesyłkę, określany jest według najwyższej klauzuli tajności materiału zawartego w przesyłce;

c) firmy dokonujące przewozu uzyskują FSC na stosownym poziomie. W takich przypadkach pracownicy zajmujący się przesyłką są odpowiednio sprawdzani zgodnie z załącznikiem I;

d) przed jakimkolwiek transgranicznym przemieszczeniem materiałów opatrzonych klauzulą tajności na poziomie CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET lub równoważnej nadawca sporządza plan przewozu, który jest zatwierdzany przez sekretarza generalnego;

e) przejazdy odbywają się w miarę możliwości bezpośrednio między dwoma punktami i kończą się tak szybko, jak pozwolą na to okoliczności;

f) droga w miarę możliwości przebiega przez terytorium państw członkowskich.

G. **PRZEKAZYWANIE INFORMACJI NIEJAWNYCH WYKONAWCOM ZNAJDUJĄCYM SIĘ W PAŃSTWACH TRZECICH**

32. Informacje niejawne są przekazywane wykonawcom i podwykonawcom znajdującym się w państwach trzecich zgodnie ze środkami bezpieczeństwa uzgodnionymi przez Parlament Europejski, jako instytucję zamawiającą, z państwem trzecim, w którym zarejestrowany jest wykonawca.

H. **WYKORZYSTYWANIE I PRZECHOWYWANIE INFORMACJI NIEJAWNYCH OPATRZONYCH KLAUZULĄ TAJNOŚCI NA POZIOMIE RESTREINT UE/EU RESTRICTED**

33. W porozumieniu, odpowiednio, z NSA państwa członkowskiego, Parlament Europejski, jako instytucja zamawiająca, jest upoważniony na podstawie przepisów umownych do przeprowadzania wizyt w obiektach wykonawców/podwykonawców, aby sprawdzić, czy wprowadzone zostały odpowiednie środki bezpieczeństwa mające zapewnić ochronę EUCI opatrzonych klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED zgodnie z wymogami umowy.

34. W zakresie, jaki jest wymagany na mocy krajowych przepisów ustawowych i wykonawczych, NSA lub jakikolwiek inny właściwy organ bezpieczeństwa są powiadamiane przez Parlament Europejski, jako instytucję zamawiającą, o umowach lub umowach o podwykonawstwo zawierających informacje niejawne opatrzone klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED.

35. W przypadku umów zawartych przez Parlament Europejski zawierających informacje niejawne o klauzuli tajności RESTREINT UE/EU RESTRICTED od wykonawców, podwykonawców ani ich personelu nie wymaga się posiadania FSC ani PSC.

36. Parlament Europejski, jako instytucja zamawiająca, analizuje odpowiedzi na ogłoszenia o przetargu w przypadku umów, które wymagają dostępu do informacji niejawnych opatrzonych klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED, niezależnie od jakichkolwiek wymogów związanych z FSC lub PSC, które mogą być określone przez krajowe przepisy ustawowe i wykonawcze.

37. Warunki, na których wykonawca może zlecić podwykonawstwo, są określone w ogłoszeniu o przetargu oraz w umowie.

38. Jeżeli umowa zakłada wykorzystywanie informacji niejawnych opatrzonych klauzulą tajności na poziomie RESTREINT UE/EU RESTRICTED w systemach komunikacyjno-informacyjnych stosowanych przez wykonawcę, Parlament Europejski, jako instytucja zamawiająca, dopilnowuje, aby w umowie lub umowie o podwykonawstwo określono niezbędne wymogi techniczne i administracyjne dotyczące akredytacji systemów komunikacyjno-informacyjnych proporcjonalnie do ocenianego ryzyka i z uwzględnieniem wszystkich istotnych czynników. Zakres akredytacji tych systemów komunikacyjno-informacyjnych jest uzgodniony między instytucją zamawiającą a właściwymi NSA.

INSTRUKCJA BEZPIECZEŃSTWA 6

NARUSZENIE BEZPIECZEŃSTWA, UTRATA LUB ZAGROŻENIE BEZPIECZEŃSTWA INFORMACJI POUFNYCH

1. Naruszenie bezpieczeństwa jest wynikiem działania lub braku działania niezgodnie z niniejszą decyzją, co może zaszkodzić informacjom poufnym lub zagrozić ich bezpieczeństwu.

2. Zagrożenie bezpieczeństwa informacji poufnych ma miejsce, gdy informacje te w całości lub częściowo dostały się w ręce osób nieupoważnionych, tzn. osób, które nie posiadają odpowiedniego poświadczenia bezpieczeństwa albo zapoznanie się z daną informacją nie należy do ich obowiązków służbowych, lub też gdy istnieje uzasadnione podejrzenie, że doszło do takiej sytuacji.

3. Zagrożenie bezpieczeństwa informacji poufnych może być wynikiem nieostrożności, zaniedbania lub braku dyskrecji, a także działalności służb, które biorą Unię za cel, lub organizacji wywrotowych.

4. W przypadku odkrycia udowodnionego lub przypuszczalnego naruszenia bezpieczeństwa, utraty lub zagrożenia bezpieczeństwa związanego z informacjami poufnymi bądź otrzymania o tym wiadomości sekretarz generalny:

a) ustala stan faktyczny;

b) dokonuje oceny i minimalizuje zaistniałe szkody;

c) podejmuje działania zapobiegające powtórzeniu się takiej sytuacji;

d) powiadamia właściwe organy strony trzeciej lub państwa członkowskiego, z których pochodzą lub które przekazały informacje poufne.

W przypadku gdy dotyczy to posła do Parlamentu Europejskiego, sekretarz generalny Parlamentu Europejskiego działa wspólnie z przewodniczącym Parlamentu.

Jeżeli informacja pochodzi od innej instytucji unijnej, sekretarz generalny działa zgodnie z odpowiednimi środkami bezpieczeństwa dotyczącymi informacji niejawnych, a także z obowiązującymi ustaleniami określonymi w porozumieniu ramowym z Komisją oraz w porozumieniu mi międzyinstytucjonalnym z Radą.

5. Wszystkie osoby, które mają wykorzystywać informacje poufne, są dogłębnie przeszkolone w zakresie procedur bezpieczeństwa, niebezpieczeństwa związanego z niedyskretnymi rozmowami oraz ich kontaktów z mediami, a w razie potrzeby podpisują oświadczenie o nieujawnianiu treści informacji poufnych osobom trzecim, przestrzeganiu obowiązku ochrony informacji niejawnych oraz świadomości konsekwencji nieprzestrzegania tych zasad. Dostęp do informacji niejawnych przez osobę, która nie została przeszkolona i nie podpisała stosownego oświadczenia, lub wykorzystywanie tych informacji przez taką osobę są uważane za naruszenie bezpieczeństwa.

6. Każdy poseł do Parlamentu Europejskiego, urzędnik Parlamentu czy inny pracownik Parlamentu pracujący dla grup politycznych lub wykonawców niezwłocznie informuje sekretarza generalnego o wszelkich naruszeniach bezpieczeństwa, utratach lub zagrożeniach bezpieczeństwa informacji poufnych, o których się dowiedział.

7. Każda osoba odpowiedzialna za zagrożenie bezpieczeństwa informacji poufnych podlega postępowaniu dyscyplinarnemu zgodnie z właściwymi przepisami ustawowymi i wykonawczymi. Postępowanie to nie stanowi uszczerbku dla postępowania sądowego, które może zostać wszczęte na mocy obowiązującego prawa.

8. Bez uszczerbku dla innego postępowania sądowego naruszenia dokonane przez urzędników Parlamentu oraz innych pracowników Parlamentu pracujących dla grup politycznych prowadzą do wszczęcia procedur i zastosowania kar określonych w tytule VI Regulaminie Pracowniczym.

9. Bez uszczerbku dla innego postępowania sądowego naruszenia dokonane przez posłów do Parlamentu Europejskiego pociągają za sobą zastosowanie art. 9 ust. 2 oraz art. 152, 153 i 154 Regulaminu Parlamentu.