DECYZJA KOMISJI

z dnia 29 listopada 2001 r.

zmieniająca jej regulamin wewnętrzny

(notyfikowana jako dokument nr C(2001) 3031)

(2001/844/WE, EWWiS, Euratom)

KOMISJA WSPÓLNOT EUROPEJSKICH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 218 ust. 2,

uwzględniając Traktat ustanawiający Europejską Wspólnotę Węgla i Stali, w szczególności jego art. 16,

uwzględniając Traktat ustanawiający Europejską Wspólnotę Energii Atomowej, w szczególności jego art. 131,

uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 28 ust. 1 i art. 41 ust. 1,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Przepisy Komisji w sprawie bezpieczeństwa, których tekst załączony jest do niniejszej decyzji, dodaje się do regulaminu Komisji, jako załącznik.

Artykuł 2

Niniejsza decyzja wchodzi w życie z dniem jej opublikowania w *Dzienniku Urzędowym Wspólnot Europejskich*.

Niniejszą decyzję stosuje się od dnia 1 grudnia 2001 r.

Sporządzono w Brukseli, dnia 29 listopada 2001 r.

W imieniu Komisji

Romano PRODI

Przewodniczący

ZAŁĄCZNIK

PRZEPISY KOMISJI W SPRAWIE BEZPIECZEŃSTWA

(1) W celu rozwijania działalności Komisji w dziedzinach wymagających zachowania stopnia poufności, odpowiednim jest ustanowienie wszechstronnego systemu bezpieczeństwa mającego zastosowanie do Komisji, innych instytucji, organów, biur i agencji, ustanowionych na mocy lub na podstawie Traktatu ustanawiającego Wspólnotę Europejską lub Traktatu o Unii Europejskiej, do Państw Członkowskich, a także innych odbiorców tajnych informacji Unii Europejskiej, zwanej dalej „informacją niejawną UE".

(2) W celu ochrony skuteczności ustanowionego w ten sposób systemu bezpieczeństwa, Komisja będzie udostępniać informację niejawną UE tylko tym zewnętrznym organom, które przedstawią gwarancje, że podjęły wszystkie niezbędne środki do stosowania zasad całkowicie równorzędnych do niniejszych przepisów.

(3) Niniejsze przepisy zostały przyjęte bez uszczerbku dla przepisów rozporządzenia nr 3 z dnia 31 lipca 1958 r. w sprawie wykonania art. 24 Traktatu ustanawiającego Europejską Wspólnotę Energii Atomowej[1], rozporządzenia Rady (WE) nr 1588/90 z dnia 11 czerwca 1990 r. w sprawie przekazywania do Urzędu Statystycznego Wspólnot Europejskich danych statystycznych objętych zasadą poufności[2] i decyzji Komisji C (95) 1510 ostatecznej z dnia 23 listopada 1995 r. w sprawie ochrony systemów informatycznych.

(4) System bezpieczeństwa Komisji oparty jest na zasadach wysuniętych w decyzji Rady 2001/264/WE z dnia 19 marca 2001 r. w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa[3], w celu zapewnienia sprawnego funkcjonowania procesu podejmowania decyzji w Unii.

(5) Komisja podkreśla znaczenie przyłączenia się, tam gdzie to właściwe, innych instytucji do zasad i norm poufności, które są konieczne w celu ochrony interesów Unii i jej Państw Członkowskich.

(6) Komisja uznaje potrzebę stworzenia swojej własnej koncepcji bezpieczeństwa, biorąc pod rozwagę wszystkie aspekty bezpieczeństwa i szczególny charakter Komisji jako instytucji.

(7) Niniejsze przepisy przyjmowane są bez uszczerbku dla postanowień art. 255 Traktatu i przepisów rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji[4];

Artykuł 1

Przepisy Komisji w sprawie bezpieczeństwa określone są w załączniku.

Artykuł 2

[1] Dz.U. L 17/58 z 6.10.1958, str. 406/58.
[2] Dz.U. L 151 z 15.6.1990, str. 1.
[3] Dz.U. L 101 z 11.4.2001, str. 1.
[4] Dz.U. L 145 z 31.5.2001, str. 43.

1. Członek Komisji odpowiedzialny za sprawy bezpieczeństwa podejmuje właściwe środki zapewniające posługiwanie się informacją niejawną UE w Komisji przez urzędników Komisji oraz innych pracowników, personel delegowany do Komisji, a także we wszystkich pomieszczeniach Komisji, włączając w to przedstawicielstwa i biura w Unii oraz ich delegacje w państwach trzecich oraz przez zewnętrznych kontrahentów Komisji, z poszanowaniem zasad, określonych w art. 1.

2. Państwa Członkowskie, inne instytucje, organy, biura czy agencje ustanowione na mocy lub na podstawie Traktatów są uprawnione do otrzymywania informacji niejawnych UE pod warunkiem zapewnienia przestrzegania, w czasie posługiwania się informacją niejawną UE w ramach ich służby i pomieszczeń, zasad całkowicie równorzędnych do tych, określonych w art. 1, w szczególności przez:

a) członków stałych przedstawicielstw Państw Członkowskich przy Unii Europejskiej, a także przez członków krajowych delegacji, biorących udział w posiedzeniach Komisji lub jej organach, lub uczestniczących w innych działaniach Komisji,

b) innych członków krajowej administracji Państw Członkowskich posługujących się informacją niejawną UE, bez względu na to czy pełnią służbę na terytorium Państw Członkowskich czy zagranicą,

c) zewnętrznych kontrahentów oraz personel delegowany, posługujący się informacją niejawną UE.

Artykuł 3

Państwa trzecie, organizacje międzynarodowe i inne organy są uprawnione do otrzymywania informacji niejawnych UE pod warunkiem, że zapewnią, że w czasie posługiwania się taką informacją są respektowane zasady całkowicie równorzędne do tych określonych w art. 1.

Artykuł 4

Trzymając się podstawowych zasad oraz minimalnych norm bezpieczeństwa zawartych w części I załącznika, członek Komisji odpowiedzialny za sprawy bezpieczeństwa może podjąć środki zgodne z częścią II załącznika.

Artykuł 5

Od dnia wejścia w życie niniejszych przepisów, tracą moc:

a) decyzja Komisji C (94) 3282 z dnia 30 listopada 1994 r. w sprawie środków bezpieczeństwa mających zastosowanie do informacji niejawnych sporządzonych lub przekazanych w związku z działalnością Unii Europejskiej;

b) decyzja Komisji C (99) 423 z dnia 25 lutego 1999 r. odnosząca się do procedur, według których urzędnicy i inni pracownicy zatrudnieni w Komisji Europejskiej mogą uzyskać dostęp do informacji niejawnych przechowywanych przez Komisję.

Artykuł 6

Od dnia zastosowania niniejszych przepisów, wszystkie informacje niejawne przechowywane przez Komisję do tego dnia, z wyjątkiem informacji niejawnych Euratom:

a) są automatycznie przeklasyfikowane na „UE ZASTRZEŻONE”, jeśli zostały sporządzone przez Komisję, chyba że ich sporządzający zdecyduje, przed dniem 31 stycznia 2002 r., o nadaniu im innej klasyfikacji. W takim przypadku sporządzający informuje o tym wszystkich adresatów danego dokumentu;

b) zachowują pierwotną klasyfikację i są traktowane jak informacje niejawne UE o tym samym poziomie zabezpieczenia, jeśli zostały sporządzone poza Komisją, chyba że ich sporządzający wyrazi zgodę na odtajnienie lub obniżenie ich stopnia.

ZAŁĄCZNIK

ZASADY BEZPIECZEŃSTWA

Treść

CZĘŚĆ I: PODSTAWOWE ZASADY I MINIMALNE NORMY BEZPIECZEŃSTWA

1. WPROWADZENIE

Niniejsze przepisy ustanawiają podstawowe zasady i minimalne normy bezpieczeństwa, które wymagają przestrzegania w należyty sposób przez Komisję we wszystkich jej miejscach zatrudnienia, a także przez wszystkich odbiorców EUCI, tak, aby zagwarantowane było bezpieczeństwo i aby każdy mógł być pewny, że ustanowione są wspólne normy bezpieczeństwa.

2. ZASADY OGÓLNE

Polityka Komisji w dziedzinie bezpieczeństwa stanowi integralną część ogólnej polityki wewnętrznego zarządzania i w ten sposób oparta jest na zasadach regulujących jej ogólną politykę.

Niniejsze zasady obejmują zgodność z prawem, przejrzystość, odpowiedzialność i pomocniczości (proporcjonalność).

Zgodność z prawem wskazuje na konieczność ścisłego przestrzegania ram prawnych w wykonywaniu funkcji bezpieczeństwa oraz na potrzebę stosowania się do wymogów prawa. Oznacza także, że obowiązki w dziedzinie bezpieczeństwa muszą być oparte o odpowiednie przepisy prawne. Przepisy regulaminu pracowniczego mają pełne zastosowanie, a w szczególności jego art. 17 dotyczący wypełniania obowiązków personelu w zakresie zachowania dyskrecji w odniesieniu do informacji Komisji, oraz jego tytuł VI w sprawie środków dyscyplinarnych. Ostatecznie oznacza ona, że naruszenia bezpieczeństwa w zakresie odpowiedzialności Komisji muszą być rozpatrywane w sposób zgodny z polityką Komisji w dziedzinie działań dyscyplinarnych i z jej polityką współpracy z Państwami Członkowskimi w dziedzinie wymiaru sprawiedliwości karnej.

Przejrzystość wskazuje na potrzebę jasności w odniesieniu do wszystkich zasad i przepisów dotyczących bezpieczeństwa, na równowagę między różnymi służbami i różnymi dziedzinami (ochrona fizyczna przeciwko ochronie informacji, itd.) oraz potrzebę spójnej i odpowiednio zbudowanej polityki świadomości bezpieczeństwa. Definiuje ona także potrzebę jasnych pisemnych wytycznych dotyczących wprowadzania w życie środków bezpieczeństwa.

Odpowiedzialność oznacza, że obowiązki w dziedzinie bezpieczeństwa będą jasno określone. Co więcej wskazuje ona na potrzebę regularnego sprawdzania, czy obowiązki te są właściwie wykonywane.

Zasada pomocniczości, lub proporcjonalności oznacza, że bezpieczeństwo jest zorganizowane na najniższym z możliwych poziomie i tak blisko jak to jest możliwe Dyrekcji Generalnych i służb Komisji. Wskazuje ona także, że działania dotyczące bezpieczeństwa są ograniczone tylko do tych elementów, które jej rzeczywiście wymagają. I oznacza ona również, że środki bezpieczeństwa są proporcjonalne w stosunku do chronionych interesów i do aktualnego lub potencjalnego ich zagrożenia, uwzględniając obronę wywołującą możliwie najmniejsze zakłócenia.

3. PODSTAWY BEZPIECZEŃSTWA

Podstawami pewnego bezpieczeństwa są:

a) w ramach każdego Państwa Członkowskiego, państwowe służby bezpieczeństwa, odpowiedzialne za:

   1. zbieranie i rejestrowanie doniesień na temat szpiegostwa, sabotażu, terroryzmu i innych działań wywrotowych, i

   2. dostarczanie informacji i porad swojemu rządowi, a za jego pośrednictwem, Komisji, o charakterze zagrożeń bezpieczeństwa i środków ochrony przed nimi.

b) w ramach każdego Państwa Członkowskiego i w ramach Komisji, techniczny organ INFOSEC (IA) odpowiedzialny za pracę z odpowiednim organem bezpieczeństwa w celu dostarczania informacji i porad w sprawie technicznych zagrożeń bezpieczeństwa i środków ochrony przed nimi;

c) regularna współpraca między rządowymi jednostkami organizacyjnymi a właściwymi służbami instytucji europejskich celem ustalenia i zalecenia, odpowiednio:

   1. która osoba, informacja i źródło wymaga ochrony, i

   2. wspólnych norm ochrony.

d) ścisła współpraca między Biurem ds. bezpieczeństwa Komisji a służbami bezpieczeństwa innych instytucji europejskich oraz z Biurem Bezpieczeństwa NATO (NOS).

4. ZASADY BEZPIECZEŃSTWA INFORMACJI

4.1. **Cele**

Bezpieczeństwo informacji ma następujące podstawowe cele:

a) ochronę informacji niejawnych UE (EUCI) przed szpiegostwem, utratą lub nieupoważnionym ujawnieniem;

b) ochronę informacji UE obsługiwanej przez systemy informatyczne i systemy łączności oraz znajdującej się w sieci, przed zagrożeniami dla jej poufności, integralności i dostępności;

c) ochronę pomieszczeń Komisji, w których przechowywane są informacje UE, przed sabotażem i umyślnym zniszczeniem mienia;

d) ocenę poniesionych szkód, ograniczenie ich konsekwencji i przyjęcie koniecznych środków zaradczych w przypadku niepowodzenia działań ochronnych.

4.2. **Definicje**

Wszędzie w niniejszych przepisach:

a) Pojęcie „informacja niejawna UE” (EUCI) oznacza każdą informację i materiał, którego nieupoważnione ujawnienie może spowodować różnego stopniaszkody dla interesów UE, lub dla jednego lub więcej jej Państw Członkowskich, bez względu na to czy informacja taka pochodzi z UE lub została otrzymana od Państwa Członkowskiego, państwa trzeciego lub organizacji międzynarodowych.

b) Pojęcie „dokument” oznacza każdy list, notatkę, protokół, sprawozdanie, memorandum, sygnał / wiadomość, szkic, fotografię, slajd, film, mapę, kartę, plan, notes, szablon, kopię kalkową, taśmę maszynową lub z drukarki, taśmę, kasetę, dysk komputerowy, CD - ROM, lub inny fizyczny nośnik, na którym została zapisana informacja.

c) Pojęcie „materiał” oznacza „dokument” tak jak jest zdefiniowany w lit. b), a także każdy przedmiot wyposażenia, albo wyprodukowany albo będący w trakcie procesu produkcji.

d) Pojęcie „powinien wiedzieć” oznacza konieczność posiadania dostępu indywidualnego pracownika do informacji niejawnych UE, w celu umożliwienia mu wykonywania funkcji lub zadania.

e) „Upoważnienie” oznacza decyzję przewodniczącego Komisji przyznającą indywidualny dostęp do EUCI określonego poziomu, na podstawie pozytywnego postępowania sprawdzającego (weryfikacja) przeprowadzonego przez organy bezpieczeństwa państwa zgodnie z prawem krajowym.

f) Pojęcie „klasyfikacja” oznacza przyznanie odpowiedniego poziomu ochrony informacji, której nieupoważnione ujawnienie może spowodować powstanie pewnego stopnia szkody dla interesów Komisji lub Państwa Członkowskiego.

g) Pojęcie „obniżenie stopnia” (déclassement) oznacza obniżenie poziomu klasyfikacji.

h) Pojęcie „odtajnienie” (déclassification) oznacza usunięcie wszelkiej klasyfikacji.

i) Pojęcie „sporządzający” oznacza należycie upoważnioną osobę, która sporządziła dokument niejawny. W ramach Komisji szefowie departamentów mogą upoważnić swój personel do tworzenia EUCI.

j) Pojęcie „departamenty Komisji” oznaczają wydziały Komisji i służby, włączając w to gabinety, we wszystkich miejscach zatrudnienia, w tym także Wspólne Centrum Badawcze, przedstawicielstwa i biura w Unii i delegatury w państwach trzecich.

4.3. **Klasyfikacja**

a) W przypadku gdy chodzi o poufny charakter informacji wymagana jest ostrożność i doświadczenie w wyborze informacji i materiałów podlegających ochronie oraz w oszacowaniu stopnia wymaganej ochrony. Podstawowe znaczenie ma tu zasada, że stopień ochrony powinien odpowiadać krytycznej granicy bezpieczeństwa indywidualnej informacji lub materiału podlegających ochronie. Celem zapewnienia sprawnego przepływu informacji podejmowane są odpowiednie kroki uniemożliwiające nadawanie zarówno zawyżonej, jak i zaniżonej klasyfikacji.

b) System klasyfikacji stanowi narzędzie, za pomocą którego nadaje się moc obowiązującą tym zasadom; podobny system klasyfikacji jest realizowany przy planowaniu i organizowaniu sposobów przeciwdziałania szpiegostwu, sabotażowi, terroryzmowi i innym zagrożeniom, tak aby zapewnić możliwie największe środki ochrony pomieszczeniom, w których przechowywane są informacje niejawne oraz ich najbardziej wrażliwym punktom.

c) Odpowiedzialność za klasyfikowanie informacji spoczywa wyłącznie na tym, kto sporządził tę informację.

d) Poziom klasyfikacji informacji może być oparty wyłącznie na jej treści.

e) W przypadku, gdy pewna liczba informacji stanowi zbiór, poziom klasyfikacji mający zastosowanie do całego zbioru jest co najmniej równy najwyższej sklasyfikowanej informacji. Zbiór informacji, może jednakże otrzymać wyższą klasyfikację niż klasyfikacja, jaką posiada każda z informacji osobno.

f) Klasyfikacja może być przyznana jedynie wtedy, gdy jest to niezbędne i na tak długo, jak to jest konieczne.

4.4. **Cele środków bezpieczeństwa**

Środki bezpieczeństwa:

a) Rozciągają się na wszystkie osoby mające dostęp do informacji niejawnych, środki przekazu informacji niejawnych, wszystkie pomieszczenia zawierające takie informacje oraz ważne urządzednia.

b) Stworzone są w celu wykrywania osób, które poprzez zajmowane stanowisko mogą narazić bezpieczeństwo informacji niejawnych oraz ważnych urządzeń, w których przechowywane są informacje niejawne, oraz przewidują wykluczenie lub usunięcie takich osób.

c) Zapobiegają dostępowi do informacji niejawnych lub urządzeń zawierających takie informacje każdej nieupoważnionej osobie.

d) Zapewniają, że informacja niejawna rozpowszechniana jest jedynie według, podstawowej dla bezpieczeństwa we wszelkich postaciach, zasady „powinien wiedzieć”.

e) Zapewniają integralność (np. zapobieganie korupcji lub nieupoważnionej zmianie lub nieupoważnionemu usunięciu) oraz dostępność wszystkich informacji, albo niejawnych albo jawnych, (np. nie odmawia się dostępu osobom, które powinny wiedzieć i są do tego upoważnione), do wszelkich informacji, tak niejawnych, jak i jawnych, w szczególności informacji gromadzonych, przetwarzanych lub przekazywanych w formie elektromagnetycznej.

5. ORGANIZACJA BEZPIECZEŃSTWA

5.1. **Wspólne minimalne normy**

Komisja zapewnia, że wspólne minimalne normy bezpieczeństwa są przestrzegane przez wszystkich odbiorców EUCI, w ramach instytucji i w ramach jej kompetencji, tzn. przez wszystkie departamenty i kontrahentów, którym informacja niejawna UE może zostać przekazana z założeniem, że będzie przechowywana z taką samą ostrożnością. Minimalne normy zawierają kryteria sprawdzania personelu oraz procedury dotyczące ochrony informacji niejawnych UE.

Komisja zezwala na dostęp do EUCI zewnętrznym organom wyłącznie pod warunkiem, że zapewnią one, że w czasie gdy posługują się EUCI, mają zastosowanie przepisy co najmniej równorzędnie rygorystyczne jak niniejsze normy minimalne.

5.2. **Organizacja**

W ramach Komisji bezpieczeństwo jest zorganizowane na dwóch poziomach:

a) Na poziomie Komisji jako całości, ustanawia się Biuro ds. bezpieczeństwa Komisji wraz ze Służbą Akredytacji Bezpieczeństwa (SAA), działającą także jako Służba Szyfrów (CrA) i jako Służba TEMPEST, wraz ze Służbą INFOSEC (IA) oraz z jednym lub więcej Centralnym Archiwum EUCI, każdy z jednym lub więcej Urzędnikiem Kontroli Archiwum (RCO).

b) Na poziomie departamentów Komisji, sprawy bezpieczeństwa znajdują się w zakresie odpowiedzialności jednego lub więcej Lokalnych Urzędników Bezpieczeństwa (LSO), jednego lub więcej Centralnych Urzędników Bezpieczeństwa Informatycznego (CISO), Lokalnych Urzędników Bezpieczeństwa Informatycznego (LISO) i Lokalnych Archiwów Informacji Niejawnych UE z jednym lub więcej Urzędnikiem Kontroli Archiwów.

c) Centralne organy bezpieczeństwa dostarczą wytyczne operacyjne lokalnym organom bezpieczeństwa.

6. BEZPIECZEŃSTWO PERSONELU

6.1. **Postępowanie sprawdzające personel**

Wszystkie osoby, których praca wymaga dostępu do informacji niejawnych klasyfikowanych jako UE POUFNE lub wyżej, podlegają stosownemu postępowaniu sprawdzającemu przed wydaniem upoważnienia do dostępu. Podobne postępowanie sprawdzające przeprowadza się w stosunku do osób, których obowiązki służbowe obejmują techniczną obsługę lub konserwowanie systemów łączności i systemów informatycznych zawierających informacje niejawne. Celem niniejszego postępowania sprawdzającego jest ustalenie czy osoby takie:

a) są niepodważalnej lojalności;

b) są takiego charakteru i rozwagi, że ich uczciwość w posługiwaniu się informacjami niejawnymi nie podlega wątpliwości, lub

c) mogą być podatne na naciski ze strony zagranicznych lub innych źródeł.

W szczególności ścisłej kontroli w trakcie postępowania sprawdzającego podlegają osoby:

d) ubiegające się o uzyskanie dostępu do informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE;

e) zajmujące stanowisko wymagającą regularnego dostępu do poważnej ilości informacji objętych klauzulą tajności UE TAJNE;

f) których obowiązki służbowe dają im możliwość specjalnego dostępu do chronionych systemów łączności i systemów informatycznych i w ten sposób stwarzają możliwość uzyskania nieupoważnionego dostępu do znacznej liczby informacji niejawnych UE lub do wyrządzenia poważnych szkód misji poprzez akty technicznego sabotażu.

W okolicznościach określonych w lit. d), e) i f), należy możliwie najpełniej praktycznie zastosować techniki zbadania przeszłości tych osób.

W sytuacji, gdy zatrudnione mają być osoby nie objęte zasadą „powinien wiedzieć", a wykonywana przez nie praca umożliwia dostęp do informacji niejawnych UE (np. kurierzy, agenci ochrony, personel konserwujący i sprzątający, itd.), podlegają one stosownemu postępowaniu sprawdzającemu przed podjęciem zatrudnienia.

6.2. **Ewidencja personelu, który uzyskał poświadczeniebezpieczeństwa**

Wszystkie departamenty Komisji posiadające informacje niejawne UE lub dysponujące zabezpieczonymi systemami łączności lub systemami informatycznymi prowadzą ewidencję ich personelu, który uzyskał poświadczenie bezpieczeństwa. Każde poświadczenie bezpieczeństwa podlega sprawdzeniu, gdy okoliczności wymagają ustalenia, czy poświadczenie jest adekwatne do bieżących zadań wykonywanych przez tę osobę; podlega ono ponownemu sprawdzeniu, jako sprawa pierwszorzędnej wagi, wtedy, gdy napłynie nowa informacja wskazująca, że dalszy przydział do pracy z informacjami niejawnymi pozostaje w sprzeczności z interesem bezpieczeństwa. Lokalny Urzędnik Bezpieczeństwa departamentu Komisji prowadzi ewidencję poświadczeń bezpieczeństwa w ramach jego lub jej dziedziny.

6.3. **Szkolenie personelu w zakresie bezpieczeństwa**

Wszystkie osoby zatrudnione na stanowiskach, na których mogą mieć dostęp do informacji niejawnych podlegają dokładnemu przeszkoleniu podczas przyjmowania zadań oraz w regularnych odstępach czasu w razie konieczności zachowania bezpieczeństwa oraz procedur do tego zmierzających. Osoby te są zobowiązane do poświadczenia na piśmie, że zapoznały się i w pełni zrozumiały niniejsze przepisy bezpieczeństwa.

6.4. **Obowiązki kierownictwa**

Kierownicy mają obowiązek poznania tych spośród ich pracowników, którzy są zaangażowani w pracę niejawną lub, którzy mają dostęp do chronionych systemów łączności lub systemów informatycznych oraz są zobowiązani do sporządzania rejestrów i sporządzania sprawozdań ze wszystkich zdarzeń lub jednoznacznie słabych punktów, które mogą mieć wpływ na bezpieczeństwo.

6.5. **Stan bezpieczeństwa personelu**

Ustanawia się procedury umożliwiające zapewnienie, w przypadku gdy zostanie ujawniona niekorzystna informacja dotycząca osoby, że jest ona zatrudniona do pracy z informacją niejawną lub ma dostęp do zabezpieczonych systemów łączności lub systemów informatycznych, oraz, że Biuro ds. bezpieczeństwa Komisji zostało o tym poinformowane. W przypadku stwierdzenia, że dana osoba stanowi ryzyko dla bezpieczeństwa, zostaje ona odsunięta lub usunięta z wykonywania zadań, w których może stanowić zagrożenie dla bezpieczeństwa.

7. BEZPIECZEŃSTWO FIZYCZNE

7.1. **Potrzeba ochrony**

Stopień środków ochrony fizycznej mających zastosowanie do zapewnienia ochrony informacji niejawnych UE jest proporcjonalny do klasyfikacji, ilości oraz zagrożeń wobec posiadanych informacji i materiałów. Wszyscy posiadacze informacji niejawnych UE stosują się do jednolitych praktyk dotyczących klasyfikacji takich informacji oraz stosują się do wspólnych norm ochrony w odniesieniu do sprawowania pieczy, przekazywania i niszczenia informacji i materiałów wymagających ochrony.

7.2. **Kontrola**

Przed opuszczeniem stref, w których znajdują się niezabezpieczone informacje niejawne UE, osoby odpowiedzialne za sprawowanie nad nimi pieczy zapewniają, że informacje te są bezpiecznie zgromadzone oraz że wszystkie urządzenia bezpieczeństwa zostały uaktywnione (zamki, alarmy, itp.). Kolejne niezależne kontrole przeprowadza się poza godzinami pracy.

7.3. **Bezpieczeństwo budynków**

Budynki, w których przechowywane są informacje niejawne UE lub zabezpieczone systemy łączności i systemy informatyczne chronione są przed nieupoważnionym dostępem. Charakter ochrony udzielonej informacji niejawnej UE, np. ryglowane okna, zamki w drzwiach, straże przy wejściu, systemy automatycznej kontroli wstępu, kontrole bezpieczeństwa i patrole, systemy alarmowe, systemy wykrywania wtargnięć i psy obronne, zależy od:

a) klasyfikacji, ilości oraz umiejscowienia, w ramach budynku, informacji i materiałów podlegających ochronie;

b) jakości szaf pancernych przeznaczonych do przechowywania tych informacji i materiałów, oraz

c) fizycznego charakteru i umiejscowienia budynku.

Podobnie, charakter ochrony przyporządkowanej systemom łączności i systemom informatycznym zależy od oceny wartości aktywów znajdujących się w systemach oraz potencjalnej szkody w przypadku, gdy systemy bezpieczeństwa zawiodą, od fizycznego charakteru i umiejscowienia budynku, w którym znajdują się te systemy, oraz od umiejscowienia system w ramach budynku.

7.4. **Plany awaryjne**

Przygotowuje się z wyprzedzeniem szczegółowe plany dotyczące ochrony informacji niejawnych w czasie lokalnych lub krajowych sytuacjach nadzwyczajnych.

8. BEZPIECZEŃSTWO INFORMACJI

Bezpieczeństwo informacji (INFOSEC) dotyczy określenia i stosowania środków bezpieczeństwa w celu ochrony informacji niejawnych UE podlegających przetwarzaniu, gromadzeniu lub przekazywaniu za pośrednictwem systemów łączności, systemów informatycznych i innych systemów elektronicznych przed utratą ich poufności, integralności lub dostępności, bez względu na to, czy nastąpiło to przypadkowo lub wskutek działań celowych. Podejmuje się odpowiednie środki zaradcze w celu zapobieżenia dostępu do informacji niejawnych UE przez nieupoważnionych użytkowników, zapobieżenia odmowie dostępu upoważnionym użytkownikom do informacji niejawnych UE, oraz w celu zapobieżenia korupcji lub nieupoważnionej modyfikacji lub usunięcia informacji niejawnych UE.

9. PRZECIWDZIAŁANIE SABOTAŻOWI I KONTROLA INNYCH FORM UMYŚLNEGO ZNISZCZENIA MIENIA

Fizyczne środki ostrożności ochraniające ważne urządzenia zawierające informacje niejawne stanowią najlepsze środki ochronne przeciwko sabotażowi i umyślnemu zniszczeniu, a samo postępowanie sprawdzające przeprowadzone wobec personelu nie jest efektywnym środkiem zastępczym. Wnioskuje się do właściwego organu krajowego o dostarczenie informacji dotyczących szpiegostwa, sabotażu, terroryzmu i innych działań wywrotowych.

NEW

10. UDOSTĘPNIANIE INFORMACJI NIEJAWNEJ PAŃSTWOM TRZECIM I ORGANIZACJOM MIĘDZYNARODOWYM

Decyzja o udostępnianiu informacji niejawnej UE pochodzącej z Komisji państwu trzeciemu lub organizacji międzynarodowej podejmowana jest przez Komisję jako organ kolegialny. Jeżeli sporządzającym informację jest podmiot inny niż Komisja, a udostępnienie informacji jest jego zdaniem pożądane, Komisja, przed jej udostępnieniem pyta sporządzającego o zgodę na jej udostępnienie. Jeśli sporządzający nie może zostać ustalony Komisja przyjmie na siebie odpowiedzialność sporządzającego.

Jeżeli Komisja uzyska informację niejawną od państw trzecich, organizacji międzynarodowych lub innej strony trzeciej, nadaje im ochronę odpowiednią do ich klasyfikacji i równorzędną do norm ustanowionych w niniejszych przepisach, dotyczących informacji niejawnej UE lub wyższych norm ochrony, jaki może być wymagany przez stronę trzecią, udostępniającą informację. Można dokonywać wzajemnej kontroli norm ochrony.

Powyższe zasady wprowadzane są w życie zgodnie ze szczegółowymi przepisami określonymi w części II pkt 26 i w dodatkach 3,4 i 5.

CZĘŚĆ II: ORGANIZACJA BEZPIECZEŃSTWA W KOMISJI

11. CZŁONEK KOMISJI ODPOWIEDZIALNY ZA SPRAWY BEZPIECZEŃSTWA

Członek Komisji odpowiedzialny za sprawy bezpieczeństwa:

a) wprowadza w życie politykę bezpieczeństwa Komisji;

b) analizuje problemy bezpieczeństwa skierowane do niego przez Komisję lub jej właściwe organy;

c) rozpatruje zagadnienia wymagające zmian w polityce bezpieczeństwa Komisji, pozostając w bliskim powiązaniu z państwowymi służbami bezpieczeństwa (lub innymi właściwymi) Państw Członkowskich (zwanymi dalej „PSB").

W szczególności członek Komisji odpowiedzialny za sprawy bezpieczeństwa odpowiada za:

a) koordynację wszelkich zagadnień bezpieczeństwa odnoszących się do działania Komisji;

b) kierowanie do wyznaczonych organów Państw Członkowskich wniosków o przeprowadzenie przez PSB postępowania sprawdzającego personel, który jest zatrudniony w Komisji, zgodnie z pkt. 20;

c) przeprowadzanie dochodzenia lub zlecanie dochodzenia w przypadkach ujawnienia informacji niejawnej UE, które, na podstawie dowodów *prima facie*, nastąpiło w Komisji;

d) żądanie wszczęcia przez odpowiednie organy bezpieczeństwa śledztwa w przypadku, gdy wydaje się, że ujawnienie informacji niejawnej UE nastąpiło poza Komisją oraz koordynowanie dochodzeń w przypadku, gdy włączony jest więcej niż jeden organ bezpieczeństwa;

e) przeprowadzanie okresowych kontroli uzgodnień dotyczących bezpieczeństwa w celu ochrony informacji niejawnej UE;

f) utrzymywanie bliskich powiązań ze wszystkimi właściwymi organami bezpieczeństwa w celu osiągnięcia całościowej koordynacji bezpieczeństwa;

g) poddawanie polityki i procedur bezpieczeństwa Komisji stałym przeglądom oraz przygotowywanie, jeśli to konieczne, stosownych zaleceń. W tym względzie członek Komisji odpowiedzialny za sprawy bezpieczeństwa przestawia Komisji roczny plan inspekcji przygotowany przez Służbę ds. Bezpieczeństwa Komisji.

12. GRUPA DORADCZA KOMISJI DS. POLITYKI BEZPIECZEŃSTWA

Ustanawia się Grupę Doradczą Komisji ds. Polityki Bezpieczeństwa. Składa się ona z członka Komisji odpowiedzialnego za sprawy bezpieczeństwa lub jego/jej delegata, który sprawuje funkcję przewodniczącego, oraz z przedstawicieli PSB każdego Państwa Członkowskiego. Do prac w Grupie mogą także zostać zaproszeni przedstawiciele innych instytucji europejskich. W posiedzeniach Grupy mogą także uczestniczyć przedstawiciele odpowiednich zdecentralizowanych agencji WE i UE, o ile przedmiotem dyskusji są zagadnienia ich dotyczące.

Grupa Doradcza Komisji ds. Polityki Bezpieczeństwa spotyka się na wniosek jej przewodniczącego lub któregokolwiek z jej członków. Zadaniem Grupy jest badanie i ocenianie wszystkich stosownych zagadnień bezpieczeństwa i przedstawianie Komisji zaleceń, tam gdzie to stosowne.

13. RADA DS. BEZPIECZEŃSTWA KOMISJI

Ustanawia się Radę ds. Bezpieczeństwa Komisji. Składa się on z sekretarza generalnego, który jej przewodniczy, oraz z dyrektorów generalnych Służby Prawnej, administracji i personelu, stosunków zewnętrznych, wymiaru sprawiedliwości i spraw wewnętrznych oraz Wspólnego Centrum Badawczego, a także Szefów Służby Audytu Wewnętrznego i Biura ds. Bezpieczeństwa Komisji. Do udziału w pracach Rady można zapraszać także innych urzędników Komisji. Mandat Rady obejmuje dokonywanie oceny środków bezpieczeństwa w ramach Komisji oraz formułowanie zaleceń w tym zakresie członkowi Komisji odpowiedzialnemu za sprawy bezpieczeństwa.

14. BIURO DS. BEZPIECZEŃSTWA KOMISJI

W celu wypełniania obowiązków wymienionych w pkt. 11 członek Komisji odpowiedzialny za sprawy bezpieczeństwa, ma do swojej dyspozycji Biuro ds. Bezpieczeństwa Komisji celem koordynowania, nadzorowania i wprowadzania w życie środków bezpieczeństwa.

Głównym doradcą ds. Bezpieczeństwa Członka Komisji odpowiedzialnego za sprawy bezpieczeństwa, jest szef Biura ds. Bezpieczeństwa Komisji, który działa jako sekretarz Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa. W tym względzie kieruje on lub ona procesem uaktualniania przepisów bezpieczeństwa i koordynuje środki bezpieczeństwa z właściwymi organami Państw Członkowskich, oraz, jeśli to właściwe, z organizacjami międzynarodowymi, związanymi z Komisją porozumieniami w sprawie bezpieczeństwa. W tym celu działa on/ona jako urzędnik łącznikowy.

Szef Biura ds. Bezpieczeństwa Komisji odpowiada za akredytację systemów i sieci IT w ramach Komisji. Szef Biura ds. Bezpieczeństwa Komisji decyduje, w porozumieniu z odpowiednią PSB, w sprawie akredytacji systemów i sieci IT obejmujących Komisję z jednej strony i każdego innego odbiorcę informacji niejawnej UE, z drugiej strony.

15. INSPEKCJE BEZPIECZEŃSTWA

Biuro ds. Bezpieczeństwa Komisji przeprowadza okresowe inspekcje uzgodnień dotyczących bezpieczeństwa w zakresie ochrony informacji niejawnej UE.

Biuro ds. Bezpieczeństwa Komisji może być wspierane przez służby bezpieczeństwa innych instytucji UE dysponujących EUCI lub przez państwową służbę bezpieczeństwa Państwa Członkowskiego[5].

Na wniosek Państwa Członkowskiego, jego PSB, w porozumieniu ze Służbą ds. Bezpieczeństwa Komisji, przeprowadzają, za wzajemną zgodą, wzajemne inspekcje EUCI.

16. KLASYFIKACJA, ZNAKI I OZNAKOWANIA BEZPIECZEŃSTWA

[5] Bez uszczerbku dla postanowień Konwencji Wiedeńskiej z dnia 1961 r. o stosunkach dyplomatycznych i Protokołu w sprawie przywilejów i immunitetów Wspólnot Europejskich z dnia 8 kwietnia 1965 r.

16.1. **Poziomy klasyfikacji**[6]

Informacje są klasyfikowane na następujących poziomach (patrz także dodatek 2):

UE ŚCIŚLE TAJNE: niniejsza klasyfikacja ma zastosowanie tylko do informacji i materiałów, których nieupoważnione ujawnienie może spowodować wyjątkowo ciężkie naruszenie podstawowych interesów Unii Europejskiej lub jednego lub więcej jej Państw Członkowskich.

UE TAJNE: niniejsza klasyfikacja ma zastosowanie do informacji i materiałów, których nieupoważnione ujawnienie może spowodować poważną szkodę w podstawowych interesach Unii Europejskiej lub jednego lub więcej jej Państw Członkowskich.

UE POUFNE: niniejsza klasyfikacja ma zastosowanie do informacji i materiałów, których nieupoważnione ujawnienie może spowodować szkodę w podstawowych interesach Unii Europejskiej lub jednego lub więcej jej Państw Członkowskich.

UE ZASTRZEŻONE: niniejsza klasyfikacja ma zastosowanie do informacji i materiałów, których nieupoważnione ujawnienie mogłoby być niekorzystne dla interesów Unii Europejskiej lub jednego lub więcej jej Państw Członkowskich.

Przyznawanie innych klasyfikacji jest zabronione.

16.2. **Znaki bezpieczeństwa**

Do ustanowienia granic ważności klasyfikacji (dla informacji niejawnej automatycznie obniżanego stopnia lub odtajnionej) można używać uzgodnionego znaku bezpieczeństwa. Znakiem tym jest albo „DO... (godzina / dzień)" albo „DO... (wydarzenie)".

Dodatkowe znaki bezpieczeństwa takie jak CRYPTO lub każdy inny, uznawany w UE znak bezpieczeństwa, stosuje się wtedy, gdy zachodzi potrzeba ograniczonego rozprowadzenia i specjalnego potraktowania, obok tego, wynikającego z klasyfikacji bezpieczeństwa.

Znaki bezpieczeństwa używa się wyłącznie w połączeniu z klasyfikacją.

16.3. **Oznakowania**

Można stosować oznakowanie w celu wyszczególnienia sfery działalności objętej dokumentem lub szczególnego rozprowadzania wtedy, gdy jest ono potrzebne, lub (dla informacji niesklasyfikowanych) do wskazania końca embarga.

Oznakowanie nie jest klasyfikacją i nie wolno go stosować zamiast niej.

Oznakowanie ESDP ma zastosowanie do dokumentów i ich kopii dotyczących bezpieczeństwa i obrony Unii lub jednego lub więcej Państw Członkowskich, lub do wojskowego lub cywilnego zarządzania w sytuacjach kryzysowych.

---

[6] Patrz tablica porównawcza dotycząca klasyfikacji bezpieczeństwa UE, NATO, UZE i Państw Członkowskich w dodatku 1.

16.4. **Umieszczanie klasyfikacji**

Klasyfikacja jest umieszczana w sposób następujący:

a) na dokumentach objętych klauzulą tajności UE ZASTRZEŻONE, środkami mechanicznymi lub elektronicznymi;

b) na dokumentach objętych klauzulą tajności UE POUFNE, środkami mechanicznymi lub ręcznie lub poprzez drukowanie na wcześniej opieczętowanym, rejestrowanym papierze;

c) na dokumentach objętych klauzulą tajności UE TAJNE i UE ŚCIŚLE TAJNE, środkami mechanicznymi lub ręcznie.

16.5. **Umieszczanie znaków bezpieczeństwa**

Znaki bezpieczeństwa umieszczane są bezpośrednio pod klasyfikacją, takimi samymi środkami jak przy umieszczaniu klasyfikacji.

17. ZARZĄDZANIE KLASYFIKACJĄ

17.1. **Przepisy ogólne**

Informacja zostaje objęta klasyfikacją jedynie wtedy, gdy jest to konieczne. Klasyfikacja jest wyraźnie i prawidłowo wskazana, i jest utrzymywana tylko tak długo jak długo informacja wymaga ochrony.

Odpowiedzialność za nadanie informacji klasyfikacji i za jakiekolwiek dalsze obniżenie jej stopnia lub jej odtajnienie spoczywa wyłącznie na sporządzającym informację.

Urzędnicy i inni pracownicy Komisji nadają klasyfikacje informacji, obniżają jej stopień lub ją odtajniają na podstawie instrukcji lub w porozumieniu z szefem ich departamentu.

Szczegółowe procedury postępowania z dokumentami niejawnymi zostały tak skonstruowane, aby zapewniały ochronę odpowiednią do informacji, które zawierają.

Liczba osób uprawnionych do sporządzania dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE ograniczona jest do minimum, a nazwiska tych osób zawiera lista sporządzona przez Biuro ds. Bezpieczeństwa Komisji.

17.2. **Stosowanie klasyfikacji**

Klasyfikacja dokumentu jest określona poziomem sensytywności jego zawartości zgodnie z definicją określoną w pkt. 16. Właściwe i ekonomiczne stosowanie klasyfikacji stanowi ważny element. Powyższe ma zastosowanie w szczególności do klasyfikacji UE ŚCIŚLE TAJNE.

Sporządzający dokument, któremu ma być nadana klasyfikacja respektuje zasady określone powyżej i powstrzymuje się przed każdą tendencja do jej zawyżania lub zaniżania.

Praktyczny przewodnik nadawania klauzul jest zawarty w dodatku 2.

Pojedyncze strony, ustępy, punkty, załączniki, dodatki, załączniki lub uzupełnienia do danego dokumentu mogą wymagać nadania innej klauzuli, która zostanie przyznana stosownie do potrzeb. Dla całego dokumentu przyznaje się najwyższą klauzulę jaka została przyznana jego części.

Klasyfikacja listu lub notatki, do których dołączone są uzupełnienia, odpowiada najwyższej klasyfikacji nadanej uzupełnieniom. Sporządzający powinien wyraźnie wskazać, jaki poziom klasyfikacji powinien być nadany po wyłączeniu z listu lub notatki uzupełnień.

Publiczny dostęp nadal podlega przepisom rozporządzenia (WE) nr 1049/2001.

17.3. **Obniżenie stopnia i odtajnienie**

Obniżenie stopnia lub odtajnienie dokumentów niejawnych UE może się odbyć tylko za zgodą sporządzającego, i jeśli to konieczne, po dyskusji z innymi zainteresowanymi stronami. Obniżenie stopnia lub odtajnienie potwierdza się na piśmie. Sporządzający odpowiedzialny jest za poinformowanie odbiorców o zmianach, a oni są odpowiednio odpowiedzialni za poinformowanie o zmianach każdego kolejnego odbiorcę, do którego wysłali lub dla którego skopiowali dokument.

Jeśli to możliwe, sporządzający określa na dokumentach niejawnych datę, okres lub zdarzenie, po którym może nastąpić obniżenie stopnia ich treści lub jej odtajnienie. W przeciwnym razie, poddają oni dokumenty rewizjom w okresach, co najmniej pięcioletnich, w celu zapewnienia, że pierwotna klasyfikacja jest niezbędna.

18. BEZPIECZEŃSTWO FIZYCZNE

18.1. **Przepisy ogólne**

Głównymi celami środków ochrony fizycznej jest zapobieganie uzyskania dostępu przez osoby nieupoważnione do informacji i/lub materiałów niejawnych UE, zapobieganie kradzieżom i niszczeniu sprzętu oraz innej własności i zapobieganie molestowaniu personelu lub każdej innej formie agresji wobec nich, innych pracowników oraz odwiedzających.

18.2. **Wymogi bezpieczeństwa**

Wszystkie pomieszczenia, tereny, budynki, pokoje, systemy łączności i systemy informatyczne, itp., w których są gromadzone i/lub użytkowane informacje i materiały niejawne UE są chronione właściwymi środkami ochrony fizycznej.

Podejmując decyzję odnośnie do stopnia koniecznych środków ochrony fizycznej należy wziąć pod uwagę wszystkie odpowiednie czynniki takie jak:

a) klasyfikacja informacji i/lub materiałów;

b) ilość i formę posiadanej informacji (np. wydruk, komputerowy nośnik pamięci);

c) lokalną ocenę zagrożenia, wywołanego przez służby wywiadowcze, których celem jest

UE, Państwa Członkowskie i/lub inne instytucje lub strony trzecie posiadające informację niejawną UE, a mianowicie w postaci sabotażu, terroryzmu i innych wywrotowych i/lub kryminalnych działań.

Stosowane środki ochrony fizycznej przeznaczone są do:

a) zapobiegania potajemnym lub siłowym wtargnięciom przez intruzów;

b) powstrzymywania, utrudniania i wykrywania działania nielojalnego personelu;

c) zapobiegania możliwości dostępu osobom, które nie potrzebują mieć dostępu do informacji niejawnej UE.

18.3. **Środki bezpieczeństwa fizycznego**

18.3.1. *Strefy bezpieczeństwa*

Strefy, w których informacje objęte klasyfikacją UE POUFNE lub wyższą, są obsługiwane i gromadzone tak, by odpowiadały jednej z następujących:

a) Strefa I klasy bezpieczeństwa: strefa, gdzie informacje klasyfikowane jako UE POUFNE lub wyżej są obsługiwane lub są gromadzone w taki sposób, że wstęp do tej strefy stanowi, pod wszelkimi względami praktycznymi, dostęp do informacji niejawnej. Taka strefa wymaga:

   (i) wyraźnie określonej i chronionej granicy, przez którą każde wejście lub wyjście podlega kontroli;

   (ii) systemu kontroli wejść, który umożliwia dostęp wyłącznie tym, którzy zostali należycie sprawdzeni i są specjalnie upoważnieni do wejścia na teren strefy;

   (iii) specyfikacji klasyfikacji informacji zazwyczaj przechowywanych w strefie, tzn. informacji, do których dostęp umożliwia wejście na teren strefy.

b) Strefa II klasy bezpieczeństwa: strefa, gdzie informacje klasyfikowane jako UE POUFNE lub wyżej są obsługiwane lub są gromadzone w taki sposób, że mogą one być chronione przed dostępem osób nieupoważnionych za pomocą środków wewnętrznej kontroli, tzn. pomieszczenia, w których zwyczajowo obsługiwane są lub są gromadzone informacje objęte klauzulą tajności UE POUFNE i w których urzędują odpowiednie służby. Taka strefa wymaga:

   (i) wyraźnie określonej i chronionej granicy, przez którą, każde wejście lub wyjście podlega kontroli;

   (ii) systemu kontroli wejść, który umożliwia wejście bez asysty wyłącznie tym, którzy zostali należycie sprawdzeni i specjalnie upoważnieni do wejścia na teren strefy; W stosunku do innych osób należy uwzględnić eskortowanie lub równoważną formę kontroli celem zapobieżenia nieupoważnionego dostępu do informacji niejawnej UE oraz niekontrolowanego wejścia do stref podlegających technicznym inspekcjom bezpieczeństwa.

Strefy, które nie są zajmowane przez personel na służbie w systemie 24 - godzinnym podlegają inspekcji niezwłocznie po zakończeniu normalnych godzin pracy, celem zagwarantowania, że informacja niejawna UE jest należycie chroniona.

18.3.2. *Strefa administracyjna*

Wokół lub na trasie wejścia do stref I lub II klasy bezpieczeństwa, można ustanowić strefy administracyjne o mniejszym stopniu bezpieczeństwa. Takie strefy wymagają widocznie określonych granic pozwalających na kontrolę personelu i pojazdów. W strefach tych mogą być obsługiwane i gromadzone wyłącznie informacje objęte klauzulą tajności UE ZASTRZEŻONE oraz informacje jawne.

18.3.3. *Kontrole wejścia i wyjścia*

Wejście do i wyjście ze stref I i II klasy bezpieczeństwa podlega kontroli za pomocą przepustek lub osobistego systemu identyfikacji, mającego zastosowanie do wszystkich członków personelu normalnie pracującego w tych strefach. Ustanawia się także system kontroli odwiedzających, przeznaczony do wykluczenia nieupoważnionego dostępu do informacji niejawnej UE. System przepustek może być wspomagany przez identyfikację automatyczną, która jednakże uważana jest za dodatkową, nie zaś jako zastępująca strażników. Zmiana w ocenie zagrożenia może spowodować wzmocnienie środków kontroli wejść i wyjść, np. w trakcie wizyt prominentnych osób.

18.3.4. *Straże patrolowe*

Patrolowanie stref I i II klasy bezpieczeństwa odbywa się poza normalnymi godzinami pracy, celem ochrony aktywów UE przed utratą, zniszczeniem lub zagubieniem. Częstotliwość patroli będzie określona z uwzględnieniem miejscowych warunków, ale jako zasada, nie powinna ona być mniejsza niż raz na 2 godziny.

18.3.5. *Szafy pancerne i skarbce*

Do gromadzenia informacji niejawnej UE używa się szaf pancernych trzech klas:

- klasa A: zatwierdzone na poziomie krajowym kasy do gromadzenia informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE w obrębie stref bezpieczeństwa klasy I lub II;

- klasa B: zatwierdzone na poziomie krajowym kasy do gromadzenia informacji objętych klauzulą tajności UE TAJNE i UE POUFNE w obrębie stref bezpieczeństwa klasy I lub II;

- klasa C: Meble służbowe nadające się wyłącznie do gromadzenia informacji objętych klauzulą tajności UE ZASTRZEŻONE.

W skarbcach, zbudowanych w strefie bezpieczeństwa klasy I lub II, oraz we wszystkich strefach bezpieczeństwa klasy I, tam gdzie informacje niejawne objęte klasyfikacją UE POUFNE lub wyższą są gromadzone na otwartych półkach lub umieszczone na kartach, mapach itp., ściany, podłogi i sufity, drzwi z zamkiem(-ami) muszą uzyskać certyfikat SAA jako dające taką samą ochronę, jak przewidziana jest dla danej klasy szaf pancernych

zatwierdzonych do gromadzenia informacji objętych tą samą klauzulą.

18.3.6. *Zamki*

Zamki używane w szafach pancernych i skarbcach, w których gromadzone są informacje niejawne UE spełniają następujące normy:

- grupa A: zatwierdzone na poziomie krajowym do szaf klasy A;

- grupa B: zatwierdzone na poziomie krajowym do szaf klasy B;

- grupa C: nadające się wyłącznie do mebli służbowych klasy C.

18.3.7. *Kontrola kluczy i szyfrów*

Klucze do szaf pancernych nie mogą być wynoszone poza teren budynków Komisji. Wiedzą na temat ustawień szyfrów do szaf pancernych dysponują wyłącznie osoby, którym jest to niezbędne. Do celu użycia w sytuacji nadzwyczajnej, urzędnik ds. Bezpieczeństwa Lokalnego Departamentu Komisji jest odpowiedzialny za posiadanie kluczy zapasowych i pisemnych wykazów każdego ustawienia szyfrów; wykazy przechowuje się w osobnych, zalakowanych i nieprzezroczystych kopertach. Klucze robocze, zapasowe klucze bezpieczeństwa oraz ustawienia szyfrów przechowywane są w osobnych szafach pancernych. Klucze te oraz ustawienia szyfrów podlegają ochronie nie mniejszej niż materiały, do których umożliwiają dostęp.

Wiedza na temat ustawienia szyfrów do szaf pancernych ograniczona jest do tak małej, jak to możliwe, liczby osób. Ustawienia są kasowane:

a) w przypadku otrzymania nowej szafy pancernej;

b) w każdym przypadku, gdy dochodzi do zmiany personelu;

c) w każdym przypadku, gdy doszło do ich ujawnienia lub gdy powstało podejrzenie ich ujawnienia;

d) w ustalonych odstępach czasu, najlepiej po upływie sześciu miesięcy, a najpóźniej po upływie dwunastu miesięcy.

18.3.8. *Urządzenia do wykrywania wtargnięć*

W sytuacji, gdy do ochrony informacji niejawnej UE używane są systemy alarmowe, wewnętrzna telewizja lub inne urządzenia elektryczne, zapewnia się dostęp do awaryjnych źródeł energii elektrycznej, umożliwiających stałą obsługę systemów w przypadku przerw w dostawach energii elektrycznej z głównego źródła. Inny podstawowy wymóg obejmuje włączenie alarmu lub innego niezawodnego sygnału ostrzegającego personel nadzoru o złym funkcjonowaniu lub o ingerowaniu w funkcjonowanie systemu.

18.3.9. *Zatwierdzony sprzęt*

Biuro ds. Bezpieczeństwa Komisji zachowuje uaktualnione wykazy według typu i modelu

sprzętu bezpieczeństwa, który został przez nie zatwierdzony do celów ochrony informacji niejawnej, stosownie do szczególnych okoliczności i warunków. Biuro ds. Bezpieczeństwa Komisji opiera te wykazy, między innymi, na informacjach z PSB.

18.3.10. *Fizyczna ochrona urządzeń kopiujących i telefaksowych*

Urządzenia kopiujące i telefaksowe podlegają fizycznej ochronie w zakresie niezbędnym do zapewnia, że wyłącznie osoby upoważnione mogą je używać do przetwarzania informacji niejawnej oraz że wszystkie niejawne produkty podlegają należytej kontroli.

18.4. **Ochrona przed nieupoważnionym wglądem i podsłuchem**

18.4.1. *Nieupoważniony wgląd*

Podejmuje się w dzień i w nocy wszelkie właściwe środki zapewniające, że do informacji niejawnej UE nie może mieć wglądu, nawet przypadkowo, osoba nieupoważniona.

18.4.2. *Podsłuch*

Służby lub strefy, w których regularnie są omawiane informacje objęte klasyfikacją UE TAJNE i wyższą, podlegają, tam gdzie ryzyko ich ujawnienia tego wymaga, ochronie przed biernymi i aktywnymi działaniami podsłuchowymi. Odpowiedzialność za ocenę ryzyka takich działań spoczywa na Biurze ds. Bezpieczeństwa Komisji, po konsultacji, jeśli to konieczne, z PSB.

18.4.3. *Wprowadzanie sprzętu elektronicznego i nagrywającego*

Zabrania się wprowadzania telefonów komórkowych, komputerów osobistych, urządzeń nagrywających, kamer i innych elektronicznych lub nagrywających urządzeń do stref bezpieczeństwa lub chronionych technicznie stref, bez uprzedniego upoważnienia ze strony szefa Biura ds. Bezpieczeństwa Komisji.

W celu ustalenia środków ochronnych, które powinny zostać podjęte w pomieszczeniach sensytywnych na podsłuch bierny (tzn. izolacja ścian, drzwi, podłóg i sufitów, pomiary odbijanych fal dźwiękowych) oraz na podsłuch aktywny (tzn. poszukiwanie mikrofonów) Biuro ds. Bezpieczeństwa Komisji może wnioskować o pomoc biegłych z PSB.

Podobnie, jeśli okoliczności tego wymagają, sprzęt telekomunikacyjny i elektryczny lub elektroniczny sprzęt biurowy jakiegokolwiek rodzaju używany w trakcie spotkań na poziomie UE TAJNE lub wyższym, może być, na wniosek szefa Biura ds. Bezpieczeństwa Komisji, kontrolowany przez specjalistów bezpieczeństwa technicznego z PSB.

18.5. **Strefy technicznie bezpieczne**

Niektóre strefy mogą być wyznaczone jako strefy technicznie bezpieczne. Przeprowadza się specjalną kontrolę wejść. Strefy te, w czasie gdy nie są zajmowane, pozostają zamknięte w zatwierdzony sposób a wszystkie klucze traktowane są jako klucze bezpieczeństwa. Strefy te podlegają regularnej kontroli fizycznej, która jest także przeprowadzana w następstwie jakiegokolwiek nieupoważnionego wejścia lub podejrzenia takiego wejścia.

Przechowuje się szczegółowy wykaz inwentarza i umeblowania celem nadzorowania jego przemieszczania. Żaden element umeblowania lub sprzętu nie może zostać wniesiony do tej strefy, zanim nie przejdzie uważnej kontroli przeprowadzonej przez odpowiednio przeszkolony personel, wyznaczony do wykrywania jakichkolwiek urządzeń podsłuchowych. Jako zasada ogólna, instalacja linii łączności w strefach technicznie bezpiecznych nie jest dopuszczalna, bez uprzedniego upoważnienia stosownego organu.

19. PRZEPISY OGÓLNE W SPRAWIE ZASADY „POWINIEN WIEDZIEĆ" ORAZ OSOBISTYCH POŚWIADCZEŃ BEZPIECZEŃSTWA UE

19.1. **Przepisy ogólne**

Upoważnienie do dostępu do informacji niejawnej UE przyznawane jest wyłącznie osobom, które objęte są zasadą „powinien wiedzieć" w celu wykonywania obowiązków służbowych lub misji. Upoważnienie do dostępu do informacji niejawnej objętej klauzulą tajności UE ŚCIŚLE TAJNE, UE TAJNE i UE POUFNE będzie przyznawane wyłącznie osobom, które posiadają właściwe poświadczenie bezpieczeństwa.

Odpowiedzialność za określenie dostępu „powinien wiedzieć" spoczywa na departamencie, w którym ma zostać zatrudniona dana osoba.

Wniosek o przeprowadzenie postępowania sprawdzającego personel pozostaje w gestii każdego departamentu.

Skutkuje to przyznaniem „osobistego poświadczenia bezpieczeństwa UE" określającego poziom informacji niejawnej, do których zweryfikowana osoba może mieć dostęp oraz datę wygaśnięcia ważności.

Osobiste poświadczenie bezpieczeństwa UE dla danej klasyfikacji może uprawniać jego posiadacza do dostępu do informacji objętej niższą klasyfikacją.

Osoby inne niż urzędnicy lub inni pracownicy, takie jak zewnętrzni kontrahenci, biegli, konsultanci, z którymi może zajść konieczność omówienia, lub w stosunku do których zachodzi potrzeba okazania informacji niejawnej UE, muszą posiadać osobiste poświadczenie bezpieczeństwa w odniesieniu do informacji niejawnej UE oraz muszą być poinformowani w skrócie o ich odpowiedzialności za bezpieczeństwo.

Publiczny dostęp pozostaje regulowany rozporządzeniem (WE) nr 1049/2001.

19.2. **Przepisy szczególne w sprawie dostępu do informacji objętych klauzulą UE ŚCIŚLE TAJNE**

Wszystkie osoby, które powinny mieć dostęp do informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE podlegają wcześniejszemu postępowaniu sprawdzającemu w zakresie dostępu do takich informacji.

Wszystkie osoby, od których wymagany jest dostęp do informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE wyznaczane są przez członka Komisji odpowiedzialnego za sprawy bezpieczeństwa, a ich nazwiska trzymane są w odpowiednim rejestrze UE ŚCIŚLE TAJNE. Biuro ds. Bezpieczeństwa Komisji stworzy i będzie prowadzić taki rejestr.

Przed uzyskaniem dostępu do informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE, wszystkie osoby podpisują zaświadczenie, że zostali w skrócie poinformowani na temat procedur bezpieczeństwa Komisji oraz że w pełni zrozumieli ich szczególną odpowiedzialność za ochronę informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE, oraz konsekwencje jakie są przewidziane przepisami UE i prawem krajowym lub przepisami administracyjnymi w sytuacji, gdy informacja niejawna przekazana zostanie w nieupoważnione ręce, bez względu na to czy umyślnie czy też w drodze zaniedbania.

W przypadku osób mających dostęp do informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE w trakcie posiedzeń, itp. właściwy urzędnik bezpieczeństwa służby lub organu, w którym zatrudniona jest osoba, powiadamia organ organizujący spotkanie, że dane osoby mają takie upoważnienie.

Nazwiska osób, które przestają wykonywać obowiązki służbowe wymagające dostępu do informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE zostają usunięte z wykazu UE ŚCIŚLE TAJNE. Dodatkowo, ponownie zwraca się uwagę tym osobom o ich szczególnej odpowiedzialności za ochronę informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE. Ponadto, podpisują one deklarację stwierdzającą, że nigdy nie będą używały ani przekazywały posiadanych informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE.

19.3. **Przepisy szczególne w sprawie dostępu do informacji objętych klauzulą UE TAJNE i UE POUFNE**

Wszystkie osoby, które powinny uzyskać dostęp do informacji objętych klauzulą UE TAJNE i UE POUFNE podlegają wcześniejszemu postępowaniu sprawdzającemu odpowiedniego stopnia.

Wszystkie osoby, które powinny uzyskać dostęp do informacji objętych klauzulą UE TAJNE i UE POUFNE zostają zaznajomione z odpowiednimi przepisami bezpieczeństwa oraz zostają pouczone o konsekwencjach zaniedbań.

W przypadku osób mających dostęp do informacji objętych klauzulą tajności UE TAJNE i UE POUFNE w trakcie posiedzeń, itp. właściwy urzędnik bezpieczeństwa organu, w którym zatrudniona jest osoba, powiadamia organ organizujący spotkanie, że dane osoby mają takie upoważnienie.

19.4. **Przepisy szczególne w sprawie dostępu do informacji objętych klauzulą UE ZASTRZEŻONE**

Osoby mające dostęp do informacji niejawnej objętej klauzulą UE ZASTRZEŻONE zostaną pouczone o przepisach bezpieczeństwa i o konsekwencjach zaniedbań.

19.5. **Przenoszenie**

W przypadku, gdy jeden z członków personelu jest przenoszony ze stanowiska wymagającego posługiwanie się materiałem niejawnym UE, Archiwum będzie nadzorować właściwe przekazywanie tego materiału od urzędnika odchodzącego urzędnikowi przychodzącemu.

W sytuacji, gdy jeden z członków personelu jest przenoszony z jednego na drugie stanowisko wymagające posługiwania się materiałem niejawnym UE, urzędnik bezpieczeństwa lokalnego odpowiednio skrótowo go pouczy.

19.6. **Specjalne instrukcje**

Osoby, od których wymagane jest posługiwanie się informacją niejawną UE powinny, podczas pierwszego przyjmowania swoich obowiązków, a następnie okresowo, być pouczone o:

a) zagrożeniach dla bezpieczeństwa wynikających z nieostrożnej rozmowy;

b) środkach ostrożności, jakie należy podjąć w stosunku do ich kontaktów z prasą lub z przedstawicielami szczególnych grup interesów;

c) zagrożeń wynikających z działalności służb wywiadowczych, których celem jest UE i Państwa Członkowskie w zakresie informacji niejawnej UE i jej działalności;

d) obowiązku niezwłocznego informowania odpowiednich organów bezpieczeństwa o każdym podejściu lub ruchu dającym podstawę do podejrzeń o działalności szpiegowskiej lub każdych niezwykłych okolicznościach odnoszących się do bezpieczeństwa.

Wszystkie osoby zwykle narażone na częste kontakty z przedstawicielami krajów, których służby wywiadowcze stawiają sobie za cel UE i Państwa Członkowskie w zakresie informacji niejawnej UE i jej działalności, zostaną pokrótce pouczone o znanych technikach wykorzystywanych przez różne służby wywiadowcze.

Nie istnieją żadne przepisy bezpieczeństwa Komisji dotyczące podróży prywatnych w jakimkolwiek kierunku przez osoby sprawdzone w zakresie dostępu do informacji niejawnej UE. Jednakże Biuro ds. Bezpieczeństwa Komisji zapozna urzędników i innych pracowników podlegających jego odpowiedzialności o przepisach dotyczących podróży, którym mogą podlegać.

20. POSTĘPOWANIE SPRAWDZAJĄCE URZĘDNIKÓW KOMISJI I INNYCH PRACOWNIKÓW

a) Tylko urzędnicy i inni pracownicy Komisji lub osoby pracujące w ramach Komisji które, z powodu ich obowiązków i wymogów służbowych potrzebują mieć wiedzę o, lub używać informacji niejawnych posiadanych przez Komisję, mają dostęp do takiej informacji.

b) W celu uzyskania dostępu do informacji niejawnej objętej klasyfikacją „UE ŚCIŚLE TAJNE", „UE TAJNE" i „UE POUFNE", osoby, określone w lit. a) muszą zostać upoważnione zgodnie z procedurą określoną w lit. c) i d) niniejszego punktu.

c) Upoważnienie zostaje udzielone wyłącznie osobom, które przeszły postępowanie sprawdzające przeprowadzone przez właściwe organy krajowe Państw Członkowskich (PSB) zgodnie z procedurą określoną w lit. i)-n).

d) Szef Biura ds. Bezpieczeństwa Komisji jest odpowiedzialny za udzielenie upoważnień, określonych w lit. a), b) i c).

e) On/ona udzieli upoważnienia po uzyskaniu opinii właściwych organów krajowych Państw Członkowskich na podstawie postępowania sprawdzającego przeprowadzonego zgodnie z lit. i)-n).

f) Biuro ds. Bezpieczeństwa Komisji zachowuje, przedłożony przez odpowiednie departamenty Komisji, uaktualniony wykaz sensytywnych stanowisk oraz wszystkich osób, którym udzielono (czasowego) upoważnienia.

g) Upoważnienie, które jest ważne przez okres pięciu lat, nie może wykraczać poza okres wykonywania zadania, na podstawie którego zostało ono przyznane. Może ono zostać odnowione zgodnie z procedurą określoną w lit. e).

h) Upoważnienie odwoływane jest przez szefa Biura ds. Bezpieczeństwa Komisji w przypadku, gdy uzna on/ona, że istnieją ku temu uzasadnione powody. Każda decyzja dotycząca odwołania upoważnienia zostanie przekazana danej osobie, która może wnioskować o wysłuchanie przez szefa Biura ds. Bezpieczeństwa Komisji oraz do właściwych organów krajowych.

i) Postępowanie sprawdzające przeprowadza się z pomocą osoby zainteresowanej i na wniosek szefa Biura ds. Bezpieczeństwa Komisji. Właściwym organem krajowym dla przeprowadzenia postępowania sprawdzającego jest organ Państwa Członkowskiego, którego obywatelem jest osoba mająca uzyskać upoważnienie. W przypadku, gdy dana osoba nie jest obywatelem Państwa Członkowskiego UE, szef Biura ds. Bezpieczeństwa Komisji wnioskuje o przeprowadzenie postępowania sprawdzającego przez Państwo Członkowskie UE, w którym osoba zamieszkuje lub ma miejsce pobytu.

j) Jako część postępowania sprawdzającego, dana osoba jest zobowiązana do wypełnienia formularza informacji osobowych.

k) Szef Biura ds. Bezpieczeństwa Komisji wyszczególnia w swoim wniosku rodzaj i poziom informacji niejawnej, która ma być dostępna dla danej osoby, tak aby właściwe organy krajowe mogły przeprowadzić postępowanie sprawdzające i wydać ich opinię stosownie do poziomu upoważnienia, które ma być udzielone tej osobie.

l) Cały proces postępowania sprawdzającego wraz z uzyskanymi wynikami podlega odpowiednim przepisom i rozporządzeniom obowiązującym w danym Państwie Członkowskim, włącznie z dotyczącymi odwołań.

m) W przypadku wydania przez właściwe organy krajowe Państwa Członkowskiego pozytywnej opinii, szef Biura ds. Bezpieczeństwa Komisji może udzielić danej osobie upoważnienie.

n) Opinia negatywna, wydana przez właściwe organy krajowe zostanie przekazana danej osobie, która może wnioskować o wysłuchanie przez szefa Biura ds. Bezpieczeństwa Komisji. Jeśli uzna on za stosowne, szef Biura ds. Bezpieczeństwa Komisji może wnioskować do właściwych organów krajowych o każde dalsze wyjaśnienia, których mogą one dostarczyć. Jeśli opinia negatywna zostanie podtrzymana, upoważnienie nie

zostaje udzielone.

o) Wszystkie osoby, które uzyskały upoważnienie w rozumieniu lit. d) i e) otrzymują, w czasie uzyskania upoważnienia, a następnie w regularnych odstępach czasu, niezbędne instrukcje dotyczące ochrony informacji niejawnej i środków zapewniających taką ochronę. Osoby te podpisują deklarację potwierdzającą otrzymanie takich instrukcji i zobowiązują się do ich przestrzegania.

p) Szef Biura ds. Bezpieczeństwa Komisji podejmuje wszelkie niezbędne środki w celu wprowadzenia w życie niniejszego punktu, w szczególności w zakresie przepisów regulujących dostęp do listy osób upoważnionych.

q) W sytuacjach wyjątkowych, jeśli wymagają tego potrzeby służby, szef Biura ds. Bezpieczeństwa Komisji może, po uprzednim powiadomieniu właściwych organów krajowych oraz z zastrzeżeniem, że nie ma z ich strony reakcji przez okres jednego miesiąca, udzielić tymczasowego upoważnienia na okres nieprzekraczający sześciu miesięcy, w oczekiwaniu na wynik postępowania sprawdzającego, określonego w lit. i).

r) Wstępne i tymczasowe upoważnienia udzielone w ten sposób nie dają dostępu do informacji niejawnej objętej klauzulą tajności UE ŚCIŚLE TAJNE; taki dostęp ograniczony jest do urzędników, którzy efektywnie przeszli postępowanie sprawdzające z wynikiem pozytywnym, zgodnie z lit. i). Oczekując na wynik postępowania sprawdzającego urzędnicy sprawdzeni w zakresie dostępu do informacji niejawnej na poziomie objętej klauzulą tajności UE ŚCIŚLE TAJNE, mogą być upoważnieni, czasowo i prowizorycznie, do dostępu do informacji niejawnej do i wyłącznie z poziomem UE TAJNE.

21. PRZYGOTOWANIE, ROZPROWADZANIE, PRZEKAZYWANIE, OSOBISTE BEZPIECZEŃSTWO KURIERÓW, ORAZ DODATKOWE KOPIE TŁUMACZEŃ I WYCIĄGÓW Z DOKUMENTÓW NIEJAWNYCH UE

21.1. **Przygotowanie**

1. Klasyfikacja UE jest stosowana, jak zostało to ustanowione w pkt. 16 i dla dokumentów objętych klauzulą tajności UE POUFNE i wyżej umieszczana jest na górze i dole po środku każdej strony, a każda strona jest ponumerowana. Każdy dokument niejawny UE posiada numer referencyjny i datę. W przypadku dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE i UE TAJNE, numer referencyjny umieszczany jest na każdej stronie. Jeśli dokumenty te mają być rozprowadzane w kilku kopiach, każdy z nich posiada numer kopii, który umieszczany jest na pierwszej stronie wraz z całkowitą liczbą stron. Wszystkie załączniki i uzupełnienia są wymienione na pierwszej stronie dokumentu objętych klauzulą tajności UE POUFNE i wyższą.

2. Dokumenty objęte klauzulą tajności UE POUFNE i wyższą są pisane, tłumaczone, gromadzone, fotokopiowane, powielane magnetycznie lub przenoszone na mikrofilmy wyłącznie przez osoby, które przeszły postępowanie sprawdzające w zakresie dostępu do informacji niejawnej co najmniej takiego poziomu klasyfikacji jak dany dokument.

3. Przepisy regulujące komputerowe wytwarzanie dokumentów niejawnych są wymienione w pkt. 25.

21.2. **Rozprowadzanie**

1. Informacje niejawne UE są rozprowadzane wyłącznie między osobami objętymi zasadą „powinien wiedzieć” i mającymi właściwe poświadczenie bezpieczeństwa. Sporządzający wyszczególnia pierwotne rozprowadzenie.

2. Dokumenty objęte klauzulą tajności UE ŚCIŚLE TAJNE są wprowadzane do obiegu za pośrednictwem archiwów UE ŚCIŚLE TAJNE (patrz ppkt 22.2). W przypadku wiadomości objętych klauzulą tajności UE ŚCIŚLE TAJNE, właściwe archiwum może upoważnić szefa centrum łączności do wykonania liczby kopii wyszczególnionych w wykazie adresatów.

3. Dokumenty klasyfikowane jako UE TAJNE i niżej mogą być ponownie rozprowadzane przez pierwotnego adresata do innych adresatów w oparciu o zasadę „powinien wiedzieć”. Jednakże organy sporządzające wyraźnie przedstawiają ograniczenia, jakie chcą nałożyć. W każdym przypadku, gdy takie ograniczenia są nałożone, adresaci mogą ponownie rozprowadzać dokumenty wyłącznie za upoważnieniem organów sporządzających.

4. Każdy dokument sklasyfikowany jako UE POUFNE i wyżej, podczas wchodzenia lub wychodzenia z DG lub służby, zapisywany jest przez lokalne archiwum EUCI danego departamentu. Należy wprowadzić takie szczegółowe dane dotyczące dokumentów (numery, datę i, gdzie ma to zastosowanie, numer kopii) tak, aby można było je zidentyfikować oraz wprowadzić do dziennika lub do specjalnie chronionego środka komputerowego (patrz ppkt 22.1).

21.3. **Przekazywanie dokumentów niejawnych UE**

21.3.1. *Pakowanie, potwierdzanie odbioru*

1. Dokumenty sklasyfikowane jako UE POUFNE i wyżej przekazywane są w mocnych, nieprzeźroczystych i podwójnych kopertach. Wewnętrzna koperta oznaczona jest właściwą klasyfikacją bezpieczeństwa UE a także, jeśli to możliwe, wszelkimi danymi szczegółowymi dotyczącymi tytułu służbowego odbiorcy oraz adresem.

2. Wyłącznie urzędnik kontroli archiwum (patrz ppkt 22.1), lub jego zastępca mogą otworzyć wewnętrzną kopertę i potwierdzić odbiór załączonego dokumentu, chyba że koperta jest adresowana do konkretnej osoby. W takim przypadku odpowiednie archiwum (patrz ppkt 22.1) wpisuje do dziennika dojście koperty, a tylko konkretna osoba, do której jest ona adresowana może ją otworzyć i potwierdzić otrzymanie dokumentów, które ona zawiera.

3. Formularz potwierdzania odbioru umieszcza się w wewnętrznej kopercie. Potwierdzenie odbioru, które nie jest klasyfikowane, powinno zawierać numer referencyjny, datę i numer kopii dokumentu, ale nigdy nie jego przedmiot.

4. Wewnętrzna koperta jest zamknięta w zewnętrznej kopercie noszącej numer przesyłki do celów potwierdzenia odbioru. W żadnych okolicznościach klasyfikacja bezpieczeństwa nie jest umieszczana na zewnętrznej kopercie.

5. Dla dokumentów sklasyfikowanych jako UE POUFNE i wyżej, kurierzy i posłańcy uzyskują potwierdzenie odbioru według numeru przesyłki.

21.3.2. *Przekazywanie w ramach budynku lub grupy budynków*

W ramach danego budynku lub grupy budynków dokumenty niejawne mogą być przenoszone w ostemplowanej kopercie oznaczonej wyłącznie nazwiskiem adresata, pod warunkiem, że są one przenoszone przez osoby sprawdzone do poziomu klasyfikacji danych dokumentów.

21.3.3. *Przekazywanie w ramach jednego kraju*

1. W ramach jednego kraju dokumenty objęte klauzulą tajności UE ŚCIŚLE TAJNE powinny być przesyłane wyłącznie za pomocą urzędowych służb posłańców lub przez osoby upoważnione do dostępu do informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE.

2. W każdym przypadku, gdy służba posłańców jest wykorzystywana do przekazywania dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE poza obrębem budynku lub grupy budynków stosuje się przepisy niniejszego rozdziału dotyczące pakowania i potwierdzania odbioru. Służby dostawcze są tak dobrane, aby zapewniały, że przesyłki zawierające dokumenty objęte klauzulą tajności UE ŚCIŚLE TAJNE pozostawały przez cały czas pod bezpośrednim nadzorem odpowiedzialnego urzędnika.

3. Wyjątkowo, dokumenty objęte klauzulą tajności UE ŚCIŚLE TAJNE mogą być wyniesione przez urzędnika, innego niż posłaniec, poza obręb budynku lub grupy budynków w celu lokalnego użycia na spotkaniach i dyskusjach, z zastrzeżeniem że:

   a) przenoszący jest upoważniony do dostępu do dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE;

   b) sposób transportu jest zgodny z przepisami regulującymi przekazywanie dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE;

   c) w żadnych okolicznościach urzędnik nie pozostawia dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE poza kontrolą;

   d) zapewnia się, aby wykaz dokumentów tak przenoszonych, był przechowywany w archiwum UE ŚCIŚLE TAJNE przechowującym te dokumenty i zarejestrowany w dzienniku oraz kontrolowany na podstawie tego rejestru przy ich powrocie.

4. W ramach danego kraju, dokumenty objęte klauzulą tajności UE TAJNE i UE POUFNE, mogą być wysyłane albo pocztą, jeśli takie przekazywanie jest dopuszczone przez przepisy krajowe i zgodnie z przepisami niniejszej regulacji, albo za pośrednictwem służb posłańców lub osób sprawdzonych w zakresie dostępu do informacji niejawnej UE.

5. Biuro ds. Bezpieczeństwa Komisji przygotuje, oparte na niniejszych przepisach, instrukcje w sprawie osobistego przenoszenia dokumentów niejawnych UE. Osoba przenosząca jest zobowiązana do przeczytania i podpisania tych instrukcji. W

szczególności instrukcje te wyraźnie wskazują, że w żadnych okolicznościach dokumenty nie mogą być:

a) pozbawione władania przez osobę przenosząca, chyba że znajdują się pod ścisłą pieczą zgodnie z przepisami zawartymi w pkt. 18;

b) pozostawione bez kontroli w publicznych środkach transportu lub prywatnym pojeździe, lub w miejscach takich, jak restauracje lub hotele. Nie mogą być gromadzone w sejfach hotelowych lub pozostawiane w pokojach hotelowych bez kontroli;

c) czytane w miejscach publicznych takich jak samolot lub pociągi.

21.3.4. *Przekazywanie z jednego Państwa Członkowskiego do drugiego*

1. Materiały klasyfikowane jako UE POUFNE i wyżej są przekazywane za pomocą dyplomatycznych lub wojskowych służb kurierskich.

2. Jednakże, osobisty przewóz materiałów, klasyfikowanych jako UE TAJNE i UE POUFNE, może być dopuszczony, jeśli przepisy dotyczące tego przewozu są tego rodzaju, iż zapewniają, że nie mogą one dostać się w ręce nieupoważnionej osoby.

3. Członek Komisji odpowiedzialny za sprawy bezpieczeństwa może wydać upoważnienie do osobistego przewozu w sytuacji, gdy dyplomatyczne lub wojskowe służby kurierskie nie są dostępne lub gdy użycie tych kurierów mogłoby skutkować opóźnieniem, które byłoby szkodliwe dla działań UE a materiał jest pilnie potrzebny wskazanemu odbiorcy. Biuro ds. Bezpieczeństwa Komisji przygotuje instrukcje, obejmujące międzynarodowy osobisty przewóz przez osoby inne niż kurierzy dyplomatyczni lub wojskowi, materiałów klasyfikowanych do i na poziomie UE TAJNE. Instrukcja wymaga, aby:

a) osoba przewożąca miała właściwe poświadczenie bezpieczeństwa;

b) odpowiedni departament Komisji lub archiwum przechowywały rejestr wszystkich materiałów przewożonych w ten sposób;

c) pakunki lub torby, zawierające materiały UE nosiły urzędową pieczęć, celem zapobieżenia lub zniechęcenia inspekcji przez służby celne oraz, aby zawierały oznaczenia z ich identyfikacją i instrukcją dla znalazcy;

d) osoba przewożąca posiadała list kurierski i/lub polecenie misji uznawane przez Państwa Członkowskie UE, upoważniające go do przewożenia przesyłki tak oznaczonej;

e) w trakcie podróży lądowej nie wolno poruszać się po ani przekraczać żadnej granicy państwa nieczłonkowskiego UE, chyba że państwo wysyłające ma szczególne gwarancje tego państwa;

f) organizacja podróży przewożącego w odniesieniu do przeznaczenia, wybranych tras i używanych środków transportu jest w zgodzie z przepisami UE lub – jeśli krajowe przepisy w tym zakresie są bardziej surowe – zgodnie z tymi przepisami;

g) nie wolno było pozostawiać materiału poza władaniem przewożącego, chyba że jest przechowywany zgodnie z przepisami dotyczącymi ścisłej pieczy, zawartymi w pkt. 18;

h) nie wolno było pozostawiać materiału bez kontroli w publicznych lub prywatnych pojazdach lub w miejscach takich jak restauracje czy hotele. Nie wolno go gromadzić w sejfach hotelowych lub pozostawiać bez kontroli w pokojach hotelowych;

i) jeśli przewożony materiał zawiera dokumenty, nie mogą one być czytane w miejscach publicznych (tzn. w samolocie, pociągach, itp.).

4. Osoba wyznaczona do przewozu materiału niejawnego musi przeczytać i podpisać skrót przepisów bezpieczeństwa, który zawiera, jako minimum, instrukcje wymienione powyżej oraz procedury, które należy wypełnić w sytuacjach zagrożenia lub w przypadkach, gdy przesyłka zawierająca materiały niejawne jest kwestionowana przez służby celne lub urzędników bezpieczeństwa na lotnisku.

21.3.5. *Przekazywanie dokumentów objętych klauzulą UE zastrzeżone*

Nie ustanawia się żadnych specjalnych przepisów dotyczących przekazywanie dokumentów objętych klauzulą tajności UE ZASTRZEŻONE, z wyjątkiem tego, że nie mogą one dostać się w ręce osoby nieupoważnionej.

21.4. **Bezpieczeństwo kurierów**

Wszyscy kurierzy i posłańcy zatrudnieni do przenoszenia dokumentów objętych klauzulą tajności UE TAJNE i UE POUFNE podlegają stosownemu postępowaniu sprawdzającemu.

21.5. **Elektroniczne i inne środki technicznego przekazu**

1. Środki bezpiecznej łączności przeznaczone są do zapewnienia ochrony przekazu informacji niejawnej UE. Szczegółowe przepisy mające zastosowanie do przekazywania takiej informacji niejawnej UE omówione są w pkt. 25.

2. Wyłącznie akredytowane centra i sieci łączności i/lub terminale i systemy mogą przekazywać informacje sklasyfikowane jako UE POUFNE i UE TAJNE.

21.6. **Dodatkowe kopie i tłumaczenia oraz wyciągi z dokumentów niejawnych UE**

1. Wyłącznie sporządzający może zatwierdzić kopię lub tłumaczenie dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE.

2. Jeśli osoba niesprawdzona w kontekście dostępu do informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE żąda dostępu do informacji, która jakkolwiek zawarta jest w dokumencie objętym klauzulą tajności UE ŚCIŚLE TAJNE, nie posiada tej klasyfikacji, szef archiwum UE ŚCIŚLE TAJNE (patrz ppkt 22.2) może zostać upoważniony do sporządzenia niezbędnej liczby wyciągów z tego dokumentu. On/ona podejmuje, w tym samym czasie, niezbędne środki zapewniające, że te wyciągi mają

przyznaną odpowiednią klasyfikację bezpieczeństwa.

3. Dokumenty sklasyfikowane jako UE TAJNE i niżej mogą być powielane i tłumaczone przez adresata, w ramach niniejszych przepisów bezpieczeństwa i pod warunkiem, że odpowiadają one ściśle zasadzie „powinien wiedzieć". Środki bezpieczeństwa mające zastosowanie do oryginalnego dokumentu stosuje się także do kopii i/lub ich tłumaczeń.

22. ARCHIWA INFORMACJI NIEJAWNEJ UE (EUCI), PRZEGLĄDY, KONTROLOWANIE, ARCHIWIZACJA I NISZCZENIE EUCI

22.1. **Lokalne archiwa EUCI**

1. W ramach Komisji, w każdym departamencie, jeśli istnieje taka potrzeba, jedno lub więcej lokalnych archiwów EUCI jest odpowiedzialnych za rejestrację, powielanie, wysyłanie, archiwizowanie i niszczenie dokumentów sklasyfikowanych jako UE TAJNE i UE POUFNE.

2. W przypadku, gdy departament nie posiada lokalnego archiwum EUCI, lokalne archiwum EUCI Sekretariatu Generalnego będzie działać jako jej archiwum EUCI.

3. Lokalne archiwa EUCI powiadamiają szefa tego departamentu, od kogo otrzymują swoje instrukcje. Szefem tych archiwów będzie urzędnik kontroli archiwów (RCO).

4. Podlegają one nadzorowi lokalnego urzędnika ds. Bezpieczeństwa w takim zakresie w jakim dotyczy to stosowania przepisów dotyczących posiadania dokumentów EUCI i zgodności z odpowiadającymi im środkami bezpieczeństwa.

5. Urzędnicy przydzieleni do lokalnych archiwów EUCI są upoważnieni do posiadania dostępu do EUCI zgodnie z pkt. 20.

6. Pod nadzorem odpowiedniego szefa departamentu lokalne archiwa EUCI:

   a) zarządzają czynnościami odnoszącymi się do rejestracji, powielania, tłumaczenia, przekazywania, wysyłki i niszczenia takich informacji;

   b) uaktualniają wykaz danych szczegółowych w sprawie informacji niejawnej;

   c) okresowo sprawdzają konieczność utrzymania klasyfikacji informacji.

7. Lokalne archiwa EUCI prowadzą rejestry dotyczące następujących danych szczegółowych:

   a) daty sporządzenia informacji niejawnej;

   b) poziomu klasyfikacji;

   c) daty ważności klasyfikacji;

   d) nazwiska i departament emitenta;

e) odbiorcy lub odbiorców, z numerami seryjnymi;

f) przedmiotu;

g) numeru;

h) numerów rozpowszechnionych kopii;

i) przygotowania spisów informacji niejawnych przysłanych do departamentu;

j) rejestru odtajniania i obniżania stopnia informacji niejawnej.

8. Ogólne przepisy, przewidziane w pkt. 21 mają zastosowanie do lokalnych archiwów. EUCI, chyba że zostały zmodyfikowane przez szczególne przepisy ustanowione w niniejszym punkcie.

22.2. **Archiwum UE ŚCIŚLE TAJNE**

22.2.1. *Przepisy ogólne*

1. Centralne archiwum UE ŚCIŚLE TAJNE zapewnia rejestrowanie, dysponowanie i rozpowszechnianie dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE, zgodnie z niniejszymi przepisami bezpieczeństwa. Szef archiwum UE ŚCIŚLE TAJNE jest urzędnikiem kontroli archiwum UE ŚCIŚLE TAJNE.

2. Centralne archiwum UE ŚCIŚLE TAJNE działa jako główny organ przyjmujący i wysyłający w Komisji, w relacjach z innymi instytucjami UE, Państwami Członkowskimi, organizacjami międzynarodowymi i państwami trzecimi, z którymi Komisja ma porozumienia w sprawie procedur bezpieczeństwa dotyczących wymiany informacji niejawnej.

3. W przypadku konieczności, można ustanawiać archiwa pomocnicze, odpowiedzialne za wewnętrzne zarządzanie dokumentami objętymi klauzulą tajności UE ŚCIŚLE TAJNE; utrzymują one uaktualnione rejestry obiegu każdego dokumentu pozostającego w pod kontrolą archiwum pomocniczego.

4. Archiwa pomocnicze UE ŚCIŚLE TAJNE są ustanowione tak, jak to określono w ppkt. 22.2.3, odpowiadając na potrzeby długoterminowe i są dołączone do archiwum centralnego UE ŚCIŚLE TAJNE. Jeśli zachodzi tylko potrzeba czasowej lub okazjonalnej konsultacji dotyczącej dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE, dokumenty te mogą być udostępniane bez konieczności ustanawiania archiwum pomocniczego UE ŚCIŚLE TAJNE, z zastrzeżeniem, że ustanowione są przepisy zapewniające, że pozostają one pod kontrolą odpowiedniego archiwum UE ŚCIŚLE TAJNE i że wszystkie fizyczne i dotyczące personelu środki bezpieczeństwa są zachowane.

5. Archiwa pomocnicze nie mogą przekazywać dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE bezpośrednio do innych archiwów pomocniczych tego samego archiwum centralnego UE ŚCIŚLE TAJNE bez wyraźnego przez nie zatwierdzenia.

6. Wszelka wymiana dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE między archiwami pomocniczymi niepołączonymi z tymi samymi archiwami centralnymi odbywa się za pośrednictwem archiwów centralnych UE ŚCIŚLE TAJNE.

22.2.2. *Centralne archiwum UE ŚCIŚLE TAJNE*

Szef archiwum centralnego UE ŚCIŚLE TAJNE jako urzędnik kontroli, jest odpowiedzialny za:

a) przekazywanie dokumentów objętych klauzulą tajności UE ŚCIŚLE zgodnie przepisami określonymi w ppkt. 21.3;

b) utrzymywanie wykazu wszystkich podległych archiwów pomocniczych UE ŚCIŚLE TAJNE włącznie z nazwiskami i podpisami mianowanych urzędników kontroli oraz ich upoważnionych zastępców;

c) przechowywanie potwierdzeń odbioru z archiwum dla wszystkich dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE rozprowadzonych przez centralne archiwum;

d) utrzymywanie rejestru posiadanych i rozprowadzonych dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE;

e) utrzymywanie uaktualnionego wykazu wszystkich centralnych archiwów. UE ŚCIŚLE TAJNE, z którymi on/ona zazwyczaj koresponduje, włącznie z nazwiskami i podpisami ich wyznaczonych urzędników kontroli oraz ich upoważnionych zastępców;

f) fizyczną ochronę wszystkich dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE posiadanych w ramach archiwum zgodnie z przepisami zawartymi w pkt. 18.

22.2.3. *Archiwa pomocnicze UE ŚCIŚLE TAJNE*

Szef archiwum pomocniczego UE ŚCIŚLE TAJNE jako urzędnik kontroli jest odpowiedzialny za:

a) przekazywanie dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE zgodnie z przepisami zawartymi w ppkt. 21.3;

b) utrzymywanie uaktualnionej listy wszystkich osób upoważnionych do posiadania dostępu do informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE, znajdujących się pod jego kontrolą;

c) rozprowadzanie dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE, zgodnie z instrukcjami sporządzającego lub na zasadzie „powinien wiedzieć”, uprzednio kontrolując czy adresat ma wymagane poświadczenie bezpieczeństwa;

d) utrzymywanie uaktualnionego rejestru wszystkich dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE posiadanych lub rozprowadzonych pod jego kontrolą lub przekazanych do innego archiwum UE ŚCIŚLE TAJNE oraz posiadanie wszelkich niezbędnych potwierdzeń odbioru;

e) utrzymywanie uaktualnionego wykazu archiwów UE ŚCIŚLE TAJNE, z którymi jest on upoważniony do wymiany dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE, łącznie z nazwiskami i podpisami ich urzędników kontroli oraz ich upoważnionych zastępców;

f) fizyczną ochronę wszystkich dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE posiadanych w ramach archiwum pomocniczego zgodnie z przepisami ustanowionymi w pkt. 18.

22.3. **Inwentaryzacje, przeglądy i sprawdzanie dokumentów niejawnych UE**

1. Każdego roku każde archiwum UE ŚCIŚLE TAJNE, określone w niniejszym podpunkcie, przeprowadza inwentaryzację wszystkich pozycji dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE. Dokument uznaje się za policzony, jeśli archiwum dokonało jego fizycznego przeglądu, lub posiada potwierdzenie odbioru z archiwum UE ŚCIŚLE TAJNE, do którego dokument został przekazany, poświadczenie zniszczenia dokumentu lub instrukcję obniżenia stopnia lub odtajnienia dokumentu. Wyniki rocznych inwentaryzacji przesyłane są członkowi Komisji odpowiedzialnemu za sprawy bezpieczeństwa, najpóźniej przed dniem 1 kwietnia każdego roku.

2. Archiwa pomocnicze UE ŚCIŚLE TAJNE przesyłają wyniki ich rocznych inwentaryzacji centralnemu archiwum, przed którym są odpowiedzialne, w dniu wskazanym przez nie.

3. Dokumenty UE sklasyfikowane poniżej poziomu UE ŚCIŚLE TAJNE podlegają wewnętrznym kontrolom zgodnie z instrukcjami przekazanymi przez członka Komisji odpowiedzialnego za sprawy bezpieczeństwa.

4. Czynności te tworzą możliwość wyrażenia opinii posiadacza w odniesieniu do:

   a) możliwości obniżenia stopnia lub odtajnienia niektórych dokumentów;

   b) dokumentów przeznaczonych do zniszczenia.

22.4. **Archiwizacja informacji niejawnych UE**

1. EUCI są przechowywane w takich warunkach, że spełniają one wszystkie wymogi wymienione w pkt. 18.

2. Celem zminimalizowania problemów związanych z gromadzeniem, urzędnicy kontroli wszystkich archiwów są upoważnieni do utrwalania dokumentów objętych klauzulą tajności UE ŚCIŚLE TAJNE, UE TAJNE i UE POUFNE na mikrofilmach lub innego ich gromadzenia na magnetycznych lub optycznych środkach zapisu do celów archiwalnych, z zastrzeżeniem że:

   a) proces utrwalania na mikrofilmach / gromadzenia jest przeprowadzany przez personel sprawdzony w odniesieniu do odpowiedniego poziomu klasyfikacji;

   b) nośnik mikrofilmu / gromadzenia ma przyznaną taką sama ochronę jak oryginalne

dokumenty;

c) o utrwalaniu na mikrofilmach / przechowywaniu każdego dokumentu objętego klauzulą tajności UE ŚCIŚLE TAJNE jest powiadamiany sporządzający;

d) rolki filmu lub innego rodzaju nośniki zawierają wyłącznie dokumenty objęte tą samą klasyfikacją UE ŚCIŚLE TAJNE, UE TAJNE lub UE POUFNE;

e) utrwalanie na mikrofilmach / przechowywanie dokumentu objętego klauzulą tajności UE ŚCIŚLE TAJNE lub UE TAJNE jest wyraźnie wskazane w rejestrze używanym do celów rocznego inwentarza;

f) oryginalne dokumenty, które mają zostać utrwalone na mikrofilmach lub w inny sposób gromadzone, są zniszczone zgodnie z przepisami wymienionymi w ppkt. 22.5.

3. Niniejsze przepisy maja także zastosowanie do każdej innej formy upoważnionego gromadzenia, takich jak nośniki elektromagnetyczne i dyski optyczne.

22.5. **Niszczenie dokumentów niejawnych UE**

1. Celem zapobieżenia zbędnej kumulacji dokumentów niejawnych UE, te z nich, które zostały uznane przez szefa placówki, która je posiada, za przedawnione i zbędne są niszczone tak szybko jak to możliwe, w następujący sposób:

a) dokumenty objęte klauzulą UE ŚCIŚLE TAJNE są niszczone wyłącznie przez centralne archiwum odpowiedzialne za nie. Każdy zniszczony dokument jest wyszczególniony w poświadczeniu zniszczenia, podpisanym przez urzędnika kontroli UE ŚCIŚLE TAJNE i przez urzędnika będącego świadkiem zniszczenia, który jest objęty postępowaniem sprawdzającym w odniesieniu do UE ŚCIŚLE TAJNE. Adnotacja o takim charakterze zostaje wprowadzona do dziennika;

b) archiwum przechowuje poświadczenia zniszczenia, wraz z notatką o rozpowszechnianiu, przez okres dziesięciu lat. Kopie zostają przekazane do sporządzającego lub do właściwego centralnego archiwum, jedynie wtedy gdy zostało to wyraźnie zażądane;

c) dokumenty objęte klauzulą UE ŚCIŚLE TAJNE, włączając w to wszystkie niejawne pozostałości powstałe na skutek przygotowywania dokumentów objętych klauzulą UE ŚCIŚLE TAJNE, takie jak zniszczone kopie, robocze projekty, drukowane notatki, dyski miękkie są niszczone pod nadzorem urzędnika kontroli archiwum UE ŚCIŚLE TAJNE, poprzez spalenie, zmielenie, poszatkowanie lub w inny sposób redukujący do nierozpoznawalnej i niemożliwej do odtworzenia formy.

2. Dokumenty objęte klauzulą UE TAJNE są niszczone przez archiwum odpowiedzialne za te dokumenty, pod nadzorem osoby posiadającej poświadczenie bezpieczeństwa, z użyciem jednego z procesów wskazanych w ust. 1 lit. c). Dokumenty UE TAJNE, które mają zostać zniszczone są wyszczególnione w podpisanych poświadczeniach zniszczenia, zachowywanych przez archiwum wraz z formularzami rozprowadzania

przez okres co najmniej trzech lat.

3. Dokumenty objęte klauzulą UE POUFNE są niszczone przez archiwa odpowiedzialne za te dokumenty, pod nadzorem osoby posiadającej poświadczenie bezpieczeństwa, z użyciem jednego z procesów wskazanych w ust. 1 lit. c). Ich zniszczenie zostanie odnotowane zgodnie z instrukcjami przekazanymi przez członka Komisji odpowiedzialnego za sprawy bezpieczeństwa.

4. Dokumenty objęte klauzulą UE ZASTRZEŻONE są niszczone przez archiwa odpowiedzialne za te dokumenty lub przez ich użytkownika, zgodnie z instrukcjami przekazanymi przez członka Komisji odpowiedzialnego za sprawy bezpieczeństwa.

22.6. **Niszczenie w sytuacjach nadzwyczajnych**

1. Departamenty Komisji przygotowują plany, oparte o lokalne warunki, dotyczące ochrony materiałów niejawnych UE w sytuacjach kryzysowych, włączając w to, jeśli to niezbędne, plany niszczenia w sytuacjach nadzwyczajnych i plany ewakuacji. Wydają one takie instrukcje, które uważane są za niezbędne dla zapobieżenia przedostania się informacji niejawnej UE w nieupoważnione ręce.

2. Ustalenia dotyczące ochrony i/lub zniszczenia materiałów objętych klauzulą tajności UE TAJNE i UE POUFNE w sytuacjach kryzysowych, w żadnych okolicznościach nie mogą negatywnie wpływać na ochronę lub zniszczenie materiałów objętych klauzulą tajności UE ŚCIŚLE TAJNE, włączając w to sprzęt szyfrujący, którego traktowanie ma priorytet nad wszystkimi innymi zadaniami.

3. Środki, które mają być przyjęte, dotyczące ochrony i zniszczenia sprzętu szyfrującego w stanach nadzwyczajnych, są określone w szczególnych instrukcjach.

4. Instrukcje powinny być dostępne na miejscu w zalakowanej kopercie. Środki / narzędzia zniszczenia muszą być dostępne.

23. ŚRODKI BEZPIECZEŃSTWA SZCZEGÓLNYCH POSIEDZEŃ KOMISJI ODBYWAJĄCYCH SIĘ POZA JEJ POMIESZCZENIAMI I Z UŻYCIEM INFORMACJI NIEJAWNEJ UE

23.1. **Przepisy ogólne**

W przypadku, gdy posiedzenie Komisji lub inne ważne spotkanie odbywa się poza pomieszczeniami Komisji i gdzie jest to uzasadnione określonymi wymogami bezpieczeństwa dotyczącymi wysokiej sensytywności omawianego zagadnienia lub informacji, podejmuje się środki bezpieczeństwa opisane poniżej. Środki te dotyczą wyłącznie ochrony informacji niejawnej UE; można zaplanować inne środki bezpieczeństwa.

23.2. **Odpowiedzialność**

23.2.1. *Biuro ds. Bezpieczeństwa Komisji*

Biuro ds. Bezpieczeństwa Komisji współpracuje z właściwymi organami Państwa Członkowskiego, na terytorium którego odbywa się posiedzenie (przyjmujące Państwo

Członkowskie), w celu zapewnienia bezpieczeństwa posiedzeń Komisji lub innych ważnych posiedzeń oraz dla bezpieczeństwa delegatów i ich personelu. W odniesieniu do ochrony bezpieczeństwa, powinno ono w szczególności zapewnić, że:

a) przygotowano plany na wypadek zagrożenia bezpieczeństwa i zdarzeń odnoszących się do zagadnień bezpieczeństwa, niezbędnych środków dotyczących w szczególności ścisłej pieczy nad dokumentami niejawnymi UE w biurach;

b) podjęto środki przewidujące możliwość dostępu do systemów łączności Komisji do celów odbierania i przekazywania wiadomości niejawnej UE. Przyjmujące Państwo Członkowskie może być poproszone o zapewnienie dostępu, jeśli to niezbędne, do chronionych systemów telefonicznych.

Biuro ds. Bezpieczeństwa Komisji działa jako doradca ds. Bezpieczeństwa w przygotowaniach do posiedzenia; powinno ono być tam reprezentowane w celu udzielenia pomocy i porady urzędnikowi ds. Bezpieczeństwa Posiedzenia (MSO) i delegacjom, jeśli zajdzie taka potrzeba.

Każda delegacja na posiedzenie proszona jest o wyznaczenie urzędnika ds. Bezpieczeństwa, który będzie odpowiedzialny za zajmowanie się sprawami bezpieczeństwa w ramach jego/jej delegacji i utrzymywania łączności z urzędnikiem ds. Bezpieczeństwa Posiedzenia, a także z przedstawicielem Biura ds. Bezpieczeństwa Komisji, jeśli będzie to niezbędne.

23.2.2. *Urzędnik ds. Bezpieczeństwa Posiedzenia (MSO)*

Wyznacza się urzędnika ds. Bezpieczeństwa Posiedzenia, który jest odpowiedzialny za ogólne przygotowanie i kontrolę ogólnych wewnętrznych środków bezpieczeństwa oraz do celów koordynacji z innymi zaangażowanymi organami bezpieczeństwa. Środki podejmowane przez MSO w zasadzie odnoszą się do:

a) środków ochronnych na miejscu posiedzenia w celu zapewnienia, że posiedzenie odbędzie się bez żadnych incydentów, które mogą narazić na utratę wykorzystywanych tam informacji niejawnych UE;

b) kontrolowania personelu, którego dostęp do miejsca posiedzenia, stref wyznaczonych dla delegacji i pomieszczeń konferencyjnych jest dozwolony oraz do kontrolowania każdego sprzętu;

c) stałej koordynacji z właściwymi organami przyjmującego Państwa Członkowskiego i z Biurem ds. Bezpieczeństwa Komisji;

d) włączenia instrukcji bezpieczeństwa do dokumentów posiedzenia, w poszanowaniu wymogów wymienionych w tych przepisach bezpieczeństwa i każdych innych instrukcjach bezpieczeństwa uważanych za niezbędne.

23.3. **Środki bezpieczeństwa**

23.3.1. *Strefy bezpieczeństwa*

Ustanawia się następujące strefy bezpieczeństwa:

a) strefa bezpieczeństwa klasy II, składająca się z pokoju przygotowawczego, biur Komisji i sprzętu powielającego, a także biur delegacji, jeśli to stosowne;

b) strefa bezpieczeństwa klasy I, składająca się z sali konferencyjnej oraz kabin tłumaczy i operatorów dźwięku;

c) strefy administracyjne, składające się ze strefy prasowej i tych części miejsca posiedzenia, które używane są do celów administracyjnych, cateringu i zakwaterowania, a także strefy bezpośrednio sąsiadujące z centrum prasowym i miejscem posiedzenia.

23.3.2. *Przepustki*

MSO na wniosek delegacji wydaje odpowiednie odznaki zgodnie z ich potrzebami. Tam gdzie to niezbędne, należy uczynić rozróżnienie w odniesieniu do dostępu do różnych stref bezpieczeństwa.

Instrukcje bezpieczeństwa na potrzeby posiedzenia wymagają, aby wszystkie osoby nosiły i okazywały swoje odznaki widoczne podczas całego czasu przebywania na terenie miejsca posiedzenia, tak aby mogły być sprawdzane, jeśli zajdzie taka potrzeba, przez personel bezpieczeństwa.

Niezależnie od uczestników, posiadaczy odznak, tak ograniczona liczba osób jak to możliwe ma dostęp do miejsca posiedzenia. MSO zezwala wyłącznie krajowym delegacjom na przyjmowanie gości w czasie trwania posiedzenia na ich wniosek. Goście powinni otrzymać odznaki dla gości. Gość wypełnia formularz przepustki gościa zawierający jego/jej nazwisko oraz nazwisko osoby odwiedzanej. Gościom towarzyszy przez cały czas strażnik lub odwiedzana osoba. Formularz przepustki gościa jest noszony przez osobę towarzyszącą, która zwraca go wraz z odznaką do personelu bezpieczeństwa po opuszczeniu przez gościa miejsca posiedzenia.

23.3.3. *Kontrola sprzętu fotograficznego i sprzętu audio*

Nie wolno wnosić aparatów fotograficznych lub sprzętu nagrywającego do strefy bezpieczeństwa klasy I, z wyjątkiem sprzętu przyniesionego przez fotografów lub operatorów dźwięku należycie upoważnionych przez MSO.

23.3.4. *Sprawdzanie teczek, przenośnych komputerów i paczek*

Posiadacze przepustek mający dostęp do strefy bezpieczeństwa mogą normalnie, bez kontrolowania, wnosić swoje teczki i przenośne komputery (wyłącznie z własnym systemem zasilania). W przypadku paczek dla delegacji, delegacje mogą przyjąć ich dostawę, która podlegać będzie inspekcji przeprowadzonej albo przez urzędnika ds. Bezpieczeństwa Delegacji, albo prześwietlona za pomocą specjalnego sprzętu lub otwarta przez personel bezpieczeństwa celem przeprowadzenia inspekcji. Jeśli MSO uzna to za niezbędne, można ustanowić bardziej rygorystyczne środki dotyczące inspekcji teczek i paczek.

23.3.5. *Bezpieczeństwo techniczne*

Sala posiedzeń może być technicznie zabezpieczona przez zespół techników bezpieczeństwa,

którzy mogą także prowadzić elektroniczny nadzór w trakcie posiedzenia.

23.3.6. *Dokumenty delegacji*

Delegacje są odpowiedzialne za przynoszenie dokumentów niejawnych UE na i z posiedzeń. Są one także odpowiedzialne za weryfikację i bezpieczeństwo tych dokumentów w czasie ich używania w powierzonych im pomieszczeniach. Można domagać się pomocy przyjmującego Państwa Członkowskiego przy transporcie dokumentów niejawnych do i z miejsca posiedzenia.

23.3.7. *Ścisła piecza nad dokumentami*

Jeśli Komisja lub delegacje nie są w stanie przechowywać ich dokumentów niejawnych zgodnie z zatwierdzonymi normami, mogą one przekazać, za potwierdzeniem odbioru, te dokumenty w zalakowanej kopercie urzędnikowi ds. Bezpieczeństwa Posiedzenia tak, aby mógł on przechowywać te dokumenty zgodnie z zatwierdzonymi normami.

23.3.8. *Sprawdzanie biur*

Urzędnik ds. Bezpieczeństwa Posiedzenia organizuje, na koniec każdego dnia roboczego, inspekcje biur Komisji i delegacji dla zapewnienia, że wszystkie dokumenty niejawne są trzymane w bezpiecznym miejscu. W przeciwnym razie on/ona podejmuje właściwe środki.

23.3.9. *Usuwanie pozostałości materiałów niejawnych UE*

Wszystkie pozostałości będą traktowane jako pozostałości materiałów niejawnych UE, a kosze na papiery lub torby powinny być przekazane Komisji lub delegacjom do ich usunięcia. Przed opuszczeniem przydzielonych pomieszczeń Komisja i delegacje zabierają pozostałości do urzędnika ds. Bezpieczeństwa Posiedzenia, który organizuje ich zniszczenie zgodnie z przepisami.

Na koniec posiedzenia wszystkie dokumenty posiadane, jednakże niepotrzebne Komisji lub delegacji, traktowane są jako pozostałości. Przeprowadza się gruntowne przeszukanie pomieszczeń Komisji i delegacji zanim zostaną zniesione środki bezpieczeństwa zatwierdzone dla posiedzenia. Dokumenty, w odniesieniu do których podpisane zostało potwierdzenie odbioru, na ile to możliwe, zostaną zniszczone w sposób wskazany w ppkt. 22.5.

24. NARUSZENIA BEZPIECZEŃSTWA I UTRATA INFORMACJI NIEJAWNEJ UE

24.1. **Definicje**

Naruszenie bezpieczeństwa ma miejsce w wyniku działania albo zaniechania sprzecznego z przepisami Komisji w sprawie bezpieczeństwa, które mogłoby narazić na niebezpieczeństwo lub utratę informacji niejawnej UE.

Utrata informacji niejawnej UE ma miejsce w przypadku, gdy w całości lub w części informacja taka znalazła się w posiadaniu osoby nieupoważnionej, tj. osoby nie posiadającej właściwego poświadczenia bezpieczeństwa lub nie objętej zasadą „powinien wiedzieć” lub gdy istnieje prawdopodobieństwo, że zdarzenie takie mogło mieć miejsce.

Informacje niejawne UE mogą być utracone w wyniku niedbalstwa, lekkomyślności lub uchybienia, jak również poprzez działania służb, wymierzone przeciw UE lub jej Państwom Członkowskim, w odniesieniu do informacji niejawnej UE i jej działań, lub przez organizacje wywrotowe.

24.2. **Zawiadomienia o naruszeniu bezpieczeństwa**

Osoby zobowiązane do obsługi informacji niejawnej UE zostają dokładnie poinformowane o ich obowiązkach w tym zakresie. Mają one obowiązek niezwłocznie poinformować o każdym zauważonym przez nią przypadku naruszenia bezpieczeństwa.

W przypadku, gdy lokalny urzędnik ds. Bezpieczeństwa lub urzędnik ds. Bezpieczeństwa Posiedzenia stwierdzi lub zostanie poinformowany o naruszeniu bezpieczeństwa dotyczącego informacji niejawnej UE lub o utracie lub zniknięciu materiałów niejawnych UE, podejmie on/ona w odpowiednim czasie działania mające na celu:

a) zabezpieczenie dowodów;

b) ustalenie stanu faktycznego;

c) ocenę powstałej szkody i zminimalizowanie jej rozmiarów;

d) niedopuszczenie do ponownego zdarzenia;

e) powiadomienie właściwych organów o skutkach naruszenia bezpieczeństwa.

W tym kontekście, należy dostarczyć następujące informacje:

(i) opis informacji, o której mowa włączając w to jej klasyfikację, numer referencyjny i numer kopii, datę, sporządzającego, przedmiot i zakres;

(ii) krótki opis okoliczności naruszenia bezpieczeństwa, włączając w to datę oraz czas, przez który informacja była wystawiona na niebezpieczeństwo;

(iii) oświadczenie o fakcie poinformowania sporządzającego.

Do obowiązków każdego organu bezpieczeństwa należy, tak szybko jak tylko został powiadomiony o możliwości wystąpienia naruszenia, poinformowanie o tym fakcie Biura ds. Bezpieczeństwa Komisji.

W przypadku informacji ZASTRZEŻONYCH UE należy przekazać informacje o naruszeniu bezpieczeństwa tylko wówczas, gdy ma ono nietypowy charakter.

Po otrzymaniu informacji o naruszeniu zasad bezpieczeństwa, członek Komisji odpowiedzialny za sprawy bezpieczeństwa podejmuje następujące działania:

a) powiadamia organy, które sporządziły informację niejawną, o której mowa;

b) występuje z wnioskiem o wszczęcie śledztwa do odpowiednich organów

bezpieczeństwa;

c) koordynuje dochodzenia w przypadku właściwości więcej niż jednego organu bezpieczeństwa;

d) przestawia sprawozdanie dotyczące okoliczności naruszenia bezpieczeństwa zawierające daty albo okres, w którym mogło dojść do naruszenia oraz okoliczności jego wykrycia, wraz ze szczegółowym opisem zawartości i klasyfikacji danego materiału. W sprawozdaniu znajdzie się informacja na temat szkód, jakie w wyniku naruszenia, poniosła UE lub jej Państwa Członkowskie oraz działań podjętych w celu zapobieżenia wystąpienia takiej sytuacji w przyszłości.

Organ sporządzający informuje adresatów i przekaże odpowiednie instrukcje.

24.3. **Działania prawne**

Każdy, kto jest odpowiedzialny za wystawienie na niebezpieczeństwo informacji niejawnej UE, podlega postępowaniu dyscyplinarnemu określonemu w odpowiednich przepisach, w szczególności w tytule VI regulaminu pracowniczego. Postępowanie dyscyplinarne pozostaje bez uszczerbku dla dalszych postępowań prawnych.

We właściwych przypadkach, na podstawie sprawozdania, określonego w ppkt. 24.2, członek Komisji odpowiedzialny za sprawy bezpieczeństwa podejmuje wszelkie konieczne kroki umożliwiające właściwym organom krajowym wszczęcie postępowania karnego.

25. OCHRONA INFORMACJI NIEJAWNYCH UE OBSŁUGIWANYCH W TECHNOLOGII INFORMATYCZNEJ I SYSTEMACH ŁĄCZNOŚCI

25.1. **Wprowadzenie**

25.1.1. *Przepisy ogólne*

Politykę bezpieczeństwa i jej wymogi stosuje się do wszystkich systemów informatycznych i systemów łączności oraz sieci (zwane dalej systemami) obsługujących informacje klasyfikowane jako UE POUFNE i wyżej. Stosuje się je jako uzupełnienie do decyzji Komisji C (95) 1510 końcowy z dnia 23 listopada 1995 r. w sprawie ochrony systemów informatycznych.

Systemy obsługujące informacje UE ZASTRZEŻONE wymagają również zastosowania środków bezpieczeństwa mających na celu ochronę poufnego charakteru tych informacji. Wszystkie systemy muszą być wyposażone w środki bezpieczeństwa mające na celu ochronę integralności i dostępności systemów oraz informacji, które zawierają.

Polityka bezpieczeństwa Komisji w dziedzinie technologii informatycznej (IT) składa się z następujących elementów:

- stanowi integralną część ogólnego bezpieczeństwa i uzupełnienie wszystkich elementów bezpieczeństwa informatycznego, personelu i fizycznego;

- podziału odpowiedzialności między właścicieli systemów technicznych, właścicieli

EUCI gromadzonych lub obsługiwanych przez systemy techniczne, specjalistów w dziedzinie bezpieczeństwa IT oraz użytkowników;

- opisu zasad bezpieczeństwa i wymogów systemów IT;

- zatwierdzenia zasad, o których mowa i spełnienia wymogów przez wyznaczone organy;

- uwzględnienia szczególnych zagrożeń i słabych punktów w ramach IT.

25.1.2. *Zagrożenia i słabe punkty systemów*

Zagrożenie może być określone jako możliwość przypadkowego albo celowego naruszenia bezpieczeństwa. W przypadku systemów, na takie naruszenia składa się utrata jednej lub więcej właściwości poufności, integralności oraz dostępności. Słabe punkty systemów można zdefiniować jako słabość lub brak kontroli, które mogą ułatwić albo pozwolić na zagrożenie szczególnych aktywów lub celów.

Informacje niejawne i jawne UE, obsługiwane w systemach w spójnej formie, przeznaczone do szybkiego wyszukiwania, łączności i użycia są podatna na wiele zagrożeń. Jest to m.in. możliwość dostępu do informacji przez nieupoważnionych użytkowników, albo przeciwnie, odmowa dostępu dla użytkowników upoważnionych. Istnieje ryzyko nieupoważnionego ujawnienia, sfałszowania, modyfikacji lub usunięcia informacji. Co więcej, skomplikowany i czasami delikatny sprzęt jest drogi, często trudny do naprawienia albo szybkiej wymiany.

25.1.3. *Główny cel środków bezpieczeństwa*

Głównym celem środków bezpieczeństwa, określonych w tym podpunkcie, jest zapewnienie ochrony przed nieupoważnionym ujawnieniem informacji niejawnej UE (utrata charakteru poufnego) oraz przed utratą integralności i dostępności informacji. W celu osiągnięcia odpowiedniej ochrony bezpieczeństwa systemów obsługujących informację niejawną UE, Biuro ds. Bezpieczeństwa Komisji określa właściwe normy bezpieczeństwa konwencjonalnego wraz z właściwymi specjalnymi procedurami bezpieczeństwa i technikami ustalonymi dla każdego z systemów.

25.1.4. *System - szczególne wymagania bezpieczeństwa systemów (SWBS)*

Dla wszystkich systemów obsługujących informacje klasyfikowane jako POUFNE UE i wyżej, musi zostać sporządzony System – szczególne wymagania bezpieczeństwa systemów (SWBS) przez właściciela systemów technicznych (TSO, patrz ppkt 25.3.4), oraz właściciela informacji (patrz ppkt 25.3.5) we współpracy przy wkładzie i pomocy personelu zaangażowanego w pracę przy projekcie i Biura ds. Bezpieczeństwa Komisji (jako organ INFOSEC – IA, patrz ppkt 25.3.3) i zatwierdzony przez Organ Akredytacji Bezpieczeństwa (SAA, patrz ppkt 25.3.2).

SWBS jest również wymagany w przypadku, gdy dostępność i integralność informacji objętej klauzulą tajności UE ZASTRZEŻONE lub informacji jawnych zostanie uznana za istotną przez Organ Akredytacji Bezpieczeństwa (SAA).

SWBS sformułowany jest w początkowym stadium prac nad projektem i jest rozwijany i wzmacniany, spełniając różne zadania w różnych stadiach projektu i cyklu funkcjonowania

systemu.

25.1.5. *Modele działań bezpieczeństwa*

Wszystkie systemy obsługujące informację klasyfikowane jako UE POUFNE i wyżej są akredytowane do działania w jednym, albo, jeśli istnieją takie wymagania odnośnie do różnych okresów, w więcej niż jednym z określonych niżej modelach działania, lub w ich krajowych odpowiednikach:

a) Dedykowany.

b) System wysoko – poziomowy.

c) System wielo – poziomowy.

25.2. **Definicje**

„Akredytacja" oznacza: upoważnienie i zatwierdzenie przyznane systemowi do przetwarzania informacji niejawnej UE w środowisku operacyjnym.

Uwaga:

Akredytacja, o której mowa, powinna zostać przyznana po wprowadzeniu w życie wszystkich procedur bezpieczeństwa i osiągnięciu wystarczającego poziomu ochrony zasobów systemu. Akredytacji udziela się na podstawie SWBS, włączając w to, co następuje:

a) oświadczenie o celu akredytacji sytemu; w szczególności jakie poziomy klasyfikacji informacji będzie on obsługiwał oraz jaki model albo modele działania systemu lub sieci są wnioskowane;

b) stworzenie przeglądu zarządzania ryzykiem w celu identyfikacji zagrożeń i słabych punktów oraz środków mających na celu przeciwdziałanie powyższym;

c) operacyjne Procedury Bezpieczeństwa (SecOPs) ze szczegółowym opisem wnioskowanych operacji (np. modele, usługi, jakie mają być świadczone) wraz z opisem funkcji bezpieczeństwa systemu, stanowiących podstawę akredytacji;

d) plan wprowadzenia w życie i utrzymania funkcji bezpieczeństwa;

e) plan rozpoczęcia oraz kontynuowania testów bezpieczeństwa systemu i sieci, ocena i certyfikacja, oraz

f) certyfikacja, gdzie to konieczne, wraz z innymi elementami akredytacji.

„Urzędnik ds. Bezpieczeństwa Informacji Centralnej" (CISO) oznacza urzędnika w centrali usług IT koordynującego i nadzorującego środki bezpieczeństwa dla centralnie zorganizowanych systemów.

„Certyfikacja" oznacza: wydanie formalnego oświadczenia, potwierdzonego niezależnym przeglądem przeprowadzonej oceny oraz jej wyników dotyczących stopnia, w jakim system

spełnia wymagania bezpieczeństwa lub, w jakim produkt bezpieczęństwa komputerowego spełnia wymagania odnoszące się do wymogów bezpieczeństwa.

„Bezpieczeństwo systemów łączności" (COMSEC) oznacza: stosowanie środków bezpieczeństwa do systemów łączności telekomunikacyjnej w celu uniemożliwienia osobom nieupoważnionym dostępu do informacji, która może zostać pozbawiona wartości w wyniku udostępnienia osobom nieupoważnionym oraz w celu zapewnienia autentyczności informacji, o której mowa.

Uwaga:

Powyższe środki obejmują kryptografię, bezpieczeństwo transmisji i emisji; włączając w to bezpieczeństwo proceduralne, fizyczne, personelu, dokumentów i komputerów.

„Bezpieczeństwo systemów komputerowych" (COMPUSEC) oznacza: stosowanie funkcji bezpieczeństwa odnośnie sprzętu, oprogramowania sprzętowe oraz oprogramowania w systemach komputerowych, w celu ochrony lub zapobieżeniu nieupoważnionemu ujawnieniu operowaniu, modyfikowaniu, usuwaniu, informacji lub odmowie wykonania usługi.

„Produkt bezpieczeństwa komputerowego" oznacza: ogólny element bezpieczeństwa komputerowego, przeznaczony do włączenia do systemu IT w celu jego ulepszenia, lub zagwarantowania poufności, integralności i dostępności obsługiwanej informacji.

„Dedykowany model działania bezpieczeństwa" oznacza: model działania, w którym WSZYSTKIE osoby korzystające z systemu, są dopuszczone do najwyższego stopnia klasyfikacji informacji obsługiwanej w ramach systemu i są objęte wspólną zasadą „powinien wiedzieć", dotyczącą WSZYSTKICH informacji przechowywanych w systemie.

Uwagi:

1) Wspólna zasada powinien wiedzieć oznacza, że nie istnieje obowiązkowy wymóg oddzielenia informacji w ramach systemu poprzez funkcje bezpieczeństwa komputerowego.

2) Inne funkcje bezpieczeństwa (np.: fizyczne, personelu i proceduralne) muszą być zgodne z wymogami przewidzianymi dla najwyższego poziomu klasyfikacji i wszystkich kategorii nazw informacji obsługiwanych w ramach systemu.

„Ocena" oznacza: szczegółowe badanie techniczne aspektów bezpieczeństwa systemu, kryptografii lub bezpiecznego produktu komputerowego, przeprowadzone przez właściwe organy.

Uwagi:

1) Ocena stwierdza istnienie wymaganej funkcjonalności bezpieczeństwa oraz brak niebezpiecznych efektów ubocznych i niezawodność funkcjonalności, o której mowa.

2) Ocena określa zakres, w jakim spełnione są wymogi bezpieczeństwa systemu lub bezpiecznego produktu komputerowego i określa poziom pewności systemu, kryptografii lub funkcji wykonywanych przez bezpieczny produkt komputerowy.

„Właściciel informacji” (IO) oznacza organ (dyrektora departamentu) odpowiedzialnego za tworzenie, przetwarzanie i używanie informacji, włączając w to podejmowanie decyzji dotyczącej osób dopuszczonych do tej informacji.

„Bezpieczeństwo informacji” (INFOSEC) oznacza: stosowanie środków bezpieczeństwa w celu ochrony przetworzonej informacji, przechowywanej lub przekazywanej w systemach łączności przed utratą poufności, integralności i dostępności, przypadkową albo celową, i ochrony samego systemu przed utratą integralności i dostępności.

„Środki INFOSEC” obejmują bezpieczeństwo komputerowe, transmisji, emisji i kryptografii oraz wykrywanie, dokumentowanie i przeciwdziałanie zagrożeniom dla informacji i systemów.

„Obszar IT” oznacza: obszar, w skład którego wchodzi jeden albo więcej komputerów, ich lokalne urządzenia peryferyjne i jednostki pamięci, dedykowaną sieć oraz urządzenia systemów łączności.

Uwaga:

Niniejszy obszar nie obejmuje oddzielnego obszaru, w którym rozmieszczone są zdalne urządzenia peryferyjne, terminale / stacje robocze, nawet jeśli są one podłączone do urządzeń w obszarze IT.

„Sieć TI” oznacza: geograficznie rozproszoną organizację systemów IT, połączonych wzajemnie w celu wymiany danych i składającą się z elementów połączonego wzajemnie systemu IT i ich interfejsów wraz z pomocniczymi danymi i sieciami łączności.

Uwagi:

1) Sieć IT może używać jednej lub więcej sieci łączności połączonych wzajemnie w celu wymiany danych; kilka sieci IT może korzystać z usług zwykłych sieci łączności.

2) Sieć IT nosi nazwę „lokalnej”, jeśli łączy kilka komputerów w tym samym miejscu.

„Funkcje bezpieczeństwa sieci IT” obejmują funkcje bezpieczeństwa systemu IT każdego z systemów IT, na który składa się sieć wraz z dodatkowymi elementami składowymi i funkcjami związanymi z siecią (np. łączność sieciowa, identyfikacja bezpieczeństwa, mechanizmy i procedury etykietowania, kontrola dostępu, programy oraz ślady rewizyjne), koniecznymi do uzyskania zadowalającego poziomu ochrony informacji niejawnej.

„System IT” oznacza: zespół urządzeń, metod i procedur, i jeśli to konieczne, personelu, zorganizowanego w celu wykonywania funkcji przetwarzania informacji.

Uwagi:

1) Oznacza to zespół urządzeń, skonfigurowanych w celu obsługi informacji w ramach systemu.

2) Systemy takie mogą być używane w celu pomocy w konsultacji, kierowaniu, kontroli,

łączności, aplikacji naukowych i administracyjnych, włączając w to edycję tekstów.

3) Granice systemu są zazwyczaj określone przez istnienie elementów pod kontrolą jednego TSO.

4) System IT może zawierać podsystemy, które same mogą stanowić oddzielne systemy IT.

„Funkcje bezpieczeństwa systemu IT" składają się z funkcji sprzętu / oprogramowania sprzętowego / oprogramowania, ich charakterystyki i funkcji; procedur operacyjnych, procedur odpowiedzialnych za prawidłowe działanie i kontrolę dostępu, obszaru IT, zdalnych terminali i stacji roboczych oraz ograniczeń w zarządzaniu, fizycznej struktury i urządzeń, personelu i kontroli systemów łączności koniecznych do osiągnięcia zadowalającego poziomu ochrony informacji niejawnej obsługiwanej przez system IT.

„Urzędnik bezpieczeństwa ds. Lokalnej Informatyki" (LISO) oznacza urzędnika w departamencie Komisji odpowiedzialnego za koordynację i nadzór nad środkami bezpieczeństwa w zakresie swojej właściwości.

„Wielopoziomowy model działania bezpieczeństwa" oznacza: model działań, w którym NIE WSZYSTKIE osoby, mające prawo dostępu do systemu, są sprawdzane w kontekście najwyższego poziomu klasyfikacji informacji obsługiwanej przez system i NIE WSZYSTKIE osoby mające prawo dostępu do systemu obowiązuje wspólna zasada „powinien wiedzieć" w stosunku do informacji obsługiwanej przez system.

Uwagi:

1) Niniejszy model pozwala na obsługę informacji o zróżnicowanym poziomie klasyfikacji oraz różnych kategorii nazw informacji.

2) Fakt, że nie wszystkie osoby są dopuszczone do najwyższego poziomu klasyfikacji oraz brak wspólnej zasady „powinien wiedzieć" wskazuje, że konieczne są komputerowe funkcje bezpieczeństwa, pozwalające na selektywny dostęp do informacji oraz do jej separacji w ramach systemu.

„Obszar zdalnego terminalu / stacji roboczej" oznacza: obszar zawierający wyposażenie komputerowe, jego lokalne urządzenia peryferyjne lub terminal / stację roboczą i każdy związany z nimi sprzęt łączności, oddzielny od obszaru IT.

„Procedury działań bezpieczeństwa" oznacza procedury utworzone przez właściciela technicznego systemu definiujące zasady, jakie muszą zostać przyjęte w sprawach bezpieczeństwa, procedury i odpowiedzialności indywidualnej.

„System wysokopoziomowy modelu działań bezpieczeństwa" oznacza: model działania, w którym WSZYSTKIE osoby mające dostęp do systemu są sprawdzane w kontekście najwyższego poziomu klasyfikacji informacji obsługiwanej przez system, ale NIE WSZYSTKIE osoby mające prawo dostępu są objęte wspólną zasadą „powinien wiedzieć" w stosunku do informacji obsługiwanej przez system.

Uwagi:

1) Brak wspólnej zasady „powinien wiedzieć” wskazuje, że konieczne są komputerowe funkcje bezpieczeństwa pozwalające na selektywny dostęp do informacji oraz do jej separacji w ramach systemu.

2) Inne funkcje bezpieczeństwa (np.: fizyczne, personelu i proceduralne) muszą być zgodne z wymogami przewidzianymi dla najwyższego poziomu klasyfikacji i wszystkich kategorii nazw informacji przechowywanych w systemie.

3) Wszystkie informacje obsługiwane lub, do których możliwy jest dostęp poprzez system w powyższym trybie działania, wraz z uzyskanymi wynikami, są chronione jako potencjalnie najwyższy poziom klasyfikacji nazw o ile nie wskazano inaczej.

„Szczególne wymagania bezpieczeństwa systemów” (SWBS) są całościowym i jasnym zestawem zasad bezpieczeństwa, które mają być przestrzegane oraz szczegółowych wymogów bezpieczeństwa, które mają zostać spełnione. Bazują one na polityce bezpieczeństwa Komisji i ocenie ryzyka, lub wynikają z parametrów określających środowisko operacyjne, najniższy poziom osobistego poświadczenia bezpieczeństwa, najwyższy poziom klasyfikacji obsługiwanej informacji, model działania procedur zabezpieczających lub wymogów dotyczących użytkowników. SWBS są integralną częścią dokumentacji projektu przedłożoną odpowiednim organom do zatwierdzenia w zakresie technicznym, budżetowym i bezpieczeństwa. W swojej końcowej postaci SWBS stanowią wyczerpujące zestawienie określające bezpieczny system.

„Właściciel systemu technicznego” (TSO) oznacza organ odpowiedzialny za stworzenie, utrzymanie, działanie i zamknięcie systemu.

„Tempest” środki zapobiegawcze: środki bezpieczeństwa mające na celu ochronę sprzętu i infrastruktury łączności przed utratą informacji niejawnej w drodze niezamierzonej emisji elektromagnetycznej i przewodności.

25.3. **Odpowiedzialność za bezpieczeństwo**

25.3.1. *Przepisy ogólne*

Zadania doradcze Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa, zdefiniowane w pkt. 12, obejmują sprawy INFOSEC. Niniejsza Grupa zorganizuje swoje działania tak, aby mogła dostarczać specjalistycznych porad w powyższych sprawach.

Biuro ds. Bezpieczeństwa Komisji jest odpowiedzialne za wydanie szczegółowych przepisów INFOSEC, bazując na przepisach niniejszego rozdziału.

W przypadku problemów odnoszących się do bezpieczeństwa (incydenty, naruszenia itd.) Biuro ds. Bezpieczeństwa Komisji podejmuje natychmiastowe działania.

Biuro ds. Bezpieczeństwa Komisji posiada jednostkę INFOSEC.

25.3.2. *Organ Akredytacji Bezpieczeństwa Komisji (SAA)*

Szef Biura ds. Bezpieczeństwa Komisji jest Organem Akredytacji Bezpieczeństwa dla

Komisji (SAA). SAA jest odpowiedzialna ogólnie za obszar bezpieczeństwa oraz w szczegółowych dziedzinach za INFOSEC, bezpieczeństwo łączności, bezpieczeństwo kryptograficzne oraz bezpieczeństwo „Tempest".

SAA jest odpowiedzialna za zapewnienie zgodności systemów z polityką bezpieczeństwa Komisji. Jednym z jej zadań jest udzielanie zatwierdzeń systemu obsługującego informacje niejawne UE do określonego poziomu klasyfikacji w ich środowisku operacyjnym.

Do właściwości Komisji SAA należą wszystkie działające systemy w obrębie pomieszczeń Komisji. Jeśli różne elementy systemu podlegają właściwości SAA Komisji i innych SAA, zainteresowane strony mogą wyznaczyć wspólną radę akredytującą, której działania będzie koordynować SAA Komisji.

25.3.3. *Organ INFOSEC (IA)*

Szef Biura ds. Bezpieczeństwa Komisji jednostki INFOSEC jest organem INFOSEC dla Komisji. Do właściwości organu INFOSEC należy:

- dostarczanie porad technicznych i pomocy SAA;

- pomoc w rozwijaniu SWBS;

- przeglądy SWBS w celu zapewnienia spójności z niniejszymi zasadami bezpieczeństwa oraz politykami INFOSEC i dokumentacją dotyczącą architektury systemów;

- udział w panelach / radach akredytacyjnych, jeśli jest to konieczne, oraz dostarczanie dla INFOSEC zaleceń w sprawie akredytacji do SAA;

- wspieranie działań szkoleniowych i edukacyjnych INFOSEC;

- dostarczanie porad technicznych podczas dochodzeń prowadzonych przez INFOSEC;

- ustalanie wskazówek dotyczących polityki technologicznej tak, aby zapewnić używanie wyłącznie autoryzowanego oprogramowania.

25.3.4. *Właściciel systemów technicznych (TSO)*

W zakresie wprowadzenia w życie, działania i kontroli specjalnych funkcji bezpieczeństwa systemu odpowiedzialność leży po stronie właściciela danego systemu, tj. właściciela systemów technicznych (TSO). Dla systemów centralnych mianuje się Centralnego Urzędnika Bezpieczeństwa Informatycznego (CISO). Każdy departament, tam gdzie sytuacja tego wymaga, mianuje lokalnych urzędników bezpieczeństwa informatycznego (LISO). TSO jest odpowiedzialny za utworzenie Operatywnych Procedur Bezpieczeństwa (SecOPs) i za rozwijanie koncepcji systemu od początkowego projektu do zakończenia jego działania.

Właściciel systemów technicznych (TSO) określa normy i praktyki bezpieczeństwa dla dostawcy systemu.

TSO może przekazać część swoich kompetencji, tam gdzie sytuacja tego wymaga urzędnikowi bezpieczeństwa ds. Lokalnej Informatyki. Pojedyncza osoba może wykonywać

różne funkcje INFOSEC.

25.3.5. *Właściciel informacji (IO)*

Właściciel informacji (IO) jest odpowiedzialny za wprowadzanie, przetwarzanie i tworzenie w systemach technicznych EUCI (i innych informacji). Określa wymogi dotyczące dostępu do informacji w systemie. Niniejsze uprawnienie może przekazać kierownikowi informacji lub kierownikowi bazy danych w zakresie jego kompetencji.

25.3.6. *Użytkownicy*

Wszyscy użytkownicy odpowiadają za swoje działania, tak aby nie wpływały one w sposób negatywny na bezpieczeństwo systemu, którego używają.

25.3.7. *Szkolenia INFOSEC*

Edukacja i szkolenia INFOSEC są dostępne dla wszystkich pracowników, którzy ich potrzebują.

25.4. **Pozatechniczne środki bezpieczeństwa**

25.4.1. *Bezpieczeństwo personelu*

Użytkownicy systemu są sprawdzeni do właściwego poziomu klasyfikacji i zawartości informacji w konkretnym systemie i muszą być objęci zasadą „powinien wiedzieć". Dostęp do niektórych informacji dotyczących zabezpieczenia systemu lub sprzętu wymaga specjalnego poświadczenia wydanego zgodnie z przepisami określonymi przez Komisję.

SAA wskazuje wszystkie sensytywne stanowiska i określi stopień wymaganego poświadczenia dla pracowników, którzy je zajmują oraz wymaganego nadzoru nad nimi.

Systemy są określone i zaprojektowane w taki sposób, aby ułatwić podział obowiązków między pracownikami oraz aby jedna osoba nie miała całościowej wiedzy lub kontroli nad najważniejszymi elementami systemu dotyczącymi jego bezpieczeństwa.

W obszarach IT oraz obszarach zdalnych terminali / stacji roboczych, w których można dokonać zmiany zabezpieczeń systemu nie może pracować tylko jeden zatwierdzonyu urzęnik lub inny pracownik.

Ustawienia zabezpieczeń systemu zostają zmienione wyłącznie przez co najmniej dwóch upoważnionych pracowników działających wspólnie.

25.4.2. *Bezpieczeństwo fizyczne*

Obszary IT i zdalnych terminali / stacji roboczych (zdefiniowane w ppkt. 25.2) w których informacja objęta klauzulą tajności UE POUFNE i wyższą, jest obsługiwana przez środki IT, lub gdzie potencjalnie jest możliwy dostęp do takiej informacji, są ustanowione obszarami bezpieczeństwa klasy I oraz II UE, tam gdzie to właściwe.

25.4.3. *Kontrola dostępu do systemu*

Każda informacja i wszystkie materiały, które umożliwiają kontrolę nad dostępem do systemu są chronione na podstawie ustaleń proporcjonalnych do najwyższego poziomu klasyfikacji i kategorii nazwy informacji, do których mogą one umożliwić dostęp.

Informacje i materiały dotyczące kontroli nad dostępem do systemu, które nie są już potrzebne są niszczone zgodnie z przepisami ppkt. 25.5.4.

25.5. **Techniczne środki bezpieczeństwa**

25.5.1 *Bezpieczeństwo informacji*

Identyfikacji i klasyfikacji dokumentów zawierających informacje dokonuje jej sporządzający, bez względu na to czy mają formę wydruku danych wyjściowych czy komputerowego nośnika pamięci. Na każdej stronie wydruku danych wyjściowych jest oznaczenie klasyfikacji (na górze lub na dole strony). Dane wyjściowe, bez względu na to czy są w formie komputerowego nośnika pamięci czy wydruku mają poziom klasyfikacji równy najwyższemu poziomowi klasyfikacji informacji, użytej do jej stworzenia. Sposób funkcjonowania systemu może również wpływać na klasyfikację danych wyjściowych.

Departamenty Komisji i ich jednostki przechowujące informacje są odpowiedzialne za rozwiązywanie problemów dotyczących agregacji jednostkowych elementów informacji i współzależności, jakie można ustalić w wyniku analizy podobnych elementów, oraz za określenie stopnia klasyfikacji dla całej informacji.

Fakt używania kodowania skrótowego, transmisyjnego lub jakiejkolwiek innej formy przedstawienia binarnego informacji nie oznacza zabezpieczenia informacji i nie powinno wpływać na jej klasyfikację.

Podczas transferu informacji z jednego systemu do drugiego systemu, informacja zabezpieczona jest zarówno w czasie transmisji jak i w systemie odbiorczym, proporcjonalnie do oryginalnej klasyfikacji i kategorii informacji.

Komputerowe nośniki pamięci są obsługiwane w sposób proporcjonalny do najwyższej klasyfikacji zawartej w nich informacji lub etykietowanego nośnika oraz przez cały czas odpowiednio chronione.

Komputerowe nośniki pamięci przystosowane do ponownego użycia, używane do zapisu informacji niejawnej UE zachowują najwyższy poziom klasyfikacji informacji, do jakiego zostały użyte, dopóki poziom klasyfikacji informacji, o której mowa nie zostanie odpowiednio obniżony lub jednostka zostanie odtajniona i dopóki nośnik nie zostanie ponownie odpowiednio sklasyfikowany, lub nośnik nie zostanie odtajniony lub zniszczony zgodnie z procedurami zatwierdzonymi przez SAA (patrz ppkt 25.5.4).

25.5.2. *Kontrola i odpowiedzialność za informację*

Dane dotyczące automatycznego (ślady rewizyjne) lub ręcznego logowania zachowuje się jako rejestr dostępu do informacji objętej klauzulą tajności UE TAJNE i wyższą. Rejestr, o których mowa przechowywany jest zgodnie z niniejszymi przepisami bezpieczeństwa.

Niejawne dane wyjściowe UE, przechowywane w obszarze IT mogą być obsługiwane jako jeden sklasyfikowany element i nie muszą być rejestrowane, pod warunkiem że materiał jest zidentyfikowany, oznakowany i sklasyfikowany oraz kontrolowany we właściwy sposób.

Przy tworzeniu danych wyjściowych z systemu obsługującego informację niejawną UE i transmisji z obszaru IT do zdalnych terminali / stacji roboczych, zostają ustanowione, za zgodą SAA, procedury ustanawiające kontrolowanie i rejestrowanie danych wyjściowych**.** Dla informacji objętych klauzulą tajności UE TAJNE i wyższą, procedury, o których mowa, zawierają szczególne instrukcje odpowiedzialności za informację.

25.5.3. *Obsługiwanie i kontrola przenośnych komputerowych nośników pamięci*

Przenośne komputerowe nośniki pamięci UE POUFNE i wyższe obsługiwane są jako materiał i stosuje się do nich przepisy ogólne. Odpowiednia identyfikacja i oznakowania wskazujące na klasyfikację muszą być przystosowane do szczególnego wglądu fizycznego jednostki, tak aby pozwalały na jej jednoznaczne rozpoznanie.

Użytkownicy są odpowiedzialni za zapewnienie, aby informacje niejawne UE były przechowywane na nośnikach posiadających odpowiednie oznakowania wskazujące na klasyfikację i ochronę. Ustanawia się procedury zapewniające, że dla wszystkich poziomów informacji niejawnej UE, przechowywanie informacji w komputerowych nośnikach pamięci jest prowadzone zgodnie z tymi przepisami bezpieczeństwa.

25.5.4 *Odtajnienie i niszczenie komputerowych nośników pamięci*

Komputerowe nośniki pamięci, używane do zapisu informacji niejawnej UE mogą podlegać obniżeniu klasyfikacji lub odtajnieniu z zgodnie z procedurą zatwierdzoną przez SAA.

Komputerowe nośniki pamięci, używane do zapisu informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE lub szczególnych kategorii informacji nie mogą podlegać odtajnieniu i nie mogą zostać powtórnie użyte.

Jeśli komputerowe nośniki pamięci nie mogą zostać odtajnione lub ponownie użyte, zostają zniszczone zgodnie z powyższą procedurą.

25.5.5. *Bezpieczeństwo łączności*

Szef Biura ds. Bezpieczeństwa Komisji pełni funkcję Organu Szyfrów.

W sytuacji, gdy informacja niejawna UE podlega transmisji elektromagnetycznej, wprowadza się w życie specjalne środki mające na celu ochronę poufności, integralności i dostępności do takiej transmisji. SAA ustali wymogi dotyczące ochrony transmisji przed wykryciem i przechwyceniem. Informacja transmitowana w systemie łączności jest chroniona w celu zachowania jej poufności, integralności i dostępności.

W przypadku, gdy w celu zapewnienia poufności, integralności i dostępności, konieczne jest posłużenie się metodą kryptograficzną, metoda ta wraz z towarzyszącymi produktami zostaje specjalnie zatwierdzona do celu określonego przez SAA jako Organ Szyfrów.

Podczas transmisji poufność informacji, objętej klauzulą tajności UE TAJNE i wyższą,

zostaje zapewniona przez użycie metody kryptograficznej lub produktu zatwierdzonego przez członka Komisji odpowiedzialnego za sprawy bezpieczeństwa, po konsultacji z Grupą Doradczą Komisji ds. Polityki Bezpieczeństwa. Podczas transmisji, poufność informacji, objętych klauzulą tajności UE POUFNE i UE ZASTRZEŻONE, zostaje zapewniona przez użycie metody kryptograficznej lub produktu zatwierdzonego przez organ kryptograficzny Komisji po konsultacji z Grupą Doradczą Komisji ds. Polityki Bezpieczeństwa.

Szczegółowe przepisy mające zastosowanie do transmisji informacji niejawnej UE zostaną wymienione w szczególnych instrukcjach bezpieczeństwa zatwierdzonych przez Biuro ds. Bezpieczeństwa Komisji po konsultacji z Grupą Doradczą Komisji ds. Polityki Bezpieczeństwa.

W wyjątkowych okolicznościach operacyjnych, informacje objęte klauzulą tajności UE ZASTRZEŻONE, UE POUFNE i UE TAJNE mogą być transmitowane w postaci zwykłego tekstu, po warunkiem, że każdy taki przypadek został wyraźnie upoważniony i zarejestrowany przez właściciela informacji. Wyjątkowe okoliczności, o których mowa, to:

a) podczas zagrażającej lub aktualnej sytuacji kryzysowej, konfliktu lub wojny, i

b) jeśli czas przekazania informacji ma wyjątkowe znaczenie a środki szyfrujące nie są dostępne i ocenia się, że informacja podlegająca transmisji nie może zostać wykorzystana na czas w celu negatywnego wpłynięcia na przeprowadzane operacje.

System może uniemożliwić dostęp do informacji niejawnej UE w każdym ze zdalnych terminali lub stacji roboczej, poprzez fizyczne rozłączenie lub specjalne oprogramowanie zatwierdzone przez SAA.

25.5.6. *Bezpieczeństwo instalacji i promieniowania*

Pierwotna instalacja systemów i każda ich większa zmiana zostaje określona tak, aby instalacja była wykonana przez sprawdzonych instalatorów pod stałym nadzorem personelu technicznego, który został sprawdzony w kontekście informacji niejawnej UE na poziomie równym najwyższej klasyfikacji, która będzie obsługiwana i przechowywana przez system.

Systemy obsługujące informacje, objęte klauzulą tajności UE POUFNE i wyższą, są chronione tak, aby ich bezpieczeństwo nie mogło być zagrożone przez emanacje i przewodność, do których kontroli i badania odnosi się „Tempest”.

Środki przeciwdziałania Tempest są zrewidowane i zatwierdzone przez organ Tempest (patrz ppkt 25.3.2).

25.6. **Bezpieczeństwo podczas obsługiwania**

25.6.1. *Operacyjne procedury bezpieczeństwa (SecOPs)*

Operacyjne procedury bezpieczeństwa (SecOPs) określają zasady, które mają być przyjęte w sprawach bezpieczeństwa, procedury operacyjne, których należy przestrzegać oraz odpowiedzialność osobistą. SecOPs są przygotowane na odpowiedzialność właściciela systemów technicznych (TSO).

25.6.2. *Zarządzanie ochroną oprogramowania / konfiguracji*

Zapewnienie bezpieczeństwa oprogramowania jest ustalone raczej na podstawie oceny klasyfikacji bezpieczeństwa programu niż na podstawie klasyfikacji informacji, którą oprogramowanie ma przetwarzać. Używane wersje oprogramowania są weryfikowane w regularnych odstępach czasu w celu zapewnienia jego integralności i prawidłowego funkcjonowania.

Nowe lub zmodyfikowane wersje oprogramowania nie są używane do obsługi informacji niejawnej UE, do czasu ich weryfikacji przez TSO.

25.6.3. *Sprawdzanie obecności złośliwego oprogramowania / wirusów komputerowych*

Sprawdzanie obecności złośliwego oprogramowania i wirusów komputerowych odbywa się regularnie zgodnie z wymogami SAA.

Wszystkie komputerowe nośniki pamięci, które nadeszły do Komisji są sprawdzane w celu wykrycia złośliwego oprogramowania lub wirusów komputerowych, przed ich wprowadzeniem do systemu.

25.6.4. *Konserwacja*

Umowy i procedury dotyczące przeglądu i naprawy okresowej systemów, dla których utworzono SWBS określają wymagania i uzgodnienia przewidziane dla personelu obsługi oraz jego sprzętu, który jest wnoszony na obszar IT.

Wymagania, o których mowa, są jasno określone w SWBS a procedury jasno określone w SecOPs. Konserwacja, wymagająca zdalnych procedur diagnostycznych jest dozwolona tylko w wyjątkowych sytuacjach pod ścisłą kontrolą bezpieczeństwa i tylko za zgodą SAA.

25.7. **Zamówienie**

25.7.1. *Przepisy ogólne*

Każdy produkt zabezpieczający, który ma być użyty w systemie, przewidziany do zamówienia, musi być albo oceniony i certyfikowany, lub być w trakcie oceny i certyfikacji przez właściwy organ certyfikujący i oceniający jednego z Państw Członkowskich, na podstawie uznanych w skali międzynarodowej kryteriów (np. ISO 15408) Procedury szczególne muszą uzyskać akceptację ACPC.

W przypadku podejmowania decyzji o kupnie albo leasingu, w szczególności odnośnie do komputerowych nośników pamięci**,** należy mieć na uwadze, że sprzęt taki, raz użyty do obsługi informacji niejawnej UE, nie może opuścić odpowiednio strzeżonego środowiska bez uprzedniego odtajnienia, następującego po uzyskaniu zgody SAA, której uzyskanie nie zawsze jest możliwe.

25.7.2. *Akredytacja*

Wszystkie systemy, dla których przed obsługiwaniem informacji niejawnej UE konieczne jest sporządzenie SWBS, są akredytowane przez SAA, na bazie informacji dostarczonej w SWBS,

SecOPs i każdej innej odpowiedniej dokumentacji. Podsystemy i zdalne terminale / stacje robocze są akredytowane jako część systemu, do którego są przyłączone. Jeśli system obsługuje zarówno Komisję jak i inne organizacje, Komisja i inne odpowiednie organy bezpieczeństwa wzajemnie podejmują decyzje odnoszącą się do udzielenia akredytacji.

Proces akredytacji może być prowadzony w zgodzie ze strategią akredytacyjną stosowną do określonego systemu i zdefiniowaną przez SAA.

25.7.3. *Ocena i certyfikacja*

Przed akredytacją, w niektórych przypadkach, funkcje bezpieczeństwa systemu w sprzęcie, oprogramowaniu sprzętowym oraz oprogramowaniu są poddane ocenie i certyfikacji, w celu ustalenia ich zdolności zabezpieczenia informacji na pożądanym poziomie klasyfikacji.

Wymogi odnoszące się do ewaluacji i certyfikacji są włączone do planowania systemu i jasno określone w SWBS.

Procesy oceny i certyfikacji są przeprowadzane, zgodnie z zatwierdzonymi wskazówkami, przez właściwie sprawdzonych, wykwalifikowanych pracowników technicznych działających w imieniu TSO.

Zespoły mogą być zapewnione przez wyznaczony organ oceny lub organ certyfikujący Państwa Członkowskiego lub jej wyznaczonego przedstawiciela, np. właściwego i sprawdzonego kontrahenta.

Stopień podjętego procesu oceny i certyfikacji może być mniejszy (np. obejmujący jedynie aspekty integracyjne), jeśli systemy są zbudowane na bezpiecznych produktach komputerowych, które przeszły proces krajowej oceny i certyfikacji.

25.7.4. *Rutynowe kontrole funkcji bezpieczeństwa w celu kontynuacji akredytacji*

TSO ustanawia rutynowe procedury kontrolne zapewniające, że nadal funkcjonują wszystkie funkcje bezpieczeństwa systemu.

Zmiany, które mogłyby prowadzić do ponownej akredytacji, lub wymagające wcześniejszego zatwierdzenia ze strony SAA są jasno określone w SWBS. Po jakiejkolwiek zmianie, naprawie lub uszkodzeniu, które mogłoby wpłynąć negatywnie na funkcje bezpieczeństwa systemu, TSO zapewnia przeprowadzenie kontroli w celu zagwarantowania prawidłowego działanie funkcji bezpieczeństwa. Przeprowadzenie następnej akredytacji systemu zależy od zadowalających wyników kontroli.

Wszystkie systemy, w których wprowadzono w życie funkcje bezpieczeństwa są przedmiotem inspekcji i rewizji okresowych dokonywanych przez SAA. W odniesieniu do systemów obsługujących UE ŚCIŚLE TAJNE inspekcje są przeprowadzane nie rzadziej niż raz na rok.

25.8. **Używanie czasowe lub okazjonalne**

25.8.1. *Bezpieczeństwo mikrokomputerów / komputerów osobistych*

Mikrokomputery / komputery osobiste (PCs) z zamontowanymi dyskami (lub innymi stałymi nośnikami pamięci) działające zarówno w zwykłym jak i sieciowym trybie oraz komputerowe urządzenia przenośne (np. przenośne komputery osobiste i elektroniczne notebooki) z zamontowanymi dyskami twardymi, są uznawane za nośniki danych tak samo jak dyskietki lub inne przenośne komputerowe nośniki pamięci.

Urządzeniom, o których mowa, przyznany jest poziom ochrony w zakresie dostępu, obsługi, przechowywania i transportu, proporcjonalny do najwyższego poziomu klasyfikacji informacji, która kiedykolwiek była tam przechowywana lub przetwarzana (do momentu obniżenia stopnia lub wyłączenia z klasyfikacji zgodnie z zatwierdzoną procedurą).

25.8.2. *Używanie prywatnych urządzeń IT do prac służbowych Komisji*

Używanie prywatnych przenośnych komputerowych nośników danych, oprogramowania, urządzeń IT (np. PCs, przenośnych urządzeń komputerowych) z możliwością przechowywania danych jest zabronione do obsługi informacji niejawnej UE.

Prywatne urządzenia komputerowe, oprogramowanie i komputerowe nośniki pamięci nie mogą być, bez pisemnego upoważnienia szefa Biura ds. Bezpieczeństwa Komisji, wnoszone do obszaru klasy I i klasy II gdzie obsługiwane są informacje niejawne UE. Upoważnienie może być wydana tylko do celów technicznych w wyjątkowych przypadkach.

25.8.3. *Używanie do prac służbowych Komisji urządzeń IT stanowiących własność kontrahenta lub dostarczonych przez państwa*

Używanie urządzeń IT i oprogramowania stanowiącego własność kontrahenta do prac służbowych Komisji może odbywać się za zgodą szefa Biura ds. Bezpieczeństwa Komisji. Używanie urządzeń IT lub oprogramowania dostarczonego przez państwa może być również dozwolone; w tym przypadku urządzenia IT podlegają kontroli właściwej jednostki organizacyjnej Komisji. W obu przypadkach, jeżeli urządzenia IT są przeznaczone do obsługi informacji niejawnej UE, należy przeprowadzić konsultacje z SAA, mające na celu zapewnienie, że elementy INFOSEC stosowane w powyższych urządzeniach są właściwie dobrane i wprowadzone w życie.

26. UDOSTĘPNIANIE INFORMACJI NIEJAWNEJ UE PAŃSTWOM TRZECIM LUB ORGANIZACJOM MIĘDZYNARODOWYM

26.1.1. *Zasady regulujące udostępnianie informacji niejawnej UE*

Komisja, jako organ kolegialny, decyduje w sprawie udostępniania informacji niejawnej UE państwom trzecim lub organizacjom międzynarodowym, na podstawie:

- charakteru i treści informacji;
- potrzeby znajomości ze strony odbiorcy;
- korzyści dla UE.

Sporządzający informację niejawną**,** która ma być udostępniona zostanie poproszony o wyrażenie zgody.

Decyzja zostanie podjęta, biorąc pod uwagę każdy z przypadków oddzielnie, w zależności od:

- stopnia woli współpracy z określonym państwem trzecim lub organizacja międzynarodową;

- stopnia zaufania do podmiotów, o których mowa – wynikającego z poziomu zabezpieczeń, które będą stosowane do informacji niejawnych UE, powierzonych państwom lub organizacjom oraz od spójności między zasadami bezpieczeństwa tam stosowanymi a zasadami stosowanymi w UE. Grupa Doradcza Komisji ds. Polityki Bezpieczeństwa przekaże Komisji techniczną opinię na ten temat.

Przyjęcie informacji niejawnych UE przez państwa trzecie lub organizacje międzynarodowe zakłada dopełnienie wszelkich starań, aby informacje nie były używane w celach innych niż te, które były powodem ich przekazania lub wymiany i że są one chronione zgodnie z wymogami Komisji.

26.1.2. *Poziomy*

Po podjęciu decyzji przez Komisję o udostępnieniu lub wymianie informacji niejawnej UE z określonym państwem lub organizacją międzynarodową, Komisja zadecyduje o poziomie współpracy jaki jest możliwy. To będzie zależeć w szczególności od polityki bezpieczeństwa i przepisów stosowanych przez dane państwo lub organizację międzynarodową.

Istnieją trzy poziomy współpracy:

Poziom 1

Współpraca z państwem trzecim lub organizacją międzynarodową, których przepisy i polityka bezpieczeństwa są bardzo podobne do przepisów i polityki bezpieczeństwa UE.

Poziom 2

Współpraca z państwem trzecim lub organizacją międzynarodową, których przepisy i polityka bezpieczeństwa są znacząco różne od przepisów i polityki bezpieczeństwa UE.

Poziom 3

Okazjonalna współpraca z państwem trzecim lub organizacją międzynarodową, których przepisy i polityka bezpieczeństwa nie może być oceniona.

Każdy z poziomów współpracy ustala procedury i przepisy bezpieczeństwa, wyszczególnione w dodatkach 3, 4, i 5.

26.1.3. *Porozumienia w sprawach bezpieczeństwa*

Po podjęciu przez Komisję decyzji o potrzebie ciągłej lub długofalowej wymiany informacji niejawnej między Komisją a państwami trzecimi lub innymi organizacjami międzynarodowymi, Komisja wraz z tymi podmiotami, o których mowa, sporządzi „Porozumienie w sprawie procedur bezpieczeństwa dla wymiany informacji niejawnej", które

będzie określać cele współpracy oraz wzajemne zasady dotyczące ochrony informacji podlegającej wymianie.

W przypadku okazjonalnej współpracy na poziomie 3, która ze swej istoty jest ograniczona czasowo i pod względem celów, zamiast „Porozumienia w sprawie procedur bezpieczeństwa dla wymiany informacji niejawnej" wystarczy sporządzić Protokół Ustaleń, który określi charakter informacji niejawnej podlegającej wymianie i wzajemne zobowiązania odnoszące się do informacji, o których mowa. Sporządzenie Protokołu Ustaleń może mieć miejsce tylko w przypadku, gdy informacja podlegająca wymianie została objęta klauzulą tajności nie wyższą niż UE ZASTRZEŻONE.

Projekty porozumienia i protokołów ustaleń zanim zostaną przedstawione Komisji, w celu podjęcia przez nią decyzji, stanowić są przedmiot dyskusji na forum Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa.

Członek Komisji odpowiedzialny za sprawy bezpieczeństwa może żądać pomocy od państwowej służby bezpieczeństwa (PSB's) Państwa Członkowskiego, w celu zapewnienia, że informacja, która ma zostać udostępniona jest używana i chroniona zgodnie z przepisami porozumienia w sprawie procedur bezpieczeństwa lub postanowieniami Protokołu Ustaleń.

Dodatek 1

PORÓWNANIE KRAJOWYCH KLASYFIKACJI BEZPIECZEŃSTWA

Klasyfikacja UE	UE ŚCIŚLE TAJNE	UE TAJNE	UE POUFNE	UE ZASTRZEŻONE
Klasyfikacja NATO[1]				
Klasyfikacja UZE	Centralnie Ściśle Tajne	UZE TAJNE	UZE POUFNE	UZE ZASTRZEŻONE
Klasyfikacja EURATOM[2]	EURATOM Ściśle Tajne	EURATOM TAJNE	EURATOM Poufne	EURATOM Zastrzeżone
Belgia	Trés Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Dania	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Niemcy	STRENG GEHEIM	GEHEIM	VS[3] - VERTRAULICH	VS - NUR FÜR DEN DIENSTGEBRAUCH
Grecja	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Hiszpania	Secreto	Reservado	Confidencial	Difusión limitada
Francja	Trés Secret Défense[4]	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irlandia	Top Secret	Secret	Confidential	Restricted
Włochy	Segretissimo	Segreto	Riservatissimo	Riservato
Luksemburg	Trés Secret	Secret	Confidentiel	Diffusion restreinte
Niderlandy	Stg. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugalia	Muito Secreto	Secreto	Confidencial	Reservado
Finlandia	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Szwecja	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Zjednoczone Królestwo	Top Secret	Secret	Confidential	Restricted

[1] NATO - odpowiedniki klasyfikacji NATO zostaną ustalone w momencie wynegocjowania porozumienia w sprawie bezpieczeństwa pomiędzy Komisją i NATO.
[2] Rozporządzenie Euratom nr 3 z dnia 31 lipca 1958 r. w sprawie ochrony informacji niejawnej Euratom.
[3] Niemcy: VS = Verschlusssache.
[4] Francja: klasyfikacja Très Secret Dèfense', obejmująca sprawy szczególnego znaczenia, może być zmienona tylko za upoważnieniem premiera.

Dodatek 2

PRAKTYCZNE WSKAZÓWKI DOTYCZĄCE KLASYFIKACJI

Niniejsze wskazówki mają charakter pomocniczy i w żadnym wypadku nie zmieniają przepisów ustanowionych w pkt. 16, 17, 20 i 21.

Klasyfikacja	Kiedy	Kto	Umieszczanie	Obniżanie stopnia / odtajnienie / zniszczenie	
				Kto	Kiedy
UE ŚCIŚLE TAJNE: Niniejsza klauzula ma zastosowanie tylko do informacji i materiałów, których nieupoważnione ujawnienie może spowodować wyjątkowo ciężkie naruszenie podstawowych interesów Unii Europejskiej lub jednego lub więcej jej Państw Członkowskich. [ppkt 16.1].	Zagrożenie aktywów sklasyfikowanych jako UE ŚCIŚLE TAJNE może: - Spowodować bezpośrednie zagrożenie dla wewnętrznej stabilności UE lub jednego z jej Państw Członkowskich lub państw zaprzyjaźnionych - Spowodować wyjątkowo poważną szkodę w odniesieniu do stosunków z zaprzyjaźnionym rządem - Prowadzić bezpośrednio do powszechnej utraty życia - Spowodować wyjątkowo poważną szkodę w odniesieniu do efektywności operacyjnej lub bezpieczeństwa Państw Członkowskich lub sił innych uczestników lub dla niezakłóconej efektywności niezmiernie ważnych działań w zakresie bezpieczeństwa lub wywiadu - Spowodować poważną szkodę w odniesieniu do gospodarki UE lub Państw Członkowskich o długofalowym charakterze.	Należycie uprawnione osoby (sporządzający), dyrektorzy Generalni, szefowie służb [ppkt 17.1] Sporządzający określają datę, okres lub zdarzenie, kiedy można obniżyć stopień zawartości lub w ją odtajnić [ppkt 16.2] W przeciwnym razie, poddają oni dokumenty rewizjom w okresach, co najmniej pięcioletnich, w celu zapewnienia, że pierwotna klasyfikacja jest niezbędna [ppkt 17.3].	Dokumenty objęte klauzulą tajności UE ŚCIŚLE TAJNE zostaną oznaczone jako UE ŚCIŚLE TAJNE wraz ze znakami bezpieczeństwa lub oznakowaniami obronności, tam gdzie to stosowne, mechanicznie lub ręcznie [ppkt 16.4, 16.5, 16.3]. Klasyfikację i znaki bezpieczeństwa UE umieszcza się w centralnym miejscu na górze i na dole każdej strony. Wszystkie strony są numerowane. Każdy dokument posiada numer referencyjny oraz datę, numer referencyjny umieszcza się na każdej stronie. Jeżeli mają one zostać rozesłane w kilku egzemplarzach, każda zostaje zaopatrzona w numer kopii, umieszczony na pierwszej razem z całkowita ilością stron. Wszystkie załączniki i uzupełnienia wymienia się na pierwszej stronie [ppkt 21.1].	Odtajnienie albo obniżenie stopnia zależy wyłącznie od sporządzającego, który o dokonanych zmianach poinformuje wszystkich adresatów, do których wysłano lub, którym powielono dokument [ppkt 17.3]. Dokumenty objęte klauzulą tajności UE ŚCIŚLE TAJNE zostają zniszczone przez Centralne archiwum lub archiwa pomocnicze, które są za nie odpowiedzialne. Każdy zniszczony dokument jest wpisywany do poświadczeń zniszczeń, podpisywanego przez urzędnika kontroli UE ŚCIŚLE TAJNEJ oraz przez urzędnika będącego świadkiem zniszczenia, który musi być poddany postępowaniu sprawdzającemu w stosunku do informacji objętych klauzulą tajności UE ŚCIŚLE TAJNE. Fakt zniszczenia odnotowywany jest w rejestrze. Archiwum przechowuje poświadczenia zniszczenia razem z notatką o rozpowszechnieniu przez okres dziesięciu lat [ppkt 22.5].	Dodatkowe kopie i zbędne dokumenty muszą być zniszczone [ppkt 22.5]. Dokumenty UE ŚCIŚLE TAJNE, włączając w to wszystkie niejawne pozostałości powstałe na skutek przygotowywania dokumentów UE ŚCIŚLE TAJNE, takie jak zniszczone kopie, robocze projekty, drukowane notatki, kalka maszynowa są zniszczone pod nadzorem urzędnika kontroli archiwum UE ŚCIŚLE TAJNE, poprzez spalenie, zmielenie, poszatkowanie lub w inny sposób redukujący do nierozpoznawalnej i niemożliwej do odtworzenia formy [ppkt 22.5].

Klasyfikacja	Kiedy	Kto	Umieszczanie	Obniżanie stopnia / wyłączenie z klasyfikacji / zniszczenie	
				Kto	Kiedy
UE TAJNE: Niniejsza klauzula ma zastosowanie do informacji i materiałów, których nieupoważnione ujawnienie może spowodować poważną szkodę w podstawowych interesach Unii Europejskiej lub jednego lub więcej jej Państw Członkowskich. [ppkt 16.1].	Zagrożenie aktywów sklasyfikowanych jako UE TAJNE może: - Wywołać napięcie międzynarodowe - Poważnie zaszkodzić stosunkom z zaprzyjaźnionym rządem - Zagrozić bezpośrednio życiu lub poważnie narusza porządek publiczny lub bezpieczeństwo osobiste lub wolność - Spowodować poważną szkodę w odniesieniu do efektywności operacyjnej lub bezpieczeństwa Państw Członkowskich lub innych służb lub efektywności niezmiernie istotnych działań wywiadowczych - Spowodować poważną szkodę w odniesieniu do interesów gospodarczych, finansowych, monetarnych i handlowych UE lub Państw Członkowskich.	Należycie upoważnione osoby (sporządzający), dyrektorzy Generalni, szefowie służb [ppkt 17.1]. Sporządzający określają datę, okres lub zdarzenie, kiedy może zostać obniżony stopień zawartości lub jej odtajnienie [ppkt 16.2] W przeciwnym razie, poddają oni dokumenty rewizjom w okresach, co najmniej pięcioletnich, w celu zapewnienia, że pierwotna klasyfikacja jest niezbędna [ppkt 17.3].	Dokumenty UE TAJNE zostaną oznaczone jako UE TAJNE wraz ze znakami bezpieczeństwa lub z oznakowaniami obronności, tam gdzie to stosowne, mechanicznie lub ręcznie [ppkt 16.4, 16.5, 16.3]. Klasyfikację i znaki bezpieczeństwa UE umieszcza się w centralnym miejscu na górze i na dole każdej strony. Wszystkie strony są numerowane. Każdy dokument posiada numer referencyjny oraz datę; numer referencyjny umieszcza się na każdej stronie. Jeżeli mają one zostać rozesłane w kilku egzemplarzach, każda zostanje zaopatrzona w numer kopii, umieszczony na pierwszej razem z całkowita ilością stron. Wszystkie załączniki i uzupełnienia wymienia się na pierwszej stronie [ppkt 21.1].	Odtajnienie albo obniżenie stopnia zależy od sporządzającego, który o dokonanych zmianach informuje wszystkich adresatów, do których wysłano lub, którym powielono dokument [ppkt 17.3]. Dokumenty objęte klauzulą tajności UE TAJNE są zniszczone przez archiwum odpowiedzialne za te dokumenty, pod nadzorem osoby posiadającej certyfikat bezpieczeństwa Dokument, który został zniszczony zostaje wymieniony na podpisanych poświadczeniach zniszczenia, które są przechowywane przez archiwum wraz z notatką o rozpowszechnieniu, przez przynajmniej trzy lata. [ppkt 22.5].	Dodatkowe kopie i zbędne dokumenty muszą być zniszczone [ppkt 22.5]. Dokumenty UE TAJNE, włączając w to wszystkie niejawne pozostałości będące wynikiem przygotowań do stworzenia dokumentacji, o której mowa, takie jak zniszczone kopie, robocze projekty, drukowane notatki, kalka maszynowa itd., zostają zniszczone poprzez spalenie, zmielenie, poszatkowanie lub zniszczone w inny sposób, dzięki któremu nie są możliwe do odtworzenia i rozpoznania [ppkt 22.5].

Klasyfikacja	Kiedy	Kto	Umieszczanie	Obniżanie stopnia / wyłączenie z klasyfikacji / zniszczenie	
				Kto	Kiedy
UE POUFNE : Klauzula ta ma zastosowanie do informacji i materiałów, których nieupoważnione ujawnienie może być niekorzystne dla podstawowych interesów Unii Europejskiej lub jednego lub więcej jej Państw Członkowskich. [ppkt 16.1].	Zagrożenie aktywów sklasyfikowanych jako UE POUFNE może: - Negatywnie wpłynąć na stosunki dyplomatyczne tj. spowodować formalny protest lub inne sankcje - Spowodować szkodę dla bezpieczeństwa i wolności osób fizycznych; - Utrudni utrzymanie efektywności operacyjnej lub bezpieczeństwa Państw Członkowskich lub innych sił uczestniczących lub efektywności niezmiernie istotnych działań w zakresie bezpieczeństwa lub wywiadowczym; - Narazić wiarygodność finansową głównych organizacji; - Utrudnić śledztwo lub ułatwić popełnienie poważnego przestępstwa; - Działać na szkodę interesów finansowych, monetarnych, gospodarczych i handlowych UE lub Państw Członkowskich; - Poważnie utrudnić rozwój lub funkcjonowanie ważniejszych polityk UE; - Uniemożliwić lub przeszkodzić istotnym działaniami UE.	Należycie upoważnione osoby (sporządzający), dyrektorzy Generalni, szefowie służb [ppkt 17.1]. Sporządzający określają datę, okres lub zdarzenie, kiedy może zostać obniżony stopień zawartości lub jej odtajnienie. W przeciwnym razie dokumenty są poddawane przeglądowi co pięć lat w celu zapewnienia że konieczne jest utrzymanie pierwotnej klasyfikacji [ppkt 17.3].	Dokumenty UE POUFNE zostają oznaczone jako UE POUFNE wraz ze znakami bezpieczeństwa lub oznakowaniami obronności, tam gdzie to stosowne, mechanicznie lub ręcznie [ppkt 16.4, 16.5, 16.3]. Klasyfikację UE umieszcza się w centralnym miejscu na górze i dole każdej strony. Wszystkie strony są numerowane. Każdy dokument posiada numer referencyjny oraz datę. Wszelkie załączniki i uzupełnienia wymienia się na pierwszej stronie [ppkt 21.1].	Odtajnienie albo obniżenie stopnia zależy od sporządzającego, który o dokonanych zmianach informuje wszystkich adresatów do których wysłano lub którym powielono dokument [ppkt 17.3]. Dokumenty objęte klauzulą tajności UE POUFNE zostają zniszczone przez archiwum, które jest za nie odpowiedzialne pod nadzorem dopuszczonej osoby. Ich zniszczenie zostaje odnotowane zgodnie z przepisami krajowymi a, w przypadku Komisji i zdecentralizowanych agencji, zgodnie z wytycznymi przewodniczącego [ppkt 22.5].	Dodatkowe kopie i zbędne dokumenty muszą być zniszczone [ppkt 22.5]. Dokumenty UE POUFNE , włączając w to wszystkie niejawne pozostałości będące wynikiem przygotowań do stworzenia dokumentacji, o której mowa, takie jak zniszczone kopie, robocze projekty, drukowane notatki, kalka maszynowa itd., zostają zniszczone pod nadzorem urzędnika kontroli ds. Dokumentacji UE POUFNE poprzez spalenie, zmielenie, poszatkowanie lub zniszczone w inny sposób, dzięki któremu materiały nie są możliwe do odtworzenia i rozpoznania [ppkt 22.5].

Klasyfikacja	Kiedy	Kto	Umieszczanie	Obniżanie stopnia / wyłączenie z klasyfikacji / zniszczenie	
				Kto	Kiedy
UE ZASTRZEŻONE: Klauzula ta ma zastosowanie tylko do informacji i materiałów, których nieupoważnione ujawnienie może spowodować naruszenie podstawowych interesów Unii Europejskiej lub jednego, lub więcej jej Państw Członkowskich. [ppkt 16.1].	Zagrożenie aktywów sklasyfikowanych jako UE ZASTRZEŻONE może: - Zaszkodzić stosunkom dyplomatycznym - Spowodować poważne niebezpieczeństwo osób - Utrudnić utrzymanie efektywności operacyjnej lub bezpieczeństwa Państw Członkowskich lub innych sił uczestniczących - Spowodować straty finansowe lub ułatwić uzyskanie nienależnego zysku lub korzyści osobom fizycznym bądź spółkom - Naruszyć odpowiednie zobowiązania w zakresie zachowania w tajemnicy informacji otrzymanych od osób trzecich - Naruszyć ograniczenia wynikające ze statutu, dotyczące ujawniania informacji - Utrudnić śledztwo lub ułatwianie popełnienia przestępstw - Działać na niekorzyść UE lub Państw Członkowskich w negocjacjach handlowych lub politycznych - Utrudnić rozwój lub funkcjonowanie ważniejszych polityk UE - Naruszać odpowiednie zarządzanie UE i jej działań.	Należycie upoważnione osoby (sporządzający), dyrektorzy Generalni, szefowie służb [ppkt 17.1]. Sporządzający określają datę, okres lub zdarzenie, kiedy może zostać obniżony stopień zawartości lub jej odtajnienie [ppkt 16.2]. W przeciwnym razie dokumenty są poddawane przeglądowi co pięć lat w celu zapewnienia, że konieczne jest utrzymanie pierwotnej klasyfikacji [ppkt 17.3].	Dokumenty UE ZASTRZEŻONE zostaną oznaczone jako UE ZASTRZEŻONE wraz ze znakami bezpieczeństwa lub oznakowaniami obronności, tam gdzie to stosowne, mechanicznie lub ręcznie [ppkt. 16.4, 16.5, 16.3]. Klasyfikację i znaki bezpieczeństwa UE umieszcza się na górze pierwszej strony. Wszystkie strony są numerowane. Każdy dokument posiada numer referencyjny oraz datę [ppkt 21.1].	Odtajnienie zależy wyłącznie od sporządzającego, który o dokonanych zmianach informuje wszystkich adresatów, do których wysłano lub którym powielono dokument [ppkt 17.3]. Dokumenty UE ZASTRZEŻONE zostają zniszczone przez archiwum, które jest za nie odpowiedzialne, lub przez użytkownika, zgodnie z wytycznymi Przewodniczącego [ppkt 22.5].	Dodatkowe kopie i zbędne dokumenty muszą być zniszczone [ppkt 22.5].

Dodatek 3

Wytyczne dotyczące udostępniania informacji niejawnej UE państwom trzecim lub organizacjom międzynarodowym: poziom 1 współpracy

PROCEDURY

1. Upoważnienie dotyczące udostępniania informacji niejawnej UE państwom, które nie są członkami Unii Europejskiej lub innym organizacjom międzynarodowym, których przepisy i polityka bezpieczeństwa są porównywalne z przepisami Unii Europejskiej spoczywa na Komisji jako organie kolegialnym.

2. Do czasu zawarcia porozumienia w sprawie bezpieczeństwa członek Komisji odpowiedzialny za sprawy bezpieczeństwa jest właściwy do zbadania wniosku o udostępnienie informacji niejawnej UE.

3. Dokonując tego on/ona:

   - uzyskuje opinie sporządzających EUCI, która ma zostać przekazana;

   - ustanawia niezbędne kontakty z organami bezpieczeństwa państw lub organizacji międzynarodowych beneficjentów informacji niejawnej, celem dokonania weryfikacji czy ich przepisy i polityka bezpieczeństwa są tego rodzaju, że gwarantują, iż informacja niejawna im udostępniona będzie chroniona zgodnie z tymi przepisami bezpieczeństwa;

   - uzyskuje opinię Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa w odniesieniu do stopnia zaufania, jakiego można udzielić państwu lub organowi międzynarodowemu będących beneficjentami.

4. Członek Komisji odpowiedzialny za sprawy bezpieczeństwa przesyła wniosek oraz opinię Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa do Komisji, która podejmuje decyzję.

PRZEPISY BEZPIECZEŃSTWA, KTÓRE MAJĄ BYĆ ZASTOSOWANE PRZEZ BENEFICJENTÓW

5. Członek Komisji odpowiedzialny za sprawy bezpieczeństwa informuje państwo lub organizację międzynarodową, beneficjentów informacji niejawnej UE o decyzji Komisji upoważniającej do udostępnienia informacji niejawnej UE.

6. Decyzja o udostępnieniu wchodzi w życie jedynie wtedy, gdy beneficjenci przekażą na piśmie zapewnienie, że będą:

   - używać informacji wyłącznie do uzgodnionych celów;

   - chronić informacje zgodnie z niniejszymi przepisami bezpieczeństwa, w szczególności ze szczególnymi zasadami określonymi poniżej.

7. Personel

a) Liczba urzędników mających dostęp do informacji niejawnej UE jest ściśle ograniczona wyłącznie do osób, których obowiązki wymagają takiego dostępu, zgodnie z zasadą powinien wiedzieć.

b) Wszyscy urzędnicy upoważnieni do dostępu do informacji niejawnej sklasyfikowanej jako UE ZASTRZEŻONE lub wyżej muszą posiadać albo certyfikat bezpieczeństwa na odpowiednim poziomie albo równoważne poświadczenie bezpieczeństwa, wydane przez rząd ich własnego państwa.

8. Przekazywanie dokumentów

a) Praktyczne procedury przekazywania dokumentów są określone w drodze porozumienia. Do czasu zawarcia takiego porozumienia stosuje się przepisy pkt. 21. Porozumienie to musi w szczególności wyszczególniać archiwa, do których ma zostać przekazana informacja niejawna UE.

b) Jeśli informacja niejawna, która została dopuszczona do udostępnienia przez Komisję, zawiera informacje sklasyfikowaną jako UE ŚCIŚLE TAJNE, państwo lub organizacja międzynarodowa będące beneficjentami, ustanawiają centralne archiwum UE i jeśli to konieczne, archiwa pomocnicze. Archiwa te ściśle stosują przepisy równoważne do tych, określonych w pkt. 22 niniejszych przepisów bezpieczeństwa.

9. Rejestracja

W chwili otrzymania przez archiwum dokumentu objętego klauzulą tajności UE ZASTRZEŻONE lub wyższą umieszczany jest on na wykazie w specjalnym rejestrze prowadzonym przez organizację, zawierającym kolumny z informacjami dotyczącymi daty otrzymania, szczegółów dotyczących dokumentu (data, numer referencyjny i numer kopii), jego klasyfikacji, tytułu, nazwy organu otrzymującego lub jego tytuł, data zwrotu potwierdzenia odbioru i data zwrotu dokumentu do jednostki sporządzającej UE lub jego zniszczenia.

10. Niszczenie

a) Dokumenty niejawne UE podlegają zniszczeniu zgodnie z instrukcjami wymienionymi w pkt. 22 niniejszych przepisów bezpieczeństwa. Kopie poświadczeń zniszczenia dla dokumentów objętych klauzulą tajności UE TAJNE i UE ŚCIŚLE TAJNE przesyłane są do archiwum UE, które przekazało dokumenty.

b) Dokumenty niejawne UE włączane są przez organy beneficjentów do planów niszczenia ich własnych dokumentów niejawnych w sytuacjach nadzwyczajnych.

11. Ochrona dokumentów

Należy podejmować wszelkie kroki zapobiegające dostępowi do informacji niejawnej UE przez osoby nieupoważnione.

12. Kopie, tłumaczenia i wyciągi

Nie wolno dokonywać żadnych fotokopii lub tłumaczeń dokumentu objętego klauzulą tajności UE ZASTRZEŻONE lub UE TAJNE, oraz sporządzać z nich wyciągów, bez upoważnienia szefa ds. Bezpieczeństwa danej organizacji, który rejestruje i sprawdza te kopie, tłumaczenia i wyciągi oraz opieczętowuje je, w niezbędnym zakresie.

Powielanie lub tłumaczenie dokumentu niejawnego objętego klauzula tajności UE ŚCIŚLE TAJNE wymaga upoważnienia wyłącznie ze strony organu sporządzającego, która określa liczbę upoważnionych kopii; jeśli organ ten nie może zostać określony, wniosek należy złożyć do Służby ds. Bezpieczeństwa Komisji.

13. Naruszenia bezpieczeństwa

W przypadku, gdy miało miejsce naruszenie bezpieczeństwa lub zachodzi uzasadnione podejrzenie naruszenia bezpieczeństwa, które dotyczyło dokumentu niejawnego UE, niezwłocznie podejmuje się następujące działania, z zastrzeżeniem zawarcia porozumienia w sprawie bezpieczeństwa:

a) przeprowadza się dochodzenie w celu ustalenia okoliczności naruszenia bezpieczeństwa;

b) zawiadamia się Biuro ds. Bezpieczeństwa Komisji, właściwe państwowe służby bezpieczeństwa i organ sporządzający, lub wyraźnie stwierdza się, że nie powiadomiono tej ostatniej, jeżeli nie zostało to uczynione;

c) podejmuje się działania zmierzające do zminimalizowania skutków naruszenia bezpieczeństwa;

d) rozważa się i wprowadza w życie środki mające na celu zapobieżenie jakiemukolwiek ponownemu naruszeniu bezpieczeństwa;

e) wprowadza się w życie wszelkie środki zalecane przez Biuro ds. Bezpieczeństwa Komisji mające na celu zapobieżenie jakiemukolwiek ponownemu naruszeniu bezpieczeństwa.

14. Inspekcje

Biuro ds. Bezpieczeństwa Komisji jest uprawnione, w drodze porozumienia z danym państwem lub z organizacją międzynarodową, do przeprowadzania oceny skuteczności środków ochrony udostępnionych informacji niejawnych UE.

15. Sprawozdawczość

Z zastrzeżeniem zawarcia porozumienia w sprawie bezpieczeństwa, tak długo jak dane państwo lub organizacja międzynarodowa posiada informacje niejawne UE, przesyłają one roczne sprawozdania, przed datą wyszczególnioną w momencie wydania upoważnienia do udostępnienia informacji niejawnej, potwierdzające, że przestrzegano niniejszych przepisów bezpieczeństwa.

Dodatek 4

Wytyczne dotyczące udostępnienia informacji niejawnej UE państwom trzecim lub organizacjom międzynarodowym: poziom 2 współpracy

PROCEDURY

1. Upoważnienie do udostępnienia informacji niejawnej UE państwu trzeciemu lub organizacji międzynarodowej, których przepisy i polityka bezpieczeństwa jest zasadniczo różna od przepisów i polityki UE spoczywa na sporządzającym. Upoważnienie do udostępnienia EUCI sporządzonej w ramach Komisji spoczywa na Komisji jako organie kolegialnym.

2. Z zasady jest to ograniczone do informacji objętych klauzulą tajności UE TAJNE włącznie; wyłącza to informacje niejawne chronionymi specjalnymi znakami lub oznakowaniami bezpieczeństwa.

3. Do czasu zawarcia porozumienia w sprawie bezpieczeństwa, członek Komisji odpowiedzialny za sprawy bezpieczeństwa jest właściwy do zbadania wniosku o udostępnienia informacji niejawnej UE.

4. Dokonując tego on/ona:

   - uzyskuje opinie sporządzających EUCI, która ma zostać udostępniona;

   - ustanawia niezbędne kontakty z organami bezpieczeństwa państw lub organizacji międzynarodowych beneficjentów informacji niejawnej celem uzyskania informacji w sprawie ich polityk i przepisów bezpieczeństwa, w szczególności celem sporządzenia tablicy porównującej klauzule tajności mające zastosowanie w UE i w danym państwie lub organizacji międzynarodowej;

   - organizuje spotkanie Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa, lub jeśli to niezbędne, w ramach „cichej procedury" uzyskuje informacje od państwowej służby bezpieczeństwa Państw Członkowskich celem uzyskania opinii Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa.

5. Opinia Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa dotyczy następujących elementów:

   - zaufania, jakie można pokładać w odniesieniu do danego państwa lub organizacji międzynarodowej beneficjenta informacji niejawnej UE w związku z oceną zagrożenia dla UE lub jej Państw Członkowskich;

   - oceny zdolności beneficjentów do ochrony informacji objętych klauzulą tajności udostępnionych przez UE;

   - propozycji dotyczących praktycznych procedur dotyczących obsługi informacji niejawnej UE (przewidujących na przykład przekazanie okrojonego tekstu) oraz przekazywanych dokumentów (utrzymując lub usuwając nagłówki klasyfikacji UE, szczególne oznakowania, itd.);

- obniżenie stopnia lub odtajnienie przed udostępnieniem informacji państwom lub organizacjom międzynarodowym, będącymi jej beneficjentami.

6. Członek Komisji odpowiedzialny za sprawy bezpieczeństwa przekazuje wniosek oraz opinię Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa Komisji celem wydania decyzji.

PRZEPISY BEZPIECZEŃSTWA, KTÓRE MAJĄ BYĆ ZASTOSOWANE PRZEZ BENEFICJENTÓW

7. Członek Komisji odpowiedzialny za sprawy bezpieczeństwa powiadamia państwa lub organizacje międzynarodowe, beneficjentów informacji niejawnej UE, o decyzji Komisji upoważniającej do udostępnienia informacji niejawnej oraz informuje o ich ograniczeniach.

8. Decyzja o udostępnieniu wchodzi w życie jedynie wtedy, gdy beneficjenci przekażą na piśmie zapewnienie, że będą:

   - używać informacji wyłącznie do uzgodnionych celów;

   - chronić informacje zgodnie z przepisami bezpieczeństwa ustanowionymi przez Komisję.

9. Stosuje się następujące zasady ochrony, chyba, że Komisja, po uzyskaniu opinii technicznej Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa, zdecyduje o szczególnej procedurze dotyczącej obsługiwania dokumentów niejawnych UE (usunięcie wskazania klasyfikacji UE, szczególne oznakowania.)

10. Personel

    a) liczba urzędników mających dostęp do informacji niejawnej UE jest ściśle ograniczona wyłącznie do osób, których obowiązki wymagają takiego dostępu, zgodnie z zasadą „powinien wiedzieć”;

    b) wszyscy urzędnicy lub obywatele upoważnieni do dostępu do informacji niejawnych udostępnionych przez Komisję, muszą posiadać albo krajowe poświadczenie bezpieczeństwa albo upoważnienie do dostępu, na poziomie odpowiadającym równoważnemu poziomowi UE, tak jak zostało to określone w tablicy porównawczej;

    c) krajowe poświadczenia bezpieczeństwa lub upoważnienia przekazywane są Przewodniczącemu do informacji.

11. Przekazywanie dokumentów

    Praktyczne procedury przekazywania dokumentów zostają określone w drodze porozumienia. Do czasu zawarcia takiego porozumienia stosuje się przepisy pkt. 21. Porozumienie to musi w szczególności wyszczególniać archiwa, do których ma zostać przekazana informacja niejawna UE, precyzować adresy, pod które dokumenty maja

być przekazane, jak również usługi kurierskie lub usługi pocztowe wykorzystane do przekazania informacji niejawnej UE.

12. Rejestracja przy wpłynięciu

Krajowy organ bezpieczeństwa, adresat informacji niejawnej lub jego odpowiednik w państwie przyjmującym, działający w imieniu jego rządu, przesłane przez Komisję informację niejawne lub Biuro ds. Bezpieczeństwa Organizacji Międzynarodowej, otwierają specjalny rejestr wpływu informacji niejawnej UE. Rejestr zawiera kolumny wskazujące datę otrzymania, szczegółowe dane dotyczące dokumentu (jego datę, numer referencyjny oraz numer kopii), jego klauzulę tajności, tytułu, nazwę adresata lub jego tytuł, datę zwrotu potwierdzenia odbioru i datę zwrotu dokumentu do UE lub jego zniszczenia.

13. Zwrot dokumentów

Gdy odbiorca zwraca Komisji dokument niejawny postępuje zgodnie z tym jak wskazano w powyższym punkcie „Przekazywanie dokumentów".

14. Ochrona

a) W przypadku, gdy dokumenty nie są wykorzystywane, są przechowywane w szafach pancernych zatwierdzonych do gromadzenia krajowych materiałów niejawnych takiej samej klasyfikacji. Szafa pancerna nie zawiera informacji na temat jej zawartości i powinna być dostępna wyłącznie do osób upoważnionych do obsługi informacji niejawnej UE. W przypadku stosowania szyfrów do szaf pancernych, szyfry te są znane wyłącznie tym urzędnikom w danym państwie lub organizacji międzynarodowej, którzy upoważnieni są do dostępu do informacji niejawnej UE, przechowywanej w szafie pancernej i podlegać będą zmianom co każde sześć miesięcy, lub częściej w przypadku przeniesienia urzędnika, cofnięcia poświadczenia bezpieczeństwa jednemu z urzędników znających szyfry lub gdy istnieje niebezpieczeństwo ujawnienia informacji niejawnej.

b) Dokumenty objęte klauzulą tajności UE mogą być wyjmowane z szafy pancernej wyłącznie przez tych urzędników, którzy zostali sprawdzeni w zakresie dostępu do dokumentów niejawnych UE i którzy objęci są zasadą powinien wiedzieć. Pozostają oni odpowiedzialni za ścisłą pieczę nad tymi dokumentami, tak długo jak długo znajdują się one w ich posiadaniu, w szczególności, że osoby nieupoważnione nie będą miały dostępu do tych dokumentów. Zapewniają oni także, że dokumenty będą przechowywane w szafach pancernych po zakończeniu przez nich konsultacji oraz po godzinach urzędowania.

c) Nie wolno dokonywać żadnych fotokopii dokumentu sklasyfikowanego jako UE ZASTRZEŻONE lub wyżej, oraz sporządzać wyciągów, bez upoważnienia Biura ds. Bezpieczeństwa Komisji.

d) Należy opracować procedurę dotyczącą szybkiego i całkowitego zniszczenia dokumentów w sytuacjach nadzwyczajnych i potwierdzić ją w Biurze ds. Bezpieczeństwa Komisji.

15. Ochrona fizyczna

a) w przypadku ich nie używania, szafy pancerne przeznaczone do przechowywania dokumentów niejawnych UE pozostają zamknięte przez cały czas;

b) w przypadku, gdy jest to niezbędne do celów konserwacji lub z uwagi na konieczność wejścia lub pracy personelu sprzątającego w pokoju, w którym znajdują się szafy pancerne, osoby te podlegają stałemu eskortowaniu przez członka służb bezpieczeństwa danego państwa lub organizacji lub przez urzędnika szczególnie odpowiedzialnego za nadzorowanie bezpieczeństwa pokoju;

c) poza normalnymi godzinami pracy (w nocy, w weekend, w dni ustawowo wolne od pracy), szafy pancerne zawierające dokumenty niejawne UE, podlegają ochronie albo przez straże albo przez automatyczny system alarmowy.

16. Naruszenia bezpieczeństwa

W przypadku, gdy miało miejsce naruszenie bezpieczeństwa lub zachodzi uzasadnione podejrzenie naruszenia bezpieczeństwa, które dotyczyło dokumentu niejawnego UE, niezwłocznie podejmuje się następujące działania:

a) niezwłocznie przesyła się sprawozdanie do Biura ds. Bezpieczeństwa Komisji lub PSB Państwa Członkowskiego, które podjęło inicjatywę przekazywania dokumentu (z kopią do Biura ds. Bezpieczeństwa Komisji);

b) przeprowadza się dochodzenie w sprawie sporządzenia pełnego sprawozdania, które przesyła się do organu bezpieczeństwa (patrz lit. a) powyżej). Następnie przyjmuje się nieodzowne środki, mające na celu zaradzenie zaistniałej sytuacji.

17. Inspekcje

Biuro ds. Bezpieczeństwa Komisji jest upoważnione, w drodze porozumienia z danym państwem lub organizacją międzynarodową, do przeprowadzenia oceny skuteczności środków ochrony udostępnionych informacji niejawnych UE.

18. Sprawozdawczość

Z zastrzeżeniem zawarcia porozumienia w sprawie bezpieczeństwa, tak długo jak dane państwo lub organizacja międzynarodowa posiada informacje niejawne UE, przesyłają one roczne sprawozdania, przed datą wyszczególnioną w momencie wydania upoważnienia do udostępniania informacji niejawnej, potwierdzające, że przestrzegano niniejszych przepisów bezpieczeństwa.

Dodatek 5

Wytyczne dotyczące udostępniania informacji niejawnej UE państwom trzecim lub organizacjom międzynarodowym: poziom 3 współpracy

PROCEDURY

1. Od czasu do czasu Komisja może życzyć sobie współpracy w pewnych szczególnych okolicznościach z państwami lub organizacjami, które nie mogą dać gwarancji wymaganych przez niniejsze przepisy bezpieczeństwa, ale współpraca z którymi może wymagać udostępnienia informacji niejawnej UE.

2. Upoważnienie do udostępnienia informacji niejawnej UE państwu trzeciemu lub organizacji międzynarodowej, których przepisy i polityki bezpieczeństwa różnią się znacząco od przepisów i polityki UE, spoczywa na sporządzającym. Upoważnienie do udostępnienia EUCI sporządzonej w ramach Komisji spoczywa na Komisji jako organie kolegialnym.

   Z zasady ograniczone jest to do informacji niejawnych sklasyfikowanych do poziomu UE TAJNE włącznie; wyłącza to informacje niejawne chronione specjalnymi znakami lub oznakowaniami bezpieczeństwa.

3. Komisja rozważa celowość udostępniania informacji niejawnej, oceniając zasadę powinien wiedzieć w kontekście beneficjenta i decyduje o charakterze informacji niejawnej, która może być przekazana.

4. Jeśli Komisja jest za udostępnianiem informacji, Członek Komisji odpowiedzialny za sprawy bezpieczeństwa:

   - uzyskuje opinie sporządzających EUCI, która ma zostać udostępniona;

   - organizuje spotkanie Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa, lub jeśli to niezbędne, w ramach „cichej procedury" uzyskuje informacje od Służb Ochrony Państwa Państw Członkowskich celem uzyskania opinii Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa.

5. Opinia Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa dotyczy następujących elementów:

   a) oceny zagrożenia bezpieczeństwa UE lub jej Państw Członkowskich;

   b) poziomu klasyfikacji informacji, która może zostać udostępniona;

   c) obniżenia stopnia lub odtajnienie przed udostępnieniem informacji;

   d) procedur dotyczących obsługi dokumentów podlegających udostępnianiu (patrz punkt powyżej);

   e) możliwych sposobów przekazania (zastosowania publicznych usług pocztowych, publicznych lub chronionych systemów telekomunikacyjnych, bagażu

dyplomatycznego, sprawdzonych kurierów, itd.).

6. Dokumenty przekazane państwom lub organizacjom określonym w niniejszym dodatku będą, co do zasady, przygotowane w taki sposób, aby nie znajdowały się na nich odniesienia do źródła informacji lub poziomu klasyfikacji UE. Grupa Doradcza Komisji ds. Polityki Bezpieczeństwa może zalecić:

   - zastosowanie szczególnych oznakowań lub nazw kodowych;

   - zastosowanie szczególnego systemu klasyfikacji łączącego sensytywność informacji ze środkami kontroli wymaganymi od sposobów przekazania dokumentów beneficjentowi.

7. Przewodniczący przekazuje opinię Grupy Doradczej Komisji ds. Polityki Bezpieczeństwa do Komisji, celem podjęcia decyzji.

8. Po zatwierdzeniu przez Komisję udostępnienia informacji niejawnej UE oraz praktycznej, wprowadzającej w życie procedury, Biuro ds. Bezpieczeństwa Komisji ustanawia niezbędny kontakt z organem bezpieczeństwa danego państwa lub organizacji, w celu ułatwienia stosowania przewidzianych środków bezpieczeństwa.

9. Członek Komisji odpowiedzialny za sprawy bezpieczeństwa informuje Państwa Członkowskie o charakterze oraz klasyfikacji informacji, wymieniając organizacje i państwa, do których może ona być przekazana, zgodnie z decyzją Komisji.

10. Biuro ds. Bezpieczeństwa Komisji podejmuje wszelkie niezbędne środki mające na celu ułatwienie oceny szkody oraz procedury rewizyjne.

    W każdym przypadku zmiany warunków współpracy, Komisja ponownie rozważa zagadnienie.

PRZEPISY BEZPIECZEŃSTWA, KTÓRE MAJĄ BYĆ ZASTOSOWANE PRZEZ BENEFICJENTÓW

11. Członek Komisji odpowiedzialny za sprawy bezpieczeństwa informuje państwa lub organizacje międzynarodowe, beneficjentów informacji niejawnej UE, o decyzji Komisji upoważniającej do udostępnienia informacji niejawnej UE, wraz ze szczegółowymi zasadami ochrony proponowanymi przez Grupę Doradczą Komisji ds. Polityki Bezpieczeństwa, a zatwierdzonymi przez Komisję.

12. Decyzja wchodzi w życie jedynie wtedy, gdy beneficjenci przekażą pisemne zapewnienie, że:

    - nie będą używać informacji do celów innych niż współpraca, o jakiej zdecydowała Komisja;

    - zapewnią ochronę informacji wymaganą przez Komisję.

13. Przekazywanie dokumentów

a) Praktyczne procedury przekazania dokumentów zostają uzgodnione między Biurem ds. Bezpieczeństwa Komisji a organami bezpieczeństwa przyjmujących państw lub organizacji międzynarodowych. W szczególności wyszczególniają one dokładny adres, na który dokumenty muszą być przekazane.

b) Dokumenty sklasyfikowane jako UE POUFNE i wyżej przekazywane są w podwójnej kopercie. Wewnętrzna koperta oznaczona jest uzgodnioną wcześniej szczególną pieczęcią lub nazwami kodowymi i wskazuje specjalną klauzulę tajności, zatwierdzoną dla dokumentu. Formularz potwierdzenia odbioru załącza się do każdego dokumentu niejawnego. Formularz potwierdzenia odbioru, który sam w sobie nie stanowi dokumentu niejawnego, przytacza wyłącznie dane szczegółowe dokumentu (jego numer referencyjny, datę, numer kopii) oraz język, nie używając tytułu.

c) Wewnętrzna koperta jest następnie umieszczana w kopercie zewnętrznej, która oznaczona jest numerem przesyłki, służącym do celów potwierdzenia odbioru. Zewnętrzna koperta nie nosi oznaczeń klasyfikacji bezpieczeństwa.

d) Potwierdzenie odbioru wskazujące numer przesyłki zawsze przekazywany jest kurierom.

14. Rejestracja przy wpłynięciu

Krajowy organ bezpieczeństwa, adresat informacji niejawnej lub jego odpowiednik w państwie przyjmującym, w imieniu jego rządu lub Biuro ds. Bezpieczeństwa Organizacji Międzynarodowej przesłane przez Komisję informacje niejawne, otwierają specjalny rejestr wpływu informacji niejawnej UE. Rejestr zawiera kolumny wskazujące datę otrzymania, szczegółowe dane dotyczące dokumentu (jego datę, numer referencyjny oraz numer kopii), jego klauzulę tajności, tytuł, nazwę adresata lub jego tytuł, datę zwrotu potwierdzenia odbioru i datę zwrotu potwierdzenia odbioru do UE oraz datę zniszczenia tego dokumentu.

15. Używanie i ochrona wymienionych informacji niejawnych

a) informacje na poziomie UE TAJNE są obsługiwane przez szczególnie wyznaczonych urzędników, upoważnionych do posiadania dostępu do informacji niejawnych posiadających tę klauzulę. Są one gromadzone w gablotach bezpieczeństwa dobrej jakości, które mogą być otwierane wyłącznie przez osoby upoważnione do dostępu do informacji, które one zawierają. Strefy, w których znajdują się te gabloty będą stale strzeżone oraz ustanawia się system weryfikacji w celu zapewnienia, że wstęp do nich mają wyłącznie osoby należycie upoważnione. Informacje z klauzulą tajności UE TAJNE przekazywane są za pomocą bagażu dyplomatycznego, chronionego systemu pocztowego lub za pośrednictwem bezpiecznych systemów telekomunikacyjnych. Dokument objęty klauzulą tajności UE TAJNE jest kopiowany wyłącznie za pisemną zgodą organu sporządzającej. Wszystkie kopie podlegają zarejestrowaniu i nadzorowaniu. Wydaje się potwierdzenie odbioru dla wszelkich czynności dotyczących dokumentów objętych klauzulą tajności UE TAJNE;

b) UE POUFNE obsługiwane są przez należycie wyznaczonych urzędników,

upoważnionych do uzyskania informacji na ich temat. Dokumenty przechowywane są w zamkniętych, bezpiecznych gablotach, znajdujących się w strefach podlegających kontroli;

UE POUFNE przekazywane są za pomocą bagażu dyplomatycznego, usług poczty wojskowej lub bezpiecznych systemów telekomunikacyjnych. Organ przyjmujący może sporządzać kopie, których numery i sposób rozprowadzania jest odnotowywany w specjalnym rejestrze;

c) Informacje objęte klauzulą tajności UE ZASTRZEŻONE przechowywane są w pomieszczeniach, które nie są dostępne dla nieupoważnionego personelu i przechowywane w zamkniętych pojemnikach. Dokumenty mogą być przekazywane za pośrednictwem publicznych usług pocztowych w podwójnej kopercie a w sytuacjach nadzwyczajnych, w trakcie operacji, przez niechronione publiczne systemy telekomunikacyjne. Przyjmujący może sporządzać kopie;

d) Informacje jawne nie wymagają szczególnych środków ochrony i mogą być przekazywane za pośrednictwem publicznych usług pocztowych i publicznych systemów telekomunikacyjnych. Przyjmujący może sporządzać kopie.

16. Niszczenie

Zbędne dokumenty podlegają zniszczeniu. W przypadku dokumentów objętych klauzulami tajności UE ZASTRZEŻONE i UE POUFNE, należy wprowadzić odpowiednią notatkę do rejestru. W przypadku dokumentów objętych klauzulą tajności UE TAJNE, wystawia się poświadczenie zniszczenia, podpisywane przez dwie osoby świadczące o ich zniszczeniu.

17. Naruszenia bezpieczeństwa

Jeśli informacja objęta klauzulą tajności UE POUFNE lub UE TAJNE została ujawniona lub powstało uzasadnione podejrzenie jej ujawnienia PSB Państwa lub szef bezpieczeństwa w organizacji przeprowadzają dochodzenie w sprawie okoliczności ujawnienia. Biuro ds. Bezpieczeństwa Komisji informowane jest o wynikach tego dochodzenia. Podejmuje się niezbędne środki celem zaradzenia powtórzenia się nieadekwatnych procedur lub sposobów przechowywania, jeśli doprowadziły one do ich ujawnienia.

Dodatek 6

WYKAZ SKRÓTÓW

ACPC	Doradczy Komitet ds. Zamówień i Kontraktów
CrA	Organ szyfrów
CISO	Centralny urzędnik ds. Bezpieczeństwa Informatycznego
COMPUSEC	Bezpieczeństwo systemów komputerowych
COMSEC	Bezpieczeństwo systemów łączności
CSO	Biuro ds. Bezpieczeństwa Komisji
ESDP	Europejska Polityka Bezpieczeństwa i Obronna
EUCI	Informacja niejawna UE
IA	Organ INFOSEC
INFOSEC	Bezpieczeństwo Informacji
IO	Właściciel Informacji
ISO	Międzynarodowa Organizacja Normalizacyjna
IT	Technologia Informatyczna
LISO	Lokalny urzędnik ds. Bezpieczeństwa Informatycznego
LSO	Lokalny urzędnik ds. Bezpieczeństwa
MSO	Urzędnik ds. Bezpieczeństwa Posiedzenia
PSB	Państwowe służby bezpieczeństwa
PC	Komputer osobisty
RCO	Urzędnik ds. Kontroli Archiwum
SAA	Organ Akredytacji Bezpieczeństwa
SecOPS	Operacyjne Procedury Bezpieczeństwa
SSRS (SWBS)	Szczególne wymagania bezpieczeństwa systemów
TA	Organ Tempest

TSO	Właściciel Systemów Technicznych