32001D0844

L 317/1 *DZIENNIK URZĘDOWY WSPÓLNOT EUROPEJSKICH* 3.12.2001

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

Niniejszym przepisy bezpieczeństwa Komisji, które są załączone do tej decyzji, zostają dodane do regulaminu wewnętrznego 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 BEZPIECZEŃSTWA KOMISJI

(1) W celu rozwoju działań Komisji w dziedzinach, które wymagają zachowania pewnego stopnia poufności, wskazane jest stworzenie całościowego systemu bezpieczeństwa obejmującego Komisję, inne instytucje, struktury, biura i agencje ustanowione na mocy Traktatu ustanawiającego Wspólnotę Europejską lub Traktatu o Unii Europejskiej, Państwa Członkowskie, a także wszelkich innych odbiorców informacji klasyfikowanych Unii Europejskiej, zwanych dalej „informacjami klasyfikowanymi UE".

(2) W celu zapewnienia skuteczności ustanowionego na tej podstawie systemu bezpieczeństwa Komisja będzie udostępniać informacje klasyfikowane UE jedynie tym zewnętrznym strukturom, które przedstawią zapewnienie, że przedsięwzięły wszystkie środki konieczne do stosowania zasad ściśle odpowiadających niniejszym przepisom.

(3) Niniejsze przepisy nie naruszają przepisów rozporządzenia nr 3 z dnia 31 lipca 1958 roku 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 C (95) 1510 z dnia 23 listopada 1995 roku w sprawie ochrony systemów informatycznych.

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

(5) Komisja podkreśla, że istotne jest, by także inne instytucje, gdy ma to zastosowanie, przyjmowały przepisy i standardy bezpieczeństwa niezbędne w celu ochrony interesów Unii i jej Państw Członkowskich.

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

(7) Niniejsze przepisy nie naruszają postanowień art. 255 Traktatu i rozporządzenia nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji [4];

Artykuł 1

Zasady bezpieczeństwa Komisji zostają określone w niniejszym załączniku.

Artykuł 2

1. Członek Komisji odpowiedzialny za kwestie bezpieczeństwa jest zobowiązany do podjęcia odpowiednich środków w celu zapewnienia, że zasady, o których mowa w art. 1, są przestrzegane w toku pracy z informacjami klasyfikowanymi UE w ramach Komisji, przez jej urzędników i innych pracowników, przez osoby delegowane do pracy w Komisji, a także we wszystkich obiektach Komisji, włącznie z jej przedstawicielstwami i biurami w Unii oraz przedstawicielstwami w państwach trzecich, a także przez zewnętrznych kontrahentów.

2. Państwa Członkowskie, inne instytucje, struktury, biura czy agencje, ustanowione z mocy lub na podstawie Traktatów, są uprawnione do otrzymywania informacji klasyfikowanych UE, pod warunkiem że zapewnią przestrzeganie w toku pracy z tymi informacjami zasad ściśle odpowiadających przepisom, o których mowa w art. 1, w ramach ich służb i obiektów, a w szczególności przez:

a) członków stałych przedstawicielstw Państw Członkowskich przy Unii Europejskiej, a także członków krajowych delegacji biorących udział w posiedzeniach Komisji lub w jej strukturach, lub też uczestniczących w innych przedsięwzięciach Komisji;

b) inne osoby będące członkami administracji Państw Członkowskich, które mają dostęp do informacji klasyfikowanych UE, niezależnie od tego, czy wykonują one swoje obowiązki na terytorium tego kraju, czy też poza jego granicami; oraz

c) zewnętrznych kontrahentów i osoby delegowane do pracy, które mają dostęp do informacji klasyfikowanych UE.

---

[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.

Artykuł 3

Państwa trzecie, organizacje międzynarodowe i inne struktury są uprawnione do otrzymywania informacji klasyfikowanych UE, pod warunkiem że zapewnią przestrzeganie w toku pracy z tymi informacjami zasad ściśle odpowiadających przepisom, o których mowa w art. 1.

Artykuł 4

W celu zapewnienia, że przestrzegane są podstawowe zasady i minimalne standardy bezpieczeństwa określone w części I załącznika, członek Komisji odpowiedzialny za kwestie bezpieczeństwa może stosować środki przewidziane w części II załącznika.

Artykuł 5

Od dnia rozpoczęcia stosowania niniejszych przepisów zastępują one:

a) decyzję Komisji C (94) 3282 z dnia 30 listopada 1994 r. w sprawie środków bezpieczeństwa stosowanych wobec informacji klasyfikowanych sporządzonych lub przekazanych w związku z działalnością Unii Europejskiej;

b) decyzję Komisji C (99) 423 z dnia 25 lutego 1999 r. odnoszącą się do procedur, na podstawie których urzędnicy i inni pracownicy Komisji Europejskiej mogą uzyskać dostęp do informacji klasyfikowanych znajdujących się w Komisji.

Artykuł 6

Od dnia rozpoczęcia stosowania niniejszych przepisów wszystkie informacje klasyfikowane, które uprzednio znalazły się w Komisji, z wyłączeniem informacji Euratom:

a) jeśli zostały wytworzone przez Komisję, zostają automatycznie przeklasyfikowane na „EU RESTRICTED", chyba że ich autor podejmie do dnia 31 stycznia 2002 r. decyzję o nadaniu im innej klauzuli. W takim przypadku autor jest zobowiązany do poinformowania o tym wszystkich adresatów danego dokumentu;

b) jeśli zostały wytworzone przez autorów spoza Komisji, zachowują oryginalną klauzulę tajności i tym samym są traktowane jak informacje klasyfikowane UE o klauzuli równorzędnej, chyba że autor wyraził zgodę na jej obniżenie lub zniesienie.

ZAŁĄCZNIK

ZASADY BEZPIECZEŃSTWA

Spis treści

CZĘŚĆ I: PODSTAWOWE ZASADY I MINIMALNE STANDARDY BEZPIECZEŃSTWA

1. WPROWADZENIE

Niniejsze przepisy ustanawiają podstawowe zasady i minimalne standardy bezpieczeństwa przeznaczone do stosowania w odpowiedni sposób przez Komisję Europejską we wszystkich miejscach prowadzenia przez nią działalności, a także przez wszystkich odbiorców informacji klasyfikowanych UE. Ich celem jest zapewnienie bezpieczeństwa oraz zagwarantowanie każdemu z wymienionych pomiotów, że został ustanowiony wspólny standard ochrony.

2. ZASADY OGÓLNE

Polityka bezpieczeństwa Komisji stanowi integralną część jej całościowej polityki wewnętrznego zarządzania i z tego względu jest oparta na zasadach rządzących całością jej działań.

Zasady te obejmują legalność, przejrzystość, odpowiedzialność i pomocniczość (proporcjonalność).

Legalność wskazuje na konieczność ścisłego przestrzegania przepisów prawa przy wykonywaniu zadań związanych z bezpieczeństwem oraz stosowania się do wymogów prawnych. Oznacza także, że zakresy odpowiedzialności w sferze bezpieczeństwa muszą być oparte na odpowiednich przepisach prawa. Pełne zastosowanie mają tu przepisy regulaminu pracowniczego, w szczególności art. 17 dotyczący obowiązku zachowania dyskrecji w odniesieniu do informacji Komisji oraz tytuł VI określający środki dyscyplinarne. Oznacza to także, że pociąganie do odpowiedzialności za przypadki nieprzestrzegania przepisów bezpieczeństwa w ramach obszaru odpowiedzialności Komisji odbywa się zgodnie z polityką Komisji w zakresie działań dyscyplinarnych i jej polityką dotyczącą współpracy z Państwami Członkowskimi w zakresie odpowiedzialności karnej.

Przejrzystość wskazuje na potrzebę zapewnienia jasności wszelkich zasad i przepisów w zakresie bezpieczeństwa, zachowania równowagi pomiędzy różnymi służbami i dziedzinami (bezpieczeństwo fizyczne przeciwko ochronie informacji itp.) oraz konieczność prowadzenia spójnej i odpowiednio ukierunkowanej polityki mającej na celu edukację w zakresie bezpieczeństwa. Określa ona także potrzebę opracowania zrozumiałych pisemnych wytycznych dotyczących wdrażania środków bezpieczeństwa.

Odpowiedzialność oznacza, że w sferze bezpieczeństwa muszą być jasno określone zakresy odpowiedzialności. Co więcej, wskazuje to na potrzebę regularnego sprawdzania, czy odpowiedzialność ta jest w odpowiedni sposób egzekwowana.

Pomocniczość, lub proporcjonalność, oznacza, że struktury bezpieczeństwa muszą być organizowane na najniższym możliwym poziomie organizacji i być jak najściślej związane z Dyrekcjami Generalnymi i służbami Komisji. Wskazuje to także, że działania w zakresie bezpieczeństwa należy ograniczyć tylko do tych komórek organizacyjnych, w których są one naprawdę potrzebne. Oznacza to również, że środki ochrony muszą być odpowiednie do chronionych interesów oraz do faktycznych lub potencjalnych zagrożeń, zapewniając obronę, która powoduje możliwie najmniejsze utrudnienia.

3. PODSTAWY BEZPIECZEŃSTWA

Podstawy bezpieczeństwa tworzą:

a) w każdym z Państw Członkowskich, instytucja odpowiedzialna za:

   1. pozyskiwanie i gromadzenie informacji operacyjnych dotyczących szpiegostwa, aktów sabotażu, terroryzmu i innych zagrożeń dla bezpieczeństwa państwa; oraz

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

b) w każdym z Państw Członkowskich, a także w ramach Komisji, władza techniczna INFOSEC, odpowiedzialna za współpracę z właściwymi władzami bezpieczeństwa w zakresie przekazywania informacji o zagrożeniach natury technicznej dla bezpieczeństwa i wskazywania środków przeciwdziałania;

c) systematyczna współpraca instytucji rządowych, agencji i właściwych służb instytucji europejskich w celu określania i zalecania, w zależności od potrzeb:

   1. które osoby, informacje i zasoby wymagają ochrony; oraz

   2. wspólnych standardów ochrony;

d) ścisła współpraca pomiędzy Biurem Bezpieczeństwa Komisji a innymi odpowiedzialnymi za bezpieczeństwo służbami instytucji europejskich oraz Biurem Bezpieczeństwa NATO (NOS).

4. ZASADY BEZPIECZEŃSTWA INFORMACJI

4.1. **Cele**

Podstawowe cele ochrony informacji to:

a) ochrona informacji klasyfikowanych UE przed szpiegostwem, narażeniem na szwank ich bezpieczeństwa lub nieupoważnionym ujawnieniem;

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

c) ochrona pomieszczeń Komisji, w których znajdują się informacje UE, przed sabotażem i celowym złośliwym uszkodzeniem;

d) zapewnienie – w przypadku gdyby zastosowane środki ochrony zawiodły – możliwości oceny wyrządzonych szkód, ograniczenia ich skali oraz zastosowania niezbędnych środków zaradczych.

4.2. **Definicje**

W rozumieniu niniejszego dokumentu:

a) Pojęcie „informacje klasyfikowane UE" oznacza wszelkie informacje i materiały, których nieupoważnione ujawnienie mogłoby w różnym stopniu narazić na szkodę interesy UE bądź jednego lub kilku Państw Członkowskich, niezależnie od tego, czy informacja ta została wytworzona w UE, czy też przekazana przez Państwa Członkowskie, państwa trzecie lub organizacje międzynarodowe

b) Pojęcie „dokument" oznacza pismo, notatkę, sprawozdanie, memorandum, sygnał/depeszę, szkic, zdjęcie, slajd, film, mapę, plan, wykres, notes, matrycę, kalkę, taśmę z maszyny do pisania lub drukarki, taśmę, kasetę, twardy dysk, CD-ROM oraz każdy inny nośnik, na którym została utrwalona informacja.

c) Pojęcie „materiał" oznacza „dokument", zgodnie z definicją zawartą w literze b) powyżej, a także dowolną część wyposażenia lub broni wyprodukowanych lub będących w trakcie produkcji.

d) Pojęcie „ograniczony dostęp" oznacza określenie, że dany pracownik powinien uzyskać dostęp do informacji klasyfikowanych UE w związku z pełnieniem swojego stanowiska lub wykonywaniem zadania.

e) „Upoważnienie" oznacza decyzję przewodniczącego Komisji o przyznaniu danej osobie dostępu do informacji klasyfikowanych UE o określonym poziomie tajności, na podstawie pozytywnego wyniku postępowania sprawdzającego, przeprowadzonego na podstawie przepisów danego państwa przez krajową władzę bezpieczeństwa.

f) Pojęcie „klauzula tajności" oznacza określenie odpowiedniego poziomu ochrony informacji, której nieupoważnione ujawnienie mogłoby w pewnym stopniu narazić na szkodę interesy Komisji lub Państwa Członkowskiego.

g) Pojęcie „obniżenie klauzuli" (déclassement) oznacza zmianę klauzuli na niższą.

h) Pojęcie „zniesienie klauzuli" (déclassfication) oznacza pozbawienie informacji klauzuli tajności.

i) Pojęcie „wytwórca" oznacza odpowiednio upoważnionego autora dokumentu klasyfikowanego. W obrębie Komisji dyrektorzy departamentów mogą upoważniać podległych im pracowników do wytwarzania informacji klasyfikowanych UE.

j) Pojęcie „departamenty Komisji" oznacza departamenty i służby Komisji, w tym gabinety, we wszystkich miejscach zatrudnienia, w tym także Wspólne Centrum Badawcze, przedstawicielstwa i biura w Unii i delegatury w państwach trzecich.

4.3. **Klauzule tajności**

a) W przypadkach gdy konieczne jest zastosowanie środków bezpieczeństwa, niezbędne jest dokonanie rozważnej i opartej na doświadczeniu oceny, które informacje i materiały wymagają ochrony, i określenie zakresu tej ochrony. Najistotniejsze jest dostosowanie jej stopnia do znaczenia – z punktu widzenia bezpieczeństwa – danej informacji lub materiału, które mają zostać objęte ochroną. W celu zapewnienia możliwie swobodnego przepływu informacji należy podjąć kroki w celu zapobiegania zarówno zawyżaniu, jak i zaniżaniu klauzuli.

b) System nadawania klauzul stanowi instrument zapewniający wdrażanie w życie powyższych zasad. Podobny system nadawania klauzul powinien być stosowany w toku planowania i realizacji działań mających na celu przeciwdziałanie szpiegostwu, aktom sabotażu, terroryzmowi i innym zagrożeniom, tak aby najściślejszą ochroną były objęte najważniejsze obiekty, w których znajdują się informacje klasyfikowane, oraz ich najbardziej newralgiczne punkty.

c) Wyłącznie wytwórca informacji odpowiada za nadanie jej klauzuli.

d) Poziom klauzuli może być określony wyłącznie na podstawie zawartości informacji.

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

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

4.4. **Cele stosowania środków bezpieczeństwa**

Środki bezpieczeństwa muszą:

a) obejmować wszystkie osoby, które mają dostęp do informacji klasyfikowanych, nośniki tych informacji, wszystkie obiekty, w których się one znajdują, oraz ważne instalacje;

b) być zaprojektowane w sposób zapewniający wykrycie osób, które z racji uplasowania mogłyby stanowić zagrożenie dla bezpieczeństwa informacji lub ważnych instalacji, w których znajdują się takie informacje, oraz pozwalający na uniemożliwienie im dostępu do informacji lub usunięcie ich ze stanowiska;

c) zapobiegać uzyskiwaniu przez osoby nieupoważnione dostępu do informacji klasyfikowanych lub zawierających je instalacji;

d) zapewnić, że wszystkie informacje klasyfikowane są udostępniane zgodnie z zasadą ograniczonego dostępu, który stanowi podstawę wszystkich wymiarów bezpieczeństwa;

e) zapewnić integralność (tzn. zapobiegać dokonywaniu zmian lub niszczeniu informacji w sposób nieupoważniony) i dostępność (tzn. zapewniać uzyskanie dostępu przez osoby, które powinny zapoznać się z informacją i zostały do tego upoważnione) wszystkich informacji, klasyfikowanych i jawnych, w szczególności przechowywanych, przetwarzanych lub przesyłanych w postaci elektromagnetycznej.

5. ORGANIZACJA SYSTEMU BEZPIECZEŃSTWA

5.1. **Wspólne standardy minimalne**

Komisja jest zobowiązana do zapewnienia, że wspólne standardy minimalne w zakresie bezpieczeństwa są przestrzegane przez wszystkich odbiorców informacji klasyfikowanych UE, w ramach instytucji i w zakresie jej właściwości, tj. przez wszystkie departamenty i kontrahentów, tak by przekazywaniu informacji klasyfikowanych UE towarzyszyła pewność, że będą one chronione z zachowaniem należytej staranności. Standardy minimalne obejmują kryteria stosowane w toku postępowań sprawdzających oraz procedury ochrony informacji klasyfikowanych UE.

Komisja zezwala na udostępnienie informacji klasyfikowanych UE podmiotom zewnętrznym wyłącznie wtedy, gdy zapewnią one, że w toku wykorzystywania tych informacji przestrzegane są przepisy co najmniej ściśle odpowiadające niniejszym standardom minimalnym.

5.2. **Organizacja**

W ramach Komisji system bezpieczeństwa ma charakter dwupoziomowy:

a) Na poziomie Komisji jako całości istnieje Biuro Bezpieczeństwa Komisji razem z władzą akredytacji bezpieczeństwa (SAA), pełniącą także funkcję władzy kryptograficznej (CrA) i władzy TEMPEST, oraz władzą bezpieczeństwa teleinformatycznego (IA), a także jedną lub kilkoma głównymi kancelariami tajnymi UE, z których każda zatrudnia jednego lub kilku urzędników kontroli kancelarii (RCO).

b) Na poziomie poszczególnych departamentów Komisji za bezpieczeństwo są odpowiedzialni jeden lub kilku lokalnych pełnomocników ochrony (LSO), jeden lub kilku głównych inspektorów bezpieczeństwa teleinformatycznego (CISO), lokalni inspektorzy bezpieczeństwa teleinformatycznego (LISO) oraz lokalne kancelarie tajne UE, zatrudniające jednego lub kilku urzędników kontroli kancelarii (RCO).

c) Struktury bezpieczeństwa funkcjonujące na poziomie centralnym są zobowiązane do nadzorowania pracy struktur lokalnych.

6. BEZPIECZEŃSTWO OSOBOWE

6.1. **Postępowania sprawdzające**

Wszystkie osoby, które powinny uzyskać dostęp do informacji o klauzuli EU CONFIDENTIAL lub wyższej, przed uzyskaniem prawa dostępu zostają odpowiednio sprawdzone. Podobne postępowanie jest wymagane w odniesieniu do osób, których obowiązki służbowe obejmują przeprowadzanie czynności technicznych związanych z dokonywaniem operacji w ramach systemów i sieci teleinformatycznych zawierających informacje klasyfikowane lub też z utrzymaniem ich funkcjonowania. Postępowanie ma za zadanie określenie, czy dana osoba:

a) jest w pełni lojalna;

b) jej charakter i dyskrecja nie nasuwają podejrzeń co do jej uczciwości w postępowaniu z informacjami klasyfikowanymi; lub

c) może być podatna na naciski ze strony zagranicznych lub innych źródeł.

Postępowania o szczególnie szerokim zakresie prowadzi się wobec osób, które:

d) mają uzyskać dostęp do informacji o klauzuli EU TOP SECRET;

e) zajmują stanowiska związane z systematycznym dostępem do dużej ilości informacji o klauzuli EU SECRET;

f) których obowiązki obejmują dostęp do szczególnie ważnych dla wypełniania zadań systemów i sieci teleinformatycznych i które z tego względu mogą uzyskać nieupoważniony dostęp do dużych ilości informacji klasyfikowanych UE lub spowodować poważne szkody poprzez akty technicznego sabotażu.

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

Obowiązkowi poddania się odpowiedniemu sprawdzeniu podlegają także osoby, które nie spełniają wymogów ograniczonego dostępu, ale mają zostać zatrudnione na stanowiskach, na których mogą uzyskać dostęp do informacji klasyfikowanych UE (jak np. kurierzy, pracownicy pionu ochrony, konserwatorzy, sprzątaczki).

6.2. **Wykazy osób, które zostały poddane postępowaniom sprawdzającym**

Wszystkie departamenty Komisji, które wykorzystują informacje klasyfikowane UE lub w których mieszczą się zabezpieczone systemy teleinformatyczne, są zobowiązane do prowadzenia wykazu zatrudnionych w nich pracowników, którzy przeszli postępowania sprawdzające. Każde postępowanie jest w miarę potrzeb poddawane weryfikacji pod względem adekwatności do stanowiska aktualnie zajmowanego przez daną osobę. Niezwłoczne przeprowadzenie takiej weryfikacji jest obligatoryjne, gdy zostanie uzyskana nowa informacja wskazująca, że dalsze zatrudnienie danej osoby na stanowisku związanym z dostępem do informacji klasyfikowanych nie jest wskazane ze względów bezpieczeństwa. Wykaz pracowników danej struktury, które zostały poddane postępowaniom sprawdzającym, jest prowadzony przez lokalnego pełnomocnika ochrony.

6.3. **Szkolenie w zakresie bezpieczeństwa**

Wszystkie osoby zatrudnione na stanowiskach związanych z możliwością uzyskania dostępu do informacji klasyfikowanych w momencie podejmowania obowiązków przechodzą dokładne przeszkolenie, które uświadomi im cel stosowania środków ochrony oraz zapozna z procedurami w zakresie bezpieczeństwa; szkolenia takie są powtarzane w regularnych odstępach czasu. Wymagane jest, by przeszkoleni pracownicy potwierdzili na piśmie, że przeczytali i w pełni rozumieją aktualne przepisy bezpieczeństwa.

6.4. **Obowiązki przełożonych**

Przełożeni mają obowiązek orientować się, którzy z podlegających im pracowników mają dostęp do informacji klasyfikowanych lub zabezpieczonych systemów i sieci teleinformatycznych. Są oni także zobowiązani do odnotowywania i zgłaszania wszelkich incydentów oraz stwierdzonych słabości systemu ochrony, które mogą mieć wpływ na bezpieczeństwo.

6.5. **Status bezpieczeństwa personelu**

Ustanawia się procedury zapewniające, że w przypadku gdy pojawią się wątpliwości w zakresie spełniania warunków bezpieczeństwa przez danego pracownika, zostanie przeprowadzone sprawdzenie, czy osoba ta wykonuje pracę związaną z dostępem do informacji klasyfikowanych lub zabezpieczonych systemów i sieci teleinformatycznych; o rezultacie tego sprawdzenia informuje się Biuro Bezpieczeństwa Komisji. W przypadku ustalenia, że osoba ta zagraża bezpieczeństwu, musi zostać odsunięta od dostępu do informacji lub systemów albo usunięta ze stanowiska, na którym może stwarzać niebezpieczeństwo.

7. BEZPIECZEŃSTWO FIZYCZNE

7.1. **Potrzeba ochrony**

Zakres środków bezpieczeństwa fizycznego, które są stosowane do ochrony informacji klasyfikowanych UE, musi odpowiadać klauzuli tajności i ilości posiadanych informacji i materiałów oraz istniejącym zagrożeniom. Wszystkie osoby, w których dyspozycji znajdują się informacje klasyfikowane UE, są zobowiązane do przestrzegania jednolitych zasad odnoszących się do określania klauzuli tych informacji i wspólnych standardów ochrony odnoszących się do postępowania z informacjami i materiałami wymagającymi ochrony, ich przesyłania i niszczenia.

7.2. **Kontrola**

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

7.3. **Bezpieczeństwo budynków**

Budynki, w których znajdują się informacje klasyfikowane UE lub zabezpieczone systemy i sieci teleinformatyczne, są chronione przed możliwością uzyskania do nich nieupoważnionego dostępu. Sposób ochrony informacji klasyfikowanych UE, np. przez zastosowanie krat w oknach, zamków, straży przy wejściach, automatycznych systemów kontroli dostępu, kontroli bezpieczeństwa i patroli, systemów alarmowych, systemów wykrywania wtargnięcia i psów strażniczych, musi być określony na podstawie:

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

b) jakości sejfów i szaf metalowych wykorzystywanych do przechowywania tych informacji i materiałów;

c) rodzaju i lokalizacji budynku.

Podobnie sposób ochrony systemów i sieci teleinformatycznych musi być określony na podstawie oceny wagi zasobów oraz stopnia szkód związanych z potencjalnym narażeniem na szwank bezpieczeństwa, rodzaju i lokalizacji budynku, w którym znajdują się systemy i sieci teleinformatyczne oraz umiejscowienia systemu w budynku.

7.4. **Plany ochrony na wypadek sytuacji nadzwyczajnych**

Wymagane jest przygotowanie szczegółowych planów ochrony informacji klasyfikowanych na wypadek wystąpienia zagrożeń o skali lokalnej lub ogólnokrajowej.

8. BEZPIECZEŃSTWO TELEINFORMATYCZNE (INFOSEC)

INFOSEC obejmuje określenie i zastosowanie środków ochrony informacji przetwarzanych, przechowywanych lub przesyłanych w systemach teleinformatycznych lub innych elektronicznych, przed utratą ich poufności, integralności i dostępności, zarówno przypadkową, jak i zamierzoną. Wymagane jest podjęcie odpowiednich środków przeciwdziałania w celu zapobiegania przypadkom: uzyskania dostępu do informacji klasyfikowanych UE przez osoby nieupoważnione, uniemożliwienia uzyskania dostępu osobom upoważnionym oraz wprowadzania nieupoważnionych zmian lub niszczenia informacji klasyfikowanych UE.

9. PRZECIWDZIAŁANIE SABOTAŻOWI ORAZ INNYM FORMOM ZŁOŚLIWEGO I CELOWEGO SZKODZENIA

Zastosowanie środków bezpieczeństwa fizycznego do ochrony ważnych instalacji, w których znajdują się informacje klasyfikowane UE, stanowi najlepsze zabezpieczenie przed sabotażem oraz złośliwym i celowym szkodzeniem; same procedury sprawdzeniowe wobec pracowników nie są wystarczające. Właściwa instytucja państwowa powinna zbierać informacje operacyjne dotyczące szpiegostwa, aktów sabotażu, terroryzmu i innych zagrożeń dla bezpieczeństwa państwa.

10. UDOSTĘPNIANIE INFORMACJI KLASYFIKOWANYCH PAŃSTWOM TRZECIM I ORGANIZACJOM MIĘDZYNARODOWYM

Decyzję o udostępnieniu informacji wytworzonej w ramach Komisji państwu trzeciemu lub organizacji międzynarodowej może podjąć wyłącznie Komisja jako ciało kolegialne. Jeśli informacja, której dotyczy wniosek, nie została wytworzona w ramach Komisji, jest ona zobowiązana do uzyskania zgody wytwórcy na jej udostępnienie. W przypadku gdy nie można ustalić wytwórcy, jego uprawnienia przejmuje Komisja.

W przypadku gdy Komisja otrzymuje informacje klasyfikowane od państw trzecich, organizacji międzynarodowych lub innych stron trzecich, jest zobligowana do zapewnienia im ochrony odpowiedniej do ich klauzuli tajności i zgodnie ze standardami określonymi przez poniższy dokument dla informacji klasyfikowanych UE lub też ściślejszej ochrony, jeśli zażąda tego strona trzecia udostępniająca informacje. Istnieje możliwość przeprowadzania wzajemnych kontroli.

Powyższe zasady są wdrażane w życie zgodnie z przepisami szczegółowymi zawartymi w części II sekcja 26 oraz dodatkach 3, 4 i 5.

CZĘŚĆ II: ORGANIZACJA BEZPIECZEŃSTWA W KOMISJI

11. CZŁONEK KOMISJI ODPOWIEDZIALNY ZA KWESTIE BEZPIECZEŃSTWA

Członek Komisji odpowiedzialny za kwestie bezpieczeństwa odpowiada za:

a) wdrażanie polityki bezpieczeństwa Komisji;

b) rozpatrywanie problemów bezpieczeństwa zgłaszanych przez Komisję lub jej właściwe struktury;

c) rozpatrywanie kwestii wiążących się z koniecznością wprowadzania zmian w polityce bezpieczeństwa Komisji, w ścisłej współpracy z krajowymi (lub innymi właściwymi) władzami bezpieczeństwa Państw Członkowskich (zwanymi dalej krajowymi władzami bezpieczeństwa).

W szczególności członek Komisji odpowiedzialny za kwestie bezpieczeństwa jest odpowiedzialny za:

a) koordynowanie wszelkich kwestii związanych z bezpieczeństwem przedsięwzięć podejmowanych przez Komisję;

b) przekazywanie za pośrednictwem wyznaczonych instytucji Państw Członkowskich wniosków do krajowych władz bezpieczeństwa o przeprowadzenie postępowań sprawdzających wobec osób zatrudnionych w Komisji, zgodnie z postanowieniami sekcji 20;

c) przeprowadzanie postępowania wyjaśniającego lub zlecanie przeprowadzenia takiego postępowania w każdym przypadku przecieku informacji klasyfikowanych UE, o którym na podstawie pierwotnego rozpoznania sądzi się, że jego źródłem jest Komisja;

d) wnioskowanie do odpowiednich władz bezpieczeństwa o rozpoczęcie postępowania wyjaśniającego, gdy wydaje się, że przeciek informacji klasyfikowanych UE miał miejsce poza Komisją, oraz koordynowanie postępowań w przypadku, gdy zaangażowanych jest więcej niż jedna władza bezpieczeństwa;

e) przeprowadzanie okresowych kontroli rozwiązań w zakresie ochrony informacji klasyfikowanych UE;

f) utrzymywanie ścisłych kontaktów ze wszystkim właściwymi władzami bezpieczeństwa w celu osiągnięcia pełnej koordynacji w zakresie ochrony informacji klasyfikowanych;

g) dokonywanie stałych przeglądów polityki bezpieczeństwa Komisji i stosowanych procedur ochrony i, gdy zachodzi taka potrzeba, opracowywanie odpowiednich zaleceń. W tym zakresie członek Komisji odpowiedzialny za kwestie bezpieczeństwa jest zobowiązany do przedstawiania Komisji rocznego planu inspekcji przygotowywanego przez służby bezpieczeństwa Komisji.

12. GRUPA DORADCZA KOMISJI DO SPRAW POLITYKI BEZPIECZEŃSTWA

Ustanawia się Grupę Doradczą Komisji do spraw Polityki Bezpieczeństwa. W jej skład wchodzą przedstawiciele krajowych władz bezpieczeństwa Państw Członkowskich. Grupie przewodniczy członek Komisji odpowiedzialny za kwestie bezpieczeństwa lub osoba przez niego wyznaczona. Do udziału w posiedzeniach mogą być także zapraszani przedstawiciele innych instytucji europejskich, a także przedstawiciele odpowiednich zdecentralizowanych agencji WE i UE, jeśli omawiane są sprawy ich dotyczące.

Grupa Doradcza Komisji do spraw Polityki Bezpieczeństwa spotyka się na wniosek przewodniczącego lub każdego z jej członków. Grupa jest uprawniona do rozpatrywania i poddawania ocenie wszystkich istotnych kwestii bezpieczeństwa oraz do przedstawiania – w miarę potrzeb – odpowiednich zaleceń Komisji.

13. RADA BEZPIECZEŃSTWA KOMISJI

Ustanawia się Radę Bezpieczeństwa Komisji. Tworzą ją sekretarz generalny, pełniący funkcję przewodniczącego, oraz dyrektorzy generalni służby prawnej, administracji i personelu, stosunków międzynarodowych, sprawiedliwości i spraw wewnętrznych oraz Połączonego Centrum Badawczego i dyrektorów służby audytu wewnętrznego oraz Biura Bezpieczeństwa Komisji. Do udziału w pracach Rady mogą być zapraszani inni urzędnicy Komisji. W zakresie właściwości Rady pozostaje dokonywanie oceny środków bezpieczeństwa stosowanych w ramach Komisji oraz przedstawianie odpowiednich zaleceń członkowi Komisji odpowiedzialnemu za kwestie bezpieczeństwa.

14. BIURO BEZPIECZEŃSTWA KOMISJI

W celu wypełnienia obowiązków określonych w sekcji 11 członek Komisji odpowiedzialny za kwestie bezpieczeństwa ma do dyspozycji Biuro Bezpieczeństwa Komisji, którego zadaniem jest koordynacja, nadzór i wdrażanie środków bezpieczeństwa.

Dyrektor Biura Bezpieczeństwa Komisji jest głównym doradcą do spraw bezpieczeństwa członka Komisji odpowiedzialnego za kwestie bezpieczeństwa oraz sprawuje funkcję sekretarza Grupy Doradczej Komisji do spraw Polityki Bezpieczeństwa. W tym zakresie jest on zobowiązany do kierowania procesem uaktualniania przepisów bezpieczeństwa oraz do koordynacji stosowania środków ochrony z właściwymi instytucjami Państw Członkowskich oraz, w miarę potrzeb, organizacjami międzynarodowymi, które zawarły z Komisją umowy o bezpieczeństwie. W tym celu będzie spełniał funkcję oficera łącznikowego.

Dyrektor Biura Bezpieczeństwa Komisji jest odpowiedzialny za zatwierdzanie systemów i sieci teleinformatycznych w ramach Komisji. Dyrektor Biura Bezpieczeństwa Komisji, w porozumieniu z właściwą krajową władzą bezpieczeństwa, podejmuje decyzje o zatwierdzeniu systemów i sieci teleinformatycznych obejmujących z jednej strony Komisję, z drugiej zaś wszelkich odbiorców informacji klasyfikowanych UE.

15. KONTROLE W ZAKRESIE BEZPIECZEŃSTWA

Biuro Bezpieczeństwa Komisji jest zobowiązane do przeprowadzania okresowych kontroli rozwiązań w zakresie ochrony informacji klasyfikowanych UE.

Biuro Bezpieczeństwa Komisji może w wykonywaniu tego zadania korzystać z pomocy służb bezpieczeństwa innych instytucji unijnych, dysponujących informacjami klasyfikowanymi UE lub krajowych władz bezpieczeństwa Państw Członkowskich ([1]).

Na wniosek Państwa Członkowskiego, jego krajowa władza bezpieczeństwa może – wspólnie i w porozumieniu ze służbami bezpieczeństwa Komisji – przeprowadzić w Komisji kontrolę w zakresie ochrony informacji klasyfikowanych UE.

([1]) Bez uszczerbku dla Konwencji wiedeńskiej z 1961 r. o stosunkach dyplomatycznych oraz Protokołu o przywilejach i immunitetach przysługujących Wspólnotom Europejskim z dnia 8 kwietnia 1965 r.

16. KLAUZULE, ZASTRZEŻENIA I OZNACZENIA

16.1. **Klauzule tajności** [1]

Informacjom mogą być nadawane następujące klauzule tajności (por. także załącznik 2):

EU TOP SECRET: klauzulę tę nadaje się tylko informacji lub materiałowi, których nieupoważnione ujawnienie spowodowałoby wyjątkowo duże szkody dla podstawowych interesów Unii Europejskiej albo jednego lub więcej Państw Członkowskich.

EU SECRET: klauzulę tę nadaje się tylko informacji lub materiałowi, których nieupoważnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom Unii Europejskiej albo jednego lub więcej Państw Członkowskich.

EU CONFIDENTIAL: klauzulę tę nadaje się informacji lub materiałowi, których nieupoważnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii Europejskiej albo jednego lub więcej Państw Członkowskich.

EU RESTRICTED: klauzulę tę nadaje się informacji lub materiałowi, których nieupoważnione ujawnienie byłoby niekorzystne z punktu widzenia interesów Unii Europejskiej albo jednego lub więcej Państw Członkowskich.

Nie dopuszcza się stosowania innych klauzul.

16.2. **Zastrzeżenia**

W celu określenia terminu obowiązywania klauzuli tajności (co w przypadku informacji klasyfikowanych oznacza automatyczne obniżenie lub zniesienie klauzuli) dopuszczalne jest stosowanie uzgodnionych zastrzeżeń. Zastrzeżenie może mieć formę „Obowiązuje do (czas/data)" lub „Obowiązuje do (wydarzenie)".

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

Zastrzeżeń używa się wyłącznie w połączeniu z klauzulą tajności.

16.3. **Oznaczenia**

Możliwe jest stosowanie dodatkowych oznaczeń w celu określenia dziedziny, do której odnosi się dokument, lub szczególnego kręgu odbiorców, zgodnie z zasadą ograniczonego dostępu, lub – w przypadku informacji nieklasyfikowanych – czasu obowiązywania embarga.

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

Oznaczenie ESDP nadaje się dokumentom dotyczącym zagadnień bezpieczeństwa i obrony Unii albo jednego lub więcej jej Państw Członkowskich, bądź odnoszącym się do wojskowego lub cywilnego zarządzania kryzysowego, a także kopiom takich dokumentów.

16.4. **Nanoszenie klauzul**

Klauzule nanosi się w następujący sposób:

a) na dokumentach EU RESTRICTED: za pomocą środków mechanicznych lub elektronicznych,

b) na dokumentach EU CONFIDENTIAL: za pomocą środków mechanicznych i ręcznie; możliwe jest także drukowanie ich na wcześniej oznakowanych i zarejestrowanych arkuszach,

c) na dokumentach EU SECRET i EU TOP SECRET: za pomocą środków mechanicznych i ręcznie.

16.5. **Nanoszenie zastrzeżeń**

Zastrzeżenia muszą być nanoszone tak samo, jak klauzule tajności, bezpośrednio pod nimi.

---

[1] Por. tabelę odpowiedniości klauzul UE, NATO i UZE oraz państw członkowskich w dodatku 1.

17. ZASADY NADAWANIA KLAUZUL

17.1. **Uwagi ogólne**

Informacja powinna być objęta klauzulą tajności tylko wtedy, gdy jest to konieczne. Klauzula musi być wyraźnie i prawidłowo naniesiona. Może być utrzymywana tylko przez niezbędny okres.

Wyłącznie wytwórca odpowiada za nadanie klauzuli oraz, następnie, za jej obniżenie lub zniesienie.

Urzędnicy i inni pracownicy Komisji mogą nadawać klauzule, obniżać je lub znosić wyłącznie na polecenie lub za zgodą dyrektora departamentu.

Szczegółowe procedury postępowania z dokumentami klasyfikowanymi zostały określone w sposób zapewniający, że są one chronione w sposób odpowiedni dla zawartych w nich informacji.

Liczba osób upoważnionych do wytwarzania dokumentów o klauzuli EU TOP SECRET musi być ograniczona do niezbędnego minimum, a ich nazwiska umieszczone na wykazie prowadzonym przez Biuro Bezpieczeństwa Komisji.

17.2. **Stosowanie klauzul**

Klauzula danego dokumentu jest określana na podstawie stopnia sensytywności zawartych w nim informacji, zgodnie z definicjami zamieszczonymi w sekcji 16. Ważne jest, by klauzule były stosowane prawidłowo i oszczędnie. Odnosi się to w szczególności do klauzuli EU TOP SECRET.

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

Praktyczne zalecenia odnoszące się do określania klauzuli są zawarte w dodatku 2.

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

Klauzula pisma przewodniego lub noty poprzedzającej załączniki musi odpowiadać najwyższej klauzuli pism do nich załączonych. Wytwórca powinien jasno określić poziom klauzuli pisma przewodniego lub noty po odłączeniu ich od załączników.

Kwestie publicznego dostępu do informacji są określone w rozporządzeniu (WE) nr 1049/2001.

17.3. **Obniżanie i znoszenie klauzul**

Klauzula tajności dokumentów klasyfikowanych UE może być obniżona lub zniesiona wyłącznie za pozwoleniem wytwórcy oraz, gdy istnieje taka potrzeba, w uzgodnieniu z innymi zainteresowanymi stronami. Decyzja o obniżeniu lub zniesieniu klauzuli musi być potwierdzona na piśmie. Wytwórca jest zobowiązany do informowania odbiorców informacji o zmianie klauzuli; adresaci są z kolei odpowiedzialni za poinformowanie o tym kolejnych osób, do których przesłali dokument lub dla których wykonali jego kopię.

Wytwórca jest zobowiązany, w miarę możliwości, do określenia na dokumencie klasyfikowanym daty lub okresu, gdy jego klauzula może zostać obniżona lub zniesiona. W przeciwnym razie wytwórcy są zobowiązani do przeprowadzania przynajmniej raz na 5 lat przeglądu dokumentów w celu dokonania oceny, czy nadana klauzula nadal jest konieczna.

18. BEZPIECZEŃSTWO FIZYCZNE

18.1. **Uwagi ogólne**

Podstawowym celem stosowania środków ochrony fizycznej jest zapobieganie: przypadkom uzyskania przez osoby nieupoważnione dostępu do informacji i/lub materiałów klasyfikowanych UE, kradzieży i niszczeniu sprzętu oraz innej własności oraz nękaniu lub wszelkim innym formom agresji wymierzonej przeciwko urzędnikom, pracownikom i gościom.

18.2. **Wymagania w zakresie bezpieczeństwa**

Wszystkie budynki, tereny, pomieszczenia biurowe, systemy teleinformatyczne itd., w których informacje klasyfikowane UE są przechowywane i/lub znajdują się w obiegu, podlegają ochronie przy zastosowaniu odpowiednich środków bezpieczeństwa fizycznego.

Podejmując decyzję o poziomie ochrony fizycznej należy wziąć pod uwagę wszystkie istotne czynniki, takie jak:

a) klauzula tajności informacji i/lub materiału;

b) ilość i forma utrwalenia informacji (np. wydruk, nośnik komputerowy);

c) ocena lokalnych zagrożeń wynikających z działalności służb wywiadowczych wymierzonej przeciwko UE, jej Państwom Członkowskim i/lub innym instytucjom i stronom trzecim posiadającym informacje klasyfikowane UE, mianowicie sabotażu, terroryzmu oraz działalności antypaństwowej lub innych działań o charakterze przestępczym.

Wymagane jest ustanowienie środków ochrony fizycznej w celu:

a) uniemożliwienia skrytego lub siłowego wejścia intruzów;

b) zniechęcenia, utrudnienia oraz wykrycia działań podejmowanych przez nielojalnych pracowników;

c) zapobieżenia uzyskaniu dostępu do informacji klasyfikowanych UE z naruszeniem zasady ograniczonego dostępu.

18.3. **Środki bezpieczeństwa fizycznego**

18.3.1. *Strefy bezpieczeństwa*

Miejsca, w których informacje o klauzuli EU CONFIDENTIAL lub wyższej są przechowywane lub znajdują się w obiegu, muszą być tak usytuowane i wyposażone, aby odpowiadały następującym wymaganiom:

a) strefa bezpieczeństwa klasy I: miejsce, w którym informacje o klauzuli EU CONFIDENTIAL lub wyższej są przechowywane lub znajdują się w obiegu w taki sposób, że – biorąc pod uwagę uwarunkowania praktyczne – wejście do strefy jest jednoznaczne z uzyskaniem dostępu do informacji klasyfikowanych. Strefa ta wymaga:

   i) wyraźnie określonych i chronionych granic, których przekraczanie w obie strony jest kontrolowane;

   ii) systemu kontroli wejść, który umożliwia wejście do strefy jedynie osobom odpowiednio sprawdzonym i wyraźnie do tego upoważnionym;

   iii) określenia klauzuli tajności i kategorii informacji, które zazwyczaj znajdują się w tym obszarze, tzn. informacji, które są dostępne po wejściu do strefy;

b) strefa bezpieczeństwa klasy II: miejsce, w którym informacje o klauzuli EU CONFIDENTIAL lub wyższej są przechowywane lub znajdują się w obiegu w sposób umożliwiający ich ochronę przed uzyskaniem dostępu przez osoby nieupoważnione dzięki środkom kontroli wewnętrznej; są to np. pomieszczenia, w których informacje o klauzuli EU CONFIDENTIAL są często przechowywane lub znajdują się one w ciągłym obiegu. Strefa ta wymaga:

   i) wyraźnie określonych i chronionych granic, których przekraczanie w obie strony jest kontrolowane;

   ii) systemu kontroli wejść, który umożliwia wejście do strefy bez nadzoru jedynie osobom odpowiednio sprawdzonym i wyraźnie do tego upoważnionym. W stosunku do wszystkich innych osób konieczne jest zapewnienie eskorty lub równoważnych środków kontroli w celu zapobieżenia uzyskaniu nieupoważnionego dostępu do informacji klasyfikowanych UE i niekontrolowanemu wejściu do miejsc objętych kontrolą bezpieczeństwa technicznego.

   Miejsca, w których nie pracuje się 24 godziny na dobę, muszą być sprawdzane bezpośrednio po zakończeniu normalnych godzin pracy w celu upewnienia się, że informacje klasyfikowane UE zostały należycie zabezpieczone.

18.3.2. *Strefa administracyjna*

Strefę administracyjną, charakteryzującą się niższym poziomem zabezpieczeń, można utworzyć wokół stref bezpieczeństwa klasy I lub II, bądź w prowadzącym do nich przejściu. Strefa taka wymaga wyraźnie określonych granic, w ramach których możliwe jest wprowadzenie kontroli osób i pojazdów. W strefach administracyjnych wolno przechowywać i wykorzystywać wyłącznie informacje o klauzuli EU RESTRICTED i nieklasyfikowane.

18.3.3. *Kontrola wejść i wyjść*

Wejścia stałych pracowników do stref bezpieczeństwa klasy I lub II muszą być kontrolowane przy zastosowaniu systemu przepustek lub identyfikacji osób. Wymagane jest także ustanowienie systemu sprawdzania osób odwiedzających w celu uniemożliwienia uzyskania nieupoważnionego dostępu do informacji klasyfikowanych UE. Możliwe jest uzupełnienie systemu przepustek o rozpoznawanie za pomocą środków technicznych; rozwiązanie takie można uznać za dodatkowy element, który jednak nie może całkowicie zastąpić strażników. Zmiana w ocenie zagrożeń może pociągnąć za sobą wzmocnienie środków kontroli wejść i wyjść, np. w trakcie wizyt osób zajmujących wysokie stanowiska.

18.3.4. *Patrolowanie przez strażników*

Po zakończeniu normalnych godzin pracy strefy bezpieczeństwa klasy I i II powinny być patrolowane w celu ochrony zasobów UE przed narażeniem na szwank ich bezpieczeństwa, uszkodzeniem lub utratą. Częstotliwość patroli określa się w zależności od warunków lokalnych, ale zaleca się, by odbywały się one co dwie godziny.

18.3.5. *Sejfy, szafy metalowe i pomieszczenia wzmocnione*

Sejfy i szafy pancerne używane do przechowywania informacji klasyfikowanych UE dzielą się na trzy klasy:

— klasa A: sejfy i szafy metalowe zatwierdzone w danym kraju do przechowywania informacji o klauzuli EU TOP SECRET w strefie bezpieczeństwa klasy I lub II;

— klasa B: sejfy i szafy metalowe zatwierdzone w danym kraju do przechowywania informacji o klauzuli EU SECRET lub EU CONFIDENTIAL w strefie bezpieczeństwa klasy I lub II;

— klasa C: meble biurowe odpowiednie do przechowywania jedynie informacji o klauzuli EU RESTRICTED.

W przypadku pomieszczeń wzmocnionych, tworzonych w obrębie strefy bezpieczeństwa klasy I lub II, oraz wszystkich stref bezpieczeństwa klasy I, w których informacje o klauzuli EU CONFIDENTIAL lub wyższej są przechowywane na odkrytych półkach lub zaznaczane na wykresach i mapach, wymagane jest, by ściany, podłogi i stropy, drzwi i zamki zostały zatwierdzone przez władzę akredytacji bezpieczeństwa (SAA); kryterium oceny stanowi zapewnienie ochrony identycznej jak zapewniana przez sejf lub szafę pancerną, dopuszczone do przechowywania informacji o tej samej klauzuli.

18.3.6. *Zamki*

Zamki stosowane do zamykania sejfów, szaf metalowych i pomieszczeń wzmocnionych, w których przechowywane są informacje klasyfikowane UE, muszą odpowiadać następującym wymaganiom:

— grupa A: zatwierdzone w danym kraju do stosowania w sejfach i szafach metalowych klasy A;

— grupa B: zatwierdzone w danym kraju do stosowania w sejfach i szafach metalowych klasy B;

— grupa C: odpowiednie tylko do mebli biurowych klasy C.

18.3.7. *Kontrola kluczy i kodów dostępu*

Klucze do sejfów i szaf metalowych nie mogą być wynoszone poza budynki Komisji. Osoby, które powinny znać kody dostępu do sejfów i szaf metalowych, muszą się ich nauczyć na pamięć. Zapasowe klucze oraz zapisane kody dostępu, które należy wykorzystywać tylko w nagłych przypadkach, muszą być przechowywane przez lokalnego pełnomocnika ochrony danego departamentu Komisji; wymagane jest umieszczenie każdego kodu dostępu w oddzielnej, nieprzezroczystej i zapieczętowanej kopercie. Klucze używane na co dzień, klucze zapasowe oraz kody dostępu należy przechowywać w oddzielnych pojemnikach. Klucze i kody wymagają równie rygorystycznej ochrony, jak informacje, do których umożliwiają dostęp.

Kody dostępu do sejfów i szaf metalowych są udostępniane jak najmniejszej liczbie osób. Wymaga się zmiany kodu:

a) przy otrzymaniu nowego sejfu lub kasy pancernej;

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

c) gdy doszło do ujawnienia kodu bądź istnieje domniemanie, że mogło to nastąpić;

d) w regularnych odstępach czasu: zaleca się dokonywanie zmian co 6 miesięcy, jednak nie rzadziej niż co 12 miesięcy.

18.3.8. *Urządzenia do wykrywania wtargnięcia*

W przypadku gdy do ochrony informacji klasyfikowanych UE są stosowane systemy alarmowe, telewizja przemysłowa i inne urządzenia elektryczne, wymagane jest zapewnienie zasilania awaryjnego w celu zapewnienia nieprzerwanego działania systemu w razie wystąpienia przerw w dostawie energii elektrycznej z głównego źródła. Kolejnym podstawowym wymogiem, jaki muszą spełnić tego rodzaju urządzenia, jest włączanie się alarmu lub innego skutecznego ostrzeżenia, kierowanego do osób monitorujących bezpieczeństwo strefy, gdy wystąpią zakłócenia w pracy urządzeń wykrywania wtargnięcia lub próby ingerencji w ich funkcjonowanie.

18.3.9. *Zatwierdzony sprzęt*

Biuro Bezpieczeństwa Komisji jest zobligowane do prowadzenia aktualnego wykazu sprzętu (uwzględniającego typy i modele urządzeń), który został przez nie zatwierdzony do bezpośredniej lub pośredniej ochrony informacji klasyfikowanych w różnych warunkach i okolicznościach. Wykaz tworzy się na podstawie – między innymi – informacji przekazywanych przez krajowe władze bezpieczeństwa.

18.3.10. *Fizyczna ochrona urządzeń kopiujących i faksujących*

Kopiarki i telefaksy należy fizycznie zabezpieczyć w sposób zapewniający, że mogą z nich skorzystać jedynie osoby upoważnione oraz że wszystkie informacje klasyfikowane UE są objęte właściwą kontrolą.

18.4. **Ochrona przed podglądem i podsłuchem**

18.4.1. *Podgląd*

Wszelkie odpowiednie środki muszą być stosowane w ciągu dnia i w nocy w celu zapewnienia, że żadna nieupoważniona osoba nie może zobaczyć, nawet przypadkowo, informacji klasyfikowanych UE.

18.4.2. *Podsłuch*

Pomieszczenia lub strefy, w których regularnie omawiane są kwestie objęte klauzulą EU SECRET lub wyższą, muszą być zabezpieczone przed podsłuchem pasywnym i aktywnym, jeśli ryzyko wystąpienia tego typu zagrożeń uzasadnia konieczność takich zabezpieczeń. Przeprowadzenie oceny ryzyka jest obowiązkiem Biura Bezpieczeństwa Komisji, które – gdy jest to konieczne – może się skonsultować z właściwymi krajowymi władzami bezpieczeństwa.

18.4.3 *Wnoszenie sprzętu elektronicznego i nagrywającego*

Nie dopuszcza się wnoszenia do stref bezpieczeństwa lub stref zabezpieczonych technicznie telefonów komórkowych, prywatnych komputerów, urządzeń nagrywających, aparatów fotograficznych i innych urządzeń elektronicznych lub pozwalających na rejestrację dźwięku bez upoważnienia dyrektora Biura Bezpieczeństwa Komisji.

Biuro Bezpieczeństwa Komisji może zwrócić się do krajowych władz bezpieczeństwa z wnioskiem o czasowe oddelegowanie ekspertów w celu określenia, jakie środki ochrony powinny zostać zastosowane w pomieszczeniach zagrożonych podsłuchem pasywnym (np. izolacja ścian, drzwi, podłóg i stropów, pomiary emanacji) i aktywnym (np. przeszukanie w celu wykrycia mikrofonów).

Podobnie, gdy wymagają tego okoliczności, dyrektor Biura Bezpieczeństwa Komisji może zwrócić się do krajowych władz bezpieczeństwa z wnioskiem o przeprowadzenie specjalistycznej kontroli sprzętu teleinformatycznego oraz elektrycznego lub elektronicznego sprzętu biurowego wszelkiego rodzaju, wykorzystywanego w trakcie spotkań na poziomie EU SECRET lub wyższym.

18.5. **Strefy zabezpieczone technicznie**

Niektóre strefy mogą być zaprojektowane jako strefy zabezpieczone technicznie. Wejście do takiej strefy podlega szczególnej kontroli. W czasie gdy strefa nie jest użytkowana, musi być zamknięta zgodnie z zatwierdzoną instrukcją, a wszystkie klucze muszą być objęte ochroną. Strefy te podlegają regularnym kontrolom bezpieczeństwa fizycznego; kontrola taka musi być przeprowadzana po stwierdzeniu próby uzyskania nieupoważnionego dostępu lub powzięciu takiego podejrzenia.

Wymagane jest prowadzenie szczegółowego wykazu mebli i urządzeń wnoszonych i wynoszonych ze strefy zabezpieczonej technicznie w celu kontroli ich ruchu. Meble i urządzenia, które mają stanowić wyposażenie strefy, muszą uprzednio zostać dokładnie sprawdzone przez przeszkolonych pracowników ochrony, czy nie ukryto w nich urządzeń podsłuchowych. Jako zasadę przyjmuje się, że w strefie zabezpieczonej technicznie nie należy instalować linii łączności bez pozwolenia właściwej władzy.

19. STOSOWANIE ZASADY OGRANICZONEGO DOSTĘPU I POSTĘPOWANIA SPRAWDZAJĄCE

19.1. **Uwagi ogólne**

Dostęp do informacji klasyfikowanych UE musi być ograniczony do osób, którym informacje te są niezbędne do wykonywania obowiązków służbowych lub zadań. Do dostępu do informacji o klauzulach EU TOP SECRET, EU SECRET i EU CONFIDENTIAL mogą być upoważnione wyłącznie osoby, w stosunku do których zostało przeprowadzone odpowiednie postępowanie sprawdzające.

Za określenie, do jakich informacji powinna mieć dostęp dana osoba, odpowiada departament, w którym dana osoba ma zostać zatrudniona, na podstawie zakresu jej obowiązków.

Departamenty są zobowiązane do występowania z wnioskami o przeprowadzenie postępowań sprawdzających.

Postępowanie kończy się wydaniem „certyfikatu bezpieczeństwa UE" określającego klauzulę informacji, do których dana osoba może mieć dostęp, oraz datę ważności.

Certyfikat bezpieczeństwa UE uprawniający do dostępu do informacji o wyższej klauzuli może uprawniać do dostępu do informacji oznaczonych niższą klauzulą tajności.

Osoby niebędące urzędnikami lub innymi pracownikami, jak np. zewnętrzni kontrahenci, eksperci i konsultanci, z którymi trzeba omówić informacje klasyfikowane UE lub których trzeba zapoznać z informacjami klasyfikowanymi UE, muszą uzyskać decyzję, że spełniają warunki bezpieczeństwa UE przewidziane dla dostępu do informacji klasyfikowanych i zostać poinformowane o swojej odpowiedzialności za ochronę informacji.

Kwestie publicznego dostępu do informacji są określone w rozporządzeniu (WE) nr 1049/2001.

19.2. **Szczególne zasady dostępu do informacji o klauzuli EU TOP SECRET**

Wszystkie osoby, które mają uzyskać dostęp do informacji o klauzuli EU TOP SECRET, muszą zostać uprzednio odpowiednio sprawdzone.

Do wyznaczenia osób, które powinny uzyskać dostęp do informacji EU TOP SECRET, jest uprawniony wyłącznie członek Komisji odpowiedzialny za kwestie bezpieczeństwa. Nazwiska tych osób muszą zostać umieszczone we właściwym wykazie EU TOP SECRET. Biuro Bezpieczeństwa Komisji stworzy i będzie prowadzić taki wykaz.

Każda osoba, przed uzyskaniem dostępu do informacji o klauzuli EU TOP SECRET, musi podpisać oświadczenie potwierdzające, że została przeszkolona na temat procedur bezpieczeństwa Komisji i że w pełni zdaje sobie sprawę ze swojej szczególnej odpowiedzialności za ochronę informacji o klauzuli EU TOP SECRET, oraz konsekwencji przewidzianych przepisami UE, prawem swojego państwa lub aktami administracyjnymi w przypadku dopuszczenia – w wyniku świadomego działania lub zaniedbania – do sytuacji, gdy informacje klasyfikowane dostaną się w niepowołane ręce.

W przypadku osób, które mają uzyskać dostęp do informacji o klauzuli EU TOP SECRET, np. w czasie spotkania, właściwy urzędnik kontroli służby lub instytucji, w której osoby te są zatrudnione, informuje organizatora spotkania, że uzyskały one odpowiednie upoważnienia.

Nazwiska osób zwolnionych z obowiązków wymagających dostępu do informacji o klauzuli EU TOP SECRET zostają usunięte z wykazu EU TOP SECRET. Ponadto osoby te informuje się, że nadal spoczywa na nich szczególna odpowiedzialność za ochronę informacji o klauzuli EU TOP SECRET. Są one zobowiązane do podpisania oświadczenia, że nigdy nie wykorzystają ani nie przekażą informacji o klauzuli EU TOP SECRET, z którymi się zapoznały.

19.3. **Szczególne zasady dostępu do informacji o klauzuli EU SECRET i EU CONFIDENTIAL**

Wszystkie osoby, które mają uzyskać dostęp do informacji o klauzuli EU SECRET lub EU CONFIDENTIAL, muszą zostać uprzednio odpowiednio sprawdzone.

Każda osoba, która ma uzyskać dostęp do informacji o klauzuli EU SECRET lub EU CONFIDENTIAL, musi zostać zapoznana z odpowiednimi przepisami bezpieczeństwa i być świadoma konsekwencji ich nieprzestrzegania.

W przypadku osób, które mają uzyskać dostęp do informacji o klauzuli EU SECRET lub EU CONFIDENTIAL, np. w czasie spotkania, właściwy pełnomocnik ochrony instytucji, w której osoby te są zatrudnione, informuje organizatora spotkania, że uzyskały one odpowiednie upoważnienia.

19.4. **Szczególne zasady dostępu do informacji o klauzuli EU RESTRICTED**

Każda osoba, która ma uzyskać dostęp do informacji o klauzuli EU RESTRICTED, musi zostać zapoznana z odpowiednimi przepisami bezpieczeństwa i być świadoma konsekwencji ich nieprzestrzegania.

19.5. **Przekazywanie**

W przypadku gdy dana osoba kończy pracę na stanowisku związanym z dostępem do materiałów klasyfikowanych UE, kancelaria tajna sprawuje nadzór nad zgodnym z przepisami przekazaniem materiałów pomiędzy odchodzącym pracownikiem a jego następcą.

Natomiast gdy członek personelu jest przenoszony na inne stanowisko, z którym wiąże się dostęp do informacji klasyfikowanych UE, właściwy lokalny pełnomocnik ochrony jest zobowiązany do przeszkolenia go.

19.6. **Szkolenia**

Osoby, które mają w swojej pracy wykorzystywać informacje klasyfikowane UE, powinny, w momencie podejmowania pracy, a następnie w regularnych odstępach czasu, być poinformowane o:

a) zagrożeniach dla bezpieczeństwa wynikającymi z nieostrożnych rozmów;

b) środkach ostrożności, które powinny być zachowywane przy kontaktach z dziennikarzami i przedstawicielami grup interesów;

c) zagrożeniach dla informacji i działań objętych klauzulą tajności, stwarzanych przez służby wywiadowcze, które prowadzą działalność wymierzoną przeciwko UE i jej Państwom Członkowskim;

d) ciążącym na nich obowiązku niezwłocznego zgłaszania odpowiednim władzom bezpieczeństwa wszelkich prób nawiązania kontaktu lub manewrów, które mogą wskazywać na działalność szpiegowską oraz wszelkich niezwykłych okoliczności związanych z bezpieczeństwem.

Wszystkie osoby pozostające w częstych kontaktach z przedstawicielami państw, których służby wywiadowcze prowadzą działania wymierzone przeciwko UE i jej Państwom Członkowskim i mogą powodować zagrożenia dla ochrony informacji i działań objętych klauzulą tajności, należy przeszkolić w zakresie technik pracy operacyjnej stosowanych przez różne służby.

Nie istnieją przepisy Komisji dotyczące prywatnych podróży do jakiegokolwiek kraju odbywanych przez osoby sprawdzone w związku z dostępem do informacji klasyfikowanych UE. Biuro Bezpieczeństwa Komisji jest jednak zobowiązane do zapoznania urzędników i innych pracowników, za których odpowiada, z regulacjami obowiązującymi w miejscu przeznaczenia.

20. SPRAWDZENIA URZĘDNIKÓW I INNYCH PRACOWNIKÓW KOMISJI

a) Dostęp do informacji klasyfikowanych UE znajdujących się w dyspozycji Komisji mogą uzyskać wyłącznie ci urzędnicy i inni pracownicy Komisji oraz inne osoby pracujące na jej rzecz, którym są one potrzebne do wykonywania obowiązków służbowych.

b) Warunkiem uzyskania dostępu do informacji o klauzulach EU TOP SECRET, EU SECRET i EU CONFIDENTIAL przez osoby określone w lit. a) powyżej jest otrzymanie upoważnienia, zgodnie z procedurą określoną w lit. c) i d) niniejszego punktu.

c) Upoważnienie może być udzielone wyłącznie osobom, w stosunku do których właściwe organy krajowe Państw Członkowskich (krajowe władze bezpieczeństwa) przeprowadziły postępowania sprawdzające, zgodnie z procedurą określoną w lit. i)–n).

d) Za udzielenie upoważnienia, o którym mowa w lit. a), b) i c), jest odpowiedzialny dyrektor Biura Bezpieczeństwa Komisji.

e) Upoważnienie udzielane jest po otrzymaniu opinii właściwych organów krajowych Państw Członkowskich, wydawanej na podstawie procedury sprawdzeniowej, określonej w lit. i)–n).

f) Biuro Bezpieczeństwa Komisji jest zobowiązane do prowadzenia aktualnego wykazu wszystkich sensytywnych stanowisk, na podstawie informacji przekazywanych przez poszczególne departamenty, oraz wszystkich osób, które uzyskały (tymczasowe) upoważnienia.

g) Upoważnienie jest wydawane na 5 lat, jednak nie może być ważne dłużej niż okres wykonywania obowiązków, w związku z którymi zostało przyznane. Może natomiast zostać przedłużone zgodnie z procedurą określoną w lit. e).

h) Dyrektor Biura Bezpieczeństwa Komisji może cofnąć upoważnienie, gdy uzna, że istnieją po temu uzasadnione przesłanki. Decyzja o cofnięciu upoważnienia jest przekazywana zainteresowanej osobie, która może ubiegać się o wysłuchanie przez dyrektora Biura Bezpieczeństwa Komisji, oraz właściwemu organowi krajowemu.

i) Procedura sprawdzeniowa jest przeprowadzana na wniosek dyrektora Biura Bezpieczeństwa Komisji przez właściwe instytucje Państwa Członkowskiego, którego dana osoba jest obywatelem; osoba sprawdzana uczestniczy w prowadzonej w stosunku do siebie procedurze. Jeśli dana osoba nie jest obywatelem Państwa Członkowskiego Unii, dyrektor Biura Bezpieczeństwa Komisji zwraca się z wnioskiem o przeprowadzenie postępowania do tego Państwa Członkowskiego UE, na którego terytorium osoba ta zamieszkuje lub często przebywa.

j) Osoba sprawdzana w ramach procedury sprawdzeniowej jest zobowiązana do wypełnienia ankiety bezpieczeństwa osobowego.

k) Dyrektor Biura Bezpieczeństwa Komisji w swoim wniosku określa rodzaj i klauzulę informacji, do których dana osoba ma uzyskać dostęp, tak aby właściwe organy krajowe mogły przeprowadzić odpowiednią procedurę i wyrazić swoją opinię, czy osobę sprawdzaną można upoważnić do dostępu do określonego typu informacji.

l) Postępowanie sprawdzające, włącznie z podjęciem decyzji końcowej, jest przeprowadzane na podstawie odpowiednich przepisów danego Państwa Członkowskiego, w tym także odnoszących się do procedur odwoławczych.

m) W przypadku przekazania pozytywnej opinii przez właściwe organy krajowe dyrektor Biura Bezpieczeństwa Komisji może udzielić danej osobie upoważnienia do dostępu do informacji klasyfikowanych.

n) Negatywna opinia właściwych organów krajowych jest przekazywana zainteresowanej osobie, która może ubiegać się o wysłuchanie przez dyrektora Biura Bezpieczeństwa Komisji. Może on, jeśli uzna to za konieczne, zwrócić się do właściwych organów krajowych z wnioskiem o przekazanie dodatkowych wyjaśnień. W przypadku potwierdzenia opinii negatywnej nie można udzielić upoważnienia do dostępu do informacji klasyfikowanych.

o) Wszystkie osoby, które uzyskają upoważnienie w rozumieniu lit. d) i e), w momencie uzyskania upoważnienia są informowane o celach i zasadach ochrony informacji klasyfikowanych i środkach zapewniających bezpieczeństwo tych informacji; szkolenia takie są następnie powtarzane w regularnych odstępach czasu. Osoby te podpisują oświadczenie, że zostały poinstruowane i zobowiązują się do przestrzegania obowiązujących przepisów.

p) Dyrektor Biura Bezpieczeństwa Komisji jest zobowiązany do podjęcia wszelkich niezbędnych działań w celu wdrożenia postanowień tego punktu, w szczególności zaś określenia zasad dostępu do wykazu osób upoważnionych.

q) W wyjątkowych przypadkach, gdy wynika to z konieczności wykonania zadań, dyrektor Biura Bezpieczeństwa Komisji może udzielić tymczasowego upoważnienia, pod warunkiem że poinformował o takim zamiarze właściwe organy krajowe i w ciągu miesiąca nie zgłosiły one sprzeciwu; upoważnienie to obowiązuje do czasu zakończenia procedury określonej w lit. i), lecz nie dłużej niż 6 miesięcy.

r) Udzielone w tym trybie tymczasowe upoważnienia nie mogą uprawniać do dostępu do informacji o klauzuli EU TOP SECRET; dostęp do tych informacji jest obligatoryjnie ograniczony wyłącznie do urzędników, którzy przeszli postępowanie sprawdzające z pozytywnym wynikiem, zgodnie z lit. i). Do czasu zakończenia procedury sprawdzeniowej urzędnicy, w stosunku do których wystąpiono o przeprowadzenie postępowania na poziomie EU TOP SECRET, mogą zostać tymczasowo upoważnieni do dostępu do informacji o klauzuli do poziomu EU SECRET włącznie.

21. SPORZĄDZANIE, DYSTRYBUCJA, PRZESYŁANIE, BEZPIECZEŃSTWO OSOBOWE KURIERÓW ORAZ DODATKOWE EGZEMPLARZE LUB TŁUMACZENIA I WYCIĄGI Z DOKUMENTÓW KLASYFIKOWANYCH UE

21.1. **Sporządzanie**

1. Klauzule tajności UE nadaje się zgodnie z postanowieniami sekcji 16; w przypadku dokumentów o klauzuli EU CONFIDENTIAL są one umieszczane u góry i na dole (wyśrodkowane) każdej strony. Strony muszą być ponumerowane. Każdy dokument klasyfikowany UE musi być oznaczony numerem korespondencyjnym i datą. W przypadku dokumentów o klauzuli EU TOP SECRET i EU SECRET wymagane jest naniesienie numeru korespondencyjnego na każdej stronie. Jeśli są one dystrybuowane w kilku egzemplarzach, każdy z nich musi mieć umieszczony na pierwszej stronie odpowiedni numer egzemplarza oraz informację o liczbie stron. Obligatoryjne jest wymienienie wszystkich załączników i dodatków na pierwszej stronie wszystkich dokumentów o klauzuli EU CONFIDENTIAL lub wyższej.

2. Dokumenty o klauzuli EU CONFIDENTIAL lub wyższej mogą być drukowane, tłumaczone, przechowywane, powielane, przegrywane lub mikrofilmowane wyłącznie przez osoby, które zostały sprawdzone w związku z dostępem do informacji klasyfikowanych UE o klauzuli tajności co najmniej równej klauzuli danego dokumentu.

3. Przepisy odnoszące się do sporządzania dokumentów klasyfikowanych przy wykorzystaniu komputerów zostały określone w sekcji 25.

21.2. **Dystrybucja**

1. Informacje klasyfikowane UE są udostępniane wyłącznie osobom odpowiednio sprawdzonym i zgodnie z zasadą ograniczonego dostępu. Pierwotny rozdzielnik jest określany przez wytwórcę.

2. Dokumenty o klauzuli EU TOP SECRET mogą być rozprowadzane wyłącznie przez kancelarie tajne EU TOP SECRET (por. sekcja 22.2). W przypadku wiadomości EU TOP SECRET przesyłanych w formie elektronicznej właściwa kancelaria tajna może upoważnić osobę kierującą centrum łączności do wykonania kopii w liczbie określonej w rozdzielniku.

3. Dokumenty o klauzuli EU SECRET i niższej mogą być przekazane przez pierwotnego odbiorcę kolejnym adresatom z zachowaniem zasady ograniczonego dostępu. Wytwórcy mają jednak prawo do wyraźnego określenia wszelkich ograniczeń dotyczących kręgu odbiorców. W przypadku gdy zostały narzucone tego typu ograniczenia, adresaci mogą przekazywać dokumenty do dalszej dystrybucji wyłącznie po uzyskaniu upoważnienia wytwórcy.

4. Wpływ i wysyłka każdego dokumentu o klauzuli EU CONFIDENTIAL lub wyższej muszą być odnotowane w lokalnej kancelarii tajnej danego departamentu. Dane, które podlegają rejestracji (numer korespondencyjny, data i – gdzie ma to zastosowanie – numer egzemplarza), muszą umożliwiać identyfikację dokumentu; są one umieszczane w dzienniku lub na chronionych nośnikach komputerowych (por. sekcja 22.1).

21.3. **Przesyłanie dokumentów klasyfikowanych UE**

21.3.1. *Pakowanie, potwierdzanie odbioru*

1. Dokumenty o klauzuli EU CONFIDENTIAL lub wyższej należy przesyłać w podwójnym, nieprzezroczystym i mocnym opakowaniu. Koperta wewnętrzna jest oznaczona właściwą klauzulą tajności UE; powinny być na niej umieszczone, w miarę możliwości, pełne dane adresata (stanowisko służbowe i adres).

2. Wyłącznie urzędnik kontroli danej kancelarii tajnej (por. sekcja 22.1), lub jego zastępca, ma prawo otworzyć wewnętrzną kopertę i potwierdzić otrzymanie znajdujących się w niej dokumentów; nie dotyczy to sytuacji, gdy koperta jest adresowana do konkretnej osoby. W takim przypadku właściwa kancelaria odnotowuje wpływ koperty, natomiast otworzyć wewnętrzną kopertę i potwierdzić otrzymanie znajdujących się w niej dokumentów może tylko osoba, do której jest ona adresowana.

3. Druk potwierdzenia jest umieszczany w wewnętrznej kopercie. Potwierdzenie, które nie może być klasyfikowane, powinno zawierać numer korespondencyjny, datę wytworzenia i numer egzemplarza dokumentu; nigdy natomiast nie wolno podawać w nim tematyki, do której odnosi się dokument.

4. Koperta wewnętrzna jest opakowana w kopertę zewnętrzną, na której podaje się numer paczki dla celów potwierdzenia odbioru. Na kopercie zewnętrznej w żadnym przypadku nie wolno umieszczać klauzuli tajności.

5. W przypadku dokumentów o klauzuli EU CONFIDENTIAL lub wyższej kurierzy i posłańcy otrzymują potwierdzenia odbioru na podstawie numerów paczek.

21.3.2. *Przesyłanie w obrębie budynku lub kompleksu*

W obrębie danego budynku lub kompleksu dokumenty klasyfikowane mogą być przenoszone przez osobę sprawdzoną w związku z dostępem do informacji o co najmniej równej klauzuli tajności, zapakowane w zapieczętowaną kopertę, na której umieszcza się tylko nazwisko adresata.

21.3.3. *Przesyłanie w granicach danego państwa*

1. Na terytorium danego państwa dokumenty o klauzuli EU TOP SECRET powinny być przesyłane wyłącznie za pośrednictwem oficjalnych służb kurierskich albo osób upoważnionych do dostępu o informacji o tej klauzuli.

2. W każdym przypadku, gdy do przesłania dokumentu o klauzuli EU TOP SECRET poza budynkiem lub kompleksem wykorzystuje się służbę kurierską, wymagane jest bezwzględne stosowanie się do przepisów dotyczących pakowania i potwierdzania odbioru dokumentów, zawartych w niniejszym rozdziale. Służba powinna być tak zorganizowana, by zapewnić, że paczki zawierające dokumenty o klauzuli EU TOP SECRET pozostają przez cały czas pod bezpośrednią kontrolą odpowiedzialnej osoby.

3. W wyjątkowych przypadkach dokumenty o klauzuli EU TOP SECRET mogą być wynoszone poza budynek lub kompleks przez osoby niebędące kurierami w celu wykorzystania w trakcie spotkania lub rozmów, pod warunkiem że:

   a) osoba ta została upoważniona do dostępu do dokumentów o klauzuli EU TOP SECRET, które wynosi;

   b) sposób ich przewozu jest zgodny z przepisami odnoszącymi się do przesyłania dokumentów o tej klauzuli;

   c) osoba ta w żadnym przypadku nie pozostawia przenoszonych dokumentów bez nadzoru;

   d) przyjęto rozwiązania zapewniające, że w kancelarii tajnej EU TOP SECRET, w której dokumenty są zarejestrowane i która sprawuje nad nimi nadzór, znajduje się wykaz przenoszonych w ten sposób dokumentów. Na jego podstawie sprawdza się kompletność dokumentów po zwróceniu ich do kancelarii.

4. Na terytorium danego państwa dokumenty o klauzuli EU SECRET i EU CONFIDENTIAL mogą być przesyłane albo za pośrednictwem poczty, jeśli jest to dopuszczane przez przepisy krajowe i z zachowaniem warunków określonych w niniejszych przepisach, albo służby kurierskiej lub osób sprawdzonych w związku z dostępem do informacji klasyfikowanych UE.

5. Biuro Bezpieczeństwa Komisji jest zobowiązane do przygotowania na podstawie niniejszych przepisów instrukcji dotyczących osobistego przewozu dokumentów klasyfikowanych UE. Osoba przewożąca dokumenty powinna przeczytać i podpisać odpowiednią instrukcję. W szczególności instrukcje te powinny wyraźnie precyzować, że pod żadnym pozorem osoba przewożąca nie może:

   a) utracić bezpośredniej kontroli nad dokumentami, chyba że przekazała je w celu zdeponowania w bezpiecznym miejscu, zgodnie z przepisami sekcji 18;

   b) pozostawić dokumentów bez nadzoru w środkach komunikacji publicznej lub pojazdach prywatnych oraz w miejscach typu restauracje czy hotele. Nie dopuszcza się pozostawiania ich w hotelowych sejfach lub pozostawiania bez nadzoru w pokojach hotelowych;

   c) czytać dokumentów w miejscach publicznych, jak np. w samolocie czy pociągu.

21.3.4. *Przesyłanie pomiędzy państwami*

1. Materiały o klauzuli EU CONFIDENTIAL i wyższej powinny być przekazywane z jednego państwa do drugiego za pośrednictwem kurierów dyplomatycznych lub wojskowych Unii Europejskiej.

2. Dopuszczany jest jednak przewóz materiałów o klauzuli EU SECRET i EU CONFIDENTIAL w bagażu podręcznym, pod warunkiem że odnoszące się do niego przepisy zapewniają, że dokumenty nie dostaną się w niepowołane ręce.

3. Członek Komisji odpowiedzialny za kwestie bezpieczeństwa może wyrazić zgodę na przewóz w bagażu podręcznym, gdy nie jest możliwe przesłanie materiałów za pośrednictwem kurierów dyplomatycznych lub wojskowych albo gdy przewóz przez kurierów spowodowałby niekorzystne dla działań UE opóźnienie, a materiał jest pilnie potrzebny odbiorcom. Biuro Bezpieczeństwa Komisji jest zobowiązane do przygotowania instrukcji dotyczącej międzynarodowego przewozu w bagażu podręcznym materiałów o klauzuli do poziomu EU SECRET włącznie przez osoby niebędące kurierami dyplomatycznymi lub wojskowymi. Instrukcja określa, że:

   a) osoba przewożąca uzyskała decyzję, że spełnia warunki bezpieczeństwa;

   b) odpowiedni departament lub kancelaria tajna prowadzi wykaz wszystkich przewożonych w ten sposób materiałów;

   c) pakiety lub worki zawierające materiały UE są opatrzone urzędową pieczęcią w celu uniknięcia lub ograniczenia kontroli celnej; umieszcza się na nich nalepkę, która służy identyfikacji przesyłki i zawiera instrukcje dla znalazcy;

   d) osoba przewożąca jest wyposażona w certyfikat kuriera lub polecenie wykonania zadania, uznawane przez wszystkie Państwa Członkowskie UE, które upoważniają ją do przewozu określonej w nim przesyłki;

   e) w przypadku drogi lądowej trasa nie prowadzi przez terytorium państwa nienależącego do UE ani nie łączy się z koniecznością przekroczenia granicy takiego państwa, chyba że państwo wysyłające przesyłkę uzyskało od tego państwa odpowiednie gwarancje;

   f) przyjęte rozwiązania dotyczące organizacji podróży osoby przewożącej, w tym miejsca przeznaczenia, trasy przejazdu i środków transportu, muszą być zgodne z przepisami UE lub – gdy przepisy krajowe regulujące te kwestie są bardziej rygorystyczne – zgodnie z przepisami danego państwa;

g) osoba przewożąca nie może nikomu przekazać materiału, chyba że w celu zdeponowania go w bezpiecznym miejscu, zgodnie z przepisami sekcji 18;

h) osoba przewożąca nie może pozostawić dokumentów bez nadzoru w środkach komunikacji publicznej lub pojazdach prywatnych oraz w miejscach typu restauracje czy hotele. Nie dopuszcza się pozostawiania ich w hotelowych sejfach lub pozostawiania bez nadzoru w pokojach hotelowych;

i) jeśli w przewożonych materiałach znajdują się dokumenty, osoba przewożąca nie może ich czytać w miejscach publicznych (np. w samolocie czy pociągu).

4. Osoba wyznaczona do przewozu materiałów klasyfikowanych w bagażu podręcznym jest zobowiązana do zapoznania się z instrukcją bezpieczeństwa (i podpisania jej), która zawiera powyżej wymienione zasady oraz procedury postępowania w przypadku wydarzeń nadzwyczajnych lub zażądania przez służby celne albo służby bezpieczeństwa lotniska otwarcia przesyłki zawierającej materiały klasyfikowane.

21.3.5. *Przesyłanie dokumentów o klauzuli EU RESTRICTED*

Nie ma żadnych szczególnych przepisów odnoszących się do przesyłania dokumentów o klauzuli EU RESTRICTED. Zasady ich przewozu muszą jednak zapewniać, że nie dostaną się one w niepowołane ręce.

21.4. **Bezpieczeństwo osobowe kurierów**

Wszyscy kurierzy i posłańcy, którzy przewożą dokumenty o klauzuli EU SECRET i EU CONFIDENTAL, muszą przejść odpowiednie postępowania sprawdzające.

21.5. **Przesyłanie elektroniczne i za pośrednictwem innych środków technicznych**

1. Środki bezpieczeństwa teleinformatycznego muszą być zaprojektowane w taki sposób, aby zapewniały bezpieczeństwo w trakcie przesyłania informacji klasyfikowanych UE. Szczegółowe zasady dotyczące przesyłania informacji klasyfikowanych UE w tej postaci są zawarte w sekcji 25.

2. Informacje o klauzuli EU CONFIDENTIAL i EU SECRET mogą być przesyłane wyłącznie za pośrednictwem zatwierdzonych centrów i sieci teleinformatycznych i/lub terminali i systemów.

21.6. **Dodatkowe kopie, tłumaczenia i wyciągi z dokumentów klasyfikowanych UE**

1. Jedynie wytwórca może wyrazić zgodę na wykonanie kopii lub tłumaczenie dokumentów o klauzuli EU TOP SECRET.

2. W przypadku gdy z informacją, która – mimo że zawarta w dokumencie o klauzuli EU TOP SECRET – nie jest objęta tą klauzulą, powinny zapoznać się osoby nieposiadające upoważnienia do dostępu do informacji o klauzuli EU TOP SECRET, kierownik właściwej kancelarii tajnej EU TOP SECRET (por. sekcja 22.2) może zostać upoważniony do wykonania niezbędnej liczby wyciągów z tego dokumentu. Jest on jednocześnie zobowiązany do podjęcia wszystkich kroków koniecznych do zapewnienia, że wyciągi te są objęte odpowiednią klauzulą tajności.

3. Adresat może wykonywać kopie i tłumaczenia z dokumentów o klauzuli EU SECRET i niższej z zachowaniem przepisów krajowych i pod warunkiem rygorystycznego stosowania zasady ograniczonego dostępu. Środki bezpieczeństwa, które odnoszą się do dokumentu oryginalnego, stosuje się także w stosunku do kopii i/lub tłumaczeń.

22. KANCELARIE TAJNE UE, KONTROLE KOMPLEKSOWE I WYRYWKOWE, ARCHIWIZOWANIE I NISZCZENIE DOKUMENTÓW KLASYFIKOWANYCH UE

22.1. **Lokalne kancelarie tajne UE**

1. W ramach Komisji lokalne kancelarie tajne UE, działające w każdym departamencie (w zależności od potrzeb jedna lub kilka), są odpowiedzialne za rejestrowanie, powielanie, wysyłanie, archiwizowanie i niszczenie dokumentów o klauzuli EU SECRET i EU CONFIDENTIAL.

2. W przypadku gdy dany departament nie ma lokalnej kancelarii tajnej UE, jej funkcje na potrzeby tego departamentu wykonuje lokalna kancelaria tajna UE Sekretariatu Generalnego.

3. Lokalne kancelarie tajne podlegają dyrektorowi departamentu; zatwierdza on instrukcje ich pracy. Kierownik takiej kancelarii jest urzędnikiem kontroli kancelarii (RCO).

4. Nadzór nad przestrzeganiem przez lokalne kancelarie tajne UE przepisów dotyczących postępowania z dokumentami klasyfikowanymi UE oraz stosowania właściwych środków ochrony sprawuje lokalny pełnomocnik ochrony (LSO).

5. Urzędnicy wyznaczeni do pracy w lokalnych kancelariach tajnych UE muszą być upoważnieni do dostępu do informacji klasyfikowanych UE, zgodnie z postanowieniami sekcji 20.

6. Lokalne kancelarie UE, działając pod zwierzchnictwem właściwego dyrektora departamentu, są zobowiązane do:

   a) nadzorowania czynności związanych z rejestracją, kopiowaniem, tłumaczeniem, przesyłaniem, przekazywaniem do odbiorców i niszczeniem informacji klasyfikowanych UE;

   b) uaktualniania danych zawartych w wykazach informacji klasyfikowanych;

   c) okresowego rozsyłania zapytań, czy wskazane jest utrzymywanie klauzuli tajności informacji.

7. Lokalne kancelarie tajne UE są zobowiązane do prowadzenia wykazu uwzględniającego następujące dane:

   a) datę opracowania danej informacji klasyfikowanej;

   b) klauzulę tajności;

   c) datę obowiązywania klauzuli;

   d) określenie autora i departamentu, w którym została opracowana dana informacja;

   e) odbiorcę lub odbiorców, z numerami egzemplarzy;

   f) przedmiot;

   g) numer dziennika;

   h) liczbę rozesłanych egzemplarzy;

   i) przygotowanie spisów informacji klasyfikowanych, które zostały przekazane do departamentu;

   j) odnotowywanie obniżania i znoszenia klauzuli tajności.

8. Do lokalnych kancelarii tajnych UE odnoszą się ogólne zasady, określone w sekcji 21, chyba że szczegółowe przepisy niniejszego punktu stanowią inaczej.

22.2 **Kancelarie tajne EU TOP SECRET**

22.2.1. *Uwagi ogólne*

1. Zadaniem kancelarii tajnych EU TOP SECRET jest zapewnienie, że rejestrowanie, wykonywanie czynności związanych z obiegiem i rozsyłanie dokumentów o tej klauzuli odbywa się zgodnie z niniejszymi przepisami bezpieczeństwa. Kierownik kancelarii tajnej EU TOP SECRET pełni funkcję urzędnika kontroli kancelarii EU TOP SECRET.

2. Główne kancelarie tajne pełnią funkcję podstawowego punktu przyjmującego i rozsyłającego informacje w Komisji, innych instytucjach unijnych, Państwach Członkowskich, organizacjach międzynarodowych i państwach trzecich, z którymi Komisja zawarła umowy w sprawie procedur bezpieczeństwa w odniesieniu do wymiany informacji klasyfikowanych.

3. Gdy istnieje taka potrzeba, ustanawia się podkancelarie odpowiedzialne za nadzór nad obiegiem wewnętrznym dokumentów o klauzuli EU TOP SECRET; ich zadaniem jest dokumentowanie obiegu wszystkich dokumentów, pozostających w gestii danej podkancelarii.

4. Podkancelarie EU TOP SECRET ustanawia się zgodnie z postanowieniami Sekcji 22.2.3. w przypadku zaistnienia potrzeby sprawowania stałego lub długotrwałego nadzoru nad dokumentami; podlegają one głównej kancelarii tajnej EU TOP SECRET. Gdy potrzeba zapoznania się z dokumentami o klauzuli EU TOP SECRET występuje rzadko i jest krótkotrwała, możliwe jest ich udostępnienie bez ustanawiania podkancelarii, pod warunkiem że stosowane są wszystkie wymagane środki bezpieczeństwa fizycznego i osobowego.

5. Podkancelarie nie mogą przesyłać dokumentów o klauzuli EU TOP SECRET bezpośrednio do innych podkancelarii podlegających tej samej głównej kancelarii tajnej EU TOP SECRET bez wyraźnego upoważnienia z jej strony.

6. Przekazywanie dokumentów o klauzuli EU TOP SECRET pomiędzy dwiema podkancelariami niepodlegającymi tej samej głównej kancelarii tajnej odbywa się za pośrednictwem nadzorujących głównych kancelarii tajnych EU TOP SECRET.

22.2.2. *Główne kancelarie tajne EU TOP SECRET*

Jako urzędnik kontroli kierownik głównej kancelarii tajnej EU TOP SECRET jest odpowiedzialny za:

a) przekazywanie dokumentów o klauzuli EU TOP SECRET zgodnie z postanowieniami sekcji 21.3;

b) prowadzenie wykazu wszystkich podległych podkancelarii EU TOP SECRET, wraz z nazwiskami i wzorami podpisów urzędników kontroli i osób upoważnionych do ich zastępowania;

c) przechowywanie otrzymanych z innych kancelarii pokwitowań za wszystkie dokumenty o klauzuli EU TOP SECRET przekazane przez główną kancelarię tajną;

d) prowadzenie wykazu wszystkich posiadanych i przekazanych do odbiorców dokumentów o klauzuli EU TOP SECRET;

e) prowadzenie aktualnego wykazu wszystkich głównych kancelarii tajnych EU TOP SECRET, z którymi prowadzi stałą wymianę dokumentów, wraz z nazwiskami i wzorami podpisów urzędników kontroli i osób upoważnionych do ich zastępowania;

f) fizyczne zabezpieczenie wszystkich dokumentów o klauzuli EU TOP SECRET, pozostających w gestii danej głównej kancelarii tajnej, zgodnie z postanowieniami sekcji 18.

22.2.3. *Podkancelarie tajne EU TOP SECRET*

Jako urzędnik kontroli, kierownik podkancelarii EU TOP SECRET jest odpowiedzialny za:

a) przekazywanie dokumentów o klauzuli EU TOP SECRET zgodnie z postanowieniami sekcji 21.3;

b) prowadzenie aktualnego wykazu wszystkich osób upoważnionych do dostępu do informacji o klauzuli EU TOP SECRET, które pozostają pod jego nadzorem;

c) przekazywanie dokumentów o klauzuli EU TOP SECRET do odbiorców zgodnie z instrukcjami wytwórcy lub na podstawie zasady ograniczonego dostępu, po uprzednim upewnieniu się, czy adresat został odpowiednio sprawdzony;

d) prowadzenie aktualnego wykazu wszystkich dokumentów o klauzuli EU TOP SECRET znajdujących się posiadaniu kancelarii i w obiegu pod jej nadzorem lub przekazanych do innych kancelarii EU TOP SECRET oraz przechowywanie wszystkich pokwitowań za udostępnione i przekazane dokumenty;

e) prowadzenie aktualnego wykazu wszystkich kancelarii tajnych EU TOP SECRET, z którymi może na podstawie upoważnienia prowadzić wymianę dokumentów o klauzuli EU TOP SECRET, wraz z nazwiskami i wzorami podpisów urzędników kontroli tych kancelarii i osób upoważnionych do ich zastępowania;

f) fizyczne zabezpieczenie wszystkich dokumentów o klauzuli EU TOP SECRET pozostających w gestii danej podkancelarii, zgodnie z postanowieniami sekcji 18.

22.3. **Przeglądy, kontrole kompleksowe i wyrywkowe**

1. Każda kancelaria tajna EU TOP SECRET, o której mowa w niniejszym punkcie, jest zobowiązana do przeprowadzania raz na 12 miesięcy szczegółowego spisu dokumentów o klauzuli EU TOP SECRET. Uznaje się, że dokument został rozliczony, jeśli stwierdzono, w wyniku bezpośredniego oglądu, że jest on przechowywany w kancelarii lub też jego przekazanie do innej kancelarii tajnej EU TOP SECRET jest udokumentowane pokwitowaniem, zniszczenie – protokołem zniszczenia, a obniżenie lub zniesienie klauzuli – odpowiednią decyzją. Kancelarie tajne EU TOP SECRET przekazują wyniki corocznego przeglądu członkowi Komisji odpowiedzialnemu za sprawy bezpieczeństwa najpóźniej do dnia 1 kwietnia każdego roku.

2. Podkancelarie EU TOP SECRET są zobowiązane do przekazania wyników corocznego przeglądu do Głównej Kancelarii Tajnej, której podlegają, w terminie przez nią określonym.

3. Informacje klasyfikowane UE o klauzuli niższej niż EU TOP SECRET podlegają wewnętrznym wyrywkowym kontrolom zgodnie z instrukcjami członka Komisji odpowiedzialnego za kwestie bezpieczeństwa.

4. Działania te stwarzają możliwość określenia:

   a) dokumentów, których klauzula może być obniżona lub zdjęta;

   b) dokumentów, które mogą zostać zniszczone.

22.4. **Archiwizowanie informacji klasyfikowanych UE**

1. Informacje klasyfikowane UE muszą być przechowywane w warunkach spełniających wymagania określone w punkcie 18.

2. W celu zminimalizowania problemów związanych z przechowywaniem urzędnicy kontroli wszystkich kancelarii tajnych są upoważnieni do mikrofilmowania dokumentów EU TOP SECRET, EU SECRET i EU CONFIDENTIAL lub też do archiwizowania ich na nośnikach magnetycznych albo optycznych, pod warunkiem że:

   a) czynności związane z mikrofilmowaniem/przeniesieniem na inne nośniki są wykonywane przez pracowników posiadających aktualną decyzję o spełnianiu warunków bezpieczeństwa do dostępu do informacji o danej klauzuli tajności;

   b) mikrofilmom/nośnikom został zapewniony identyczny stopień ochrony, jak dokumentom oryginalnym;

   c) fakt mikrofilmowania/przeniesienia na inne nośniki dokumentu o klauzuli EU TOP SECRET został zgłoszony wytwórcy;

   d) rolki filmu lub inne nośniki zawierają wyłącznie dokumenty objęte jedną z klauzul: EU TOP SECRET, EU SECRET lub EU CONFIDENTIAL;

   e) fakt mikrofilmowania/przeniesienia na inny nośnik dokumentu o klauzuli EU TOP SECRET lub EU SECRET jest wyraźnie odnotowany w wykazie/dzienniku wykorzystywanym przy przeprowadzaniu corocznego spisu dokumentów;

   f) po mikrofilmowaniu lub przeniesieniu na inny nośnik oryginalne dokumenty zostały zniszczone, zgodnie z przepisami określonymi w sekcji 22.5.

3. Powyższe zasady odnoszą się także do innych, dopuszczonych przez odpowiednie władze, form przechowywania dokumentów, jak np. na nośnikach elektromagnetycznych lub dyskach optycznych.

22.5. **Niszczenie dokumentów klasyfikowanych UE**

1. Aby zapobiec przechowywaniu nadmiernych ilości dokumentów klasyfikowanych UE, należy niszczyć jak najszybciej te informacje, które kierownik dysponującej nimi instytucji uznał za nieaktualne lub też przechowywane w zbyt dużej liczbie egzemplarzy. Niszczenie powinno odbywać się zgodnie z poniższymi zasadami:

   a) dokumenty o klauzuli EU TOP SECRET mogą być niszczone wyłącznie w głównej kancelarii tajnej, pod której nadzorem pozostają. Każdy zniszczony dokument musi być odnotowany w protokole zniszczenia, który podpisuje urzędnik kontroli EU TOP SECRET i urzędnik będący świadkiem niszczenia; urzędnik ten musi być sprawdzony w związku z dostępem do informacji o tej klauzuli. Fakt zniszczenia dokumentu musi być odnotowany w odpowiednim dzienniku;

   b) kancelaria tajna przechowuje przez 10 lat protokoły zniszczenia, razem z kartami zapoznania z dokumentem. Kopie protokołów są przekazywane wytwórcy lub właściwej głównej kancelarii tajnej tylko na wyraźne życzenie;

   c) dokumenty o klauzuli EU TOP SECRET, w tym także zbędne materiały powstałe w toku wytwarzania dokumentów o tej klauzuli, jak np. uszkodzone kopie, szkice robocze, notatki maszynowe, dyskietki komputerowe, muszą być zniszczone – pod nadzorem urzędnika kontroli EU TOP SECRET – przez spalenie, przetworzenie na miazgę, pocięcie w niszczarce lub w inny sposób zapewniający, że staną się one nierozpoznawalne i niemożliwe do odtworzenia.

2. Dokumenty o klauzuli EU SECRET są niszczone w kancelarii, która sprawuje nad nimi nadzór, pod kontrolą odpowiednio sprawdzonej osoby, na jeden ze sposobów określonych w ust. 1 lit. c). Wykaz zniszczonych dokumentów o tej klauzuli musi zostać umieszczony w podpisanym protokole zniszczenia, który jest co najmniej przez 3 lata przechowywany przez daną kancelarię razem z kartami zapoznania z dokumentem.

3. Dokumenty o klauzuli EU CONFIDENTIAL są niszczone w kancelarii, która sprawuje nad nimi nadzór, pod kontrolą odpowiednio sprawdzonej osoby, na jeden ze sposobów określonych w ust. 1 lit. c). Fakt zniszczenia jest dokumentowany zgodnie z instrukcjami członka Komisji odpowiedzialnego za kwestie bezpieczeństwa.

4. Dokumenty o klauzuli UE RESTRICTED są niszczone w kancelarii, która sprawuje nad nimi nadzór, lub osobę, która z nich korzystała, zgodnie z instrukcjami członka Komisji odpowiedzialnego za kwestie bezpieczeństwa.

22.6. **Niszczenie w sytuacjach nadzwyczajnych**

1. Poszczególne departamenty Komisji są zobowiązane do opracowania dostosowanych do lokalnych uwarunkowań planów ochrony materiałów klasyfikowanych UE w sytuacjach kryzysowych, uwzględniających możliwość – w przypadku konieczności podjęcia takich działań – zniszczenia lub ewakuacji materiałów klasyfikowanych. W ramach każdej struktury należy podać do ogólnej wiadomości instrukcje postępowania uznane za konieczne, by zapobiec dostaniu się informacji klasyfikowanych UE w niepowołane ręce.

2. Ochrona i/lub niszczenie materiałów o klauzuli EU SECRET i EU CONFIDENTIAL w sytuacji kryzysowej nie może w żadnym przypadku utrudniać lub zakłócać ochrony lub niszczenia materiałów o klauzuli EU TOP SECRET, w tym urządzeń szyfrujących, których ochrona ma pierwszeństwo w stosunku do wszelkich innych działań.

3. Środki ochrony i niszczenia urządzeń szyfrujących w sytuacjach kryzysowych zostaną określone w instrukcjach postępowania przyjmowanych w każdym konkretnym przypadku.

4. Instrukcje muszą być przechowywane w miejscu niszczenia w zapieczętowanej kopercie. Należy zapewnić dostępność środków/narzędzi niszczenia.

23. ŚRODKI BEZPIECZEŃSTWA STOSOWANE W TRAKCIE SPOTKAŃ ODBYWAJĄCYCH SIĘ POZA SIEDZIBĄ KOMISJI, W TOKU KTÓRYCH WYKORZYSTYWANE SĄ INFORMACJE KLASYFIKOWANE UE

23.1. **Uwagi ogólne**

1. Opisane poniżej środki bezpieczeństwa należy stosować w przypadku, gdy posiedzenie Komisji lub też inne mające istotne znaczenie spotkanie jest organizowane poza budynkami Komisji i gdy ich użycie jest uzasadnione szczególną sensytywnością omawianych kwestii lub wykorzystywanych informacji. Środki te odnoszą się jedynie do ochrony informacji klasyfikowanych UE; nie można wykluczyć, że wystąpi konieczność zaplanowania innych środków ochrony.

23.2. **Zakresy odpowiedzialności**

23.2.1. *Biuro Bezpieczeństwa Komisji*

Biuro Bezpieczeństwa Komisji jest zobowiązane do współpracy z właściwymi organami Państwa Członkowskiego, na którego terytorium odbywa się spotkanie (państwa przyjmującego), w celu zapewnienia bezpieczeństwa posiedzenia Komisji lub innego ważnego spotkania oraz bezpieczeństwa przewodniczących delegacji i ich personelu. W odniesieniu do bezpieczeństwa powinno ono w szczególności zapewnić:

a) przygotowanie planów postępowania na wypadek wystąpienia zagrożeń dla ochrony informacji, ze szczególnym uwzględnieniem środków mających na celu ochronę informacji klasyfikowanych UE znajdujących się w pomieszczeniach biurowych;

b) możliwość dostępu do systemu teleinformatycznego Komisji pozwalającego na odbieranie i wysyłanie wiadomości klasyfikowanych UE. Jeśli istnieje taka potrzeba, należy zwrócić się do państwa przyjmującego z wnioskiem o zapewnienie dostępu do zabezpieczonych linii telefonicznych.

Biuro Bezpieczeństwa Komisji powinno doradzać w kwestiach bezpieczeństwa związanych z przygotowaniami do spotkania; powinno być także reprezentowane na miejscu, by w miarę potrzeb doradzać i pomagać pełnomocnikowi ochrony spotkania i delegacjom.

Każda delegacja uczestnicząca w spotkaniu powinna wyznaczyć osobę odpowiedzialną za bezpieczeństwo (pełnomocnik ochrony delegacji), do której obowiązków będzie należało zajmowanie się kwestiami bezpieczeństwa w ramach delegacji oraz utrzymywanie kontaktów z pełnomocnikiem ochrony spotkania, a także, w miarę potrzeb, z przedstawicielem Biura Bezpieczeństwa Komisji.

23.2.2. *Pełnomocnik ochrony spotkania*

Należy wyznaczyć pełnomocnika ochrony, który odpowiada za przygotowanie i nadzór nad całością wewnętrznych środków ochrony oraz współpracę z innymi właściwymi władzami bezpieczeństwa. Podjęte środki powinny obejmować:

a) środki ochrony w miejscu, gdzie odbywa się spotkanie, w celu zapewnienia, że jego przebieg nie zostanie zakłócony żadnymi incydentami, które mogłyby narazić na szwank bezpieczeństwo wykorzystywanych w jego toku informacji klasyfikowanych UE;

b) sprawdzanie pracowników, którzy uzyskali prawo dostępu do miejsca spotkania, stref przeznaczonych dla poszczególnych delegacji oraz sal konferencyjnych, a także sprawdzanie sprzętu;

c) stałą współpracę z właściwymi organami państwa przyjmującego oraz Biurem Bezpieczeństwa Komisji;

d) włączenie do materiałów dotyczących spotkania instrukcji na temat bezpieczeństwa, uwzględniających wymogi określone w niniejszych przepisach oraz wszelkich innych instrukcji odnoszących się do bezpieczeństwa, jakie zostaną uznane za konieczne.

23.3. **Środki ochrony**

23.3.1. *Strefy bezpieczeństwa*

Należy utworzyć opisane poniżej strefy bezpieczeństwa:

a) strefę bezpieczeństwa klasy II obejmującą pomieszczenia, w których opracowywane będą projekty i kolejne wersje dokumentów, pomieszczenia biurowe Komisji i sprzęt powielający, a także, gdy ma to zastosowanie, pomieszczenia biurowe delegacji;

b) strefę bezpieczeństwa klasy I obejmującą sale konferencyjne, a także pomieszczenia tłumaczy i inżynierów dźwięku;

c) strefy administracyjne obejmujące strefę dostępną dla dziennikarzy oraz części obiektu, w którym odbywa się konferencja, wykorzystywane do prac administracyjnych, serwowania posiłków oraz zakwaterowania, a także strefę bezpośrednio przylegającą do centrum prasowego i miejsca, w którym odbywa się spotkanie.

23.3.2. *Przepustki*

Pełnomocnik ochrony spotkania powinien wydawać odpowiednie identyfikatory zgodnie z potrzebami zgłoszonymi przez delegacje. Gdzie jest to wymagane, można wprowadzić zróżnicowanie prawa dostępu do poszczególnych stref bezpieczeństwa.

Instrukcja bezpieczeństwa spotkania powinna zobowiązywać wszystkich uczestników, by przez cały czas przebywania w miejscu spotkania nosili identyfikatory w widocznym miejscu, tak by mogły być sprawdzane przez służby ochrony.

Do miejsca spotkania powinno się wpuszczać możliwie jak najmniej osób, które nie są uczestnikami spotkania i nie noszą identyfikatorów. Wyłącznie pełnomocnik ochrony spotkania może wyrazić – na wniosek delegacji krajowych – zgodę na przyjmowanie przez nie gości. Osobom tym zostaną wydane przepustki dla gości; w tym celu muszą one wypełnić formularz wydania przepustki, podając swoje imię i nazwisko oraz imię i nazwisko osoby zapraszającej. Goście powinni być cały czas eskortowani przez strażnika lub zapraszającego. Osoba towarzysząca powinna mieć formularz wydania przepustki; oddaje go służbom ochrony, wraz z przepustką, po opuszczeniu przez gościa miejsca spotkania.

23.3.3. *Kontrola sprzętu fotograficznego i nagrywającego*

Do strefy bezpieczeństwa klasy I nie można wnosić żadnego sprzętu fotograficznego ani nagrywającego, poza sprzętem przyniesionym przez fotografów i inżynierów dźwięku odpowiednio upoważnionych przez pełnomocnika ochrony spotkania.

23.3.4. *Kontrola teczek, przenośnych komputerów i pakietów*

Noszący identyfikatory uczestnicy, którzy mają prawo dostępu do strefy bezpieczeństwa, w normalnych warunkach mogą wnosić swoje teczki i przenośne komputery (wyłącznie z własnym źródłem zasilania) bez sprawdzeń. Delegacje mogą dostarczać na miejsce spotkania przeznaczone do własnego użytku pakiety, przy czym muszą być one albo sprawdzone przez pełnomocnika ochrony delegacji, albo prześwietlone za pomocą specjalistycznego sprzętu lub też otwarte w celu skontrolowania ich zawartości przez służby ochrony. Jeśli pełnomocnik ochrony spotkania uzna to za konieczne, można przyjąć bardziej rygorystyczne zasady kontroli teczek i pakietów.

23.3.5. *Bezpieczeństwo techniczne*

Pomieszczenie, w którym odbywa się spotkanie, może zostać zabezpieczone technicznie przez grupę bezpieczeństwa technicznego; może ona także prowadzić elektroniczny nadzór spotkania.

23.3.6. *Dokumenty należące do delegacji*

Delegacje odpowiadają za dostarczanie dokumentów klasyfikowanych UE na spotkania i zabieranie ich po zakończeniu. Ich obowiązkiem jest także sprawdzenie i zapewnienie bezpieczeństwa tych dokumentów w czasie, gdy pracują z nimi w przydzielonych im pomieszczeniach. Mogą występować z wnioskiem o udzielenie przez państwo przyjmujące pomocy w zakresie transportu dokumentów klasyfikowanych do i z miejsca spotkania.

23.3.7. *Bezpieczne przechowywanie dokumentów*

Jeśli Komisja lub delegacje nie mają możliwości przechowywania znajdujących się w ich gestii dokumentów klasyfikowanych UE zgodnie z obowiązującymi standardami, mogą umieścić te dokumenty w zapieczętowanej kopercie i zostawić je za pokwitowaniem u pełnomocnika ochrony spotkania, który przechowa je w sposób zgodny z przepisami bezpieczeństwa.

23.3.8. *Kontrole pomieszczeń*

Pełnomocnik ochrony spotkania jest zobowiązany do zapewnienia, że pomieszczenia biurowe Komisji oraz delegacji zostaną na koniec każdego dnia pracy dokładnie sprawdzone w celu upewnienia się, że wszystkie dokumenty klasyfikowane UE są przechowywane w bezpiecznym miejscu. W przypadku stwierdzenia nieprawidłowości podejmuje właściwe kroki.

23.3.9. *Niszczenie zbędnych wydruków zawierających informacje klasyfikowane UE*

Wszystkie zbędne wydruki powinny być traktowane jak dokumenty klasyfikowane UE. Przedstawiciele Komisji i delegacje powinny zostać wyposażone w specjalne kosze lub worki, do których można je wyrzucać. Przed opuszczeniem pomieszczeń, które zostały im przydzielone, Komisja i delegacje powinny oddać swoje zbędne wydruki pełnomocnikowi ochrony spotkania, która zapewni ich zniszczenie zgodnie z obowiązującymi przepisami.

Po zakończeniu spotkania wszystkie nieprzydatne już dokumenty znajdujące się w dyspozycji Komisji lub delegacji należy traktować jako zbędne wydruki. Przed zniesieniem środków bezpieczeństwa należy przeprowadzić dokładne przeszukanie pomieszczeń, które były przydzielone Komisji i delegacjom. Dokumenty, których odbiór został pokwitowany, powinny – w miarę możliwości – zostać zniszczone zgodnie z postanowieniami sekcji 22.5.

24. NIEPRZESTRZEGANIE PRZEPISÓW BEZPIECZEŃSTWA I NARAŻENIE NA SZWANK BEZPIECZEŃSTWA INFORMACJI KLASYFIKOWANYCH UE

24.1. **Definicje**

Nieprzestrzeganie przepisów bezpieczeństwa jest wynikiem działania lub zaniechania sprzecznego z przepisami Komisji, które może narazić na szwank bezpieczeństwo informacji klasyfikowanych UE.

Narażenie na szwank bezpieczeństwa informacji klasyfikowanych UE ma miejsce, gdy informacje te w całości lub częściowo dostały się w ręce osób nieupoważnionych, tzn. takich, które nie zostały odpowiednio sprawdzone albo zapoznanie się z daną informacją nie jest im potrzebne do wykonywania obowiązków służbowych, lub też gdy istnieje uzasadnione podejrzenie, że doszło do takiej sytuacji.

Bezpieczeństwo informacji klasyfikowanych UE może zostać narażone na szwank wskutek braku ostrożności, zaniedbania lub niedyskrecji, a także w wyniku działań służb, które dążą do uzyskania pozostających w gestii UE albo Państw Członkowskich informacji klasyfikowanych UE lub rozpoznania przedsięwzięć objętych klauzulą tajności, lub też działań organizacji antypaństwowych.

24.2. **Zgłaszanie przypadków nieprzestrzegania przepisów bezpieczeństwa**

Wszystkie osoby korzystające z informacji klasyfikowanych UE muszą zostać dokładnie zapoznane ze swoimi obowiązkami w tym zakresie. Są zobowiązane do bezzwłocznego zgłaszania wszelkich przypadków nieprzestrzegania przepisów bezpieczeństwa, o których się dowiedziały.

W przypadku ustalenia lub uzyskania informacji o naruszeniu przepisów bezpieczeństwa, utracie lub zaginięciu informacji klasyfikowanej UE, lokalny pełnomocnik ochrony lub pełnomocnik ochrony spotkania są zobligowani do niezwłocznego podjęcia działań w celu:

a) zabezpieczenia dowodów;

b) ustalenia faktów;

c) dokonania oceny i zminimalizowania powstałych szkód;

d) podjęcia środków uniemożliwiających powtórzenie się takiej sytuacji w przyszłości;

e) poinformowania właściwych władz o skutkach nieprzestrzegania przepisów bezpieczeństwa.

W zawiadomieniu o przypadku nieprzestrzegania przepisów bezpieczeństwa wymagane jest podanie następujących informacji:

i) opis informacji, których sprawa dotyczy, w tym ich klauzula, numer dziennika i egzemplarza, data, określenie wytwórcy, przedmiot i zakres;

ii) zwięzły opis okoliczności, w których doszło do nieprzestrzegania przepisów bezpieczeństwa, w tym podanie daty i określenie czasu, przez jaki bezpieczeństwo informacji było narażone na szwank;

iii) oświadczenie, czy poinformowano wytwórcę.

Każda władza bezpieczeństwa jest zobowiązana, gdy tylko zostanie poinformowana o przypadku nieprzestrzegania przepisów bezpieczeństwa, do natychmiastowego jego zgłoszenia do Biura Bezpieczeństwa Komisji.

Przypadki dotyczące informacji o klauzuli EU RESTRICTED podlegają zgłaszaniu tylko wtedy, gdy towarzyszyły im niezwykłe okoliczności.

Po uzyskaniu informacji o przypadku nieprzestrzegania przepisów bezpieczeństwa, członek Komisji odpowiedzialny za kwestie bezpieczeństwa jest zobowiązany do podjęcia następujących działań:

a) powiadamia wytwórcę danej informacji;

b) występuje do właściwych władz bezpieczeństwa z wnioskiem o przeprowadzenie odpowiedniego postępowania;

c) koordynuje prowadzenie postępowań wyjaśniających, gdy sprawa pozostaje we właściwości więcej niż jednej władzy bezpieczeństwa;

d) otrzymuje raport dotyczący okoliczności przypadku nieprzestrzegania przepisów bezpieczeństwa; daty lub okresu, kiedy mogło do tego dojść i kiedy fakt ten został stwierdzony; ze szczegółowym opisem zawartości i klauzuli tajności materiału, którego sprawa dotyczy. Wymagane jest także uwzględnienie oceny szkód wyrządzonych interesom UE lub też jednemu albo większej grupie Państw Członkowskich oraz informacji, jakie podjęto działania w celu zapobieżenia możliwości powtórzenia się takiej sytuacji w przyszłości.

Wytwórca informuje o zdarzeniu adresatów i przekazuje im odpowiednie instrukcje postępowania.

24.3. **Odpowiedzialność prawna**

Każda osoba, która doprowadziła do narażenia na szwank bezpieczeństwa informacji klasyfikowanych UE, podlega postępowaniu dyscyplinarnemu określonemu w odpowiednich przepisach, w szczególności w tytule VI regulaminu pracowniczego. Działania takie nie stanowią przeszkody dla wszelkich innych działań podjętych na podstawie przepisów prawa.

Gdy jest to uzasadnione, na podstawie raportu, o którym mowa w sekcji 24.2, członek Komisji odpowiedzialny za kwestie bezpieczeństwa jest zobowiązany do podjęcia wszelkich kroków w celu umożliwienia właściwym organom krajowym wszczęcia postępowania karnego.

25. OCHRONA INFORMACJI KLASYFIKOWANYCH UE PRZETWARZANYCH W SYSTEMACH TELEINFORMATYCZNYCH

25.1. **Wprowadzenie**

25.1.1. *Uwagi ogólne*

Niniejsza polityka bezpieczeństwa i wymogi odnoszą się do wszystkich systemów i sieci teleinformatycznych (dalej określanych jako systemy), w których przetwarzane są informacje o klauzuli EU CONFIDENTIAL lub wyższej. Są one przeznaczone do stosowania jako uzupełnienie decyzji Komisji C (95) 1510 z dnia 23 listopada 1995 r. w sprawie ochrony systemów informatycznych.

Systemy, w których przetwarzane są informacje o klauzuli EU RESTRICTED, także wymagają zastosowania środków bezpieczeństwa w celu ochrony poufności tych informacji. Wszystkie systemy wymagają zastosowania środków bezpieczeństwa w celu ochrony integralności i dostępności zarówno samych systemów, jak i znajdujących się w nich informacji.

Na politykę w zakresie bezpieczeństwa teleinformatycznego realizowaną przez Komisję składają się następujące elementy:

— Stanowi ona integralną część całego systemu bezpieczeństwa i uzupełnia wszystkie elementy bezpieczeństwa obiegu informacji, osobowego i fizycznego;

— Podział obowiązków pomiędzy technicznych właścicieli systemów, właścicieli informacji klasyfikowanych przechowywanych lub przetwarzanych w systemach technicznych, specjalistów w zakresie bezpieczeństwa teleinformatycznego oraz użytkowników;

— Opis zasad bezpieczeństwa oraz wymogów dla każdego systemu teleinformatycznego;

— Uzyskanie akceptacji tych zasad i wymogów przez wyznaczone organy;

— Uwzględnienie specyficznych zagrożeń i słabych punktów w strefie IT.

25.1.2. *Zagrożenia i słabe punkty systemów*

Zagrożenie można zdefiniować jako możliwość przypadkowego lub celowego narażenia na szwank bezpieczeństwa. W odniesieniu do systemów narażenie na szwank oznacza utratę poufności, integralności lub dostępności. Słaby punkt można zdefiniować jako niedostateczną kontrolę lub jej brak, co może ułatwić lub umożliwić stworzenie zagrożenia dla konkretnych zasobów lub celów.

Klasyfikowane i nieklasyfikowane informacje UE przetwarzane w systemach w sposób zintegrowany i w postaci gotowej do szybkiego przeszukiwania, przekazywania i wykorzystania, są podatne na wiele zagrożeń. Zagrożenia te mogą polegać na uzyskaniu dostępu do informacji przez osoby nieupoważnione lub, przeciwnie, uniemożliwieniu dostępu osobom upoważnionym. Ponadto gromadzone w ten sposób informacje są narażone na nieupoważnione ujawnienie, zniekształcenie treści, wprowadzenie zmian lub zniszczenie. Co więcej, sprzęt komputerowy, złożony i czasami podatny na uszkodzenia, jest kosztowny i często trudno go szybko naprawić lub wymienić.

25.1.3. *Cel stosowania środków ochrony*

Środki ochrony omawiane w poniższej sekcji mają przede wszystkim na celu zabezpieczenie przed nieupoważnionym ujawnieniem informacji (utratą poufności) oraz przed utratą ich integralności i dostępności. Aby zapewnić odpowiednią ochronę systemów, w których przetwarzane są informacje klasyfikowane UE, konieczne jest określenie przez Biuro Bezpieczeństwa Komisji właściwych standardów bezpieczeństwa ogólnego oraz szczególnych procedur i rozwiązań technicznych, przeznaczonych dla danego systemu.

25.1.4. *Szczególne wymagania bezpieczeństwa systemu (SWBS)*

Właściciel systemów technicznych (TSO; por. sekcja 25.3.4) oraz właściciel informacji (por. sekcja 25.3.5) są zobowiązani do opracowania dla każdego systemu, w którym przetwarzane są informacje o klauzuli EU CONFIDENTIAL i wyższej, szczególnych wymagań bezpieczeństwa systemu (SWBS) we współpracy – w zależności od potrzeb, w formie czynnego udziału lub doradztwa – z zespołem, który zaprojektował system oraz pracownikami Biura Bezpieczeństwa Komisji (jako władzy bezpieczeństwa teleinformatycznego INFOSEC; por. sekcja 25.3.3). SWBS podlega następnie zatwierdzeniu przez władze akredytacji bezpieczeństwa (SAA; por. sekcja 25.3.2).

Wymagane jest opracowanie SWBS także w przypadku, gdy w ocenie SAA istotne znaczenie ma zapewnienie dostępności i integralności informacji o klauzuli EU RESTRICTED lub nieklasyfikowanych.

SWBS należy sformułować w początkowej fazie projektowania systemu, a następnie uzupełniać i udoskonalać w miarę rozwoju prac nad projektem, w ten sposób zapewniając wypełnianie różnych funkcji na różnych etapach realizacji projektu, a następnie w kolejnych okresach funkcjonowania systemu.

25.1.5. *Tryby bezpiecznego funkcjonowania*

Wszystkie systemy, w których przetwarzane są informacje o klauzuli EU CONFIDENTIAL i wyższej, podlegają zatwierdzeniu jako funkcjonujące w jednym lub – gdy uzasadniają to zmienne wymagania w różnych okresach – w kilku z następujących trybów bezpiecznego funkcjonowania (możliwe jest też zastosowanie krajowych odpowiedników):

a) ogólnosystemowy;

b) ogólnosystemowy zróżnicowany;

c) wielopoziomowy.

25.2. **Definicje**

„Akredytacja" (dopuszczanie do eksploatacji) oznacza udzielenie zezwolenia i zatwierdzenie systemu jako zdolnego do przetwarzania informacji klasyfikowanych UE w danym środowisku pracy.

Uwaga:

Akredytacji należy dokonywać po wdrożeniu odpowiednich procedur bezpieczeństwa i osiągnięciu satysfakcjonującego poziomu ochrony zasobów systemu. Podstawą akredytacji są zazwyczaj SWBS. Akredytacja systemu powinna zawierać:

a) określenie celu akredytacji; w szczególności określenie klauzuli tajności informacji, które będą przetwarzane w systemie, oraz trybu bezpiecznego funkcjonowania, jaki jest proponowany dla danego systemu lub sieci;

b) przeprowadzenie przeglądu danych na temat zarządzania ryzykiem w celu identyfikacji zagrożeń i słabych punktów oraz ustalenia środków przeciwdziałania;

c) operacyjne procedury bezpieczeństwa (SecOP) wraz ze szczegółowym opisem proponowanych funkcji (tzn. trybów i usług, które mają być dostarczane użytkownikom); muszą także uwzględniać opis zastosowanych w systemie zabezpieczeń, gdyż stanowi to podstawę akredytacji;

d) plan wdrożenia zabezpieczeń i nadzoru nad ich prawidłowym funkcjonowaniem;

e) plan pierwotnego i okresowego testowania bezpieczeństwa funkcjonowania systemu lub sieci, ewaluacji i certyfikacji;

f) certyfikację, gdy istnieje taka potrzeba, wraz z innymi elementami akredytacji.

„Główny inspektor bezpieczeństwa teleinformatycznego" (CISO) oznacza urzędnika w centralnej służbie IT, który koordynuje stosowanie środków bezpieczeństwa w scentralizowanych systemach i nadzoruje ich funkcjonowanie.

„Certyfikacja" oznacza wydanie, na podstawie niezależnego przeglądu przebiegu i wyników ewaluacji, formalnej oceny stopnia, w jakim dany system spełnia wymagania bezpieczeństwa, lub w jaki urządzenie ochraniające komputer faktycznie zapewnia deklarowany poziom bezpieczeństwa.

„Bezpieczeństwo łączności" (COMSEC) oznacza stosowanie w systemach i sieciach teleinformatycznych środków ochrony w celu uniemożliwienia osobom nieupoważnionym uzyskania dostępu do istotnych informacji, które można uzyskać na podstawie wejścia w posiadanie i zbadanie urządzeń i zastosowanych rozwiązań, jak również w celu uwierzytelnienia przekazu w ramach tych systemów i sieci.

Uwaga:

Środki te obejmują bezpieczeństwo kryptograficzne, przesyłania i emisji, jak również bezpieczeństwo proceduralne, obiegu dokumentów, fizyczne, osobowe i komputerów.

„Bezpieczeństwo komputerów" (COMPUSEC) oznacza stosowanie w systemie komputerowym sprzętu, oprzyrządowania i oprogramowania w celu ochrony przed nieupoważnionym ujawnieniem informacji, wykonywaniem na nich operacji, wprowadzaniem zmian lub niszczeniem, a także ochrony przed uniemożliwieniem korzystania z urządzenia lub programu.

„Urządzenia ochraniające komputer" są to urządzenia komputerowe lub elementy komputerów, które można włączyć do systemu teleinformatycznego w celu zapewnienia lub podniesienia poziomu ochrony poufności, integralności i dostępności przetwarzanych informacji.

„Ogólnosystemowy tryb bezpiecznego funkcjonowania" oznacza tryb pracy, w którym WSZYSTKIE osoby, które mają dostęp do systemu, są sprawdzone do najwyższej klauzuli przetwarzanych w nim informacji, a ich obowiązki służbowe wiążą się z koniecznością zapoznawania się ze WSZYSTKIMI informacjami znajdującymi się w systemie.

Uwagi:

1) Ze względu na fakt, że wszystkie osoby korzystające z prawa dostępu do systemu powinny mieć możliwość zapoznawania się ze wszystkimi informacjami, nie ma potrzeby stosowania środków, które pozwalałyby na oddzielanie od siebie poszczególnych kategorii informacji w ramach systemu.

2) Inne formy zabezpieczenia (np. fizyczne, osobowe i proceduralne) muszą być zgodne z wymogami odnoszącymi się do najwyższej klauzuli oraz dodatkowych oznaczeń informacji, które znajdują się w systemie.

„Ewaluacja" oznacza przeprowadzenie przez właściwe organy szczegółowego technicznego badania rozwiązań w zakresie bezpieczeństwa, zastosowanych w systemie lub też produkcie kryptograficznym, albo urządzeniu ochraniającym komputer.

Uwagi:

1) Celem ewaluacji jest sprawdzenie, czy zostały zastosowane wymagane zabezpieczenia, czy nie powodują one negatywnych skutków ubocznych, istotnych dla bezpieczeństwa, i czy są odporne na próby nieuprawnionej ingerencji.

2) Ewaluacja określa zakres, w jakim zostały spełnione wymagania bezpieczeństwa systemu, deklarowane bezpieczeństwo urządzenia ochraniającego komputer, i określa poziom pewności zaufanych funkcji systemu, środków kryptograficznych i urządzeń ochraniających komputer.

„Właściciel informacji" (IO) oznacza organ (dyrektora departamentu), z którym wiąże się odpowiedzialność za wytwarzanie, przetwarzanie i wykorzystanie informacji, w tym podejmowanie decyzji o udzielaniu pracownikom prawa dostępu do tych informacji.

„Bezpieczeństwo teleinformatyczne" INFOSEC oznacza stosowanie środków bezpieczeństwa w celu ochrony informacji przetwarzanych, przechowywanych lub przesyłanych w systemach teleinformatycznych lub innych elektronicznych przed utratą poufności, integralności lub dostępności, wynikającą z przypadku lub celowego działania, oraz zapobieganie utracie integralności lub dostępności samych systemów.

„Środki INFOSEC" obejmują środki ochrony komputerów, przesyłania, emisji oraz środki bezpieczeństwa kryptograficznego, a także wykrywanie, dokumentowanie i przeciwdziałanie zagrożeniom dla informacji i systemów.

„Strefa IT" oznacza strefę, w której znajduje się jeden lub więcej komputerów, ich lokalne urządzenia peryferyjne i służące do przechowywania danych, jednostki sterowania oraz sprzęt przeznaczony do obsługi sieci i łączności.

Uwaga:

Pojęcie to nie obejmuje wydzielonej strefy, w której znajdują się odległe urządzenia peryferyjne lub terminale/stacje robocze, nawet jeśli są one połączone z urządzeniami znajdującymi się w strefie IT.

„Sieć teleinformatyczna" oznacza zorganizowany zespół rozproszonych geograficznie systemów teleinformatycznych, połączonych ze sobą w celu wymiany danych, obejmujący elementy połączonych systemów oraz ich złącza, wraz z danymi pomocniczymi lub sieciami łączności.

Uwagi:

1) Sieć teleinformatyczna może wykorzystywać jedną lub kilka sieci łączności, połączonych ze sobą w celu wymiany danych; kilka sieci teleinformatycznych może wykorzystywać jedną wspólną sieć łączności.

2) Sieć teleinformatyczną określa się jako „lokalną", gdy łączy ona kilka komputerów znajdujących się w tym samym obiekcie.

„Zabezpieczenia sieci teleinformatycznej" obejmują zarówno zabezpieczenia poszczególnych systemów teleinformatycznych wchodzących w skład sieci, jak i dodatkowe elementy i zabezpieczenia chroniące samą sieć (jak np. łączność w ramach sieci, uwierzytelnianie oraz mechanizmy i procedury identyfikacji zawartości zbiorów, kontrola dostępu, programy i metody rejestracji zmian), konieczne do zapewnienia możliwego do akceptacji poziomu ochrony informacji klasyfikowanych.

„System teleinformatyczny" oznacza zbiór obejmujący sprzęt, metody i procedury oraz – gdy jest to konieczne – personel, który ma za zadanie wykonywanie funkcji związanych z przetwarzaniem informacji.

Uwagi:

1) Pojęcie to odnosi się do zbioru urządzeń skonfigurowanych w celu przetwarzania informacji w ramach systemu.

2) Systemy tego rodzaju mogą być wykorzystywane przy konsultacjach, dowodzeniu, kontroli lub łączności, a także mieć zastosowanie w pracy naukowej i administracyjnej, włączając przetwarzanie tekstu.

3) Granice systemu muszą być wyraźnie określone jako elementy pozostające pod kontrolą jednego właściciela systemów technicznych (TSO).

4) W skład systemu teleinformatycznego mogą wchodzić podsystemy, które same mogą być systemami teleinformatycznymi.

„Zabezpieczenia systemu teleinformatycznego" oznaczają wszelkie funkcje, właściwości i cechy sprzętu, oprogramowania firmowego i użytkowego; procedury operacyjne, rozliczania oraz kontroli dostępu; strefę IT, odległe terminale i stacje robocze, a także środki kontroli zarządzania, fizyczną strukturę i urządzenia, personel i zarządzanie systemem łączności, konieczne w celu zapewnienia możliwego do zaakceptowania poziomu ochrony informacji klasyfikowanych, które mają być przetwarzane w danym systemie teleinformatycznym.

„Lokalny inspektor bezpieczeństwa teleinformatycznego" (LISO) oznacza urzędnika departamentu Komisji, który jest odpowiedzialny za koordynację stosowania środków bezpieczeństwa w ramach swoich właściwości i nadzór nad ich funkcjonowaniem.

„Wielopoziomowy tryb bezpiecznego funkcjonowania" oznacza tryb, w którym NIE WSZYSTKIE osoby, które mają dostęp do systemu, są sprawdzone do najwyższej klauzuli przetwarzanych w nim informacji i NIE WSZYSTKIM zapoznanie się z całością informacji znajdujących się w systemie jest potrzebne do wykonywania obowiązków służbowych.

Uwagi:

1) Ten tryb funkcjonowania pozwala na jednoczesne przetwarzanie informacji o różnych klauzulach tajności i zróżnicowanych oznaczeniach dodatkowych.

2) Ze względu na fakt, że nie wszystkie osoby korzystające z prawa dostępu do systemu są sprawdzone do najwyższej klauzuli informacji przetwarzanych w systemie oraz nie wszystkie powinny mieć możliwość zapoznawania się ze wszystkimi informacjami, istnieje potrzeba zastosowania środków pozwalających na częściowe udostępnianie zasobów systemu oraz oddzielenie od siebie poszczególnych kategorii informacji w ramach tego systemu.

„Strefa odległych terminali/stacji roboczych" oznacza strefę, w której znajdują się pewne urządzenia komputerowe, ich lokalne urządzenia peryferyjne lub terminale/stacje robocze oraz środki łączności i przekazu znajdujące się poza strefą IT.

„Operacyjne procedury bezpieczeństwa" określają przygotowane przez właściciela systemów technicznych (TSO) zasady odnoszące się do bezpieczeństwa, procedury działania, których należy przestrzegać, oraz zakresy obowiązków pracowników.

„Ogólnosystemowy zróżnicowany tryb bezpiecznego funkcjonowania" oznacza tryb, w którym WSZYSTKIE osoby, które mają dostęp do systemu, są sprawdzone do najwyższej klauzuli przetwarzanych w nim informacji, ale NIE WSZYSTKIM zapoznanie się z całością informacji znajdujących się w systemie jest potrzebne do wykonywania obowiązków służbowych.

Uwagi:

1) Ze względu na fakt, że nie wszystkie osoby korzystające z prawa dostępu do systemu powinny mieć możliwość zapoznawania się ze wszystkimi informacjami, istnieje potrzeba zastosowania środków pozwalających na częściowe udostępnianie zasobów systemu oraz oddzielenie od siebie poszczególnych kategorii informacji w ramach tego systemu.

2) Inne formy zabezpieczenia (np. fizyczne, osobowe i proceduralne) muszą być zgodne z wymogami odnoszącymi się do najwyższej klauzuli oraz dodatkowych oznaczeń informacji, które znajdują się w systemie.

3) Wszystkie informacje przetwarzane lub dostępne w systemie, funkcjonującym w tym trybie, łącznie z produktami (opracowaniami) wytworzonymi na ich podstawie, muszą być – aż do czasu ustalenia innych zasad – chronione zgodnie z wymaganiami odnoszącymi się do najwyższej klauzuli informacji oraz oznaczeń dodatkowych informacji przetwarzanych w systemie, chyba że istnieje możliwy do zaakceptowania poziom zaufania, które można pokładać w dowolnej istniejącej funkcji identyfikującej zawartość zbiorów.

„Szczególne wymagania bezpieczeństwa systemu" (SWBS) stanowią pełne i jednoznaczne określenie zasad bezpieczeństwa, które muszą być przestrzegane, oraz szczegółowych wymagań w zakresie bezpieczeństwa, którym należy sprostać. SWBS opierają się na polityce bezpieczeństwa Komisji oraz ocenie stopnia ryzyka lub też są zdeterminowane przez parametry odnoszące się do środowiska funkcjonowania, najniższego poziomu sprawdzenia pracowników, najwyższej klauzuli informacji, trybu bezpiecznego funkcjonowania albo wymagań użytkowników. SWBS stanowią integralną część dokumentacji projektu, przestawianej właściwym organom w celu uzyskania akceptacji dla proponowanych rozwiązań technicznych, budżetowych i związanych z bezpieczeństwem. W swojej ostatecznej formie, SWBS stanowi wyczerpującą definicję zabezpieczonego systemu.

„Właściciel systemów technicznych" (TSO) oznacza organ odpowiedzialny za stworzenie, utrzymanie, funkcjonowanie i zakończenie działania systemu.

„Środki przeciwdziałania TEMPEST" są to środki bezpieczeństwa przeznaczone do ochrony sprzętu i infrastruktury łączności przed narażeniem na szwank bezpieczeństwa informacji klasyfikowanych poprzez niezamierzoną emisję elektromagnetyczną i poprzez przewodnictwo.

25.3. **Zakresy odpowiedzialności**

25.3.1. *Uwagi ogólne*

Zakres uprawnień doradczych Grupy Doradczej Komisji do spraw Polityki Bezpieczeństwa, określonej w sekcji 12, obejmuje także kwestie INFOSEC. Grupa Doradcza jest zobowiązana do takiego zorganizowania swojej działalności, by mogła udzielać profesjonalnych rad na ten temat.

Biuro Bezpieczeństwa Komisji odpowiada za wydanie – na podstawie regulacji zawartych w niniejszym rozdziale – szczegółowych przepisów dotyczących kwestii INFOSEC.

W przypadku stwierdzenia problemów związanych z bezpieczeństwem (incydenty, nieprzestrzeganie przepisów itd.), Biuro Bezpieczeństwa Komisji jest zobowiązane do natychmiastowego podjęcia działań.

W skład Biura Bezpieczeństwa Komisji wchodzi wydział INFOSEC.

25.3.2. *Władza akredytacji bezpieczeństwa*

Funkcje władzy akredytacji bezpieczeństwa (SAA) na potrzeby Komisji pełni dyrektor Biura Bezpieczeństwa Komisji. Władza akredytacji bezpieczeństwa odpowiada za ogólne bezpieczeństwo oraz za wyspecjalizowane sfery INFOSEC, bezpieczeństwa przekazu, bezpieczeństwo kryptograficzne i bezpieczeństwo TEMPEST.

Władza akredytacji bezpieczeństwa odpowiada za zapewnienie, że systemy spełniają wymaganie określone w polityce bezpieczeństwa Komisji. Jednym z wykonywanych przez nie zadań jest wydawanie zgody na przetwarzanie przez dany system informacji o określonej klauzuli tajności w jego środowisku pracy.

Pod jurysdykcją władzy akredytacji bezpieczeństwa Komisji pozostają wszystkie systemy, które działają w pomieszczeniach należących do Komisji. W przypadku gdy różne części składowe systemu znajdują się jednocześnie pod jurysdykcją władzy akredytacji bezpieczeństwa Komisji i innych władz akredytacji bezpieczeństwa, wszystkie strony – pod przewodnictwem władzy akredytacji bezpieczeństwa Komisji – powołują wspólny zespół do spraw akredytacji.

25.3.3. *Władza bezpieczeństwa teleinformatycznego (INFOSEC)*

Dyrektor wydziału INFOSEC Biura Bezpieczeństwa Komisji pełni funkcję władzy bezpieczeństwa teleinformatycznego; oznacza to, że odpowiada za:

— udzielanie rad technicznych i pomocy władzy akredytacji bezpieczeństwa,

— udzielanie pomocy przy opracowywaniu SWBS,

— dokonywanie przeglądów SWBS w celu zapewnienia, że są one zgodne z niniejszymi przepisami bezpieczeństwa a także polityką w zakresie INFOSEC i podstawowymi dokumentami regulującymi te kwestie,

— udział, w miarę potrzeb, w pracach rad/zespołów do spraw akredytacji, oraz przekazywanie władzy akredytacji bezpieczeństwa rekomendacji w odniesieniu do INFOSEC,

— udzielanie pomocy przy organizacji szkoleń i innych działań mających na celu zapoznawanie z problematyką INFOSEC,

— udzielanie porad technicznych w toku prowadzenia postępowań wyjaśniających związanych z incydentami w sferze INFOSEC,

— ustalenie ogólnych zaleceń technicznych w celu zapewnienia, że użytkowane jest jedynie zatwierdzone oprogramowanie.

25.3.4. *Właściciel systemów technicznych (TSO)*

Odpowiedzialność za wdrożenie i funkcjonowanie kontroli i specjalnych zabezpieczeń spoczywa na właścicielu danego systemu, właścicielu systemów technicznych (TSO). W przypadku systemów scentralizowanych obligatoryjne jest wyznaczenie głównego inspektora bezpieczeństwa teleinformatycznego (CISO). Każdy departament, w miarę potrzeb, wyznacza lokalnego inspektora bezpieczeństwa teleinformatycznego (LISO). Odpowiedzialność technicznego właściciela systemu obejmuje cały cykl życiowy tego systemu, od etapu tworzenia projektu aż do ostatecznego wycofania go z użycia; do jego obowiązków należy także opracowanie operacyjnych procedur bezpieczeństwa (SecOP).

TSO jest zobowiązany do określenia standardów bezpieczeństwa i wymogów, które muszą być spełnione przez dostawcę systemu.

TSO, gdzie jest to uzasadnione, może przekazać część swoich uprawnień lokalnemu inspektorowi bezpieczeństwa teleinformatycznego. Różne funkcje w ramach INFOSEC mogą być wypełniane przez jedną osobę.

25.3.5. *Właściciel informacji (IO)*

Właściciel informacji (IO) odpowiada za informacje klasyfikowane UE (i inne informacje), które mają być wprowadzone, przetwarzane i wytwarzane w systemach technicznych. Jest zobowiązany do określenia wymagań w zakresie dostępu do informacji w systemach. W ramach swoich właściwości może delegować te obowiązki na osobę zarządzającą informacjami lub bazą danych.

25.3.6. *Użytkownicy*

Wszyscy użytkownicy są zobowiązani do zapewnienia, że ich działania nie stworzą zagrożenia dla bezpieczeństwa systemu, z którego korzystają.

25.3.7. *Szkolenie w zakresie INFOSEC*

Szkolenie i informacje na temat INFOSEC muszą być dostępne dla wszystkich pracowników, którym są one potrzebne.

25.4. **Nietechniczne środki ochrony**

25.4.1. *Bezpieczeństwo osobowe*

Użytkownicy systemu muszą być odpowiednio sprawdzeni, a zakres udostępnianych im informacji przetwarzanych w ramach danego systemu, zarówno pod względem klauzuli tajności, jak i ich zawartości, powinien być dostosowany do zakresu ich obowiązków służbowych. Dostęp do niektórych urządzeń lub informacji istotnych dla bezpieczeństwa systemu wymaga uzyskania przeprowadzenia specjalnej procedury sprawdzeniowej, realizowanej zgodnie z procedurami przyjętymi przez Komisję.

Władza bezpieczeństwa akredytacji jest zobowiązana do określenia stanowisk wymagających dodatkowych sprawdzeń personelu, poziomu tych sprawdzeń oraz zasad nadzoru nad osobami zajmującymi te stanowiska.

Systemy są zaprojektowane i skonstruowane w sposób ułatwiający określenie uprawnień i obowiązków poszczególnych pracowników, tak by nie dopuścić do powstania sytuacji, gdy jedna osoba posiada kompletną wiedzę lub kontrolę nad kluczowymi elementami systemu bezpieczeństwa.

W strefach IT oraz odległych terminali/stacji roboczych, w których istnieje możliwość wprowadzenia zmian w systemie ochrony systemu, nie może pracować tylko jedna upoważniona osoba/inny urzędnik.

Do wprowadzenia zmian w ochronie systemu lub sieci konieczna musi być współpraca dwóch lub większej liczby osób.

25.4.2. *Bezpieczeństwo fizyczne*

Strefy IT oraz odległych terminali/stacji roboczych (określone w sekcji 25.2), w których wykorzystuje się środki INFOSEC do przetwarzania informacji o klauzuli EU CONFIDENTIAL i wyższej lub w których możliwe jest uzyskanie dostępu do takich informacji, muszą odpowiadać wymaganiom określonym dla stref bezpieczeństwa UE klasy I lub II.

25.4.3. *Kontrola dostępu do systemu*

Wszystkie informacje i materiały umożliwiające zarządzanie dostępem do danego systemu podlegają ochronie przewidzianej dla najwyższej klauzuli i oznaczenia specjalnego informacji, do których mogą umożliwić dostęp.

Informacje i materiały związane z kontrolą dostępu, gdy nie są już wykorzystywane, podlegają zniszczeniu w sposób określony w sekcji 25.5.4.

25.5. **Techniczne środki ochrony**

25.5.1. *Bezpieczeństwo informacji*

Na wytwórcy informacji ciąży obowiązek określenia i nadania klauzuli wszystkim dokumentom zawierającym informacje klasyfikowane, niezależnie od tego, czy mają one formę wydruku, czy też znajdują się na nośnikach komputerowych. Na każdej stronie wydruku, na dole i u góry, musi być naniesiona klauzula tajności. Ostateczne opracowanie, zarówno w postaci wydruku, jak i pliku komputerowego, musi być oznaczone klauzulą odpowiadającą najwyższej klauzuli informacji wykorzystanej przy jego tworzeniu. Również sposób funkcjonowania systemu może mieć wpływ na określanie klauzuli produktów, które zostały w nim wytworzone.

Na departamentach Komisji i osobach korzystających z jej informacji ciąży obowiązek rozważenia kwestii agregacji informacji oraz problemów, jakie mogą wyniknąć z połączenia poszczególnych elementów, i określenia na tej podstawie, czy cały zbiór informacji należy objąć wyższą klauzulą tajności.

Fakt, że informacja może mieć postać krótkotrwałego kodu, kodu transmisyjnego lub też jakąkolwiek inną formę binarną, nie zapewnia żadnej ochrony i z tego względu nie powinien być brany pod uwagę przy ustalaniu klauzuli tajności tej informacji.

Informacja musi być chroniona w czasie przekazywania pomiędzy systemami oraz w systemie, do którego została przesłana, w sposób odpowiadający jej klauzuli tajności i kategorii.

Ze wszystkimi komputerowymi nośnikami danych należy postępować w sposób odpowiadający najwyższej klauzuli informacji na nich przechowywanej lub zapisem identyfikującym nośnik; muszą być one objęte stałą ochroną na odpowiednim poziomie.

Komputerowe nośniki danych wielokrotnego użytku, wykorzystywane do zapisywania informacji klasyfikowanych UE, muszą zachować klauzulę tajności zgodną z najwyższą klauzulą informacji, jaka się na nich kiedykolwiek znajdowała, do czasu, aż klauzula ta zostanie obniżona lub zniesiona zgodnie z obowiązującymi procedurami i w konsekwencji zostanie zmieniona klauzula nośnika danych; klauzula nośnika może być także zmieniona lub sam nośnik zniszczony zgodnie z procedurami zatwierdzonymi przez władzę akredytacji bezpieczeństwa (por. sekcja 25.5.4).

25.5.2. *Kontrola i rozliczanie z odpowiedzialności za informacje*

W odniesieniu do informacji o klauzuli EU SECRET lub wyższej wymagane jest zachowanie prowadzonego automatycznie (rejestrowanie zmian) lub ręcznie zapisu uzyskiwania dostępu, które tworzą rejestr przypadków zapoznania się z daną informacją. Zapisy te należy przechowywać zgodnie z niniejszymi przepisami bezpieczeństwa.

Klasyfikowane dane UE powstałe w wyniku operacji teleinformatycznych, znajdujące się w ramach strefy IT, mogą być traktowane jako jeden przedmiot objęty klauzulą tajności i nie muszą być rejestrowane, pod warunkiem że materiał ten jest wyraźnie określony, oznaczony klauzulą tajności i w odpowiedni sposób kontrolowany.

Wymagane jest ustanowienie, zatwierdzonych przez władzę akredytacji bezpieczeństwa, procedur sprawowania kontroli nad danymi, które zostały wytworzone w systemie przetwarzającym informacje klasyfikowane UE i przesłane ze strefy IT do strefy odległych terminali/stacji roboczych. W przypadku informacji o klauzuli EU SECRET i wyższej procedury takie obejmują szczegółowe instrukcje rozliczania się z odpowiedzialności za informacje.

25.5.3. *Zasady postępowania z wyjmowalnymi komputerowymi nośnikami danych i kontrola nad nimi*

Wszystkie wyjmowalne komputerowe nośniki danych o klauzuli EU CONFIDENTIAL i wyższej należy traktować jak materiały; zastosowanie mają tu ogólne zasady. Odpowiednie oznaczenie i klauzule muszą być nanoszone w sposób uwzględniający specyfikę danego nośnika, jednak pozwalający na ich jednoznaczną identyfikację jako materiału klasyfikowanego.

Użytkownicy są odpowiedzialni za zapewnienie, że informacje klasyfikowane UE są przechowywane na nośnikach oznaczonych klauzulami i odpowiednio chronionych. Wymagane jest ustanowienie procedur w celu zapewnienia, że sposób przechowywania informacji poszczególnych klauzul na nośnikach komputerowych jest zgodny z niniejszymi przepisami bezpieczeństwa.

25.5.4. *Znoszenie klauzuli i niszczenie komputerowych nośników danych*

Klauzula komputerowych nośników danych, wykorzystywanych do zapisywania informacji klasyfikowanych UE, może być obniżona lub zniesiona pod warunkiem zastosowania procedur zatwierdzonych przez władzę akredytacji bezpieczeństwa.

Nie dopuszcza się obniżenia klauzuli i ponownego wykorzystania komputerowych nośników danych, na których znajdowały się informacje o klauzuli EU TOP SECRET lub kategorii specjalnych.

W przypadku gdy nie ma możliwości obniżenia klauzuli komputerowych nośników danych lub też nie nadają się one do ponownego wykorzystania, podlegają zniszczeniu z zastosowaniem wymienionych powyżej procedur.

25.5.5. *Bezpieczeństwo łączności*

Dyrektor Biura Bezpieczeństwa Komisji pełni funkcję władzy CRYPTO.

W przypadku gdy informacje klasyfikowane UE są przesyłane elektromagnetycznie, wymagane jest zastosowanie specjalnych środków w celu ochrony poufności, integralności i dostępności takiego przekazu. Władza akredytacji bezpieczeństwa jest zobowiązana do określenia wymogów ochrony przekazu przed wykryciem i przechwyceniem. Informacje przesyłane w systemach łączności muszą być chronione zgodnie z wymaganiami odnoszącymi się do poufności, integralności i dostępności.

W przypadku gdy w celu ochrony poufności, integralności i dostępności wymagane jest zastosowanie metod kryptograficznych, metody te oraz związane z nimi produkty muszą zostać zatwierdzone do użycia przez właściwą władzę akredytacji bezpieczeństwa jako władzę CRYPTO.

W toku przesyłania poufność informacji o klauzuli EU SECRET i wyższej musi być chroniona przy użyciu metod i produktów kryptograficznych zatwierdzonych przez członka Komisji odpowiedzialnego za kwestie bezpieczeństwa po zasięgnięciu opinii Grupy Doradczej Komisji do spraw Polityki Bezpieczeństwa. Poufność przesyłanych informacji o klauzuli EU CONFIDENTIAL lub EU RESTRICTED musi być chroniona przy użyciu metod i produktów kryptograficznych zatwierdzonych przez władzę CRYPTO Komisji po zasięgnięciu opinii Grupy Doradczej Komisji do spraw Polityki Bezpieczeństwa.

Szczegółowe zasady dotyczące przesyłania informacji klasyfikowanych UE zostaną określone w odnoszących się do tej kwestii instrukcjach bezpieczeństwa zatwierdzonych przez Biuro Bezpieczeństwa Komisji po zasięgnięciu opinii Grupy Doradczej Komisji do spraw Polityki Bezpieczeństwa.

W wyjątkowych okolicznościach informacje o klauzulach EU RESTRICTED, EU CONFIDENTIAL i EU SECRET mogą być przesyłane w formie niezaszyfrowanej, pod warunkiem uzyskania upoważnienia właściciela informacji (IO) i odpowiedniego zarejestrowania. Przez wyjątkowe okoliczności rozumie się:

a) narastanie lub występowanie kryzysu, konfliktu lub sytuacji wojennej; oraz

b) przypadki, gdy decydujące znaczenie ma szybkość przekazania informacji a środki kryptograficzne nie są dostępne i uznano, że przesyłana informacja nie może być wykorzystana wystarczająco szybko, by przeszkodzić w przeprowadzanych działaniach.

Każdy system musi być wyposażony w funkcję uniemożliwienia – gdy wymaga tego sytuacja – dostępu do informacji klasyfikowanych UE w każdej lub wszystkich odległych stacjach roboczych lub terminalach albo przez fizyczne rozłączenie, albo przez zastosowanie specjalnego oprogramowania zatwierdzonego przez władzę akredytacji bezpieczeństwa.

25.5.6. *Bezpieczeństwo instalacji i ochrona przed radiacją*

Pierwotna instalacja systemów, a następnie dokonywanie w nich jakichkolwiek poważniejszych zmian, musi być tak przygotowana, aby prace były prowadzone przez odpowiednio sprawdzonych pracowników firmy instalującej i pod stałym nadzorem personelu o kwalifikacjach technicznych, dopuszczonego do dostępu do informacji klasyfikowanych UE na poziomie odpowiadającym najwyższej klauzuli informacji, które mają być przechowywane i przetwarzane w systemie.

Systemy, w których są przetwarzane informacje o klauzuli EU CONFIDENTIAL i wyższej, muszą być objęte ochroną zapewniającą, że ich bezpieczeństwu nie zagraża niezamierzona emisja; badania nad emisją i kontrola nad nią są określane terminem „TEMPEST".

Środki przeciwdziałania TEMPEST muszą być poddane badaniu i zatwierdzone przez władze TEMPEST (por. sekcja 25.3.2).

25.6. **Bezpieczeństwo przetwarzania informacji**

25.6.1. *Operacyjne procedury bezpieczeństwa*

Operacyjne procedury bezpieczeństwa (SecOP) określają zasady, które należy przyjąć w odniesieniu do bezpieczeństwa, procedury działania, których należy przestrzegać, oraz zakresy obowiązków pracowników. Przygotowanie SecOP pozostaje w gestii właściciela systemów technicznych (TSO).

25.6.2. *Ochrona oprogramowania/zarządzanie konfiguracją*

Ochrona bezpieczeństwa stosowanych programów powinna być określona raczej na podstawie oceny, jaka klauzula tajności przysługuje samemu programowi, niż na podstawie klauzuli tajności informacji, do których przetwarzania program ten ma służyć. Używane wersje oprogramowania powinny być systematycznie weryfikowane w celu zapewnienia ich integralności i prawidłowego funkcjonowania.

Nie należy wykorzystywać do przetwarzania informacji klasyfikowanych UE nowych lub zmodyfikowanych wersji oprogramowania, dopóki nie zostaną one zweryfikowane przez TSO.

25.6.3. *Wykrywanie wirusów komputerowych*

Wymagane jest okresowe przeprowadzanie sprawdzenia w celu wykrycia obecności wirusów komputerowych.

Wszystkie komputerowe nośniki danych, które są przekazywane do Komisji, przed wprowadzeniem do systemu powinny zostać sprawdzone w celu wykrycia obecności wirusów komputerowych.

25.6.4. *Usługi serwisowe*

W przypadku systemów, dla których opracowano SWBS, umowy i przyjęte procedury okresowych i doraźnych usług serwisowych muszą precyzować wymagania i obowiązujące zasady odnoszące się do pracowników wykonujących usługi i sprzętu wnoszonego przez nich do strefy IT.

Wymogi muszą być jasno określone w SWBS, a procedury – w operacyjnych procedurach bezpieczeństwa. Wykonywanie usług wymagających zastosowania zdalnych procedur diagnostycznych może być dopuszczone jedynie w nadzwyczajnych okolicznościach i pod warunkiem uzyskania akceptacji władzy akredytacji bezpieczeństwa.

25.7. **Zakup sprzętu i oprogramowania**

25.7.1. *Uwagi ogólne*

Każdy produkt bezpieczeństwa, który ma być zastosowany w systemie, musi być albo poddany ewaluacji i certyfikowany, albo znajdować się w toku ewaluacji i certyfikacji prowadzonej przez właściwą instytucję do spraw ewaluacji i certyfikacji któregoś z Państw Członkowskich UE na podstawie powszechnie uznawanych kryteriów (takich jak Wspólne kryteria ewaluacji bezpieczeństwa technologii informatycznych, ISO 15 408). Szczególne procedury muszą uzyskać akceptację Komitetu Doradczego do spraw Zakupów i Kontraktów (ACPC).

Przy podejmowaniu decyzji, czy sprzęt, a w szczególności komputerowe nośniki danych, należy zakupić czy też wziąć w leasing, należy uwzględnić, iż po wykorzystaniu danego produktu do przetwarzania lub przechowywania informacji klasyfikowanych UE nie można go udostępniać poza odpowiednio zabezpieczonym środowiskiem bez uprzedniego zniesienia klauzuli przeprowadzonego za zgodą właściwej władzy akredytacji bezpieczeństwa, a wydanie takiej zgody nie zawsze jest możliwe.

25.7.2. *Akredytacja (dopuszczenie do eksploatacji)*

Wszystkie systemy, dla których opracowano SWBS, zanim rozpocznie się przetwarzanie w nich informacji klasyfikowanych UE, muszą zostać dopuszczone do eksploatacji przez władzę akredytacji bezpieczeństwa, która podejmuje decyzję na podstawie informacji zawartych w SWBS, operacyjnych procedur bezpieczeństwa i innej dokumentacji systemu. Podsystemy oraz odległe terminale/stacje robocze podlegają akredytacji jako część systemu, z którym są połączone. W przypadku gdy system jest wykorzystywany jednocześnie przez Komisję i inne instytucje, Komisja i właściwe władze bezpieczeństwa muszą wspólnie wyrazić zgodę na akredytację.

Proces dopuszczania do eksploatacji może być prowadzony zgodnie ze strategią akredytacji właściwą dla danego systemu, określoną przez władzę akredytacji bezpieczeństwa.

25.7.3. *Ewaluacja i certyfikacja*

W niektórych przypadkach akredytację systemu musi poprzedzać ewaluacja i certyfikacja zabezpieczeń sprzętu, oprogramowania firmowego i użytkowego; celem jest sprawdzenie, czy zapewniają one ochronę informacji w sposób odpowiadający ich przewidywanej klauzuli tajności.

Wymagania dotyczące ewaluacji i certyfikacji muszą być uwzględnione przy planowaniu systemu i wyraźnie określone w SWBS.

Czynności związane z ewaluacją i certyfikacją są prowadzone przez osoby pracujące na rzecz TSO, które posiadają kwalifikacje techniczne i zostały odpowiednio sprawdzone, zgodnie z zatwierdzonymi wytycznymi.

Zespoły przeprowadzające czynności związane z ewaluacją i certyfikacją mogą być kierowane przez wyznaczoną władzę do spraw ewaluacji lub certyfikacji Państwa Członkowskiego lub jej wyznaczonych przedstawicieli, np. kompetentne i odpowiednio sprawdzone przedsiębiorstwo.

W przypadku gdy system jest stworzony w oparciu o poddane już w danym państwie ewaluacji i certyfikacji urządzenia ochraniające komputer, dopuszczane jest ograniczenie zakresu ewaluacji i certyfikacji (np. uwzględnienie tylko aspektów integracji).

25.7.4. *Rutynowa kontrola środków zabezpieczających w celu utrzymania akredytacji*

TSO jest zobowiązany do ustanowienia procedur rutynowej kontroli, które pozwolą na potwierdzenie, że wszystkie zabezpieczenia systemu nadal spełniają obowiązujące wymagania.

SWBS musi wyraźnie określać, jakiego typu zmiany będą powodować konieczność ponownej akredytacji lub też uzyskania uprzedniej akceptacji władzy bezpieczeństwa akredytacji. Po wprowadzeniu jakiejkolwiek modyfikacji, naprawie lub awarii, które mogły mieć wpływ na zabezpieczenia systemu, TSO ma obowiązek przeprowadzenia kontroli celem sprawdzenia, czy środki zabezpieczenia funkcjonują w prawidłowy sposób. Przeprowadzenie z wynikiem pozytywnym wymaganych sprawdzeń stanowi warunek zachowania przez system akredytacji.

Władza bezpieczeństwa akredytacji jest zobowiązana do przeprowadzania okresowych kontroli lub przeglądów wszystkich systemów, w których zastosowano zabezpieczenia. W odniesieniu do systemów, w których przetwarzane są informacje o klauzuli EU TOP SECRET, inspekcje takie przeprowadza się nie rzadziej niż raz do roku.

25.8. **Okresowe lub doraźne korzystanie ze sprzętu komputerowego**

25.8.1. *Bezpieczeństwo komputerów osobistych*

Komputery osobiste ze stałymi twardymi dyskami (lub inne trwałe komputerowe nośniki danych), funkcjonujące jako pojedyncze stanowiska lub w konfiguracji sieciowej, oraz przenośne urządzenia komputerowe (np. przenośne PC i elektroniczne „notebooki") z wbudowanymi twardymi dyskami są uznawane za nośniki danych tego samego typu, jak dyskietki i inne wyjmowalne nośniki danych.

Wymagane jest objęcie tych urządzeń ochroną w odniesieniu do dostępu, obsługi, przechowywania i przewozu, na poziomie przewidzianym dla najwyższej klauzuli informacji, jaka była na nich kiedykolwiek zapisana lub przetwarzana (do czasu obniżenia lub zniesienia tej klauzuli zgodnie z zatwierdzonymi procedurami).

25.8.2. *Wykorzystywanie prywatnego sprzętu IT do wykonywania zadań Komisji*

Zakazane jest wykorzystywanie stanowiących własność prywatną wyjmowalnych komputerowych nośników danych, oprogramowania i urządzeń (np. komputerów osobistych i przenośnych urządzeń komputerowych) wyposażonych w pamięć do przetwarzania informacji klasyfikowanych UE.

Stanowiący własność prywatną sprzęt, oprogramowanie i nośniki danych nie mogą być wnoszone na teren stref bezpieczeństwa klasy I lub II, w których przetwarza się informacje klasyfikowane UE, bez wydanego na piśmie zezwolenia dyrektora Biura Bezpieczeństwa Komisji. Upoważnienie takie może być udzielone wyłącznie ze względów technicznych i w nadzwyczajnych przypadkach.

25.8.3. *Wykorzystywanie sprzętu IT należącego do wykonawcy umowy lub przywiezionego z kraju do wykonywania zadań Komisji*

Dyrektor Biura Bezpieczeństwa Komisji może wyrazić zgodę na wykorzystanie sprzętu komputerowego i oprogramowania danej instytucji w celu wykonania zadań Komisji. Dozwolone jest także wykorzystywanie sprzętu komputerowego i oprogramowania dostarczonych przez Państwo Członkowskie; w tym wypadku wymagane jest umieszczenie sprzętu komputerowego w odpowiednim wykazie inwentarzowym Komisji. W obu przypadkach, jeśli sprzęt komputerowy ma być wykorzystywany do przetwarzania informacji klasyfikowanych UE, należy się skonsultować z władzą akredytacji bezpieczeństwa w celu zapewnienia, że zostały określone i wdrożone stosowne rozwiązania w zakresie INFOSEC.

26. UDOSTĘPNIANIE INFORMACJI KLASYFIKOWANYCH UE PAŃSTWOM TRZECIM I ORGANIZACJOM MIĘDZYNARODOWYM

26.1.1. *Zasady odnoszące się do udostępniania informacji klasyfikowanych UE*

Decyzję o udostępnieniu informacji klasyfikowanych UE państwom trzecim lub organizacjom międzynarodowym podejmuje Komisja jako ciało kolegialne na podstawie analizy:

— charakteru i treści informacji;

— związku informacji z zadaniami, jakie wykonuje odbiorca;

— korzyści dla UE.

Obligatoryjne jest wystąpienie z wnioskiem o wyrażenie zgody na udostępnienie informacji klasyfikowanej UE do wytwórcy tej informacji.

Decyzje są podejmowane w trybie indywidualnym, przy czym bierze się pod uwagę:

— pożądany stopień współpracy z danym państwem lub organizacją międzynarodową;

— stopień zaufania, jakim można obdarzyć dane państwo lub organizację międzynarodową; ocena jest dokonywana na podstawie poziomu ochrony, która zostanie zapewniona powierzonym im informacjom klasyfikowanym UE, oraz stopnia zgodności pomiędzy zasadami bezpieczeństwa stosowanymi przez danego odbiorcę i obowiązującymi w UE. Grupa Doradcza Komisji do spraw Polityki Bezpieczeństwa przekazuje Komisji techniczną opinię na ten temat.

Przyjęcie przez państwa trzecie lub organizacje międzynarodowe informacji klasyfikowanych UE jest jednoznaczne z zapewnieniem, że informacje nie zostaną wykorzystane w celach innych niż te, w których zostały przekazane lub wymienione, oraz że zostanie im zapewniona ochrona zgodna z wymogami Komisji.

26.1.2. *Poziomy współpracy*

Komisja, po dokonaniu oceny, że możliwe jest udostępnienie informacji klasyfikowanych danemu państwu lub organizacji międzynarodowej, określa możliwy poziom współpracy z tym państwem lub organizacją. Poziom ten zależy w szczególności od polityki bezpieczeństwa i regulacji prawnych obowiązujących w danym państwie lub organizacji.

Wyróżnia się 3 poziomy współpracy:

Poziom 1

Współpraca z państwami trzecimi lub organizacjami międzynarodowymi, których polityka bezpieczeństwa i regulacje prawne są bardzo zbliżone do obowiązujących w UE.

Poziom 2

Współpraca z państwami trzecimi lub organizacjami międzynarodowymi, których polityka bezpieczeństwa i regulacje prawne istotnie się różnią od obowiązujących w UE.

Poziom 3

Incydentalna współpraca z państwami trzecimi lub organizacjami międzynarodowymi, których polityki bezpieczeństwa i regulacji prawnych nie da się ocenić.

Każdemu poziomowi współpracy są przypisane procedury i zasady bezpieczeństwa są szczegółowo określone w dodatkach 3, 4 i 5.

26.1.3. *Umowy o bezpieczeństwie*

W przypadku gdy Komisja oceni, że potrzeba wymiany informacji klasyfikowanych pomiędzy UE a państwami trzecimi lub organizacjami międzynarodowymi ma charakter stały i długotrwały, przygotuje „umowy o procedurach bezpieczeństwa w zakresie wymiany informacji klasyfikowanych", w których określi cel współpracy oraz wzajemne zasady ochrony wymienianych informacji.

W przypadku incydentalnej współpracy na poziomie 3, która z definicji ma ograniczony zakres i czas trwania, „umowę o procedurach bezpieczeństwa w zakresie wymiany informacji klasyfikowanych" może zastąpić protokół ustaleń określający charakter informacji podlegających wymianie oraz wzajemne obowiązki odnoszące się do ich ochrony; rozwiązanie takie jest jednak możliwe tylko wtedy, gdy przedmiotem wymiany są informacje o klauzuli nieprzekraczającej EU RESTRICTED.

Projekty umów o procedurach bezpieczeństwa lub zapewnień o wzajemnym zrozumieniu, zanim zostaną przedstawione do akceptacji Komisji, muszą zostać poddane ocenie Grupy Doradczej Komisji do spraw Polityki Bezpieczeństwa.

Krajowe władze bezpieczeństwa udzielą członkowi Komisji odpowiedzialnemu za kwestie bezpieczeństwa wszelkiej niezbędnej pomocy w celu zapewnienia, że informacje, które mają zostać udostępnione, są wykorzystywane i chronione zgodnie z postanowieniami umów o procedurach bezpieczeństwa lub protokołów ustaleń.

Dodatek 1

ZESTAWIENIE PORÓWNAWCZE KLAUZUL TAJNOŚCI

Klauzule tajności UE	EU TOP SECRET	EU SECRET	EU CONFIDENTIAL	EU RESTRICTED
Klauzule tajności NATO (1)				
Klauzule tajności UZE	Focal Top Secret	WEU secret	WEU Confidential	WEU Restricted
Klauzule tajności EURATOM (2)	EURATOM Top Secret	EURATOM SECRET	EURATOM Confidential	EURATOM Restricted
Belgia	Très 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 DIENSTGEBRAUCH
Grecja	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Hiszpania	Secreto	Reservado	Confidencial	Difusion Limitada
Francja	Très Secret Défense (4)	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irlandia	Top Secret	Secret	Confidential	Restricted
Włochy	Segretissimo	Segreto	Riservatissimo	Riservato
Luksemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Niderlandy	Stg. Zeer Geheim	Stg. Geheim	Stg. Confidentieel	
Austria	Streng Geheim	Geheim	Vertaulich	Eingeschränkt
Portugalia	Muito Secreto	Secreto	Confidencial	Reservato
Finlandia	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Szwecja	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Zjednoczone Królestwo	Top Secret	Secret	Confidential	Restricted

(1) NATO - odpowiedniki klauzul tajności 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: klauzula Très Secret Défense, która odnosi się do zagadnień o kluczowym znaczeniu dla rządu, może być zmieniona wyłącznie za zgodą premiera.

Dodatek 2

PRAKTYCZNY PRZEWODNIK NADAWANIA KLAUZUL

Poniższy przewodnik ma jedynie charakter instrukcji i nie może być wykorzystywany w sposób zmieniający znaczenie podstawowych przepisów zawartych w sekcjach 16, 17, 20 i 21.

Klauzula tajności	Kiedy	Kto	Oznaczenia	Obniżanie klauzuli/znoszenie klauzuli/niszczenie	
				Kto	Kiedy
EU TOP SECRET: Tę klauzulę nadaje się tylko informacji lub materiałowi, których nieupoważnione ujawnienie spowodowałoby wyjątkowo duże szkody podstawowym interesom Unii Europejskiej albo jednemu lub więcej jej Państw Członkowskich [16.1].	Narażenie na szwank bezpieczeństwa zasobów oznaczonych EU TOP SECRET mogłoby: — zagrozić bezpośrednio wewnętrznej stabilności UE lub jednego z Państw Członkowskich lub państwa przyjaźnie nastawionego, — narazić na wyjątkowo duże szkody stosunki z przyjaźnie nastawionymi rządami, — bezpośrednio spowodować utratę życia wielu osób, — wyrządzić wyjątkowo duże szkody operacyjnym zdolnościom lub bezpieczeństwu Państw Członkowskich lub sił zbrojnych innych uczestników, lub też utrzymaniu skuteczności wyjątkowo ważnych działań wywiadowczych lub w sferze bezpieczeństwa, — spowodować poważne i długotrwałe szkody gospodarcze w skali UE lub poszczególnych Państw Członkowskich.	Odpowiednio upoważnione osoby (wytwórcy), dyrektorzy generalni, szefowie służb [17.1]. Wytwórcy są zobowiązani do określenia daty lub okresu, gdy klauzula informacji może zostać obniżona lub zniesiona. [16.2]. W przeciwnym razie są oni zobowiązani do przeprowadzania przynajmniej raz na 5 lat przeglądu dokumentów w celu dokonania oceny, czy nadana klauzula nadal jest konieczna [17.3].	Klauzula EU TOP SECRET jest nanoszona na dokumentach EU TOP SECRET; uzupełniona – gdzie ma to zastosowanie – dodatkowym zastrzeżeniem i/lub oznaczeniem związanym z obronnością ESDP, za pomocą środków mechanicznych i ręcznie [16.4, 16.5, 16.3]. Klauzula tajności UE musi być umieszczona u góry i na dole każdej strony, a wszystkie strony muszą być ponumerowane. Każdy dokument musi mieć naniesiony numer korespondencyjny i datę; wymagane jest umieszczenie numeru korespondencyjnego na każdej stronie. W przypadku gdy dokumenty mają być dystrybuowane w kilku egzemplarzach, każdy z nich musi mieć umieszczony na pierwszej stronie numer egzemplarza oraz informację o liczbie stron. Obligatoryjne jest wymienienie na pierwszej stronie wszystkich załączników i aneksów [21.1].	Prawo do obniżenia lub zniesienia klauzuli pozostaje wyłącznie w gestii wytwórcy; jest on zobowiązany do poinformowania o zmianie wszystkich odbiorców informacji, do których przesłał dokument lub dla których wykonał jego kopię [17.3]. Dokumenty o klauzuli EU TOP SECRET mogą być niszczone wyłącznie w głównej kancelarii tajnej lub podkancelarii, pod której nadzorem pozostają. Każdy zniszczony dokument musi być odnotowany w protokole zniszczenia, który podpisuje urzędnik kontroli EU TOP SECRET i urzędnik będący świadkiem niszczenia; urzędnik ten musi być sprawdzony w związku z dostępem do informacji o tej klauzuli. Fakt zniszczenia dokumentu musi być odnotowany w odpowiednim dzienniku. Kancelaria tajna przechowuje protokoły zniszczenia, razem z kartami zapoznania się z dokumentem, przez 10 lat [22.5].	Zbędne egzemplarze i dokumenty, które nie są już potrzebne, podlegają zniszczeniu [22.5]. Dokumenty o klauzuli EU TOP SECRET, w tym także zbędne materiały powstałe w toku wytwarzania dokumentów o tej klauzuli, jak np. uszkodzone kopie, szkice robocze, notatki i kalki maszynowe, muszą być zniszczone – pod kontrolą urzędnika kontroli EU TOP SECRET – przez spalenie, przetworzenie na miazgę, pocięcie w niszczarce lub w inny sposób, który zapewnia, że staną się one nierozpoznawalne i niemożliwe do odtworzenia [22.5].

Klauzula tajności	Kiedy	Kto	Oznaczenia	Obniżanie klauzuli/znoszenie klauzuli/niszczenie	
				Kto	Kiedy
EU SECRET UE: Tę klauzulę nadaje się tylko informacji lub materiałowi, których nieupoważnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom Unii Europejskiej albo jednego lub więcej jej Państw Członkowskich [16.1].	Narażenie na szwank bezpieczeństwa zasobów oznaczonych EU SECRET mogłoby: — spowodować napięcia w stosunkach międzynarodowych, — narazić na szkodę stosunki z przyjaźnie nastawionymi rządami, — wywołać zagrożenie utraty życia lub poważnie zagrozić porządkowi publicznemu, bezpieczeństwu osób lub ich swobodom, — wyrządzić poważne szkody operacyjnym zdolnościom lub bezpieczeństwu Państw Członkowskich lub sił zbrojnych innych uczestników, lub też utrzymaniu skuteczności ważnych działań wywiadowczych lub w sferze bezpieczeństwa, — spowodować istotne szkody materialne dla UE lub dla finansowych, monetarnych, ekonomicznych lub handlowych interesów któregoś z Państw Członkowskich.	Upoważnione osoby (wytwórcy), dyrektorzy generalni, szefowie służb [17.1]. Wytwórcy są zobowiązani do określenia daty lub okresu, gdy klauzula informacji może zostać obniżona lub zniesiona [16.2]. W przeciwnym razie są oni zobowiązani do przeprowadzania przynajmniej raz na 5 lat przeglądu dokumentów w celu dokonania oceny, czy nadana klauzula nadal jest konieczna [17.3].	Klauzula EU SECRET jest nanoszona na dokumentach EU SECRET; uzupełniona – gdzie ma to zastosowanie – zastrzeżeniem i/lub oznaczeniem związanym z obronnością ESDP, za pomocą środków mechanicznych i ręcznie [16.4, 16.5, 16.3]. Klauzula tajności UE musi być umieszczona u góry i na dole każdej strony, a wszystkie strony muszą być ponumerowane. Każdy dokument musi mieć naniesiony numer korespondencyjny i datę; wymagane jest umieszczenie numeru korespondencyjnego na każdej stronie. W przypadku gdy dokumenty mają być dystrybuowane w kilku egzemplarzach, każdy z nich musi mieć umieszczony na pierwszej stronie numer egzemplarza oraz informację o liczbie stron. Obligatoryjne jest wymienienie na pierwszej stronie wszystkich załączników i aneksów [21.1].	Prawo do obniżenia lub zniesienia klauzuli pozostaje wyłącznie w gestii wytwórcy; jest on zobowiązany do poinformowania o zmianie wszystkich odbiorców informacji, do których przesłał dokument lub dla których wykonał jego kopię [17.3]. Dokumenty o klauzuli EU SECRET mogą być niszczone wyłącznie w kancelarii, która sprawuje nad nimi nadzór, pod kontrolą odpowiednio sprawdzonej osoby. Zniszczone dokumenty o klauzuli EU SECRET muszą być odnotowane w podpisanych protokołach zniszczenia, które są co najmniej przez 3 lata przechowywane przez daną kancelarię, razem z kartami zapoznania z dokumentem [22.5].	Zbędne egzemplarze i dokumenty, które nie są już potrzebne, podlegają zniszczeniu [22.5]. Dokumenty o klauzuli EU SECRET, w tym także zbędne materiały powstałe w toku wytwarzania dokumentów o tej klauzuli, jak np. uszkodzone kopie, szkice robocze, notatki i kalki maszynowe, muszą być zniszczone przez spalenie, przetworzenie na miazgę, pocięcie w niszczarce lub w inny sposób, który zapewnia, że staną się one nierozpoznawalne i niemożliwe do odtworzenia [22.5].

Klauzula tajności	Kiedy	Kto	Oznaczenia	Obniżanie klauzuli/znoszenie klauzuli/niszczenie	
				Kto	Kiedy
EU CONFIDENTIAL: Tę klauzulę nadaje się informacji lub materiałowi, których nieupoważnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii Europejskiej albo jednego lub więcej jej Państw Członkowskich [16.1].	Narażenie na szwank bezpieczeństwa zasobów oznaczonych EU CONFIDENTIAL mogłoby: — istotnie zaszkodzić stosunkom dyplomatycznym, tzn. spowodować formalne protesty lub zastosowanie innych sankcji, — narazić na szkodę bezpieczeństwo osób lub ich swobody, — zaszkodzić operacyjnym zdolnościom lub bezpieczeństwu Państw Członkowskich lub sił zbrojnych innych uczestników, lub też skuteczności ważnych działań wywiadowczych lub w sferze bezpieczeństwa, — poważnie osłabić finansowe podstawy funkcjonowania istotniejszych organizacji, — utrudnić prowadzenie śledztwa lub ułatwić popełnienie poważnego przestępstwa, — być niezgodne z finansowymi, monetarnymi, ekonomicznymi lub handlowymi interesami UE lub jej Państw Członkowskich, — poważnie utrudnić rozwój lub realizację istotnych kierunków polityki UE, — zablokować lub w inny sposób istotnie przeszkodzić w prowadzeniu ważnych działań UE.	Upoważnione osoby (wytwórcy), dyrektorzy generalni i szefowie służb [17.1]. Wytwórcy są zobowiązani do określenia daty lub okresu, gdy klauzula informacji może zostać obniżona lub zniesiona [16.2]. W przeciwnym razie są oni zobowiązani do przeprowadzania przynajmniej raz na 5 lat przeglądu dokumentów w celu dokonania oceny, czy nadana klauzula nadal jest konieczna [17.3].	Klauzula EU CONFIDENTIAL jest nanoszona na dokumentach EU CONFIDENTIAL; uzupełniona – gdzie ma to zastosowanie – zastrzeżeniem i/lub oznaczeniem związanym z obronnością ESDP, za pomocą środków mechanicznych i ręcznie lub przez drukowanie na wcześniej oznakowanych i zarejestrowanych arkuszach [16.4, 16.5, 16.3]. Klauzula tajności UE musi być umieszczona u góry i na dole każdej strony, a wszystkie strony muszą być ponumerowane. Każdy dokument musi mieć naniesiony numer korespondencyjny i datę. Obligatoryjne jest wymienienie na pierwszej stronie wszystkich załączników i aneksów [21.1].	Prawo do obniżenia lub zniesienia klauzuli pozostaje wyłącznie w gestii wytwórcy; jest on zobowiązany do poinformowania o zmianie wszystkich odbiorców informacji, do których przesłał dokument lub dla których wykonał jego kopię [17.3]. Dokumenty o klauzuli EU CONFIDENTIAL mogą być niszczone wyłącznie w kancelarii, która sprawuje nad nimi nadzór, pod kontrolą odpowiednio sprawdzonej osoby. Fakt zniszczenia jest dokumentowany zgodnie z przepisami krajowymi, a w przypadku Komisji lub zdecentralizowanych agencji UE, zgodnie z instrukcjami jej przewodniczącego [22.5].	Zbędne egzemplarze i dokumenty, które nie są już potrzebne, podlegają zniszczeniu [22.5]. Dokumenty o klauzuli EU CONFIDENTIAL, w tym także zbędne materiały powstałe w toku wytwarzania dokumentów o tej klauzuli, jak np. uszkodzone kopie, szkice robocze, notatki i kalki maszynowe, muszą być zniszczone przez spalenie, przetworzenie na miazgę, pocięcie w niszczarce lub w inny sposób, który zapewnia, że staną się one nierozpoznawalne i niemożliwe do odtworzenia [22.5].

Klauzula tajności	Kiedy	Kto	Oznaczenia	Obniżanie klauzuli/znoszenie klauzuli/niszczenie	
				Kto	Kiedy
EU RESTRICTED: Tę klauzulę nadaje się informacji lub materiałowi, których nieupoważnione ujawnienie byłoby niekorzystne z punktu widzenia interesów Unii Europejskiej albo jednego lub więcej jej Państw Członkowskich [16.1].	Narażenie na szwank bezpieczeństwa zasobów oznaczonych EU RESTRICTED mogłoby: — zaszkodzić stosunkom dyplomatycznym, — spowodować istotne niedogodności dla osób, — utrudnić utrzymanie operacyjnych zdolności lub bezpieczeństwa Państw Członkowskich lub sił zbrojnych innych uczestników, — spowodować straty finansowe lub też ułatwić czerpanie nieuzasadnionych zysków lub korzyści przez osoby lub przedsiębiorców, — naruszyć właściwe rozwiązania przyjęte w celu zachowania poufności informacji przekazanych przez strony trzecie, — naruszyć obowiązujące ograniczenia dotyczące ujawniania informacji, — utrudnić prowadzenie śledztwa lub ułatwić popełnienie przestępstwa, — niekorzystnie wpłynąć na przebieg handlowych lub politycznych negocjacji prowadzonych przez UE lub Państwa Członkowskie z innymi podmiotami, — utrudnić rozwój lub realizację istotnych kierunków polityki UE, — utrudnić odpowiednie zarządzanie UE i jej działaniami.	Upoważnione osoby (wytwórcy), dyrektorzy generalni, szefowie służb [17.1]. Wytwórcy są zobowiązani do określenia daty lub okresu, gdy klauzula informacji może zostać obniżona lub zniesiona. [16.2]. W przeciwnym razie są oni zobowiązani do przeprowadzania przynajmniej raz na 5 lat przeglądu dokumentów w celu dokonania oceny, czy nadana klauzula nadal jest konieczna [17.3].	Klauzula EU RESTRICTED jest nanoszona na dokumentach EU RESTRICTED; uzupełniona – gdzie ma to zastosowanie – zastrzeżeniem i/lub oznaczeniem związanym z obronnością ESDP, za pomocą środków mechanicznych lub elektronicznych [16.4, 16.5, 16.3]. Klauzula tajności UE musi być umieszczona u góry i na dole każdej strony, a wszystkie strony muszą być ponumerowane. Każdy dokument musi mieć naniesiony numer korespondencyjy i datę [21.1].	Prawo do obniżenia lub zniesienia klauzuli pozostaje wyłącznie w gestii wytwórcy; jest on zobowiązany do poinformowania o zmianie wszystkich odbiorców informacji, do których przesłał dokument lub dla których wykonał jego kopię [17.3]. Dokumenty o klauzuli EU RESTRICTED mogą być niszczone wyłącznie w kancelarii, zgodnie z instrukcjami przewodniczącego Komisji [22.5].	Zbędne egzemplarze i dokumenty, które nie są już potrzebne, podlegają zniszczeniu [22.5].

Dodatek 3

Zalecenia odnoszące się do udostępniania informacji klasyfikowanych UE państwom trzecim lub organizacjom międzynarodowym: współpraca na poziomie 1

PROCEDURY

1. Uprawnienie do podejmowania decyzji o udostępnieniu informacji klasyfikowanych UE państwom, które nie należą do Unii Europejskiej, lub innym organizacjom międzynarodowym, których polityka bezpieczeństwa i regulacje prawne są porównywalne z rozwiązaniami przyjętymi w UE, pozostaje w kompetencjach Komisji jako ciała kolegialnego.
2. Pod warunkiem że została zawarta umowa o bezpieczeństwie, członek Komisji odpowiedzialny za kwestie bezpieczeństwa jest właściwy do rozpatrywania wniosków o udostępnienie informacji klasyfikowanych UE.
3. W toku rozpatrywania wniosku członek Komisji odpowiedzialny za kwestie bezpieczeństwa:
   — zasięga opinii wytwórcy informacji, która ma być przedmiotem udostępnienia,
   — nawiązuje kontakty z odpowiedzialnymi za bezpieczeństwo instytucjami państw lub organizacji międzynarodowych, którym informacje mają być przekazane, w celu dokonania weryfikacji, czy ich polityka bezpieczeństwa i regulacje prawne gwarantują, że udostępnione informacje klasyfikowane będą chronione zgodnie z niniejszymi przepisami bezpieczeństwa,
   — zasięga opinii Grupy Doradczej Komisji do spraw Polityki Bezpieczeństwa na temat wiarygodności państw lub struktur międzynarodowych, którym mają być przekazane informacje.
4. Członek Komisji odpowiedzialny za kwestie bezpieczeństwa przekazuje Komisji, w celu podjęcia decyzji, wniosek wraz otrzymaną opinią Grupy Doradczej do spraw Polityki Bezpieczeństwa.

PRZEPISY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PODMIOTY, KTÓRYM PRZEKAZYWANE SĄ INFORMACJE

5. Członek Komisji odpowiedzialny za kwestie bezpieczeństwa informuje państwa lub organizacje międzynarodowe, którym mają być przekazane informacje, o pozytywnej decyzji Komisji.

6. Decyzja o udostępnieniu informacji może zostać wykonana jedynie wtedy, gdy odbiorcy przekażą pisemne zapewnienie, że:
   — nie będą wykorzystywać udostępnionych informacji w innych celach, niż zostało to uzgodnione,
   — będą chronić udostępnione informacje zgodnie z niniejszymi przepisami bezpieczeństwa, a zwłaszcza ze szczególnymi zasadami określonymi poniżej.

7. Bezpieczeństwo osobowe
   a) Grupa urzędników mających dostęp do informacji klasyfikowanych UE musi być ściśle określona, zgodnie z zasadą ograniczonego dostępu, i obejmować tylko te osoby, których obowiązki służbowe wymagają uzyskania takiego dostępu.
   b) Wszyscy urzędnicy lub obywatele danego państwa, upoważnieni do dostępu do informacji o klauzuli EU CONFIDENTIAL lub wyższej, muszą posiadać albo certyfikat bezpieczeństwa na odpowiednim poziomie, albo uzyskać równorzędną decyzję potwierdzającą spełnianie przez nich warunków bezpieczeństwa; każdy z tych dokumentów jest wydawany przez struktury rządowe danego państwa.

8. Przesyłanie dokumentów
   a) Praktyczne rozwiązania dotyczące przesyłania dokumentów muszą być określone w umowie. Zastosowanie mają przepisy sekcji 21, pod warunkiem zawarcia takiej umowy. W szczególności muszą zostać wskazane kancelarie, do których będą przekazywane informacje klasyfikowane UE.
   b) W przypadku gdy wśród informacji, na udostępnienie których Komisja wyraziła zgodę, znajdują się informacje o klauzuli EU TOP SECRET, państwo lub organizacja międzynarodowa, którym informacje te mają zostać przekazane, są zobowiązane do ustanowienia Głównej Kancelarii Tajnej UE oraz, gdy istnieje taka potrzeba, podkancelarii UE. Kancelarie te muszą stosować się do przepisów ściśle odpowiadających postanowieniom sekcji 22 niniejszych przepisów bezpieczeństwa.

9. Rejestrowanie

   Kancelaria, niezwłocznie po otrzymaniu dokumentów klasyfikowanych UE o klauzuli EU CONFIDENTIAL lub wyższej, odnotowuje ich wpływ w specjalnym rejestrze prowadzonym w danej instytucji. Wpis do rejestru musi zawierać następujące dane: datę otrzymania, dane identyfikujące dokument (datę wytworzenia, numer dziennika korespondencyjnego, numer egzemplarza), klauzulę tajności, tytuł, tytuł lub nazwisko odbiorcy, datę zwrotu potwierdzenia odbioru oraz datę zwrotu dokumentu do wytwórcy w UE lub jego zniszczenia.

10. Niszczenie

a) dokumenty klasyfikowane UE podlegają niszczeniu zgodnie z instrukcjami podanymi w sekcji 22 niniejszych przepisów bezpieczeństwa. Wymagane jest przekazanie kopii protokołów zniszczenia dokumentów o klauzuli EU SECRET i EU TOP SECRET do kancelarii tajnej UE, od której otrzymano te dokumenty.

b) Obowiązkowe jest uwzględnienie dokumentów klasyfikowanych UE w przygotowywanych przez instytucje, które je otrzymały, planach niszczenia własnych dokumentów klasyfikowanych w sytuacjach nadzwyczajnych.

11. Ochrona dokumentów

Muszą zostać podjęte wszelkie kroki w celu uniemożliwienia osobom nieupoważnionym uzyskania dostępu do informacji klasyfikowanych UE.

12. Kopie, tłumaczenia i wyciągi

Kopie i tłumaczenia z dokumentów o klauzuli EU CONFIDENTIAL lub EU SECRET, a także wyciągi, nie mogą być wykonywane bez upoważnienia kierownika właściwej struktury ochrony, do którego obowiązków należy dokonanie rejestracji i sprawdzenie wykonanych kopii, tłumaczeń i wyciągów oraz, gdy jest to wymagane, ich ostemplowanie.

Zgodę na wykonanie kopii lub tłumaczenia dokumentu o klauzuli EU TOP SECRET może wyrazić jedynie instytucja, w której został on wytworzony, określając jednocześnie liczbę egzemplarzy, w jakiej dany dokument lub jego tłumaczenie może być powielone. W przypadku gdy nie ma możliwości określenia instytucji, która wytworzyła dokument, wniosek należy kierować do Służby Bezpieczeństwa Komisji.

13. Nieprzestrzeganie przepisów bezpieczeństwa

Gdy stwierdzono, że doszło do nieprzestrzegania przepisów bezpieczeństwa w odniesieniu do ochrony dokumentów klasyfikowanych UE lub istnieje takie podejrzenie, niezwłocznie należy podjąć określone poniżej działania, pod warunkiem zawarcia umowy o bezpieczeństwie:

a) przeprowadzić postępowanie wyjaśniające w celu ustalenia okoliczności, w jakich doszło do nieprzestrzegania przepisów bezpieczeństwa;

b) poinformować Biuro Bezpieczeństwa Komisji, krajową władzę bezpieczeństwa oraz instytucję, która wytworzyła dokument, lub też – gdy nie została ona poinformowana – wyraźnie to zaznaczyć;

c) podjąć działania w celu zminimalizowania skutków nieprzestrzegania przepisów bezpieczeństwa;

d) ponownie rozważyć i wdrożyć środki w celu zapobieżenia powtarzaniu się takich sytuacji w przyszłości;

e) wdrożyć wszelkie środki zalecane przez Biuro Bezpieczeństwa Komisji w celu zapobieżenia powtarzaniu się takich sytuacji w przyszłości.

14. Inspekcje

Biuro Bezpieczeństwa Komisji, na podstawie umowy z danym państwem lub organizacją międzynarodową, ma prawo do dokonywania oceny skuteczności środków zastosowanych do ochrony udostępnionych informacji klasyfikowanych UE.

15. Potwierdzanie przestrzegania przepisów

Państwo lub organizacja międzynarodowa, przez cały okres, gdy dysponują dokumentami klasyfikowanymi UE – pod warunkiem że została zawarta umowa o bezpieczeństwie – powinny co roku przekazywać raport potwierdzający, że przestrzegano niniejszych przepisów bezpieczeństwa, w terminie określonym w momencie upoważnienia do udostępnienia im informacji.

Dodatek 4

Zalecenia odnoszące się do udostępniania informacji klasyfikowanych UE państwom trzecim lub organizacjom międzynarodowym: współpraca na poziomie 2

PROCEDURY

1. Uprawnienie do podejmowania decyzji o udostępnieniu informacji klasyfikowanych UE państwom, których polityka bezpieczeństwa i regulacje prawne istotnie różnią się od obowiązujących w UE, pozostaje w kompetencjach wytwórcy. Prawo do podjęcia takiej decyzji w odniesieniu do informacji wytworzonych w ramach Komisji należy do Komisji jako ciała kolegialnego.
2. Możliwość udostępnienia takim podmiotom informacji klasyfikowanych UE jest w zasadzie ograniczona do informacji objętych klauzulą do poziomu EU SECRET.
3. Pod warunkiem że została zawarta umowa o bezpieczeństwie, członek Komisji odpowiedzialny za kwestie bezpieczeństwa jest właściwy do rozpatrywania wniosków o udostępnienie informacji klasyfikowanych UE.
4. W toku rozpatrywania wniosku członek Komisji odpowiedzialny za kwestie bezpieczeństwa:

   — zasięga opinii wytwórcy informacji, która ma być przedmiotem udostępnienia,

   — nawiązuje kontakty z odpowiedzialnymi za bezpieczeństwo instytucjami państw lub organizacji międzynarodowych, którym informacje mają być przekazane, w celu uzyskania informacji na temat ich polityki bezpieczeństwa i regulacji prawnych, a także w celu opracowania tabeli odpowiedniości klauzul stosowanych w UE oraz danym państwie lub organizacji międzynarodowej,

   — zwołuje spotkanie Grupy Doradczej Komisji do spraw Polityki Bezpieczeństwa lub – gdy jest to konieczne – w drodze procedury milczenia zasięga opinii krajowych władz bezpieczeństwa Państw Członkowskich w celu uzyskania opinii technicznej Grupy.
5. Techniczna opinia Grupy Doradczej Komisji do spraw Polityki Bezpieczeństwa obejmuje następujące kwestie:

   — wiarygodność państw lub organizacji międzynarodowych, którym mają być przekazane informacje, z uwzględnieniem zagrożeń w sferze bezpieczeństwa, jakie udostępnienie mogłoby spowodować dla UE lub jej państw członkowskich,

   — ocenę zdolności odbiorcy do ochrony udostępnionych informacji klasyfikowanych UE,

   — propozycje konkretnych procedur postępowania z informacjami klasyfikowanymi UE (np. przekazywanie tekstu w „oczyszczonej" wersji) i przekazywanymi dokumentami (zachowanie lub usunięcie nazw klauzul tajności UE, dodatkowych oznaczeń itd.),

   — obniżenie lub zniesienie klauzuli tajności przez instytucję, która wytworzyła informację, przed udostępnieniem jej danemu państwu lub organizacji międzynarodowej.
6. Członek Komisji odpowiedzialny za kwestie bezpieczeństwa przekazuje Komisji, w celu podjęcia decyzji, wniosek wraz z otrzymaną opinią Grupy Doradczej do spraw Polityki Bezpieczeństwa.

PRZEPISY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PODMIOTY, KTÓRYM PRZEKAZYWANE SĄ INFORMACJE

7. Członek Komisji odpowiedzialny za kwestie bezpieczeństwa informuje państwa lub organizacje międzynarodowe, którym mają być przekazane informacje, o pozytywnej decyzji Komisji.

8. Decyzja o udostępnieniu informacji może zostać wykonana jedynie wtedy, gdy odbiorcy przekażą pisemne zapewnienie, że:

   — nie będą wykorzystywać udostępnionych informacji w innych celach, niż zostało to uzgodnione,

   — będą chronić udostępnione informacje zgodnie z przepisami określonymi przez Radę UE.

8. Zastosowanie mają poniższe zasady ochrony, pod warunkiem że Komisja po otrzymaniu technicznej opinii Grupy Doradczej Komisji do spraw Polityki Bezpieczeństwa nie podejmie decyzji o zastosowaniu szczególnych procedur postępowania z dokumentami klasyfikowanymi UE (usunięcie odniesień do klauzul tajności UE, dodatkowych oznaczeń itd.).

10. Bezpieczeństwo osobowe

    a) Grupa urzędników mających dostęp do informacji klasyfikowanych UE musi być ściśle określona, zgodnie z zasadą ograniczonego dostępu, i obejmować tylko te osoby, których obowiązki służbowe wymagają uzyskania takiego dostępu.

    b) Wszyscy urzędnicy lub obywatele danego państwa, upoważnieni do dostępu do informacji klasyfikowanych UE, muszą uzyskać decyzję potwierdzającą spełnianie przez nich warunków bezpieczeństwa lub upoważnienie do dostępu do krajowych informacji niejawnych na poziomie odpowiadającym klauzuli informacji klasyfikowanych UE, zgodnie z tabelą odpowiedniości klauzul.

    c) Informacja o wydanych decyzjach lub upoważnieniach jest przekazywana do wiadomości przewodniczącego Komisji.

11. Przesyłanie dokumentów

Praktyczne rozwiązania dotyczące przesyłania dokumentów muszą być określone w umowie. Zastosowanie mają przepisy sekcji 21, pod warunkiem zawarcia takiej umowy. W szczególności muszą zostać wskazane kancelarie, do których będą przekazywane informacje klasyfikowane UE, wraz ze szczegółowym adresem, oraz służby kurierskie lub pocztowe wykorzystywane do przesyłania informacji klasyfikowanych UE.

12. Rejestrowanie w momencie otrzymania

Krajowa władza bezpieczeństwa państwa otrzymującego informacje lub jej odpowiednik odbierający w imieniu rządu informacje klasyfikowane przekazane przez Komisję, lub też biuro bezpieczeństwa organizacji międzynarodowej, są zobowiązani do stworzenia specjalnego rejestru do odnotowywania wpływu informacji klasyfikowanych UE. Wpis do rejestru musi zawierać następujące dane: datę otrzymania, dane identyfikujące dokument (datę wytworzenia, numer dziennika korespondencyjnego, numer egzemplarza), klauzulę tajności, tytuł, tytuł lub nazwisko odbiorcy, datę zwrotu potwierdzenia odbioru oraz datę zwrotu dokumentu do wytwórcy w UE lub jego zniszczenia.

13. Zwracanie dokumentów

Odbiorca, zwracając dokumenty klasyfikowane do Komisji, postępuje w sposób określony w sekcji „Przesyłanie dokumentów".

14. Ochrona dokumentów

a) Dokumenty, w czasie gdy nie są wykorzystywane, muszą być przechowywane w sejfach lub szafach metalowych, zatwierdzonych do przechowywania krajowych materiałów o równorzędnej klauzuli tajności. Na sejfie lub szafie nie umieszcza się żadnych oznaczeń wskazujących na ich zawartość; dostęp do nich mogą mieć jedynie osoby upoważnione do wykonywania czynności związanych z obiegiem informacji klasyfikowanych UE. W przypadku używania zamków szyfrowych kombinacje mogą znać jedynie ci urzędnicy danego państwa lub organizacji międzynarodowej, którzy zostali upoważnieni do dostępu do informacji klasyfikowanych UE przechowywanych w danym sejfie lub szafie pancernej. Kombinacje muszą być zmieniane co sześć miesięcy lub przed upływem tego okresu, jeśli któryś z urzędników został przeniesiony, jeśli w stosunku do któregoś z nich została cofnięta decyzja o spełnianiu warunków bezpieczeństwa lub gdy istnieje zagrożenie, że bezpieczeństwo informacji zostanie narażone na szwank.

b) Dokumenty klasyfikowane UE mogą być pobierane z sejfu lub szafy metalowej wyłącznie przez urzędników, którzy zostali odpowiednio sprawdzeni, a zapoznanie się z informacjami jest konieczne do wykonywania przez nich obowiązków służbowych. Przez okres, kiedy dokumenty znajdują się w ich posiadaniu, są oni odpowiedzialni za zapewnienie im bezpieczeństwa, a w szczególności za zapewnienie, że nie uzyska do nich dostępu osoba nieupoważniona. Muszą także zapewnić, że dokumenty, po wykorzystaniu lub po zakończeniu godzin pracy, są przechowywane w sejfie lub szafie metalowej.

c) Kopie i wyciągi z dokumentów o klauzuli EU CONFIDENTIAL lub wyższej mogą być wykonywane wyłącznie za zgodą Biura Bezpieczeństwa Komisji.

d) Wymagane jest określenie procedury szybkiego i skutecznego niszczenia dokumentów w sytuacjach nadzwyczajnych; musi być ona potwierdzona przez Biuro Bezpieczeństwa Komisji.

15. Bezpieczeństwo fizyczne

a) Sejfy i szafy metalowe, wykorzystywane do przechowywania dokumentów klasyfikowanych UE, muszą być zamknięte na klucz przez cały czas, gdy nie są z nich pobierane lub do nich odkładane dokumenty.

b) Gdy konieczne jest wejście i praca personelu sprzątającego lub ekip remontowych w pomieszczeniu, w którym znajdują się sejfy lub szafy metalowe, osobom wykonującym prace musi cały czas towarzyszyć pracownik służby bezpieczeństwa danego państwa lub organizacji lub też urzędnik odpowiedzialny za nadzór nad bezpieczeństwem danego pomieszczenia.

c) Poza normalnymi godzinami pracy (w nocy, w weekendy oraz święta) sejfy lub szafy metalowe, w których są przechowywane informacje klasyfikowane UE, muszą być chronione albo przez strażników, albo przez zastosowanie automatycznego systemu alarmowego.

16. Nieprzestrzeganie przepisów bezpieczeństwa

Gdy stwierdzono, że doszło do nieprzestrzegania przepisów bezpieczeństwa w odniesieniu do ochrony dokumentów klasyfikowanych UE lub istnieje takie podejrzenie, niezwłocznie należy podjąć określone poniżej działania:

a) natychmiast przesłać raport do Biura Bezpieczeństwa Komisji lub krajowej władzy bezpieczeństwa państwa członkowskiego, które było inicjatorem przekazania dokumentów (wraz z kopią dla Biura Bezpieczeństwa Komisji);

b) przeprowadzić postępowanie wyjaśniające, a po jego zakończeniu przekazać pełny raport jednemu z podmiotów wymienionych w lit. a) powyżej. Należy podjąć odpowiednie środki w celu poprawy sytuacji.

17. Inspekcje

Biuro Bezpieczeństwa Komisji, na podstawie umowy z danym państwem lub organizacją międzynarodową, ma prawo do dokonywania oceny skuteczności środków zastosowanych do ochrony udostępnionych informacji klasyfikowanych UE.

18. Potwierdzanie przestrzegania przepisów

Państwo lub organizacja międzynarodowa, przez cały okres, gdy dysponują dokumentami klasyfikowanymi UE – pod warunkiem że została zawarta umowa o bezpieczeństwie – powinny co roku przekazywać raport potwierdzający, że przestrzegano niniejszych przepisów bezpieczeństwa, w terminie określonym w momencie upoważnienia do udostępnienia im informacji.

Dodatek 5

Zalecenia odnoszące się do udostępniania informacji klasyfikowanych UE państwom trzecim lub organizacjom międzynarodowym: współpraca na poziomie 3

PROCEDURY

1. Od czasu do czasu, w szczególnych okolicznościach, Komisja może uznać, że istnieje potrzeba współpracy, wiążącej się z koniecznością udostępnienia informacji klasyfikowanych UE, z państwami lub organizacjami, które nie mogą udzielić zapewnień wymaganych przez niniejsze przepisy bezpieczeństwa.

2. Uprawnienie do podejmowania decyzji o udostępnieniu informacji klasyfikowanych UE państwom, których polityka bezpieczeństwa i regulacje prawne istotnie różnią się od obowiązujących w UE, pozostaje w kompetencjach wytwórcy. Prawo do podjęcia takiej decyzji w odniesieniu do informacji wytworzonych w ramach Komisji należy do Komisji jako ciała kolegialnego.

   Możliwość udostępnienia takim podmiotom informacji klasyfikowanych UE jest w zasadzie ograniczona do informacji objętych klauzulą do poziomu EU SECRET.

3. Komisja rozważy zasadność udostępnienia informacji klasyfikowanych, dokona oceny związku tych informacji z zadaniami wykonywanymi przez potencjalnego odbiorcę oraz podejmie decyzję, jakiego rodzaju informacje mogą zostać przekazane.

4. Jeśli Komisja podejmie decyzję pozytywną, członek Komisji odpowiedzialny za kwestie bezpieczeństwa:

   — zasięga opinii wytwórcy informacji, która ma być przedmiotem udostępnienia,

   — zwołuje spotkanie Grupy Doradczej Komisji do spraw Polityki Bezpieczeństwa lub – gdy jest to konieczne – w drodze procedury milczenia zasięga opinii krajowych władz bezpieczeństwa państw członkowskich w celu uzyskania opinii technicznej Grupy.

5. Techniczna opinia Grupy Doradczej do spraw Polityki Bezpieczeństwa obejmuje następujące kwestie:

   a) ocenę zagrożeń w sferze bezpieczeństwa, które udostępnienie mogłoby spowodować dla UE lub jej państw członkowskich;

   b) klauzulę tajności informacji, które mogłyby zostać udostępnione;

   c) obniżenie lub zniesienie klauzuli tajności informacji przed jej udostępnieniem;

   d) procedury postępowania z dokumentami, które mają zostać udostępnione (por. poniższe paragrafy);

   e) możliwe sposoby przesłania (wykorzystanie ogólnodostępnych służb pocztowych, ogólnodostępnych lub zabezpieczonych systemów teleinformatycznych, worków dyplomatycznych, sprawdzonych kurierów itd.).

6. Dokumenty udostępniane państwom trzecim lub organizacjom na podstawie niniejszego załącznika są, w zasadzie, pozbawiane odniesień do ich pochodzenia lub klauzuli tajności UE. Grupa Doradcza Komisji do spraw Polityki Bezpieczeństwa może zalecić:

   — użycie szczególnych oznaczeń lub kryptonimów,

   — wykorzystanie szczególnego systemu klauzul wiążącego stopień sensytywności informacji ze środkami kontroli przesyłania dokumentów, do stosowania których jest zobowiązany odbiorca.

7. Przewodniczący przekazuje Komisji, w celu podjęcia decyzji, opinię Grupy Doradczej do spraw Polityki Bezpieczeństwa.

8. Po wyrażeniu przez Komisję zgody na udostępnienie informacji klasyfikowanych UE i zaakceptowaniu praktycznych rozwiązań dotyczących wykonania tej decyzji, Biuro Bezpieczeństwa Komisji ustanawia niezbędne kontakty z instytucją odpowiedzialną za bezpieczeństwo w danym państwie lub organizacji w celu ułatwienia wdrożenia przewidzianych środków ochrony.

9. Członek Komisji odpowiedzialny za kwestie bezpieczeństwa informuje wszystkie Państwa Członkowskie o charakterze i klauzuli udostępnianych informacji wraz z wykazem organizacji i państw, którym zostaną one przekazane na podstawie decyzji Komisji.

10. Biuro Bezpieczeństwa Komisji podejmuje wszelkie konieczne środki w celu ułatwienia oceny możliwych szkód oraz dokonania przeglądu procedur.

    W każdym przypadku, gdy ulegają zmianie warunki współpracy, Komisja jest zobowiązana do ponownego rozważenia decyzji.

PRZEPISY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PODMIOTY, KTÓRYM PRZEKAZYWANE SĄ INFORMACJE

11. Członek Komisji odpowiedzialny za kwestie bezpieczeństwa informuje państwa lub organizacje międzynarodowe, którym mają być przekazane informacje, o pozytywnej decyzji Komisji, jednocześnie przekazując szczegółowe zasady ochrony zaproponowane przez Grupę Doradczą do spraw Polityki Bezpieczeństwa i zaakceptowane przez Komisję.

12. Decyzja o udostępnieniu informacji może zostać wykonana jedynie wtedy, gdy odbiorcy przekażą pisemne zapewnienie, że:

— nie będą wykorzystywać udostępnionych informacji w innych celach, niż zostało to uzgodnione,

— zapewnią udostępnionym informacjom stopień ochrony wymagany przez Komisję.

13. Przesyłanie dokumentów

a) Praktyczne rozwiązania dotyczące przesyłania dokumentów zostaną uzgodnione pomiędzy Biurem Bezpieczeństwa Komisji a odpowiedzialnymi za bezpieczeństwo instytucjami danego państwa lub organizacji międzynarodowej. W szczególności muszą zostać określone adresy, na które dokumenty mają być przekazywane.

b) Dokumenty o klauzuli EU CONFIDENTIAL i wyższej muszą być przesyłane w podwójnym opakowaniu. Na kopercie wewnętrznej muszą być naniesione ustalona szczególna pieczątka lub kryptonim oraz odniesienie do szczególnej klasyfikacji przyjętej dla danego dokumentu. Do każdego dokumentu klasyfikowanego dołącza się formularz potwierdzenia odbioru. Formularz ten nie jest klasyfikowany; podaje się w nim dane identyfikujące dokumentu (numer dziennika korespondencyjnego, datę, numer egzemplarza) oraz język, w którym został sporządzony; nie podaje się natomiast tytułu.

c) Koperta wewnętrzna jest umieszczana w drugiej kopercie, na której naniesiony jest numer paczki potrzebny do potwierdzania odbioru. Na kopercie zewnętrznej nie umieszcza się klauzuli tajności.

d) Kurierzy zawsze otrzymują potwierdzenie odbioru zawierające numer paczki.

14. Rejestrowanie w momencie otrzymania

Krajowa władza bezpieczeństwa państwa otrzymującego informacje lub jej odpowiednik odbierający w imieniu rządu informacje klasyfikowane przekazane przez UE, lub też biuro bezpieczeństwa organizacji międzynarodowej, są zobowiązani do stworzenia specjalnego rejestru do odnotowywania wpływu informacji klasyfikowanych UE. Wpis do rejestru musi zawierać następujące dane: datę otrzymania, dane identyfikujące dokument (datę wytworzenia, numer dziennika korespondencyjnego, numer egzemplarza), klauzulę tajności, tytuł, tytuł lub nazwisko odbiorcy, datę zwrotu potwierdzenia odbioru oraz datę zwrotu dokumentu do wytwórcy w UE lub jego zniszczenia.

15. Wykorzystanie i ochrona przekazanych informacji klasyfikowanych

a) Do dokumentów o klauzuli na poziomie EU SECRET mogą mieć dostęp wyłącznie specjalnie wyznaczeni urzędnicy, upoważnieni do dostępu do informacji objętych tą klauzulą. Mogą być przechowywane wyłącznie w dobrej jakości sejfach, które mogą być otwierane jedynie przez osoby upoważnione do dostępu do informacji, które się w nich znajdują. Strefy, w których sejfy te się znajdują, muszą być pod stałą ochroną; wymagane jest ustanowienie systemu weryfikacji dostępu w celu zapewnienia, że wpuszczane są tylko osoby odpowiednio do tego upoważnione. Informacje o klauzuli na poziomie EU SECRET mogą być przesyłane wyłącznie w worku dyplomatycznym, za pośrednictwem bezpiecznych służb pocztowych lub zabezpieczonych systemów teleinformatycznych. Warunkiem powielenia takiego dokumentu jest uzyskanie pisemnej zgody instytucji, która go wytworzyła. Wszystkie kopie muszą zostać zarejestrowane i poddane kontroli obiegu. Wszystkie czynności związane z dokumentami o tej klauzuli są dokumentowane odpowiednimi potwierdzeniami.

b) Do dokumentów o klauzuli na poziomie EU CONFIDENTIAL mogą mieć dostęp odpowiednio wyznaczeni urzędnicy, upoważnieni do dostępu do informacji na dany temat. Mogą być one przechowywane wyłącznie w zamykanych na klucz sejfach znajdujących się w strefach poddanych kontroli.

Informacje o klauzuli na poziomie EU CONFIDENTIAL są przesyłane w worku dyplomatycznym, za pośrednictwem poczty wojskowej lub zabezpieczonych systemów teleinformatycznych. Odbiorcy mogą wykonywać kopie, z zastrzeżeniem, że liczba kopii i ich dystrybucja są odnotowywane w specjalnych rejestrach.

c) Dokumenty o klauzuli na poziomie EU RESTRICTED mogą być wykorzystywane wyłącznie w pomieszczeniach niedostępnych dla osób nieupoważnionych i przechowywane w szafach lub innych meblach zamykanych na klucz. Dokumenty mogą być przesyłane za pośrednictwem ogólnodostępnych służb pocztowych jako przesyłki polecone; wymagane jest zapakowanie ich w dwie koperty. W sytuacjach nadzwyczajnych, w toku działań, dopuszczalne jest przesyłanie przez niezabezpieczone systemy teleinformatyczne. Odbiorcy mogą wykonywać kopie.

d) Dokumenty nieklasyfikowane nie wymagają stosowania szczególnych środków ochrony i mogą być przesyłane za pośrednictwem poczty i ogólnodostępnych systemów teleinformatycznych. Adresaci mogą wykonywać kopie.

16. Niszczenie

Niepotrzebne już dokumenty podlegają zniszczeniu. W przypadku zniszczenia dokumentów o klauzuli na poziomie EU RESTRICTED i EU CONFIDENTIAL należy dokonać odpowiedniego wpisu do rejestru. W odniesieniu do dokumentów o klauzuli na poziomie EU SECRET wymagane jest sporządzenie protokołów zniszczenia, które muszą być podpisane przez dwie osoby będące świadkami zniszczenia.

17. Nieprzestrzeganie przepisów bezpieczeństwa

Gdy stwierdzono, że doszło do nieprzestrzegania przepisów bezpieczeństwa w odniesieniu do ochrony dokumentów o klauzuli na poziomie EU CONFIDENTIAL lub EU SECRET, lub istnieje takie podejrzenie, krajowa władza bezpieczeństwa lub szef bezpieczeństwa danej organizacji przeprowadza postępowanie wyjaśniające w celu ustalenia okoliczności zdarzenia. O wynikach postępowania obligatoryjnie informuje się Biuro Bezpieczeństwa Komisji. Niezbędne jest podjęcie koniecznych kroków w celu dokonania zmian w nieefektywnych procedurach lub sposobach przechowywania informacji, jeśli to one stały się przyczyną zdarzenia.

Dodatek 6

WYKAZ SKRÓTÓW

ACPC	Komitet Doradczy do spraw Zakupów i Kontraktów
CrA	władza CRYPTO
CISO	główny inspektor bezpieczeństwa teleinformatycznego
COMPUSEC	bezpieczeństwo komputerów
COMSEC	bezpieczeństwo łączności
CSO	Biuro Bezpieczeństwa Komisji
ESDP	europejska polityka bezpieczeństwa i obrony
EUCI	informacje klasyfikowane Unii Europejskiej
IA	władza bezpieczeństwa teleinformatycznego
IO	właściciel informacji
ISO	Międzynarodowa Organizacja do spraw Standaryzacji
IT	technologia teleinformatyczna
LISO	lokalny inspektor bezpieczeństwa teleinformatycznego
LSO	lokalny pełnomocnik ochrony
MSO	pełnomocnik ochrony spotkania
NSA	krajowa władza bezpieczeństwa
PC	komputer osobisty
RCO	urzędnik kontroli kancelarii
SAA	władza akredytacji bezpieczeństwa
SecOP	operacyjne procedury bezpieczeństwa
SSRS	szczególne wymagania bezpieczeństwa systemu
TA	władza TEMPEST
TSO	właściciel systemów technicznych