Dokument ten służy wyłącznie do celów dokumentacyjnych i instytucje nie ponoszą żadnej odpowiedzialności za jego zawartość

►B

DECYZJA RADY

z dnia 19 marca 2001 r.

w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa

(2001/264/WE)

(Dz.U. L 11 z 11.4.2001, str. 1)

zmieniona przez:

		Dziennik Urzędowy		
		nr	strona	data
►M1	Decyzja Rady 2004/194/WE, z dnia 10 lutego 2004 r.	L 63	48	28.2.2004
►M2	Decyzja Rady 2005/571/WE, z dnia 12 lipca 2005 r.	L 193	31	23.7.2005
►M3	Decyzja Rady 2005/952/WE, z dnia 20 grudnia 2005 r.	L 346	18	29.12.2005

▼B

DECYZJA RADY

z dnia 19 marca 2001 r.

w sprawie przyjęcia przepisów Rady dotyczących bezpieczeństwa

(2001/264/WE)

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat ustanawiający Wspólnotę Europejską, w szczególności jego art. 207 ust. 3,

uwzględniając decyzję Rady 2000/396/WE, EWWiS, Euratom z dnia 5 czerwca 2000 r. przyjmującą regulamin Rady ([1]), w szczególności jej art. 24,

a także mając na uwadze, co następuje:

(1) W celu rozwoju działań Rady w dziedzinach wymagających stopnia poufności, właściwe jest ustanowienie powszechnego systemu bezpieczeństwa obejmującego Radę, jej Sekretariat Generalny oraz Państwa Członkowskie.

(2) Taki system powinien ujmować w pojedynczym tekście zagadnienia zawarte we wszystkich poprzednich decyzjach i przepisach w tej dziedzinie.

(3) W praktyce, główna część informacji UE, oznaczonych klauzulą „CONFIDENTIEL UE" i wyżej będzie dotyczyć Wspólnej Polityki Bezpieczeństwa i Obronnej.

(4) W celu zapewnienia skuteczności systemu bezpieczeństwa ustanowionego w ten sposób, Państwa Członkowskie powinny włączyć się w jego funkcjonowanie poprzez podjęcie krajowych środków niezbędnych do przestrzegania przepisów niniejszej decyzji, w przypadku gdy ich właściwe organy i pracownicy mają do czynienia z informacjami niejawnymi UE.

(5) Rada z zadowoleniem przyjmuje zamiar Komisji do wprowadzenia, przed terminem zastosowania niniejszej decyzji, systemu generalnego zgodnego z załącznikami do niniejszej decyzji, w celu zapewnienia sprawnego funkcjonowania procesu podejmowania decyzji Unii.

(6) Rada podkreśla znaczenie włączenia się, w odpowiednim przypadku, Parlamentu Europejskiego i Komisji, do przestrzegania reguł i norm poufności, niezbędnych w celu ochrony interesów Unii oraz jej Państw Członkowskich.

(7) Niniejsza decyzja zostaje podjęta bez uszczerbku dla przepisów art. 255 Traktatu oraz jego dokumentów wykonawczych.

(8) Niniejsza decyzja zostaje podjęta bez uszczerbku dla istniejących praktyk w Państwach Członkowskich w odniesieniu do powiadamiania ich parlamentów narodowych na temat działalności Unii,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Przepisy Rady dotyczące bezpieczeństwa, zawarte w Załączniku, zostają niniejszym zatwierdzone.

Artykuł 2

1. Sekretarz Generalny/Wysoki Przedstawiciel podejmuje właściwe środki w celu zapewnienia, że podczas korzystania z informacji niejawnych UE, przepisy określone w art. 1 są przestrzegane w ramach Sekre-

([1]) Dz.U. L 149 z 23.6.2000, str. 21.

▼B

tariatu Generalnego Rady (zwanego dalej SGR) przez urzędników i innych pracowników SGR, przez wykonawców zewnętrznych oraz przez personel oddelegowany do SGR, zarówno w siedzibach Rady, jak i zdecentralizowanych agencjach UE ([1]).

2. Państwa Członkowskie podejmują właściwe środki, zgodnie z krajowymi uzgodnieniami, w celu zapewnienia, że podczas korzystania z informacji niejawnych UE, w ramach ich służb i siedzib, przepisy określone w art. 1 są przestrzegane przez:

a) członków stałych przedstawicielstw Państw Członkowskich w Unii Europejskiej, a także członków delegacji krajowych uczestniczących w posiedzeniach Rady lub jej organów, lub biorących udział w innych formach działalności Rady;

b) innych członków krajowych administracji Państw Członkowskich korzystających z informacji niejawnych UE, zarówno podczas pełnienia obowiązków na terytorium Państw Członkowskiego lub poza jego granicami; oraz

c) zewnętrznych wykonawców Państw Członkowskich oraz oddelegowany personel, korzystający z informacji niejawnych UE.

Państwa Członkowskie niezwłocznie powiadamiają SGR o podjętych środkach.

3. Środki określone w ust. 1 i 2 zostają podjęte przed dniem 30 listopada 2001 r.

Artykuł 3

Zgodnie z podstawowymi zasadami i minimalnymi normami bezpieczeństwa zawartymi w części I Załącznika, Sekretarz Generalny/Wysoki Przedstawiciel może podejmować środki zgodnie z częścią II sekcji I ust. 1 i 2 Załącznika.

Artykuł 4

Począwszy od dnia zastosowania, niniejsza decyzja zastępuje:

a) decyzję Rady 98/319/WE z dnia 27 kwietnia 1988 r. odnoszącą się do procedur, według których urzędnikom oraz pracownikom Sekretariatu Generalnego Rady można umożliwić dostęp do informacji niejawnych posiadanych przez Radę ([2]);

b) decyzję Sekretarza Generalnego/Wysokiego Przedstawiciela z dnia 27 lipca 2000 r. w sprawie środków ochrony niejawnych informacji stosowanych w odniesieniu do Sekretariatu Generalnego Rady ([3]);

c) decyzję 433/97 Sekretarza Generalnego Rady z dnia 27 maja 1997 r. w sprawie procedury postępowania sprawdzającego urzędników odpowiedzialnych za funkcjonowanie sieci Cortesy.

Artykuł 5

1. Niniejsza decyzja staje się skuteczna w dniu jej opublikowania.

2. Niniejszą decyzję stosuje się od dnia 1 grudnia 2001 r.

([1]) Patrz wnioski Rady z dnia 10 listopada 2000 r.
([2]) Dz.U. L 140 z 12.5.1998, str. 12.
([3]) Dz.U. C 239 z 23.8.2000, str. 1

▼B

ZAŁĄCZNIK

PRZEPISY RADY UNII EUROPEJSKIEJ DOTYCZĄCE BEZPIECZEŃSTWA

▼B

SPIS TREŚCI

CZĘŚĆ I

Podstawowe zasady i minimalne normy bezpieczeństwa

CZĘŚĆ II

SEKCJA I

Organizacja bezpieczeństwa w Radzie Unii Europejskiej

SEKCJA II

Klasyfikacje i oznaczenia

SEKCJA III

Zarządzanie w zakresie klasyfikowania

SEKCJA IV

Bezpieczeństwo fizyczne

SEKCJA V

Ogólne reguły dotyczące zasady potrzeby niezbędnej wiedzy oraz postępowanie sprawdzające

SEKCJA VI

Procedura sprawdzająca w zakresie bezpieczeństwa dla urzędników SGR i innych pracowników

SEKCJA VII

Przygotowanie, rozpowszechnianie, przekazywanie, przechowywanie oraz niszczenie materiałów niejawnych UE

SEKCJA VIII

Rejestry très secret UE/EU top secret

SEKCJA IX

Środki bezpieczeństwa stosowane w czasie nadzwyczajnych posiedzeń odbywających się poza siedzibą Rady i dotyczące kwestii wysoko sensytywnych

SEKCJA X

Naruszenie zasad bezpieczeństwa i wejście w posiadanie informacji niejawnych UE przez osoby nieupoważnione

SEKCJA XI

Ochrona informacji przetwarzanych przez technologię informacyjną i systemy łączności

SEKCJA XII

Udostępnienie informacji niejawnych państwom trzecim oraz organizacjom międzynarodowym

Dodatki

Dodatek I

Wykaz krajowych organów bezpieczeństwa

Dodatek 2

Porównanie krajowych klauzul tajności

Dodatek 3

Praktyczny przewodnik po klasyfikacji

Dodatek 4

▼B

Wytyczne w sprawie udostępniania informacji niejawnych UE państwom trzecim lub organizacjom międzynarodowym

— Współpraca na poziomie 1

Dodatek 5

Wytyczne w sprawie udostępniania informacji niejawnych UE państwom trzecim lub organizacjom międzynarodowym

— Współpraca na poziomie 2

Dodatek 6

Wytyczne w sprawie udostępniania informacji niejawnych UE państwom trzecim lub organizacjom międzynarodowym

— Współpraca na poziomie 3

▼B

CZĘŚĆ I

PODSTAWOWE ZASADY I MINIMALNE NORMY BEZPIECZEŃSTWA

WPROWADZENIE

1. Niniejsze przepisy ustanawiają podstawowe zasady i minimalne normy bezpieczeństwa, które mają być we właściwy sposób przestrzegane przez Radę, Sekretariat Generalny Rady (zwany dalej SGR), Państwa Członkowskie i zdecentralizowane agencje Unii Europejskiej (zwane dalej zdecentralizowanymi agencjami UE), tak, aby bezpieczeństwo było zapewnione i wszystkie te podmioty mogły mieć pewność, że została wprowadzona wspólna norma ochrony.

2. Określenie „informacja niejawna UE" oznacza każdą informację i materiał, którego nieuprawnione ujawnienie mogłoby w różnym stopniu zaszkodzić interesom UE, jednego lub więcej Państw Członkowskich, bez względu na to, czy taka informacja pochodzi z terytorium UE, czy też została otrzymana z Państwa Członkowskiego, państwa trzeciego lub organizacji międzynarodowej.

3. W niniejszych przepisach:

   a) przez „dokument" rozumie się każdy list, notatkę, protokół, sprawozdanie, memorandum, znak/wiadomość, szkic, zdjęcie, przeźrocze, film, mapę, wykres, plan, notatnik, szablon, kalkę, taśmy do maszyn do pisania i drukarek, taśmę magnetofonową, kasetę magnetofonową, dysk komputerowy, CD ROM lub inne fizyczne nośniki, na których informacja została zarejestrowana;

   b) przez „materiał" rozumie się dokument określony powyżej w lit. a) oraz każdy przedmiot wyposażenia lub broń, zarówno gotowe, jak i będące w procesie produkcji.

4. Podstawowe cele bezpieczeństwa są następujące:

   a) zabezpieczenie informacji niejawnych UE przed szpiegostwem, ujawnieniem lub nieuprawnionym rozpowszechnieniem;

   b) zabezpieczenie informacji UE przetwarzanych w systemach i sieciach łączności i informacji przed groźbą naruszenia ich integralności i dostępności;

   c) zabezpieczenie obiektów służących do przechowywania informacji UE przed sabotażem oraz złośliwym, umyślnym uszkodzeniem;

   d) w przypadku nie zachowania środków bezpieczeństwa, dokonanie oceny powstałych szkód, ograniczenie ich konsekwencji i przyjęcie niezbędnych środków zaradczych.

5. Podstawami silnego systemu bezpieczeństwa są:

   a) w każdym Państwie Członkowskim, krajowa organizacja do spraw bezpieczeństwa odpowiedzialna za:

      i) zbieranie i rejestrowanie danych dotyczących szpiegostwa, sabotażu, terroryzmu i innych działań wywrotowych; oraz

      ii) powiadamianie i doradzanie własnemu rządowi oraz, za jego pośrednictwem Radzie o charakterze zagrożeń dla bezpieczeństwa i środków ochrony przed nimi;

   b) w każdym Państwie Członkowskim oraz w SGR, techniczny organ INFOSEC, odpowiedzialny za współpracę z zainteresowanymi organami bezpieczeństwa w celu dostarczania informacji i doradztwa w odniesieniu do technicznych zagrożeń dla bezpieczeństwa i środków ochrony przed nimi;

   c) regularna współpraca między służbami rządowymi, agencjami i służbami SGR, w celu ustalenia, i zalecenia, gdzie właściwe:

      i) jakie informacje, zasoby i obiekty wymagają ochrony; oraz

▼B

ii) wspólnych norm ochrony.

6. W przypadku gdy chodzi o poufność, niezbędna jest szczególna dbałość i doświadczenie w wyborze informacji i materiałów wymagających ochrony oraz przy ocenie wymaganego stopnia ochrony. Istotne jest, żeby stopień ochrony odpowiadał krytycznemu poziomowi bezpieczeństwa każdej części informacji oraz materiału, który ma zostać objęty ochroną. W celu zapewnienia sprawnego przepływu informacji, należy podjąć kroki, zapobiegające zawyżaniu klasyfikacji. System klasyfikacji jest instrumentem wykonawczym do niniejszych zasad; podobny system klasyfikacji powinien być używany w planowaniu i organizowaniu sposobów przeciwdziałania szpiegostwu, sabotażowi, terroryzmowi i innym zagrożeniom, tak aby najszersze środki ochrony zostały skierowane do najważniejszych siedzib służących do przechowywania informacji niejawnych i najbardziej wrażliwych punktów tych siedzib.

PODSTAWOWE ZASADY

7. Środki bezpieczeństwa:

a) obejmują wszystkie osoby mające dostęp do informacji niejawnych, nośników informacji niejawnych, siedzib, w których znajdują się informacje niejawne i ważne obiekty;

b) są przeznaczone do wykrywania osób, których postawa może zagrozić bezpieczeństwu informacji niejawnych oraz ważnych obiektów służących do przechowywania informacji niejawnych oraz zapewniają ich wyłączenie lub wycofanie;

c) zapobieganie dostępowi osób nieupoważnionych do informacji niejawnych lub obiektów, w których są przechowywane;

d) zapewniają, że informacje niejawne są rozpowszechniane wyłącznie na podstawie zasady potrzeby niezbędnej wiedzy, która jest podstawowa dla wszystkich aspektów bezpieczeństwa;

e) zapewniają integralność (tzn. zapobieganie zniszczeniu lub nieuprawnionemu wprowadzaniu zmian lub nieuprawnionemu usunięciu) oraz dostępność (tzn. nie można odmówić dostępu osobom, które potrzebują z nich skorzystać i są do tego upoważnione) wszystkich informacji, zarówno niejawnych, jak i jawnych, w szczególności, gdy takie informacje są przechowywane, przetwarzane lub przekazywane w formie elektromagnetycznej.

ORGANIZACJA BEZPIECZEŃSTWA

Wspólne normy minimalne

8. Rada oraz każde Państwo Członkowskie zapewniają, że wspólne minimalne normy bezpieczeństwa są przestrzegane we wszystkich służbach administracyjnych i/lub rządowych, innych instytucjach UE, agencjach oraz przez wykonawców, aby informacje niejawne UE mogły być przekazywane w przeświadczeniu, że zainteresowani będą korzystać z nich z taka samą dbałością. Takie minimalne normy obejmują kryteria dotyczące postępowania sprawdzającego w odniesieniu do pracowników oraz procedur ochrony informacji niejawnych UE. ►M3 Takie minimalne normy obejmują również minimalne normy, które mają zastosowanie, w przypadku gdy SGR na podstawie umowy powierza zadania obejmujące informacje niejawne UE, wiążące się z takimi informacjami lub je zawierające podmiotom prowadzącym działalność przemysłową lub inną: takie wspólne minimalne normy zawarte są w sekcji XIII części II. ◄

BEZPIECZEŃSTWO PRACOWNIKÓW

Postępowanie sprawdzające w odniesieniu do pracowników

9. Wszystkie osoby wnioskujące o dostęp do informacji oznaczonych klauzulą CONFIDENTIEL UE lub wyżej, są odpowiednio sprawdzane przed uzyskaniem zgody na taki dostęp. Podobne postępowanie sprawdzające jest wymagane w przypadku osób, których obowiązki obejmują obsługę techniczną lub konserwację systemów łączności lub informacji zawierających

▼B

informacje niejawne. Takie postępowanie sprawdzające jest przeznaczone do ustalenia, czy takie osoby:

a) są osobami, których lojalność nie budzi wątpliwości;

b) posiadają takie cechy charakteru i są na tyle rozważne, że nie nasuwają się wątpliwości co do ich rzetelności podczas korzystania z informacji niejawnych; lub

c) mogą być podatne na naciski ze źródeł zagranicznych lub innych, na przykład ze względu na poprzednie miejsce zamieszkania lub powiązania z przeszłości, które mogłyby stanowić zagrożenie dla bezpieczeństwa.

Szczególnie dokładnej kontroli w toku procedur sprawdzających należy poddać osoby:

d) którym ma zostać udzielona zgoda na dostęp do informacji oznaczonych klauzulą TRÈS SECRET EU/TOP SECRET EU;

e) zajmujące stanowiska wymagające regularnego dostępu do znacznej ilości informacji oznaczonych klauzulą SECRET UE;

f) których obowiązki umożliwiają im specjalny dostęp do systemów łączności i informacji używanych w sytuacjach krytycznych, a przez to możliwość uzyskania nieupoważnionego dostępu do dużej ilości informacji niejawnych UE, lub spowodowania poważnych szkód w takiej sytuacji, w wyniku aktów sabotażu technicznego.

W okolicznościach, określonych w lit. d), e) i f), należy zastosować najszersze możliwe wykorzystanie techniki badania przeszłości.

10. W przypadku gdy osoby nie posiadające ustalonej „potrzeby niezbędnej wiedzy" mają zostać zatrudnione w warunkach, w których mogą mieć dostęp do informacji niejawnych UE (na przykład: posłańcy, agenci ochrony, pracownicy obsługi, personel sprzątający itp.), uprzednio zostają one poddane postępowaniu sprawdzającemu.

Ewidencja postępowania sprawdzającego w odniesieniu do pracowników

11. Wszystkie służby, organy lub instytucje korzystające z informacji niejawnych UE lub posiadające systemy łączności i informacyjne, używane w sytuacjach kryzysowych, prowadzi ewidencję upoważnień do dostępu przyznanych pracownikom tam zatrudnianym. Każde upoważnienie do dostępu jest weryfikowane, jeżeli wymaga tego sytuacja, w celu zapewnienia, że odpowiada obecnemu stanowisku danej osoby; upoważnienie takie zostaje ponownie zbadane w pierwszej kolejności w każdym przypadku, po uzyskaniu nowej informacji wskazującej, że dalsze zatrudnienie danej osoby przy wykonywaniu pracy o charakterze poufnym nie jest zgodne z interesem bezpieczeństwa. Ewidencja postępowania sprawdzającego jest przechowywana przez szefa bezpieczeństwa odpowiednich służb, organów lub instytucji.

Instrukcje bezpieczeństwa dla pracowników

12. Wszyscy pracownicy zatrudnieni na stanowiskach, na których mogą mieć dostęp do informacji niejawnych są dokładnie instruowani podczas zatrudniania oraz w regularnych odstępach czasu o wymogach bezpieczeństwa oraz procedurach mających na celu ich spełnienie. Użyteczną procedurą jest wymóg, aby wszyscy tacy pracownicy poświadczali pisemnie, że w pełni rozumieją przepisy dotyczące bezpieczeństwa odpowiadające ich stanowisku.

Obowiązki kierownictwa

13. Kierownicy mają obowiązek znać te osoby z ich personelu, które są zaangażowane w wykonywanie pracy o charakterze poufnym, lub które mają dostęp do systemów łączności i informacji, używanych w sytuacjach krytycznych, oraz ewidencjonowanie i zgłaszanie wszelkich zdarzeń lub widocznych słabych punktów, które mogłyby mieć wpływ na bezpieczeństwo.

Status bezpieczeństwa pracowników

▼B

14. Ustanawia się procedury w celu zapewnienia, że w przypadku uzyskania niekorzystnej informacji dotyczącej pracownika, jest określone, czy dana osoba jest zatrudniona przy klasyfikacji informacji lub czy ma dostęp do ważnych systemów łączności i informacji oraz powiadamia się zainteresowane organy. Jeżeli ustala się, że taka osoba stanowi zagrożenie dla bezpieczeństwa, zostaje ona (mężczyzna lub kobieta) zwolniona lub odsunięta od stanowiska, na którym mogłaby zagrozić bezpieczeństwu.

BEZPIECZEŃSTWO FIZYCZNE

Potrzeba ochrony

15. Stopień środków bezpieczeństwa fizycznego stosowanych w celu zapewnienia ochrony informacji niejawnych UE jest proporcjonalny do zaklasyfikowania, ilości oraz zagrożenia przechowywanych informacji i materiałów. Dlatego należy dołożyć starań, aby uniknąć zaniżania jak i zawyżania klasyfikowania, jak również poddawać klasyfikowanie regularnej weryfikacji. Wszyscy posiadacze informacji niejawnych UE przestrzegają jednolitych praktyk dotyczących klasyfikacji tych informacji i spełniają wspólne normy ochrony dotyczące nadzoru, przekazywania oraz dysponowania informacjami i materiałami wymagającymi ochrony.

Sprawdzanie

16. Przed opuszczeniem obszaru, na którym znajdują się niechronione informacje niejawne UE, do osób sprawujących nad nimi nadzór należy zapewnienie bezpiecznego przechowywania oraz, że uruchomiono wszystkie urządzenia zabezpieczające (zamki, systemy alarmowe itp.). Dalsze niezależne kontrole są przeprowadzane po godzinach pracy.

Bezpieczeństwo budynków

17. Budynki, w których przechowuje się informacje niejawne UE, lub w których mieszczą się ważne systemy łączności i informacji są chronione przed nieupoważnionym dostępem. Charakter środków ochrony przyznanych informacjom niejawnym UE, na przykład: okratowanie okien, zamki w drzwiach, strażnicy przy wejściach, zautomatyzowane systemy kontroli dostępu, kontrole zabezpieczeń i patrole, systemy alarmowe, systemy wykrywające intruzów, psy stróżujące, zależą od:

    a) zaklasyfikowania, ilości i lokalizacji w budynku informacji i materiałów podlegających ochronie;

    b) jakości pojemników ochronnych, zawierających takie informacje i materiały;

    c) fizycznej struktury i lokalizacji budynku.

18. Podobnie charakter środków ochrony przyznanych systemom łączności i informacji zależy od oszacowanej wartości danych aktywów, potencjalnych szkód w przypadku naruszenia bezpieczeństwa, fizycznej struktury i lokalizacji budynku, w którym system jest przechowywany oraz od lokalizacji systemu w budynku.

Plany awaryjne

19. Szczegółowy plan ochrony informacji niejawnych podczas zagrożenia o charakterze lokalnym lub o zasięgu krajowym, przygotowuje się z odpowiednim wyprzedzeniem.

BEZPIECZEŃSTWO INFORMACJI (INFOSEC)

20. INFOSEC dotyczy identyfikacji i stosowania środków bezpieczeństwa w celu ochrony informacji przetworzonych, przechowywanych lub przekazywanych za pośrednictwem systemów łączności i informacji i innych systemów elektronicznych przed utratą poufnego charakteru, integralności lub dostępności, spowodowaną przypadkowo lub w sposób zamierzony. Podejmuje się odpowiednie środki zapobiegania, w celu uniemożliwienia dostępu do informacji UE nieupoważnionym użytkownikom, uniemożliwienia odmowy dostępu do informacji UE upoważnionym użytkownikom,

▼B

oraz uniemożliwienia zniszczenia lub dokonania nieuprawnionej zmiany lub usunięcia informacji UE.

PRZECIWDZIAŁANIE SABOTAŻOWI ORAZ INNYM FORMOM ZŁOŚLIWYCH, UMYŚLNYCH SZKÓD

21. Fizyczne środki ostrożności stosowane w odniesieniu do ochrony ważnych obiektów, służących do przechowywania informacji niejawnych są najlepszymi ochronnymi środkami zabezpieczającymi przeciw sabotażowi oraz złośliwym, umyślnym szkodom; samo postępowanie sprawdzające w odniesieniu do pracowników nie jest skutecznym środkiem zastępczym. Właściwy organ krajowy gromadzi dane dotyczące szpiegostwa, sabotażu, terroryzmu i innych działań wywrotowych.

UDOSTĘPNIENIE INFORMACJI NIEJAWNYCH PAŃSTWOM TRZECIM LUB ORGANIZACJOM MIĘDZYNARODOWYM

22. Decyzję dotyczącą udostępnienia informacji niejawnych pochodzących z Rady państwom trzecim lub organizacjom międzynarodowym podejmuje Rada. Jeżeli źródłem informacji, których udostępnienie jest pożądane, nie jest Rada, Rada najpierw zwraca się o zgodę źródła informacji na takie udostępnienie. Jeżeli źródło informacji nie może zostać ustalone, Rada przejmie na siebie jego odpowiedzialność.

23. Jeżeli Rada otrzymuje informację niejawną od państwa trzeciego, organizacji międzynarodowej lub innej strony trzeciej, udziela takiej informacji ochrony właściwej w odniesieniu do jej klasyfikacji oraz równoważnej normom ustanowionym w niniejszych przepisach dotyczących informacji niejawnych UE, lub takim wyższym normom, jakich może wymagać strona trzecia udostępniająca informację. Możliwe jest zorganizowanie wspólnych kontroli.

24. Powyższe zasady wykonuje się zgodnie ze szczegółowymi przepisami wymienionymi w części II.

▼B

CZĘŚĆ II

SEKCJA I

ORGANIZACJA BEZPIECZEŃSTWA W RADZIE UNII EUROPEJSKIEJ

Sekretarz Generalny/Wysoki Przedstawiciel

1. Sekretarz Generalny/Wysoki Przedstawiciel:

   a) realizuje politykę Rady dotyczącą bezpieczeństwa;

   b) rozpatruje problemy przedstawione mu przez Radę lub jej właściwe organy;

   c) bada kwestie wprowadzania zmian w polityce Rady dotyczącej bezpieczeństwa, przy ścisłej współpracy z Organami Bezpieczeństwa Narodowego (lub innymi właściwymi organami) Państw Członkowskich (zwanymi dalej „OBN"). Dodatek 1 zawiera wykaz tych organów.

2. W szczególności Sekretarz Generalny/Wysoki Przedstawiciel jest odpowiedzialny za:

   a) koordynowanie wszystkich spraw związanych z bezpieczeństwem odnoszących się do działalności Rady;

   b) występowanie z wnioskiem do wszystkich Państwa Członkowskie o ustanowienie centralnego rejestru TRÈS SECRET EU/EU TOP SECRET i wymaganie, w odpowiednim przypadku, aby taki rejestr został ustanowiony w zdecentralizowanych agencjach UE;

   c) zwracanie się do wyznaczonych organów Państw Członkowskich z wnioskiem o przeprowadzenie przez OBN postępowania sprawdzającego w odniesieniu do pracowników zatrudnionych w SGR, zgodnie z sekcją VI;

   d) przeprowadzanie dochodzeń lub zlecanie ich przeprowadzenia w przypadku każdego wycieku informacji niejawnych UE, który, na podstawie dowodów na pierwszy rzut oka, miał miejsce w SGR lub w którejkolwiek ze zdecentralizowanych agencji UE;

   e) występowanie z wnioskiem do właściwych organów bezpieczeństwa dotyczącym wszczęcia dochodzenia w przypadku pojawienia się wycieku informacji niejawnych UE poza SGR lub zdecentralizowanymi agencjami UE, oraz koordynację postępowań, jeżeli w sprawę zaangażowany jest więcej niż jeden organ bezpieczeństwa;

   f) przeprowadzanie, wspólnie i w porozumieniu z zainteresowanym OBN, okresowych kontroli uzgodnień w dziedzinie bezpieczeństwa dotyczących ochrony informacji niejawnych UE w Państwach Członkowskich;

   g) utrzymywanie ścisłej współpracy ze wszystkimi zainteresowanymi organami bezpieczeństwa, w celu osiągnięcia całkowitej koordynacji działań w zakresie bezpieczeństwa;

   h) dokonywanie stałego przeglądu procedur i polityki bezpieczeństwa Rady, oraz, jeżeli jest to niezbędne, przygotowanie właściwych zaleceń. W tym względzie, przedstawia Radzie roczny plan kontroli, opracowany przez Biuro ds. Bezpieczeństwa SGR.

Komitet Rady ds. Bezpieczeństwa

3. Powołuje się Komitet ds. Bezpieczeństwa. Składa się on z przedstawicieli OBN wszystkich Państw Członkowskich. Przewodniczy mu Sekretarz Generalny/Wysoki Przedstawiciel lub jego/jej delegat. Do uczestnictwa w pracach Komitetu mogą również zostać zaproszeni przedstawiciele zdecentralizowanych agencji UE, jeżeli dyskutowane kwestie ich dotyczą.

4. Komitet ds. Bezpieczeństwa zbiera się, zgodnie z instrukcjami Rady, na wniosek Sekretarza Generalnego/Wysokiego Przedstawiciela lub OBN. Komitet ma prawo do badania i oceny wszystkich kwestii dotyczących bezpieczeństwa i odnoszących się do działań Rady, oraz, jeżeli jest to niezbędne, przedstawiania zaleceń Radzie. W odniesieniu do działań SGR,

▼B

Komitet ma prawo formułowania zaleceń w kwestiach dotyczących bezpieczeństwa sekretarzowi generalnemu/wysokiemu przedstawicielowi.

Biuro ds. Bezpieczeństwa Sekretariatu Generalnego Rady

5. W celu wypełnienia obowiązków wymienionych w akapicie 1 i 2, Sekretarz Generalny/Wysoki Przedstawiciel posiada do dyspozycji Biuro ds. Bezpieczeństwa SGR koordynujące, nadzorujące i wykonujące środki bezpieczeństwa.

6. Szef Biura ds. Bezpieczeństwa SGR jest głównym doradcą Sekretarza Generalnego/Wysokiego Przedstawiciela w zakresie spraw dotyczących bezpieczeństwa oraz występuje jako sekretarz Komitetu ds. Bezpieczeństwa. W tym względzie kieruje on uaktualnianiem przepisów dotyczących bezpieczeństwa i koordynuje, wraz z właściwymi organami Państw Członkowskich oraz, gdzie właściwe, wraz z międzynarodowymi organizacjami powiązanymi z Radą porozumieniami dotyczącymi bezpieczeństwa, środki bezpieczeństwa. W tym celu działa on/ona jako oficer łącznikowy.

7. Szef Biura ds. Bezpieczeństwa SGR jest odpowiedzialny za akredytację systemów i sieci IT w SGR. Szef Biura ds. Bezpieczeństwa SGR oraz właściwe OBN wspólnie decydują, w odpowiednim przypadku, w sprawie akredytacji systemów i sieci IT obejmujących SGR, Państwa Członkowskie, zdecentralizowane agencje UE i/lub strony trzecie (państwa lub organizacje międzynarodowe).

Zdecentralizowane agencje UE

8. Każdy dyrektor zdecentralizowanej agencji UE jest odpowiedzialny za wprowadzanie w życie zasad bezpieczeństwa w ramach swojej instytucji. Nominuje on/ona zwykle swojego pracownika jako osobę odpowiedzialną przed nim/nią w tej dziedzinie. Pracownik ten jest mianowany na urzędnika do spraw bezpieczeństwa.

Państwa Członkowskie

9. Każde Państwo Członkowskie wyznacza OBN odpowiedzialny za bezpieczeństwo informacji niejawnych UE ([1]).

10. W ramach administracji każdego z Państw Członkowskich, odpowiednie OBN powinny być odpowiedzialne za:

    a) utrzymanie bezpieczeństwa informacji niejawnych UE przechowywanych przez jakiekolwiek służby krajowe, organ lub instytucję, publiczną lub prywatną, w kraju lub zagranicą;

    b) upoważnienie do ustanowienia rejestrów TRÈS SECRET UE/UE TOP SECRET (to upoważnienie może zostać przekazane urzędnikowi ds. kontroli centralnego rejestru TRÈS SECRET UE/UE TOP SECRET);

    c) okresową kontrolę uzgodnień w dziedzinie bezpieczeństwa dotyczących ochrony informacji niejawnych UE;

    d) zapewnienie, że wszyscy obywatele, jak również obcokrajowcy, zatrudnieni w służbach krajowych, organach lub instytucjach, którzy mogą mieć dostęp do rejestrów TRÈS SECRET EU/EU TOP SECRET, SECRET UE i CONFIDENTIEL UE podlegają postępowaniu sprawdzającemu;

    e) opracowanie takich planów bezpieczeństwa, jakie są niezbędne w celu uniemożliwienia dostania się informacji niejawnych UE w niepowołane ręce.

Wspólne kontrole bezpieczeństwa

11. Okresowe kontrole uzgodnień w dziedzinie bezpieczeństwa dotyczące ochrony informacji niejawnych EU w SGR i w stałych przedstawicielstwach Państw Członkowskich w Unii Europejskiej, jak również w siedzibach

([1]) Wykaz OBN odpowiedzialnych za bezpieczeństwo informacji niejawnych UE znajduje się w dodatku 1.

▼B

Państw Członkowskich w budynkach Rady, są przeprowadzane wspólnie, za obopólną zgodą ([1]), przez Biuro ds. Bezpieczeństwa SGR oraz dany OBN.

12. Okresowe kontrole uzgodnień w dziedzinie bezpieczeństwa dotyczących ochrony informacji niejawnych UE w zdecentralizowanych agencjach UE, są przeprowadzane przez Biuro ds. Bezpieczeństwa SGR lub, na wniosek sekretarza generalnego, przez OBN przyjmującego Państwa Członkowskiego.

([1]) Bez uszczerbku dla Konwencji wiedeńskiej z 1961 r. o stosunkach dyplomatycznych.

▼B

SEKCJA II

KLASYFIKACJE I OZNACZENIA

POZIOMY KLASYFIKACJI ([1])

Informacje są klasyfikowane według następujących klauzul:

1. TRÈS SECRET UE/UE TOP SECRET: tę klauzulę stosuje się wyłącznie do informacji i materiałów, których nieuprawnione ujawnienie mogłoby spowodować wyjątkowo poważną szkodę dla podstawowych interesów Unii Europejskiej lub jednego lub kilku jej Państw Członkowskich;

2. SECRET UE: tę klauzulę stosuje się do informacji i materiałów, których nieuprawnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom Unii Europejskiej lub jednego lub kilku jej Państw Członkowskich;

3. CONFFIDENTIEL UE: tę klauzulę stosuje się do informacji i materiałów, których nieuprawnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii Europejskiej lub jednego lub kilku jej Państw Członkowskich;

4. RESTREINT UE: tę klauzulę stosuje się do informacji i materiałów, których nieuprawnione ujawnienie mogłoby być niekorzystne dla interesów Unii Europejskiej lub jednego lub kilku jej Państw Członkowskich.

OZNACZENIA

5. Oznaczenie zastrzegające może być używane do określenia dziedziny objętej dokumentem lub szczególnego podziału na zasadzie „potrzeby niezbędnej wiedzy”.

6. Oznaczenie ESDP/PESD jest stosowane w odniesieniu do dokumentów i ich kopii dotyczących bezpieczeństwa i obrony Unii lub jednego lub kilku jej Państw Członkowskich, bądź dotyczących wojskowego lub nie-wojskowego zarządzania kryzysami.

7. Niektóre dokumenty odnoszące się do systemów technologii informacyjnych (IT) mogą nosić dodatkowe oznaczenia powodujące zastosowanie dodatkowych środków bezpieczeństwa określonych we właściwych rozporządzeniach.

PRZYZNAWANIE KLAUZULI I OZNACZEŃ

8. Klasyfikacje i oznaczenia stosuje się w sposób następujący:

   a) na dokumentach RESTREINT UE – przy pomocy urządzeń mechanicznych lub elektronicznych;

   b) na dokumentach CONFIDENTIEL UE – przy pomocy urządzeń mechanicznych oraz ręcznie lub poprzez nadruk na zarejestrowanych drukach, uprzednio ostemplowanych;

   c) na dokumentach SECRET/TRÈS SECRET EU/EU TOP SECRET – przy pomocy urządzeń mechanicznych oraz ręcznie.

([1]) Tabela porównawcza stopni tajności stosowanych w UE, NATO, UZE i Państwach Członkowskich znajduje się w dodatku 2.

▼B

SEKCJA III

ZARZĄDZANIE W ZAKRESIE KLASYFIKOWANIA

1. Informacje poddaje się klasyfikacji jedynie wtedy, gdy jest to niezbędne. Zaklasyfikowanie jest wyraźnie i poprawnie wskazane i jest utrzymywane jedynie tak długo, jak długo informacja wymaga ochrony.

2. Odpowiedzialność za klasyfikowanie informacji oraz za późniejsze obniżanie klasyfikacji lub jej deklasyfikację ([1]) spoczywa wyłącznie na autorze informacji.

   Urzędnicy i inni pracownicy SGR klasyfikują, obniżają klasyfikację lub deklasyfikują informacje zgodnie z instrukcją lub za zgodą ich Dyrektora-Generalnego.

3. Szczegółowe procedury dotyczące traktowania dokumentów niejawnych zostały sformowane w taki sposób, aby zapewnić, że podlegają one ochronie właściwej do charakteru informacji, które zawierają.

4. Liczba osób upoważnionych do tworzenia dokumentów TRÈS SECRET UE/EU TOP SECRET jest ograniczona do minimum, a nazwiska tych osób umieszcza się na liście sporządzonej przez SGR, każde Państwo Członkowskie, oraz w odpowiednim przypadku, przez każdą ze zdecentralizowanych agencji UE.

STOSOWANIE KLASYFIKACJI

5. Klasyfikację dokumentu ustala się w zależności od poziomu sensytywności jego zawartości, zgodnie z definicją podaną w sekcji II ust. 1–4. Ważne jest, aby klasyfikacja została zastosowana poprawnie i z umiarem. Stosuje się to w szczególności w odniesieniu do klauzuli TRÈS SECRET UE/EU TOP SECRET.

6. Autor dokumentu, który podlega klasyfikacji, ma na uwadze przepisy określone powyżej oraz powstrzymuje się przed zawyżeniem lub zaniżeniem klasyfikacji.

   Chociaż wyższa klasyfikacja może, na pierwszy rzut oka, wydawać się gwarancją większej ochrony, jednak rutynowe zawyżanie klasyfikacji może spowodować spadek zaufania do ważności systemu klasyfikowania.

   Z drugiej strony, nie zaniża się klasyfikacji dokumentów w celu uniknięcia ograniczeń związanych z ochroną.

   Praktyczny przewodnik po klasyfikacji znajduje się w dodatku 3.

7. Poszczególne strony, ustępy, sekcje, załączniki, dodatki, załączone dokumenty i uzupełnienia danego dokumentu mogą wymagać różnych klasyfikacji i zostają odpowiednio oznaczone. Za klasyfikację dokumentu jako całości uznaje się najwyższą klasyfikację nadaną jednej z jego części.

8. Zaklasyfikowanie listów lub notatek zawierających załączniki jest na takim poziomie jak najwyższa klasyfikacja nadana ich załącznikom. Autor powinien wyraźnie wskazać poziom, na który powinno się je klasyfikować po oddzieleniu od załączników.

OBNIŻENIE KLASYFIKACJI I DEKLASYFIKACJA

9. Obniżenia klasyfikacji lub deklasyfikacji dokumentów niejawnych UE można dokonać jedynie za zgodą autora, oraz, jeżeli to niezbędne, po uzgodnieniu z innymi zainteresowanymi stronami. Obniżenie klasyfikacji lub deklasyfikacja zostają pisemnie potwierdzone. Instytucja, będąca źródłem dokumentu, Państwo Członkowskie, biuro, organizacja sukcesyjna lub organ wyższy jest odpowiedzialny za powiadomienie adresatów o zmianie, a te z kolei są odpowiedzialne za powiadomienie o zmianie dalszych adresatów, którym przesłano dokument lub jego kopię.

([1]) Obniżenie klasyfikacji (déclassement) oznacza obniżenie poziomu klasyfikacji; deklasyfikacja (déclassification) oznacza zniesienie klauzuli.

▼B

10. Jeżeli jest to możliwe, autorzy określają na dokumentach niejawnych datę lub okres, z upływem których można obniżyć klasyfikację lub zdeklasyfikować zawartość dokumentu. W przeciwnym razie, dokonują przeglądu dokumentów przynajmniej co pięć lat, w celu uzyskania pewności, że pierwotnie przyznana klasyfikacja jest nadal konieczna.

▼B

SEKCJA IV

BEZPIECZEŃSTWO FIZYCZNE

PRZEPISY OGÓLNE

1. Głównym celem środków fizycznego bezpieczeństwa jest uniemożliwienie uzyskania dostępu do informacji i/lub materiałów niejawnych UE osobie nieupoważnionej.

WYMOGI BEZPIECZEŃSTWA

2. Wszystkie siedziby, strefy, budynki, biura, pomieszczenia, systemy łączności i informacji itd., w których przechowywane są i/lub przetwarzane informacje i materiały niejawne UE, podlegają ochronie przy zastosowaniu właściwych środków bezpieczeństwa fizycznego.

3. Przy określaniu niezbędnego stopnia ochrony bezpieczeństwa fizycznego, uwzględnia się wszystkie stosowne czynniki, takie jak:

   a) klasyfikację informacji i/lub materiałów;

   b) ilość i formę (np. kopia trwała, komputerowe nośniki danych) przechowywanych informacji;

   c) ocenę lokalnego zagrożenia dokonaną przez służby wywiadowcze, na jakie narażone jest Unia Europejska, Państwa Członkowskie i/lub inne instytucje lub strony trzecie przechowujące informacje niejawne UE, mianowicie sabotażu, terroryzmu i innych działań wywrotowych i/lub przestępczych.

4. Zastosowane środki bezpieczeństwa fizycznego są przeznaczone do:

   a) uniemożliwienia, dyskretnego lub dokonanego przy użyciu siły, wtargnięcia intruza;

   b) zapobiegania, udaremnienia i ujawniania działań nielojalnych pracowników (w tym szpiegów);

   c) zapobiegania, by urzędnicy i inni pracownicy SGR, służb rządowych Państw Członkowskich i/lub innych instytucji lub stron trzecich, którzy nie mają potrzeby niezbędnej wiedzy, mieli dostęp do informacji niejawnych UE.

ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO

Strefy bezpieczeństwa

5. Strefy, gdzie informacje oznaczone klauzulą CONFIDENTIEL EU lub wyższą są przetwarzane i przechowywane posiadają taką organizację i strukturę, aby odpowiadać jednej z poniższych charakterystyk:

   a) Strefa bezpieczeństwa klasy I: strefa, gdzie dokumenty oznaczone klauzulą CONFIDENTIEL lub wyższą są przetwarzane i przechowywane w taki sposób, że wejście do strefy, w każdym praktycznie celu, stanowi dostęp do informacji niejawnych. Taka strefa wymaga:

      i) wyraźnie określonych i chronionych granic, na których wszystkie wejścia i wyjścia są kontrolowane;

      ii) systemu kontroli wejść, który dopuszcza tylko osoby należycie sprawdzone i specjalnie upoważnione do wejścia na teren strefy;

      iii) specyfikacji klasyfikacji informacji niejawnych, zwykle przechowywanych w strefie, tzn. informacji, do których uzyskuje się dostęp wraz z wejściem do strefy.

   b) Strefa bezpieczeństwa klasy II: strefa, gdzie dokumenty oznaczone klauzulę CONFIDENTIEL EU lub wyżej są przetwarzane i przechowywane w taki sposób, że mogą być chronione przed dostępem osób nieupoważnionych środkami wewnętrznie ustanowionych kontroli, tzn. są to obiekty posiadające biura, w których dokumenty oznaczone klauzulą CONFIDENTIEL EU lub wyżej są regularnie przetwarzane i przechowywane. Taka strefa wymaga:

▼B

i) wyraźnie określonych i chronionych granic, na których wszystkie wejścia i wyjścia są kontrolowane;

ii) systemu kontroli wejść, który dopuszcza bez eskorty jedynie osoby należycie sprawdzone i specjalnie upoważnione do wejścia na teren strefy. W odniesieniu do wszystkich innych osób, zostają wprowadzone przepisy wymagające posiadania eskorty lub objęcia równoważną kontrolą, w celu uniemożliwienia nieupoważnionego dostępu do informacji niejawnych UE i niekontrolowanego wejścia do stref podlegających kontrolom bezpieczeństwa technicznego.

Te strefy, w których pracownicy nie pracują w systemie całodobowym, są poddawane kontroli niezwłocznie po normalnych godzinach pracy w celu zapewnienia, że informacje niejawne UE są właściwie zabezpieczone.

Strefa administracyjna

6. Wokół stref bezpieczeństwa klasy I i II lub na drogach dojazdowych do nich można ustanowić strefę administracyjną o niższym poziomie zabezpieczeń. Taka strefa wymaga widocznie oznaczonych granic, na których istnieje możliwość kontroli pracowników i pojazdów. W strefach administracyjnych są przetwarzane i przechowywane jedynie informacje RESTREINT UE.

Kontrole wejść i wyjść

7. Wejście na teren stref bezpieczeństwa klasy I i klasy II podlega kontroli na podstawie przepustki lub systemu rozpoznawania osób. Ustanowiony zostaje również system sprawdzania gości mający na celu uniemożliwienie nieupoważnionego dostępu do informacji niejawnych UE. System przepustek może być wspomagany systemem automatycznej identyfikacji, który jest traktowany jako uzupełnienie, ale nie całkowite zastąpienie strażników. Zmiana oceny stopnia zagrożenia może pociągnąć za sobą wzmocnienie środków kontroli wejścia i wyjścia, na przykład podczas wizyt ważnych osobistości.

Patrole strażników

8. Patrole w strefach bezpieczeństwa klasy I i II odbywają się poza normalnymi godzinami pracy i maja na celu ochronę aktywów UE przed ujawnieniem, zniszczeniem lub utratą. Częstotliwość patroli będzie ustalana zależnie od warunków lokalnych, ale wytyczną jest, aby były przeprowadzane co dwie godziny.

Pojemniki bezpieczeństwa i wzmocnione pomieszczenia

9. Do przechowywania informacji niejawnych UE są wykorzystywane trzy klasy pojemników:

— Klasa A: pojemniki zatwierdzone na szczeblu krajowym do przechowywania informacji TRÈS SECRET UE/UE TOP SECRET na terenie strefy bezpieczeństwa klasy I i II,

— Klasa B: pojemniki zatwierdzone na szczeblu krajowym do przechowywania informacji SECRET UE i CONFIDENTIEL UE na terenie strefy bezpieczeństwa klasy I i II,

— Klasa C: mebel biurowy nadający się do przechowywania jedynie informacji RESTREINT UE.

10. W odniesieniu do wzmocnionych pomieszczeń zbudowanych na terenie strefy bezpieczeństwa klasy I i klasy II, i w odniesieniu do wszystkich stref bezpieczeństwa klasy I, gdzie informacje oznaczone klauzulą CONFIDENTIEL UE i wyżej są przechowywane na otwartych półkach lub znajdują się na wykresach, mapach itd., ściany, podłogi, sufity, drzwi z zamkami są zatwierdzane przez OBN jako zapewniające równoważną ochronę do klasy pojemnika ochronnego zatwierdzonego do przechowywania informacji o tej samej klasyfikacji.

Zamki

11. Zamki używane do zamykania pojemników ochronnych i wzmocnionych pomieszczeń, w których przechowywane są informacje niejawne UE spełniają następujące normy:

▼B

— Grupa A: zatwierdzone na szczeblu krajowym dla pojemników klasy A,

— Grupa B: zatwierdzone na szczeblu krajowym dla pojemników klasy B,

— Grupa C: odpowiednie jedynie dla mebli biurowych klasy C.

Kontrola kluczy i kombinacji szyfrowych

12. Klucze do pojemników ochronnych nie mogą być wynoszone poza budynek biurowy. Kombinacje szyfrowe do pojemników ochronnych są zapamiętywane przez osoby, które muszą je znać. W celu użycia w nagłym wypadku, urzędnik do spraw bezpieczeństwa danej instytucji jest odpowiedzialny za przechowywanie kluczy zapasowych i wszystkich kombinacji szyfrowych w formie pisemnej; te ostatnie są przechowywane w oddzielnych, opieczętowanych i nieprzezroczystych kopertach. Używane klucze, zapasowe klucze bezpieczeństwa oraz kombinacje szyfrowe są przechowywane w oddzielnych pojemnikach ochronnych. Te klucze i kombinacje szyfrowe powinny podlegać ochronie niemniej rygorystycznej niż materiały, do których umożliwiają dostęp.

13. Znajomość kombinacji szyfrowych do pojemników ochronnych jest ograniczona do możliwie jak najmniejszej ilości osób. Kombinacje szyfrowe są zmieniane:

a) w przypadku otrzymania nowego pojemnika;

b) w każdym przypadku, gdy następuje zmiana pracowników;

c) w każdym przypadku, gdy następuje ujawnienie lub podejrzenie ujawnienia;

d) najlepiej w odstępach sześciu miesięcy, lub co najmniej raz na 12 miesięcy.

Urządzenia do wykrywania intruzów

14. Jeżeli systemy alarmowe, telewizja przemysłowa i inne urządzenia elektryczne są wykorzystywane do ochrony informacji niejawnych UE, udostępnia się awaryjne źródło energii elektrycznej zapewniające ciągłą obsługę systemu, jeżeli nastąpi przerwa w dostawie energii z głównego źródła zasilania. Innym podstawowym wymogiem jest zapewnienie, by nieprawidłowe działanie lub manipulacja przy takim systemie powodowały uruchomienie alarmu lub w inny niezawodny sposób ostrzegały pracowników nadzoru.

Zatwierdzone wyposażenie

15. OBN utrzymują aktualne wykazy, sporządzane we własnym zakresie lub pochodzącego ze źródeł dwustronnych, rodzajów i modeli wyposażenia bezpieczeństwa, które zatwierdziły do bezpośredniej lub pośredniej ochrony informacji niejawnych w różnych szczególnych okolicznościach i warunkach. Biuro ds. Bezpieczeństwa SGR utrzymuje podobny wykaz, oparty, między innymi, na informacjach pochodzących z OBN. Zdecentralizowane agencje UE, przed dokonaniem zakupu takiego wyposażenia, zasięgają opinii Biura ds. Bezpieczeństwa SGR i odpowiednio OBN ich przyjmującego Państw Członkowskiego.

Fizyczna ochrona urządzeń kopiujących i telefaksowych

16. Urządzenia kopiujące i telefaksowe są chronione fizycznie w zakresie niezbędnym do zapewnienia, że wyłącznie osoby upoważnione ich używają oraz, że wszystkie produkty niejawne podlegają właściwym kontrolom.

OCHRONA PRZECIWKO PODGLĄDOWI I PODSŁUCHOWI

Podgląd

17. Podejmuje się wszelkie właściwe środki, zarówno w dzień jak i w nocy, w celu zapewnienia, że informacje niejawne UE nie są oglądane, nawet przypadkowo, przez jakąkolwiek osobę nieupoważnioną.

Podsłuch

▼B

18. Pomieszczenia biurowe lub strefy, w których regularnie omawia się informacje oznaczone klauzulą SERCRET UE lub wyżej, są chronione przed biernym i czynnym podsłuchem, w przypadku gdy istnieje takie zagrożenie. Ocena stopnia zagrożenia takimi aktami jest obowiązkiem właściwego organu bezpieczeństwa po konsultacji, gdy to niezbędne z OBN.

19. W celu ustalenia środków ochrony, jakie należy podjąć w pomieszczeniach narażonych na bierny podsłuch (np. izolacja ścian, drzwi, podłóg i sufitów, pomiar emisji dźwięku) i czynny podsłuch (np. poszukiwanie mikrofonów), Biuro ds. Bezpieczeństwa SGR może wnioskować o pomoc ze strony ekspertów z OBN. Urzędnik do spraw bezpieczeństwa zdecentralizowanych agencji UE może wnioskować o przeprowadzenie kontroli technicznych przez Biuro ds. Bezpieczeństwa SGR i/lub o pomoc ze strony ekspertów z OBN.

20. Podobnie, jeśli wymagają tego okoliczności, urządzenia telekomunikacyjne oraz wyposażenie elektryczne lub elektroniczne wyposażenie biura wszelkiego rodzaju, używane podczas posiedzeń na poziomie SECRET UE lub wyższym, mogą, na wniosek właściwego urzędnika do spraw bezpieczeństwa, zostać poddane kontroli przez technicznych specjalistów do spraw bezpieczeństwa OBN.

STREFY BEZPIECZEŃSTWA TECHNICZNEGO

21. Niektóre strefy mogą być wyznaczone na strefy bezpieczeństwa technicznego. Wykonuje się specjalną kontrolę przy wjeździe. Takie strefy są zamykane przy użyciu zatwierdzonych metod, jeżeli nikt w nich nie przebywa, i wszystkie klucze są traktowane jako klucze bezpieczeństwa. Takie strefy podlegają regularnym fizycznym kontrolom, które będą podejmowane w następstwie nieupoważnionego wejścia lub podejrzenia o takim wejściu.

22. W celu kontroli przemieszczania, przechowuje się szczegółowy spis wyposażenia i umeblowania. Żadnego elementu umeblowania lub wyposażenia nie można wnieść na teren takiej strefy, zanim nie zostanie poddany starannej kontroli dokonanej przez specjalnie przeszkolony personel bezpieczeństwa, wyznaczony do wykrywania wszelkich urządzeń podsłuchowych. Zgodnie z ogólnie przyjętą zasadą, powinno się unikać instalowania linii komunikacyjnych w strefach bezpieczeństwa technicznego.

▼B

SEKCJA V

OGÓLNE REGUŁY DOTYCZĄCE ZASADY POTRZEBY NIEZBĘDNEJ WIEDZY ORAZ POSTĘPOWANIE SPRAWDZAJĄCE

1. Do dostępu do informacji niejawnych UE zostaną upoważnione jedynie osoby, które mają potrzebę uzyskania wiedzy do wykonywania swoich obowiązków lub misji. Do dostępu do informacji TRÈS SECRET UE/EU TOP SECRET i CONFIDENTIEL UE zostaną upoważnione jedynie osobom, które posiadają właściwe poświadczenie bezpieczeństwa.

2. Odpowiedzialność za określenie „potrzeby niezbędnej wiedzy" zależnie od wymogów zadań, spoczywa na SGR, zdecentralizowanych agencjach UE, urzędzie lub wydziale Państwa Członkowskiego, w którym zainteresowana osoba ma zostać zatrudniona.

3. Za przeprowadzenie postępowania sprawdzającego pracownika na podstawie właściwych stosowanych procedur, odpowiedzialny jest jego pracodawca. W odniesieniu do urzędników i innych pracowników SGR, procedura postępowania sprawdzającego jest przewidziana w sekcji VI.

   Wynikiem powyższego jest wydanie „poświadczenia bezpieczeństwa" określającego stopień tajności informacji, do których dostęp może mieć sprawdzona osoba oraz datę wygaśnięcia jego ważności.

   Poświadczenie bezpieczeństwa dla danej klasyfikacji może dać również jego posiadaczowi dostęp do informacji o niższej klasyfikacji.

4. Osoby inne niż urzędnicy lub inni pracownicy SGR lub Państw Członkowskich, na przykład członkowie, urzędnicy lub pracownicy instytucji UE, z którymi dyskusja może być niezbędna, lub którym niezbędne jest pokazanie informacji niejawnych UE, muszą posiadać poświadczenie bezpieczeństwa w odniesieniu do informacji niejawnych UE i zostać powiadomieni o ich odpowiedzialności za bezpieczeństwo. Ta sama reguła jest stosowana, w podobnych okolicznościach, do zewnętrznych wykonawców, ekspertów i konsultantów.

SZCZEGÓLNE REGUŁY DOTYCZĄCE DOSTĘPU DO INFORMACJI TRÈS SECERT UE/EU TOP SECRET

5. Wszystkie osoby, które mają mieć dostęp do informacji TRÈS SECRET UE/EU TOP SECRET muszą uprzednio zostać sprawdzone w celu uzyskania dostępu do takich informacji.

6. Wszystkie osoby, które są zobowiązane do posiadania dostępu do informacji TRÈS SECRET UE/EU TOP SECRET zostają wyznaczone przez szefa ich służby, a ich nazwiska są przechowywane w rejestrach TRÈS SECRET UE/EU TOP SECRET.

7. Przed uzyskaniem dostępu do informacji TRÈS SECRET UE/EU TOP SECRET, wszystkie osoby podpisują oświadczenie stwierdzające, że zostały powiadomione o procedurach Rady dotyczących bezpieczeństwa oraz że w pełni rozumieją swoją szczególną odpowiedzialność za zabezpieczenie informacji TRÈS SECRET UE/EU TOP SECRET i konsekwencje przewidziane w przepisach UE i prawa krajowego oraz przepisach administracyjnych, w przypadku przedostania się informacji niejawnych w ręce osób nieupoważnionych, na skutek działania rozmyślnego lub wskutek zaniedbania.

8. W przypadku osób posiadających dostęp do informacji TRÈS SECRET UE/EU TOP SECRET podczas posiedzeń itp., właściwy urzędnik ds. kontroli służby lub organu, w którym dana osoba jest zatrudniona, powiadamia organ zwołujący posiedzenie, że zainteresowane osoby posiadają takie upoważnienie.

9. Nazwiska wszystkich osób, które przestają być zatrudnione na stanowiskach wymagających dostępu do informacji TRÈS SECRET UE/UE TOP SECRET są usuwane z listy TRÈS SECRET UE/EU TOP SECRET. Dodatkowo, należy zwrócić uwagę wszystkich tych osób na ich szczególną odpowiedzialność za zabezpieczenie informacji TRÈS SECRET UE/EU TOP SECRET. Podpisują one także deklarację stwierdzającą, że nigdy nie

▼B

użyją i nie przekażą nikomu posiadanych informacji TRÈS SECRET UE/EU TOP SECRET.

SZCZEGÓLNE REGUŁY DOTYCZĄCE DOSTĘPU DO INFORMACJI SECRET UE I CONFIDENTIEL UE

10. Wszystkie osoby, które mają mieć dostęp do informacji SECRET UE lub CONFIDENTIEL UE muszą uprzednio zostać sprawdzone w sposób odpowiedni do właściwego stopnia tajności.

11. Wszystkie osoby, które mają mieć dostęp do informacji SECRET UE lub CONFIDENTIEL UE zapoznają się z właściwymi przepisami bezpieczeństwa i są powiadamiane o konsekwencjach zaniedbań.

12. W przypadku osób posiadających dostęp do informacji oznaczonych klauzulą SECRET UE lub CONFIDENTIEL UE w czasie posiedzeń itp., właściwy urzędnik ds. kontroli służby lub organu, w którym dana osoba jest zatrudniona, powiadamia organ zwołujący posiedzenie, że zainteresowane osoby posiadają takie upoważnienie.

SZCZEGÓLNE REGUŁY DOTYCZĄCE DOSTĘPU DO INFORMACJI RESTREINT UE

13. Osoby posiadające dostęp do informacji RESTREINT UE zostaną powiadomione o niniejszych przepisach bezpieczeństwa i o konsekwencjach zaniedbań.

PRZENIESIENIA

14. Jeżeli pracownik zostaje przeniesiony ze stanowiska wymagającego korzystanie z materiałów niejawnych UE, registratura nadzoruje przeniesienie tych materiałów od urzędnika odchodzącego do urzędnika przychodzącego.

INSTRUKCJE SPECJALNE

15. Osoby, które są zobowiązane do przetwarzania informacji niejawnych UE, powinny być, podczas pierwszego obejmowania obowiązków, a następnie okresowo, powiadomione o:

    a) zagrożeniu dla bezpieczeństwa wynikającym z prowadzenia niedyskretnych rozmów;

    b) środkach ostrożności, jaką należy podejmować w kontaktach z prasą;

    c) zagrożeniu, jakie wiąże się z działalnością służb wywiadowczych, których celem są Unia Europejska i Państwa Członkowskie w odniesieniu do informacji niejawnych i działalności UE;

    d) obowiązku niezwłocznego sprawozdawania właściwym organom bezpieczeństwa o każdym działaniu lub posunięciu, które wzbudzają podejrzenia o działalności szpiegowskiej lub o każdych niezwykłych okolicznościach dotyczących bezpieczeństwa.

16. Wszystkie osoby narażone na częsty kontakt z przedstawicielami państw, których służby wywiadowcze interesują się Unią Europejską i Państwami Członkowskimi w odniesieniu do niejawnych informacji i działalności UE, są powiadamiane o znanych technikach stosowanych przez różne służby wywiadowcze.

17. Nie istnieją żadne przepisy Rady w zakresie bezpieczeństwa dotyczące prywatnych podróży do dowolnego miejsca przeznaczenia pracowników upoważnionych do dostępu do informacji niejawnych UE. Jednakże właściwe organy bezpieczeństwa powiadamiają urzędników i innych pracowników przed nimi odpowiedzialnych o przepisach dotyczących podróży, którym mogą podlegać. Obowiązkiem urzędników ds. bezpieczeństwa będzie organizacja zebrań utrwalających wiedzę o tych specjalnych instrukcjach dla pracowników.

▼B

SEKCJA VI

PROCEDURY SPRAWDZAJĄCE W ZAKRESIE BEZPIECZEŃSTWA DLA URZĘDNIKÓW SGR I INNYCH PRACOWNIKÓW

1. Jedynie urzędnicy i inni pracownicy SGR, lub osoby pracujące w SGR, które ze względu na swoje obowiązki oraz z uwagi na wymagania służbowe, muszą posiadać wiedzę zawartą w niejawnych informacjach przechowywanych przez Radę lub z niej korzystać, posiadają dostęp do takich informacji.

2. W celu posiadania dostępu do informacji oznaczonych klauzulą „TRÈS SECRET UE/EU TOP SECRET", „SECRET UE i CONFIDENTIEL UE", osoby określone w ust. 1 muszą zostać upoważnione zgodnie z procedurą określoną w ust. 4 i 6.

3. Upoważnienie przyznaje się tylko osobom, które zostały poddane procedurze sprawdzającej w zakresie bezpieczeństwa przez właściwe organy krajowe Państw Członkowskich (OBN) zgodnie z procedurą określoną w ust. 6–10.

4. Organ mianujący w rozumieniu art. 2 pierwszy akapit regulaminu pracowniczego jest odpowiedzialny za przyznanie upoważnienia, określonego w ust. 1, 2 i 3

   Organ mianujący przyznaje upoważnienie po uzyskaniu opinii właściwych organów krajowych Państwa Członkowskiego na podstawie procedury sprawdzającej w zakresie bezpieczeństwa przeprowadzonej zgodnie z ust. 6–12.

5. Upoważnienie, które jest ważne przez okres pięciu lat, nie może przekraczać czasu wykonywania zadań, na których podstawie zostało przyznane. Może zostać odnowione przez organ mianujący zgodnie z procedurą określoną w ust. 4.

   Upoważnienie zostaje wycofane przez organ mianujący, w przypadku gdy uznaje on, że istnieją ku temu uzasadnione podstawy. O każdej decyzji o wycofaniu upoważnienia powiadamia się właściwy organ krajowy oraz zainteresowaną osobę, która może wystąpić z wnioskiem o wysłuchanie przez organ mianujący.

6. Celem procedury sprawdzającej w zakresie bezpieczeństwa jest ustalenie, że nie ma przeszkód na zezwolenie danej osobie na dostęp do informacji niejawnych przechowywanych przez Radę.

7. Procedura sprawdzająca w zakresie bezpieczeństwa jest przeprowadzana przy udziale zainteresowanej osoby, oraz na wniosek organu mianującego, przez właściwe organy krajowe Państwa Członkowskiego, którego obywatelem jest osoba ubiegająca się o upoważnienie. Jeżeli zainteresowana osoba ma miejsce zamieszkania na terytorium innego Państwa Członkowskiego, odnośne organy krajowe mogą zapewnić współpracę z organami państwa zamieszkania.

8. Jednym z wymogów procedury sprawdzającej w zakresie bezpieczeństwa jest wypełnienie formularza osobowego.

9. Organ mianujący określa w swoim wniosku rodzaj i poziom zaklasyfikowanej informacji, które zostają udostępnione danej osobie, tak aby właściwe organy krajowe mogły przeprowadzić procedurę sprawdzającą w zakresie bezpieczeństwa i wydać właściwą opinię dotyczącą stopnia upoważnienia, który mógłby zostać przyznany danej osobie.

10. Cały proces procedury sprawdzającej w zakresie bezpieczeństwa wraz z uzyskanymi wynikami podlega właściwym regułom i przepisom obowiązującym w danym Państwie Członkowskim, włączając te dotyczące odwołań.

11. W przypadku gdy właściwe organy krajowe Państwa Członkowskiego wydają pozytywną opinię, organ mianujący może przyznać upoważnienie zainteresowanej osobie.

▼B

12. O negatywnej opinii wydanej przez właściwe organy krajowe powiadamia się zainteresowaną osobę, która może wystąpić z wnioskiem o wysłuchanie przez organ mianujący. Organ mianujący, jeżeli uzna to za konieczne, może wystąpić do właściwych organów krajowych o dostarczenie wszelkich dalszych wyjaśnień. Jeżeli negatywna opinia zostaje potwierdzona, upoważnienia się nie przyznaje.

13. Wszystkie osoby, którym przyznano upoważnienie w rozumieniu ust. 4 i 5, w chwili przyznania upoważnienia, o następnie w regularnych odstępach czasu, otrzymują wszelkie niezbędne instrukcje dotyczące ochrony informacji niejawnych i środków zapewniających taką ochronę. Takie osoby podpisują oświadczenie stwierdzające otrzymanie instrukcji i zobowiązanie do ich przestrzegania.

14. Organ mianujący podejmuje wszelkie niezbędne środki w celu wykonania przepisów niniejszej sekcji, szczególnie w odniesieniu do zasad regulujących dostęp do list upoważnionych osób.

15. W drodze wyjątku, jeśli wymagają tego obowiązki służbowe, organ właściwy do udzielenia może, po powiadomieniu właściwych organów krajowych i pod warunkiem braku ich reakcji w ciągu miesiąca, przyznać tymczasowe upoważnienie na okres nieprzekraczający sześciu miesięcy, w zależności od wyników procedury sprawdzającej w zakresie bezpieczeństwa określonej w ust. 7.

16. Prowizoryczne i tymczasowe upoważnienia, przyznane w ten sposób, nie dają prawa dostępu do informacji TRÈS SECRET UE/EU TOP SECRET; taki dostęp jest ograniczony do urzędników, którzy zostali skutecznie poddani procedurze sprawdzającej w zakresie bezpieczeństwa z wynikiem pozytywnym, zgodnie z ust. 7. Do czasu uzyskania wyniku procedury sprawdzającej w zakresie bezpieczeństwa, urzędnicy, którzy zgodnie z wnioskiem mają być poddani takiej procedurze na poziomie TRÈS SECRET UE/EU TOP SECRET, mogą zostać upoważnieni prowizorycznie i tymczasowo do dostępu do informacji zaklasyfikowanej do poziomu łącznie z SECRET UE.

▼B

SEKCJA VII

PRZYGOTOWANIE, ROZPOWSZECHNIANIE, PRZEKAZYWANIE, PRZECHOWYWANIE ORAZ NISZCZENIE MATERIAŁÓW NIEJAWNYCH UE

Spis treści

Przepisy ogólne	
Rozdział I	Przygotowanie i rozpowszechnianie dokumentów niejawnych UE
Rozdział II	Przekazywanie dokumentów niejawnych UE
Rozdział III	Elektryczne i inne środki technicznego przekazu
Rozdział IV	Dodatkowe egzemplarze, tłumaczenia oraz wyciągi z dokumentów niejawnych UE
Rozdział V	Przeglądy i kontrole, przechowywanie i niszczenie dokumentów niejawnych UE
Rozdział VI	Szczególne reguły mające zastosowanie do dokumentów przeznaczonych dla Rady

▼B

Przepisy ogólne

Niniejsza sekcja wyszczególnia środki odnoszące się do przygotowania, rozpowszechniania, przekazywania, przechowywania i niszczenia dokumentów niejawnych UE, jak określono w ust. 3 lit. a) podstawowych zasad i minimalnych norm bezpieczeństwa, wymienionych w części I niniejszego załącznika. Należy je wykorzystywać jako odniesienie do przyjęcia tych środków dla innych materiałów niejawnych UE, zgodnie z ich rodzajem i na zasadzie jednostkowych przypadków.

Rozdział I

Przygotowanie i rozpowszechnianie dokumentów niejawnych UE

PRZYGOTOWANIE

1. Klasyfikacja UE i oznaczenia są stosowane jak ustanowiono w sekcji II i są umieszczane centralnie na dole i na górze każdej strony, a każda strona jest ponumerowana. Każdy dokument niejawny UE jest opatrzony numerem referencyjnym oraz datą. W przypadku dokumentów TRÈS SECRET UE/EU TOP SECRET i SECRET UE ten numer referencyjny umieszcza się na każdej stronie. Jeżeli dokument jest rozpowszechniany w kilku egzemplarzach, każdy z nich zawiera numer egzemplarza, który umieszcza się na pierwszej stronie, łącznie z całkowitą liczbą stron. Wszystkie załączniki i dołączenia są wymienione na pierwszej stronie dokumentu oznaczonego klauzulą CONFIDENTIEL UE i wyższą.

2. Dokumenty oznaczone klauzulą CONFIDENTIEL UE i wyżej są przepisywane na maszynie, tłumaczone, przechowywane, kopiowane, powielane na nośnikach magnetycznych lub mikrofilmach jedynie przez osoby, które zostały sprawdzone, aby uzyskać dostęp do informacji niejawnych UE przynajmniej do właściwej klauzuli tajności danego dokumentu, z wyjątkiem specjalnych przypadków omówionych w ust. 27 niniejszej sekcji.

   Przepisy regulujące komputerowe sporządzanie dokumentów niejawnych są określone w sekcji XI.

ROZPOWSZECHNIANIE

3. Informacje niejawne UE mogą być rozpowszechniane jedynie osobom mającym potrzebę niezbędnej wiedzy i posiadającym właściwe upoważnienie do dostępu. Wstępne rozpowszechnianie zostaje określone przez autora informacji.

4. Dokumenty TRÈS SECRET UE/EU TOP SECRET są rozprowadzane za pośrednictwem rejestrów TRÈS SECRET UE/EU TOP SECRET (patrz Sekcja VIII). W przypadku wiadomości TRÈS SECRET UE/EU TOP SECRET, właściwy rejestr może upoważnić szefa centrum łączności do sporządzenia liczby egzemplarzy określonej na liście adresatów.

5. Dokumenty oznaczone klauzulą SECRET UE i niżej, mogą być ponownie rozpowszechniane przez pierwotnego adresata innym adresatom w oparciu o zasadę potrzeby niezbędnej wiedzy. Jednakże organy wystawiające dokument wyraźnie określają wszelkie zastrzeżenia, jakie chcą wprowadzić. W każdym przypadku gdy wprowadza się takie zastrzeżenia, adresaci mogą ponownie rozpowszechniać dokumenty jedynie za zgodą organów wystawiających.

6. Każdy dokument oznaczony klauzulą CONFIDENTIEL UE i wyżej, wpływający do lub wychodzący z instytucji, jest ewidencjonowany w rejestrze instytucji. Szczegółowe dane do wprowadzenia (numer referencyjny, data i, w odpowiednim przypadku, numer egzemplarza) podaje się w sposób wystarczający do identyfikacji dokumentu i są one wprowadzane do dziennika lub na specjalnie zabezpieczony nośnik komputerowy.

▼B

Rozdział II

Przekazywanie dokumentów niejawnych UE

OPAKOWANIE

7. Dokumenty oznaczone klauzulą CONFIDENTIEL UE i wyżej są przekazywane w podwójnej wytrzymałej, nieprzezroczystej kopercie. Na wewnętrznej kopercie znajduje się właściwa klauzula tajności UE oraz, jeżeli jest to możliwe, kompletne dane szczegółowe dotyczące stanowiska oraz adresu odbiorcy.

8. Jedynie urzędnik rejestru do spraw kontroli, lub jego zastępca, może otworzyć wewnętrzną kopertę i potwierdzić odbiór załączonych dokumentów, chyba że ta koperta jest zaadresowana do konkretnej osoby. W takim przypadku właściwy rejestr odnotowuje wpłynięcie koperty i jedynie osoba, do której wewnętrzna koperta jest zaadresowana, może ją otworzyć i potwierdzić odbiór dokumentów w niej zawartych.

9. W wewnętrznej kopercie znajduje się potwierdzenie odbioru. Potwierdzenie, które nie będzie oznaczone klauzulą tajności, powinno zawierać numer referencyjny, datę oraz numer egzemplarza dokumentu, ale nigdy jego przedmiotu.

10. Wewnętrzna koperta znajduje się w zewnętrznej kopercie opatrzonej numerem przesyłki do celów potwierdzenia odbioru. W żadnym wypadku oznaczenie klauzuli tajności nie może widnieć na zewnętrznej kopercie.

11. W odniesieniu do dokumentów oznaczonych klauzulą CONFIDENTIEL UE i wyżej, kurierzy i posłańcy uzyskują potwierdzenie odbioru odpowiadające numerom przesyłki.

PRZEKAZYWANIE DOKUMENTÓW W OBRĘBIE JEDNEGO BUDYNKU LUB GRUPY BUDYNKÓW

12. W ramach danego budynku lub grupy budynków, dokumenty niejawne mogą być przenoszone w zapieczętowanej kopercie, na której znajduje się jedynie nazwisko adresata, pod warunkiem że są one przenoszone przez osobę sprawdzoną do poziomu klasyfikacji dokumentów.

PRZEKAZYWANIE DOKUMENTÓW UE W OBRĘBIE KRAJU

13. W obrębie kraju, dokumenty TRÈS SECRET UE/EU TOP SECRET powinny być przesyłane jedynie za pośrednictwem oficjalnych firm kurierskich lub osób upoważnionych do dostępu do informacji TRÈS SECRET UE/EU TOP SECRET.

14. W każdym przypadku gdy w celu przekazania dokumentów TRÈS SECRET UE/EU TOP SECRET poza granice budynku lub grupy budynków korzysta się z usług firmy kurierskiej, należy zachować zgodność z przepisami dotyczącymi pakowania i potwierdzenia odbioru zawartymi w niniejszym rozdziale. Firmy doręczające zatrudniają odpowiedni personel w celu zapewnienia, że przesyłki zawierające dokumenty TRÈS SECRET UE/EU TOP SECRET pozostają przez cały czas pod bezpośrednim nadzorem odpowiedzialnego urzędnika.

15. Wyjątkowo, dokumenty oznaczone klauzulą TRÈS SECRET UE/EU TOP SECRET mogą być przenoszone przez urzędników innych niż posłańcy, poza granice budynku lub grupy budynków w celu ich miejscowego wykorzystania na posiedzeniach i w dyskusjach, pod warunkiem że:

    a) oddawca jest upoważniony do dostępu do tych dokumentów TRÈS SECRET UE/EU TOP SECRET;

    b) sposób przenoszenia dokumentów jest zgodny z krajowymi zasadami regulującymi tryb przekazywania krajowych dokumentów TOP SECRET;

    c) w żadnym wypadku urzędnik nie pozostawia bez dozoru dokumentów TRÈS SECRET UE/EU TOP SECRET;

▼B

d) zostają dokonane uzgodnienia, aby wykaz dokumentów tak przenoszonych został umieszczony w rejestrze TRÈS SECRET UE/EU TOP SECRET przechowującym i ewidencjonującym dokumenty w dzienniku i sprawdzającym dokumenty według ewidencji po ich zwrocie.

16. W ramach danego państwa, dokumenty oznaczone klauzulą SECRET UE i CONFIDENTIEL UE mogą zostać wysyłane albo pocztą, jeżeli takie przekazanie jest dozwolone na mocy krajowych przepisów i jest zgodne z przepisami niniejszych regulacji albo za pośrednictwem firmy kurierskiej lub osób upoważnionych do dostępu do informacji niejawnych UE.

17. Każde Państwo Członkowskie lub zdecentralizowana agencja UE powinny przygotować instrukcję dotyczącą osobistego przenoszenia dokumentów niejawnych UE, opartą na niniejszych przepisach. Od oddawcy wymaga się przeczytania i podpisania takiej instrukcji. W szczególności, z takiej instrukcji powinno wyraźnie wynikać, że w żadnym wypadku dokumenty nie mogą:

a) nie znajdować się w posiadaniu osoby przenoszącej, chyba że są bezpiecznie przechowywane zgodnie z przepisami zawartymi w sekcji IV;

b) zostać pozostawione bez dozoru w środkach transportu publicznego lub prywatnych pojazdach, albo w miejscach takich jak restauracje czy hotele. Nie mogą być przechowywane w sejfach hotelowych lub pozostawione bez dozoru w pokojach hotelowych;

c) być odczytywane w miejscach publicznych, jak samolot lub pociąg.

PRZEKAZYWANIE Z JEDNEGO PAŃSTWA CZŁONKOWSKIEGO DO INNEGO

18. Materiały oznaczone klauzulą CONFIDENTIEL UE i wyżej, powinny być przewożone z jednego Państwa Członkowskiego do innego za pośrednictwem dyplomatycznych lub wojskowych służb kurierskich.

19. Jednakże można zezwolić na osobiste przewożenie materiałów oznaczonych klauzulą SECRET UE i CONFIDENTIEL UE, jeżeli przepisy dotyczące przewożenia zapewniają, że materiały te nie mogą wpaść w ręce nieupoważnionej osoby.

20. OBN mogą zezwolić na osobiste przewożenie, jeżeli kurierzy dyplomatyczni i wojskowi nie są dostępni lub jeżeli korzystanie z usług takich kurierów spowodowałoby opóźnienia ze szkodą dla działalności UE, a materiały są pilnie wymagane przez odbiorcę. Każde Państwo Członkowskie powinno opracować instrukcje dotyczące osobistego przewożenia materiałów oznaczonych klauzulą do poziomu SECRET UE włącznie na szczeblu międzynarodowym przez osoby inne niż dyplomatyczni i wojskowi kurierzy. Instrukcje powinny wymagać, aby:

a) osoba przenosząca posiadała właściwe upoważnienie do dostępu przyznane przez Państwo Członkowskie;

b) ewidencja wszystkich materiałów tak przewożonych jest przechowywana we właściwym urzędzie lub rejestrze;

c) na paczkach lub torbach zawierających materiały UE znajdowała się pieczęć urzędowa, w celu uniknięcia lub zapobieżenia kontroli przez organy celne, a także etykiety identyfikacyjne i instrukcje dla znalazcy;

d) osoba przenosząca posiadała świadectwo kurierskie i/lub zlecenie zadania, uznawane przez wszystkie Państwa UE upoważniające daną osobę do przewożenia przesyłki;

e) podróż lądowa nie odbywała się przez państwa nienależące do Wspólnoty ani ich granice, chyba że państwo wysyłające posiada specjalne gwarancje takiego państwa;

f) uzgodnienia dotyczące podróży osoby przenoszącej w odniesieniu do miejsc przeznaczenia, tras przejazdu i środków transportu były zgodne

▼B

z przepisami UE lub – jeżeli przepisy krajowe odnoszące się do tych kwestii są bardziej rygorystyczne – zgodnie z takimi przepisami;

g) materiały znajdowały w posiadaniu osoby przenoszącej, chyba że są przechowywane zgodnie z przepisami dotyczącymi bezpiecznego przechowywania zawartymi w sekcji IV;

h) materiały nie były pozostawiane bez dozoru w publicznych lub prywatnych pojazdach, albo w miejscach takich jak restauracje lub hotele. Materiały te nie mogą być przechowywane w sejfach hotelowych ani pozostawione bez dozoru w pokojach hotelowych;

i) jeżeli przewożony materiał zawiera dokumenty, nie mogą one być odczytywane w miejscach publicznych (na przykład w samolocie, pociągu itd.)

Osoby wyznaczone do przewożenia materiałów niejawnych musza przeczytać i podpisać instrukcję bezpieczeństwa, która zawiera co najmniej wyżej wymienione instrukcje oraz procedury postępowania w nagłych wypadkach lub w przypadku gdy przesyłka zawierająca materiały niejawne zostaje zakwestionowana przez urzędników celnych lub urzędników ochrony lotniska.

PRZEKAZYWANIE DOKUMENTÓW OZNACZONYCH KLAUZULĄ RESTREINT UE

21. Nie zostają ustanowione żadne szczególne przepisy dotyczące przewożenia dokumentów RESTREINT UE, z wyjątkiem tych, które powinny zapewniać, że dokumenty te nie mogą wpaść w nieupoważnione ręce.

ZASADY BEZPIECZEŃSTWA W ODNIESIENIU DO SŁUŻB KURIERSKICH

22. Wszyscy kurierzy i posłańcy zatrudnieni w celu przewożenia dokumentów SECRET UE i CONFIDENTIEL UE zostają poddani właściwemu postępowaniu sprawdzającemu.

Rozdział III

Elektryczne i inne środki technicznego przekazywania

23. Środki bezpieczeństwa w odniesieniu do łączności są przeznaczone do zapewnienia bezpieczeństwa przekazywania informacji niejawnych UE. Szczegółowe reguły mające zastosowanie do przekazywania takich informacji niejawnych UE zostały opisane w sekcji XI.

24. Informacje oznaczone klauzulą CONFIDENTIEL UE i SECRET UE mogą być przesyłane jedynie za pośrednictwem przypisanych centrów i sieci łączności i/lub terminali i systemów.

Rozdział IV

Dodatkowe egzemplarze, tłumaczenia oraz wyciągi z dokumentów niejawnych UE

25. Jedynie autor dokumentu może wyrazić zgodę na sporządzenie kopii lub tłumaczenie dokumentów TRÈS SECRET UE/EU TOP SECRET.

26. Jeżeli osoby nie posiadające poświadczenia bezpieczeństwa upoważniającego do dostępu do dokumentów TRÈS SECRET UE/EU TOP SECRET potrzebują informacji, które pomimo iż są zawarte w dokumencie TRÈS SECRET UE/EU TOP SECRET nie posiadają tego stopnia tajności, szef rejestru TRÈS SECRET UE/EU TOP SECRET może zostać upoważniony do sporządzenia niezbędnej ilości wyciągów z tego dokumentu. Jednocześnie, podejmuje on/ona niezbędne kroki w celu zapewnienia, że tym wyciągom nadano właściwe klauzule tajności.

27. Dokumenty oznaczone klauzulą SECRET UE i niżej mogą być powielane i tłumaczone przez adresata w ramach krajowych przepisów bezpieczeństwa oraz pod warunkiem ścisłej zgodności z zasadą niezbędnej wiedzy. Środki bezpieczeństwa stosowane do oryginalnego dokumentu stosuje się również w odniesieniu do dokumentów powielanych i/lub ich tłumaczeń. Zdecentralizowane agencje UE przestrzegają tych przepisów bezpieczeństwa.

▼B

Rozdział V

Przeglądy i kontrole, przechowywanie i niszczenie dokumentów niejawnych UE

PRZEGLĄDY I KONTROLE

28. Każdego roku, każdy rejestr TRÈS SECRET UE/EU TOP SECRET, określony w sekcji VIII przeprowadza szczegółowy przegląd dokumentów TRÈS SECRET UE/EU TOP SECRET, zgodnie z przepisami określonymi w sekcji VIII, ust. 9–11. Dokumenty niejawne UE zaklasyfikowane poniżej poziomu TRÈS SECRET UE/EU TOP SECRET podlegają wewnętrznej kontroli, zgodnie z krajowymi wytycznymi, a w przypadku SGR lub zdecentralizowanych agencji UE, zgodnie z instrukcjami Sekretarza Generalnego/Wysokiego Przedstawiciela.

    Powyższe czynności stwarzają urzędnikom możliwość uzyskania poglądu w odniesieniu do:

    a) możliwości obniżenia lub zniesienia stopnia tajności niektórych dokumentów;

    b) przeznaczenia dokumentów do zniszczenia.

ARCHIWIZOWANIE INFORMACJI NIEJAWNYCH UE

29. W celu ograniczenia problemów dotyczących archiwizowania, urzędnicy ds. kontroli wszystkich rejestrów są upoważnieni do przechowywania dokumentów TRÈS SECRET UE/EU TOP SECRET, SECRET UE i CONFIDENTIEL UE na mikrofilmach lub w inny sposób przechowywanych na nośnikach magnetycznych lub optycznych w celach archiwizacji, pod warunkiem że:

    a) proces kopiowania na mikrofilmy/przechowywania jest podejmowany przez pracowników posiadających aktualne poświadczenie bezpieczeństwa upoważniające do dostępu do odpowiadającego właściwego poziomu klasyfikacji;

    b) mikrofilmowi/nośnikowi, na którym przechowywane są dokumenty zapewnia się taki sam poziom bezpieczeństwa jak dokumentom oryginalnym;

    c) o kopiowaniu na mikrofilm/przechowywaniu dokumentów oznaczonych klauzulą TRÈS SECRET UE/EU TOP SECRET powiadamia się autora dokumentu;

    d) klisze filmowe, lub inne rodzaje nośników zawierają wyłącznie dokumenty o tej samej klauzurze TRÈS SECRET UE/SECRET UE lub CONFIDENTIEL UE;

    e) kopiowanie na mikrofilm/przechowywanie dokumentów TRÈS SECRET UE/EU TOP SECRET lub SECRET UE jest wyraźnie wskazane w ewidencji wykorzystywanej do celów corocznej inwentaryzacji;

    f) oryginały dokumentów, których kopie sporządzono na mikrofilmach lub przechowywane w inny sposób zostają zniszczone zgodnie z przepisami określonymi w ust. 31 do 36.

30. Niniejsze przepisy stosują się również do wszelkich innych form przechowywania, zatwierdzonych przez OBN, takich jak nośniki elektromagnetyczne i dyski optyczne.

RUTYNOWE NISZCZENIE DOKUMENTÓW NIEJAWNYCH UE

31. W celu zapobieżenia niepotrzebnego nagromadzenia dokumentów niejawnych UE, dokumenty uznane przez szefa instytucji przechowującej je za nieaktualne i zgromadzone w nadmiernej liczbie, zostają zniszczone w możliwie najkrótszym terminie, w następujący sposób:

    a) dokumenty TRÈS SECRET UE/EU TOP SECRET są niszczone wyłącznie przez centralny rejestr dla nich właściwy. Każdy zniszczony dokument zostaje umieszczony na świadectwie zniszczenia, podpisanym przez urzędnika ds. kontroli TRÈS SECRET UE/EU TOP SECRET oraz

▼B

urzędnika będącego świadkiem zniszczenia, którymi są osoby upoważnione do dostępu do dokumentów TRÈS SECRET UE/EU TOP SECRET. Adnotacji w tym celu dokonuje się w dzienniku;

b) Protokoły zniszczenia wraz z kartami obiegu przechowuje się w rejestrze przez okres 10 lat. Kopie tych dokumentów zostają przekazane autorowi lub właściwemu rejestrowi centralnemu jedynie wtedy gdy wyraźnie o nie wnioskuje;

c) dokumenty TRÈS SECRET UE/EU TOP SECRET, łącznie z odpadami niejawnymi powstającymi podczas przygotowywania dokumentów TRÈS SECRET UE/EU TOP SECRET, jak np. uszkodzone kopie, wersje robocze, notatki maszynowe czy kalki, są niszczone pod nadzorem urzędnika do spraw TRÈS SECRET UE/EU TOP SECRET przez spalenie, zmiażdżenie, pocięcie lub w inny sposób uniemożliwiający ich identyfikację bądź odtworzenie.

32. Dokumenty SECRET UE zostają zniszczone przez rejestr właściwy dla tych dokumentów pod nadzorem osoby upoważnionej do dostępu używając jednego z procesów określonych w ust. 31 lit. c). Zniszczone dokumenty zostają umieszczone w protokołach zniszczenia, przechowywanych w rejestrze wraz z kartami obiegu przez okres co najmniej 3 lat.

33. Dokumenty CONFIDENTIEL UE zostają zniszczone przez rejestr właściwy dla tych dokumentów pod nadzorem osoby upoważnionej do dostępu używając jednego z procesów określonych w ust. 31 lit. c). Zniszczenie tych dokumentów ewidencjonuje się zgodnie z krajowymi przepisami, a w przypadku SGR lub zdecentralizowanej agencji UE, zgodnie z instrukcjami Sekretarza Generalnego/Wysokiego Przedstawiciela.

34. Dokumenty RESTREINT UE zostają zniszczone przez rejestr właściwy dla tych dokumentów lub przez użytkownika, zgodnie z krajowymi przepisami, a w przypadku SGR lub zdecentralizowanej agencji UE, zgodnie z instrukcjami Sekretarza Generalnego/Wysokiego Przedstawiciela.

NISZCZENIE W NAGŁYCH WYPADKACH

35. SGR, Państwa Członkowskie i zdecentralizowane agencje UE, w oparciu o lokalne warunki, opracowują plany zabezpieczenia materiałów niejawnych UE w sytuacjach kryzysowych, obejmujące, w razie potrzeby, plany niszczenia i ewakuacji materiałów w nagłych wypadkach; publikują one w ramach swoich organizacji, instrukcje uważane za niezbędne w celu zapobieżenia wpadnięcia materiałów niejawnych UE w nieupoważnione ręce.

36. Uzgodnienia dotyczące zabezpieczenia i/lub niszczenia materiałów SECRET UE i CONFIDENTIEL UE w sytuacji kryzysowej, w żadnym wypadku nie mogą mieć negatywnego wpływu na zabezpieczenie lub zniszczenie materiałów TRÈS SECRET UE/EU TOP SECRET, łącznie z urządzeniami szyfrującymi, których traktowanie ma pierwszeństwo przed wszystkimi innymi zadaniami. Środki przyjęte w celu zabezpieczenia i niszczenia urządzeń szyfrujących w wypadkach nagłych znajdują się w instrukcjach *ad hoc*.

Rozdział VI

Szczególne reguły mające zastosowanie do dokumentów przeznaczonych dla Rady

37. W ramach SGR, „Biuro Informacji Poufnych” monitoruje informacje oznaczone klauzulą SECRET UE lub CONFIDENTIEL UE zawarte w dokumentach przeznaczonych dla Rady.

Z upoważnienia Dyrektora Generalnego ds. Zatrudnienia i Administracji, Biuro:

a) zarządza działalnością odnosząca się do rejestracji, powielania, tłumaczenia, przesyłania i niszczenia takich informacji;

b) aktualizuje wykazy danych szczegółowych dotyczących informacji niejawnych;

▼B

c) okresowo sprawdza kwestie dotyczące potrzeby utrzymania stopnia tajności informacji;

d) ustanawia, we współpracy z Biurem ds. Bezpieczeństwa, praktyczne uzgodnienia dotyczące nadawania lub znoszenia stopni tajności informacji.

38. Biuro ds. Informacji Niejawnych prowadzi ewidencję następujących danych szczegółowych:

a) data sporządzenia informacji niejawnej;

b) stopień tajności;

c) data wygaśnięcia klauzuli;

d) nazwisko i służbę wystawcy dokumentu;

e) odbiorcę lub odbiorców, wraz z numerem seryjnym;

f) przedmiot;

g) numer;

h) liczbę egzemplarzy w obiegu;

i) przygotowanie spisów informacji niejawnych przedłożonych Radzie;

j) rejestr znoszenia i obniżania stopnia tajności informacji niejawnych.

39. Ogólne reguły przewidziane w rozdziałach I–V niniejszej sekcji stosują się do Biura ds. Informacji Niejawnych SGR, chyba że zostały zmienione przez szczególne reguły ustanowione w niniejszym rozdziale

▼B

SEKCJA VIII

REJESTRY TRÈS SECRET UE/EU TOP SECRET

1. Celem rejestrów TRÈS SECRET UE/EU TOP SECRET jest zapewnienie, że ewidencja, korzystanie i rozpowszechnianie dokumentów TRÈS SECRET UE/EU TOP SECRET odbywa się zgodnie z przepisami bezpieczeństwa. Szef rejestru TRÈS SECRET UE/EU TOP SECRET, odpowiednio w każdym Państwie Członkowskim, w SGR oraz, gdzie właściwe, w zdecentralizowanych agencjach UE, będzie urzędnikiem ds. kontroli dokumentów TRÈS SECRET UE/EU TOP SECRET.

2. Centralne rejestry będą działać w charakterze głównych organów odpowiedzialnych za odbiór i rozsyłanie dokumentów w Państwach Członkowskich, w SGR oraz w zdecentralizowanych agencjach UE, w których takie rejestry zostały powołane, jak również, gdzie właściwe, w innych instytucjach UE, organizacjach międzynarodowych i państwach trzecich, z którymi Rada podpisała porozumienia w sprawie procedur bezpieczeństwa w odniesieniu do wymiany informacji niejawnych.

3. Jeżeli jest to niezbędne, powołuje się rejestry pomocnicze, odpowiedzialne za wewnętrzne zarządzanie dokumentami TRÈS SECRET UE/EU TOP SECRET; takie rejestry prowadzą bieżąca ewidencję obiegu każdego dokumentu za który jest odpowiedzialny.

4. Rejestry pomocnicze TRÈS SECRET UE/EU TOP SECRET powołuje się jak określono w Sekcji I, w odpowiedzi na długoterminowe potrzeby i podlegają centralnym rejestrom TRÈS SECRET UE/EU TOP SECRET. Jeżeli istnieje potrzeba tylko okresowego i doraźnego konsultowania dokumentów TRÈS SECRET UE/EU TOP SECRET, mogą one być wydawane bez potrzeby powoływania rejestru pomocniczego, pod warunkiem ustanowienia reguł w celu zapewnienia, że te dokumenty pozostają pod kontrolą właściwego rejestru TRÈS SECRET UE/EU TOP SECRET oraz, że są przestrzegane środki bezpieczeństwa oraz dotyczące pracowników.

5. Rejestry pomocnicze nie mogą przekazywać dokumentów TRÈS SECRET UE/EU TOP SECRET bezpośrednio innym rejestrom pomocniczym w ramach tego samego centralnego rejestru TRÈS SECRET UE/EU TOP SECRET bez wyrażenia zgody tego ostatniego.

6. Każda wymiana dokumentów TRÈS SECRET UE/EU TOP SECRET między rejestrami pomocniczymi nie podlegającymi temu samemu centralnemu rejestrowi odbywa się za pośrednictwem centralnych rejestrów TRÈS SECRET UE/EU TOP SECRET.

CENTRALNE REJESTRY TRÈS SECRET UE/EU TOP SECRET

7. Szef centralnego rejestru TRÈS SECRET UE/EU TOP SECRET, jako urzędnik ds. kontroli, jest odpowiedzialny za:

   a) przekazywanie dokumentów TRÈS SECRET UE/EU TOP SECRET zgodnie z przepisami określonymi w sekcji VII;

   b) utrzymywanie wykazu wszystkich podlegających mu rejestrów pomocniczych TRÈS SECRET UE/EU TOP SECRET, wraz z nazwiskami i podpisami powołanych urzędników ds. kontroli oraz ich upoważnionych zastępców;

   c) przechowywanie potwierdzeń odbioru z rejestrów w odniesieniu do wszystkich dokumentów TRÈS SECRET UE/EU TOP SECRET udostępnianych przez centralny rejestr;

   d) prowadzenie ewidencji dokumentów TRÈS SECRET UE/EU TOP SECRET przechowywanych i udostępnianych;

   e) utrzymywanie aktualnego wykazu wszystkich centralnych rejestrów TRÈS SECRET UE/EU TOP SECRET, z którymi normalnie utrzymuje korespondencję, wraz z nazwiskami i podpisami powołanych urzędników ds. kontroli oraz ich upoważnionych zastępców;

▼B

f) ochronę fizyczną wszystkich dokumentów TRÈS SECRET UE/EU TOP SECRET przechowywanych w rejestrze zgodnie z przepisami zawartymi w sekcji IV.

REJESTRY POMOCNICZE TRÈS SECRET UE/EU TOP SECRET

8. Szef rejestru pomocniczego TRÈS SECRET UE/EU TOP SECRET, jako urzędnik ds. kontroli, jest odpowiedzialny za:

a) przekazywanie dokumentów TRÈS SECRET UE/EU TOP SECRET zgodnie z przepisami zawartymi w sekcji VII oraz w ust. 5 i 6 w sekcji VIII;

b) utrzymywanie aktualizowanej listy wszystkich podległych mu osób upoważnionych do dostępu do informacji TRÈS SECRET UE/EU TOP SECRET;

c) udostępnianie dokumentów TRÈS SECRET UE/EU TOP SECRET zgodnie z instrukcjami autora lub na podstawie zasady potrzeby niezbędnej wiedzy, po uprzednim sprawdzeniu, że adresat posiada wymagane poświadczenie bezpieczeństwa;

d) prowadzenie bieżącej ewidencji wszystkich dokumentów TRÈS SECRET UE/EU TOP SECRET, przechowywanych lub będących w obiegu, które są pod jego kontrolą lub które zostały przekazane do innych rejestrów TRÈS SECRET UE/EU TOP SECRET oraz przechowywanie wszystkich odpowiadających potwierdzeń odbioru;

e) utrzymywanie aktualnego wykazu rejestrów TRÈS SECRET UE/EU TOP SECRET, z którymi jest uprawniony do wymiany dokumentów oznaczonych klauzulą TRÈS SECRET UE/EU TOP SECRET, wraz z nazwiskami i podpisami urzędników ds. kontroli oraz ich upoważnionych zastępców;

f) ochronę fizyczną wszystkich dokumentów TRÈS SECRET UE/EU TOP SECRET przechowywanych w rejestrze pomocniczym zgodnie z przepisami określonymi w sekcji IV.

INWENTARYZACJA

9. Co dwanaście miesięcy, każdy rejestr TRÈS SECRET UE/EU TOP SECRET przeprowadza szczegółową inwentaryzację wszystkich dokumentów TRÈS SECRET UE/EU TOP SECRET, za które jest odpowiedzialny. Dokument uważa się za zaksięgowany, jeżeli rejestr fizycznie przegląda dokument, lub przechowuje potwierdzenie odbioru z rejestru TRÈS SECRET UE/EU TOP SECRET, do którego dokument został przekazany, lub świadectwo zniszczenia tego dokumentu, lub instrukcje obniżenia lub zniesienia stopnia tajności tego dokumentu.

10. Rejestry pomocnicze przesyłają wyniki corocznych inwentaryzacji centralnemu rejestrowi, któremu podlegają, w terminie wyznaczonym przez ten ostatni.

11. OBN, jak również te instytucje UE, organizacje międzynarodowe i zdecentralizowane agencje UE, w których zostały powołane centralne rejestry TRÈS SECRET UE/EU TOP SECRET, przesyłają wyniki corocznych inwentaryzacji przeprowadzonych w centralnych rejestrach TRÈS SECRET UE/EU TOP SECRET Sekretarzowi Generalnemu/Wysokiemu Przedstawicielowi nie później niż do dnia 1 kwietnia każdego roku.

▼B

SEKCJA IX

ŚRODKI BEZPIECZEŃSTWA STOSOWANE W CZASIE NADZWYCZAJNYCH POSIEDZEŃ ODBYWAJĄCYCH SIĘ POZA SIEDZIBĄ RADY I DOTYCZĄCE KWESTII WYSOKO SENSYTYWNYCH

PRZEPISY OGÓLNE

1. Jeżeli posiedzenia Rady Europejskiej, Rady, posiedzenia na szczeblu ministerialnym lub inne ważne posiedzenia odbywają się poza siedzibami Rady w Brukseli i Luksemburgu, oraz w przypadku gdy jest to uzasadnione szczególnymi względami bezpieczeństwa odnoszącymi się do wysokiej wrażliwości poruszanych kwestii lub informacji, należy podejmować środki bezpieczeństwa opisane poniżej. Środki te dotyczą wyłącznie ochrony informacji niejawnych UE; mogą zostać przewidziane inne środki bezpieczeństwa.

ZAKRES OBOWIĄZKÓW

Przyjmujące Państwo Członkowskie

2. Państwo Członkowskie, na którego terytorium ma odbyć się posiedzenie (przyjmujące Państwo Członkowskie) powinno być odpowiedzialne, wspólnie z Biurem ds. Bezpieczeństwa SGR, za bezpieczeństwo posiedzeń Rady Europejskiej, Rady, posiedzeń na szczeblu ministerialnym lub innych ważnych posiedzeń oraz za bezpieczeństwo fizyczne głównych delegatów i ich pracowników.

   W odniesieniu do zapewnienia bezpieczeństwa, powinno ono w szczególności zapewniać:

   a) opracowanie planów działania w sytuacjach zagrożenia bezpieczeństwa i podczas zdarzeń związanych z bezpieczeństwem, danych środków obejmujących w szczególności bezpieczne przechowywanie dokumentów niejawnych UE w pomieszczeniach biurowych;

   b) podjęcie środków zapewniających umożliwienie dostępu do systemu łączności Rady w celu odbierania i przekazywania informacji niejawnych UE. Przyjmujące Państwo Członkowskie zapewni również dostęp, jeżeli jest wymagany, do bezpiecznych systemów telefonicznych.

Państwa Członkowskie

3. Organy Państw Członkowskich powinny podjąć niezbędne kroki w celu zapewnienia tego, aby:

   a) właściwe poświadczenie bezpieczeństwa zostały zapewnione ich krajowym delegatom, jeżeli jest to niezbędne, za pomocą sygnału lub faksu, bezpośrednio urzędnikowi do spraw bezpieczeństwa posiedzenia lub za pośrednictwem Biura ds. Bezpieczeństwa SGR;

   b) o każdym szczególnym zagrożeniu zostały powiadomione władze przyjmującego Państwa Członkowskiego oraz odpowiednio Biuro ds. Bezpieczeństwa SGR, tak aby mogły zostać podjęte właściwe działania.

Urzędnik do spraw bezpieczeństwa posiedzenia

4. Należy powołać urzędnika do spraw bezpieczeństwa posiedzenia, który powinien być odpowiedzialny za ogólne przygotowanie i kontrolę ogólnych środków bezpieczeństwa wewnętrznego oraz za koordynację z innymi zainteresowanymi organami bezpieczeństwa. Środki przez niego/nią podjęte powinny zasadniczo odnosić się do:

   a) i) środków ochrony w miejscu posiedzenia, w celu zapewnienia, że posiedzenie zostaje przeprowadzone bez zaistnienia żadnych zdarzeń, które mogłyby doprowadzić do ujawnienia jakichkolwiek informacji niejawnych UE, które mogą być tam wykorzystywane;

      ii) kontrola pracowników, którzy mają pozwolenie na dostęp do miejsca posiedzenia, stref przebywania delegatów i sal konferencyjnych, oraz kontrola całego wyposażenia;

▼B

iii) ciągłego współdziałania z właściwymi władzami przyjmującego Państwa Członkowskiego oraz z Biurem ds. Bezpieczeństwa SGR.

b) włączenia instrukcji bezpieczeństwa do dokumentacji posiedzenia z należytym uwzględnieniem wymogów wymienionych w tych przepisach dotyczących bezpieczeństwa, jak również wszelkich innych, uznanych za niezbędne, instrukcji bezpieczeństwa.

Biuro ds. Bezpieczeństwa SGR

5. Biuro ds. Bezpieczeństwa SGR powinno działać jako organ doradczy w kwestiach bezpieczeństwa przy organizacji posiedzeń; powinno być reprezentowane na miejscu w celu pomocy i doradztwa urzędnikowi ds. bezpieczeństwa posiedzenia oraz delegacjom, jeżeli jest to niezbędne.

6. Każda delegacja na posiedzenie powinna wyznaczyć urzędnika do spraw bezpieczeństwa, który będzie odpowiedzialny za kwestie bezpieczeństwa w ramach swojej delegacji oraz za utrzymywanie łączności z urzędnikiem do spraw bezpieczeństwa posiedzenia, jak również, jeżeli jest to niezbędne, z przedstawicielem Biura ds. Bezpieczeństwa SGR.

ŚRODKI BEZPIECZEŃSTWA

Strefy bezpieczeństwa

7. Należy ustanowić następujące strefy bezpieczeństwa:

a) strefa bezpieczeństwa klasy II, obejmująca sale, w których odbywają się posiedzenia robocze, biura SGR, urządzenia reprograficzne, a także pomieszczenia biurowe delegacji, gdzie właściwe;

b) strefa bezpieczeństwa klasy I obejmująca sale konferencyjne oraz kabiny tłumaczy i inżynierów dźwięku;

c) strefy administracyjna obejmujące miejsca wydzielone dla prasy oraz te części miejsca posiedzenia, które są wykorzystywane do celów administracyjnych, gastronomicznych oraz zakwaterowania, jak również strefy bezpośrednio sąsiadujące z centrum prasowym i miejscem posiedzenia.

Przepustki

8. Urzędnik do spraw bezpieczeństwa posiedzenia, na wniosek delegacji i zgodnie z ich potrzebami, powinien wydać odpowiednie identyfikatory. W przypadku gdy jest to wymagane, może zostać wprowadzone rozróżnienie identyfikatorów, w zależności od dostępu do różnych stref bezpieczeństwa.

9. Instrukcje bezpieczeństwa dotyczące posiedzenia powinny posiadać wymóg, żeby wszystkie zainteresowane osoby nosiły identyfikatory w widocznym miejscu w każdym czasie w trakcie posiedzenia, aby mogły być, w razie potrzeby, sprawdzone przez pracowników do spraw bezpieczeństwa.

10. Oprócz uczestników posiadających identyfikatory, do miejsca posiedzenia powinno dopuszczać się jak najmniej osób. Delegacje krajowe, które w trakcie posiedzeń chciałyby przyjmować gości, powinny powiadomić o tym urzędnika do spraw bezpieczeństwa. Każda odwiedzająca osoba powinna otrzymać identyfikator gościa. Odwiedzająca osoba powinna wypełnić formularz przepustki, podając w niej nazwisko swoje oraz osoby, którą odwiedza. Odwiedzającym osobom powinien cały czas towarzyszyć strażnik lub osoba odwiedzana. Formularz przepustki osoby odwiedzającej przechowuje osoba odwiedzana, która zwraca go, wraz z identyfikatorem gościa, pracownikom do spraw bezpieczeństwa w chwili, gdy osoba odwiedzająca opuszcza miejsce posiedzenia.

Kontrola sprzętu fotograficznego i audio

11. Na teren strefy bezpieczeństwa klasy I nie wolno wnosić kamer ani sprzętu nagrywającego, z wyjątkiem sprzętu wniesionego przez fotografów i inżynierów dźwięku, należycie upoważnionych przez urzędnika do spraw bezpieczeństwa posiedzenia.

Kontrola walizek, komputerów przenośnych i paczek

▼B

12. Osoby posiadające przepustki upoważniające do przebywania na terenie strefy bezpieczeństwa mogą zwykle wnosić swoje walizki i komputery przenośne (wyłącznie z własnym źródłem zasilania) bez przeprowadzania kontroli. W przypadku paczek dla delegacji, które delegacje mogą przyjmować, zostaną one albo skontrolowane przez urzędnika do spraw bezpieczeństwa wyznaczonego przez delegację albo prześwietlone przy użyciu specjalnych urządzeń albo otwarte w celu kontroli przez pracowników do spraw bezpieczeństwa. Jeżeli urzędnik do spraw bezpieczeństwa posiedzenia uznaje to za niezbędne, mogą zostać ustanowione bardziej rygorystyczne środki kontroli walizek i paczek.

Bezpieczeństwo techniczne

13. Sala obrad może zostać technicznie zabezpieczona przez personel do spraw bezpieczeństwa technicznego, który może również sprawować obsługę elektroniczną podczas posiedzenia.

Dokumenty delegacji

14. Delegacje powinny być odpowiedzialne za wnoszenie i wynoszenie dokumentów niejawnych na i z posiedzeń. Powinny być również odpowiedzialne za weryfikację i bezpieczeństwo tych dokumentów podczas ich wykorzystywania w pomieszczeniach przydzielonych tym delegacjom. Można wnioskować do przyjmującego Państwa Członkowskiego o pomoc w przewozie dokumentów niejawnych do i z miejsca posiedzenia.

Bezpieczne przechowywanie dokumentów

15. Jeśli SGR, Komisja lub delegacje nie są w stanie przechowywać swoich dokumentów niejawnych zgodnie z zatwierdzonymi normami, mogą, za potwierdzeniem odbioru, złożyć te dokumenty w zapieczętowanej kopercie urzędnikowi do spraw bezpieczeństwa posiedzenia, który przechowuje je zgodnie z zatwierdzonymi normami.

Kontrola pomieszczeń biurowych

16. Urzędnik do spraw bezpieczeństwa posiedzenia organizuje kontrolę pomieszczeń biurowych delegacji i SGR, na koniec każdego dnia roboczego w celu zapewnienia, że wszystkie dokumenty niejawne UE znajdują się w bezpiecznym miejscu; w przeciwnym razie powinien podjąć odpowiednie środki.

Usuwanie niepotrzebnych materiałów niejawnych UE

17. Wszystkie niepotrzebne materiały powinny być traktowane jako niejawne UE; delegacjom i SGR należy udostępnić kosze i worki na te niepotrzebne materiały. Przed opuszczeniem zajmowanych pomieszczeń, delegacje i pracownicy SGR, powinni przekazać te odpady urzędnikowi do spraw bezpieczeństwa posiedzenia, który organizuje ich zniszczenie zgodnie z przepisami.

18. Na koniec spotkania, wszystkie dokumenty będące w posiadaniu delegacji i SGR, które nie są już im potrzebne, powinny traktowane być jak niepotrzebne materiały. Pomieszczenia zajmowane przez SGR i delegacje, przez zniesieniem środków bezpieczeństwa przyjętych na czas trwania posiedzenia, należy gruntownie przeszukać. Dokumenty, które zostały wydane za potwierdzeniem odbioru, należy, w granicach obowiązujących przepisów, zniszczyć w sposób określony w sekcji VII.

▼B

SEKCJA X

NARUSZENIE ZASAD BEZPIECZEŃSTWA I NIEUPRAWNIONE UJAWNIENIE INFORMACJI NIEJAWNYCH

1. Naruszenie zasad bezpieczeństwa powstaje w wyniku działania lub zaniechania, sprzecznego z przepisami Rady dotyczącymi bezpieczeństwa lub krajowymi przepisami dotyczącymi bezpieczeństwa, które może narazić na niebezpieczeństwo lub nieuprawnione ujawnienie informacji niejawnej UE.

2. Nieuprawnione ujawnienie informacji niejawnej ma miejsce, gdy taka informacja, w całości lub w części wpada w ręce osób nieupoważnionych, tzn. osób, które albo nie posiadają właściwego poświadczenia bezpieczeństwa albo potrzeby niezbędnej wiedzy albo jeżeli istnieje przypuszczenie, że takie zdarzenie miało miejsce.

3. Nieuprawnione ujawnienie informacji niejawnej może nastąpić w wyniku niedbalstwa, zaniedbania obowiązków, niedyskrecji, jak również w wyniku działań służb których celem jest UE lub jej Państwa Członkowskie, w odniesieniu do informacji niejawnych lub działalności UE lub w wyniku działań organizacji wywrotowych,

4. Ważne jest, aby wszystkie osoby, które są zobowiązane do korzystania z informacji niejawnych UE zostały dokładnie poinstruowane o procedurach bezpieczeństwa, zagrożeniach związanych z niedyskretną rozmową i relacjach z prasą. Takie osoby powinny być świadome znaczenia niezwłocznego sprawozdawania organowi bezpieczeństwa Państwa Członkowskiego, instytucji lub agencji, w których są zatrudnione, na temat wszelkich naruszeń zasad bezpieczeństwa, o których im wiadomo.

5. Jeżeli organy bezpieczeństwa odkrywają lub zostają powiadomione o naruszeniu zasad bezpieczeństwa odnoszących się do informacji niejawnych EU lub stracie bądź zniknięciu materiałów niejawnych UE, podejmują niezwłoczne działania, w celu:

   a) ustalenia stanu faktycznego;

   b) dokonania oceny i zminimalizowania zaistniałych szkód;

   c) uniemożliwienia zaistnienia takiego samego naruszenia w przyszłości;

   d) powiadomienia właściwych organów o skutkach naruszenia zasad bezpieczeństwa;

   W tym kontekście, należy dostarczyć następujących informacji:

   i) charakterystykę informacji, której sprawa dotyczy, łącznie z jej stopniem tajności, numerem referencyjnym i numerem egzemplarza, datą, oznaczeniem autora informacji, przedmiotem i zakresem;

   ii) krótkiego opisu okoliczności, w jakich doszło do naruszenia, wraz z datą i okresem, podczas którego informacja była narażona na nieuprawnione ujawnienie;

   iii) oświadczenia, czy powiadomiono autora informacji.

6. Obowiązkiem każdego organu bezpieczeństwa, kiedy tylko uzyskuje powiadomienie, że takie naruszenie zasad bezpieczeństwa miało miejsce, jest niezwłoczne złożenie sprawozdanie z tego faktu przy zastosowaniu następującej procedury: rejestr pomocniczy EU TOP SECRET zdaje sprawozdanie w sprawie do Biura ds. Bezpieczeństwa SGR za pośrednictwem swojego centralnego rejestru EU TOP SECRET; w przypadku nieuprawnionego ujawnienia informacji niejawnej UE, w obrębie jurysdykcji Państwa Członkowskiego, sprawozdanie zdaje się do Biura ds. Bezpieczeństwa SGR, jak określono zgodnie z ust. 5 i za pośrednictwem właściwego OBN.

7. O przypadkach dotyczących informacji oznaczonych klauzulą RESTREINT UE, powiadamia się jedynie wtedy, gdy towarzyszą im nadzwyczajne okoliczności.

8. Sekretarz Generalny/Wysoki Przedstawiciel po powiadomieniu o naruszeniu zasad bezpieczeństwa:

▼B

a) powiadamia organ, który wytworzył daną informację niejawną;

b) zwraca się do właściwych organów bezpieczeństwa o wszczęcie dochodzenia;

c) w przypadku gdy sprawa dotyczy więcej niż jednego organu, koordynuje ich działania;

d) przyjmuje sprawozdanie zawierające charakterystykę okoliczności, w których doszło do naruszenia, datę lub okres, w trakcie którego mogło do niego dojść i kiedy zostało odkryte, wraz ze szczegółowym opisem zawartości i stopnia tajności danego materiału. W sprawozdaniu powinno się także uwzględnić informacje na temat szkód wyrządzonych interesom UE lub jednemu lub więcej jej Państw Członkowskich oraz działań podjętych w celu uniemożliwienia zaistnienia takiego samego naruszenia w przyszłości.

9. Organ wytwarzający informację powiadamia adresatów i udziela im właściwych instrukcji.

10. Każda osoba, która jest odpowiedzialna za nieuprawnione ujawnienie informacji niejawnej UE, podlega postępowaniu dyscyplinarnemu zgodnie z właściwymi regułami i przepisami. Takie postępowanie nie narusza żadnych działań prawnych.

▼B

SEKCJA XI

OCHRONA INFORMACJI PRZETWARZANYCH ZA POŚREDNICTWEM TECHNOLOGII INFORMACYJNYCH ORAZ SYSTEMÓW ŁĄCZNOŚCI

Spis treści

Rozdział I	Wprowadzenie
Rozdział II	Definicje
Rozdział III	Odpowiedzialność w zakresie bezpieczeństwa
Rozdział IV	Nietechniczne środki bezpieczeństwa
Rozdział V	Techniczne środki bezpieczeństwa
Rozdział VI	Bezpieczeństwo podczas korzystania
Rozdział VII	Zakup
Rozdział VIII	Korzystanie tymczasowe lub sporadyczne

▼B

Rozdział I

Wprowadzenie

WSKAZÓWKI OGÓLNE

1. Polityka dotycząca bezpieczeństwa oraz wymogi bezpieczeństwa przedstawione w niniejszej sekcji mają zastosowanie do wszystkich systemów i sieci łączności i informacyjnych (zwanych dalej SYSTEMAMI), przeznaczonych do przetwarzania informacji oznaczonych klauzulą CONFIDENTIEL UE i wyżej.

2. SYSTEMY przetwarzające informacji RESTREINT UE wymagają również środków bezpieczeństwa w celu ochrony poufności tych informacji. Wszystkie SYSTEMY wymagają środków bezpieczeństwa w celu ochrony integralności i dostępności tych systemów i informacji, które zawierają. Środki bezpieczeństwa w odniesieniu do tych systemów, zostaną określone przez wyznaczony Organ Bezpieczeństwa ds. Akredytacji (SAA), proporcjonalnie do oceny stopnia zagrożenia oraz zgodnie z polityką określoną w niniejszych przepisach bezpieczeństwa.

3. Ochrona systemów sensorowych zawierających wbudowane SYSTEMY IT zostaje ustanowiona i określona w ogólnym kontekście systemów, do których należą, wykorzystując mające zastosowanie przepisy niniejszej sekcji, w zakresie, w jakim jest to niezbędne.

ZAGROŻENIA I SŁABE PUNKTY SYSTEMÓW

4. W ujęciu ogólnym, zagrożenie może być zdefiniowane jako potencjalne ryzyko przypadkowego lub celowego naruszenia bezpieczeństwa. W przypadku SYSTEMÓW, takie naruszenie obejmuje utratę jednej lub więcej z cech poufności, integralności i dostępności. Słaby punkt może być zdefiniowany jako słabość lub brak kontroli, które mogą ułatwić lub umożliwić powstanie zagrożenia w odniesieniu do określonego aktywa lub celu. Słaby punkt może być wynikiem zaniedbania lub może wiązać się z brakami w sprawności, kompleksowości lub spójności kontroli; może mieć charakter techniczny, proceduralny lub operacyjny.

5. Informacje niejawne i jawne przetwarzane w SYSTEMACH, w spójnej postaci przeznaczonej do szybkiego wyszukiwania, łączności i korzystania są narażone na wiele zagrożeń. Zagrożenia te obejmują dostęp do informacji przez nieupoważnionych użytkowników, lub odwrotnie, odmowę dostępu użytkownikom upoważnionym. Istnieją również zagrożenia nieuprawnionego ujawnienia, zniszczenia, modyfikacji lub usunięcia informacji. Ponadto, złożone i niejednokrotnie wrażliwe wyposażenie jest kosztowne i często trudno szybko je naprawić lub wymienić. Dlatego SYSTEMY te są atrakcyjnym celem dla działań wywiadu gromadzącego dane i sabotażu, w szczególności jeżeli środki bezpieczeństwa są uznawane za nieskuteczne.

ŚRODKI BEZPIECZEŃSTWA

6. Głównym celem środków bezpieczeństwa określonych w niniejszej sekcji jest zapewnienie ochrony przed nieuprawnionym ujawnieniem informacji (utratą poufności) oraz przed utratą integralności i dostępności informacji. W celu osiągnięcia odpowiedniego poziomu zabezpieczenia SYSTEMU przetwarzającego informacje niejawne UE, określa się właściwe normy konwencjonalnego bezpieczeństwa, łącznie z właściwymi specjalnymi procedurami i technikami indywidualnie przeznaczonymi dla każdego SYSTEMU.

7. W celu stworzenia bezpiecznego środowiska dla funkcjonowania SYSTEMU, zostaje ustalony i wykonany zrównoważony zestaw środków bezpieczeństwa. Obszary stosowania tych środków dotyczą elementów fizycznych, pracowników, procedur nie-technicznych oraz komputerowych i łącznościowych procedur operacyjnych.

8. Komputerowe środki bezpieczeństwa (właściwości sprzętu komputerowego i oprogramowania odpowiedzialnego za bezpieczeństwo) są wymagane w celu wykonywania zasady niezbędnej wiedzy oraz zapobiegania lub wykrywania nieuprawnionego ujawnienia informacji. Zakres, w jakim

▼B

polega się na komputerowych środkach bezpieczeństwa zostaje ustalony podczas procesu ustanawiania wymogów bezpieczeństwa. W procesie akredytacji ustala się, czy istnieje odpowiedni stopień pewności w celu zwiększenia zakresu, w jakim można polegać na komputerowych środkach bezpieczeństwa.

OŚWIADCZENIE O SPECJALNYCH WYMOGACH BEZPIECZEŃSTWA SYSTEMU (SSRS)

9. W odniesieniu do wszystkich SYSTEMÓW przetwarzających informacje oznaczone klauzulą CONFIDENTIEL UE i wyżej wymaga się sporządzenia przez Organ Operacyjny Systemu IT (ITSOA) oświadczenia o specjalnych wymogach bezpieczeństwa systemu (SSRS), we współpracy i przy współudziale oraz wsparciu wymaganym ze strony zespołu projektantów i zwierzchnictwa INFOSEC, oraz zatwierdzonego przez Urząd Bezpieczeństwa ds. Akredytacji (SAA). SSRS jest również wymagane w przypadku gdy dostępność i integralność informacji RESTREINT UE lub informacji jawnych zostają uznane za istotne przez SAA.

10. SSRS jest formułowane w początkowej fazie powstawania projektu, a następnie uzupełniane i udoskonalane w miarę rozwoju projektu, wypełniając różnorodne zadania na poszczególnych etapach realizacji danego projektu i w okresie funkcjonowania SYSTEMU.

11. SSRS stanowi wiążące porozumienie między Organem Operacyjnym Systemu IT a SSA, na podstawie którego zostaje dokonana akredytacja SYSTEMU.

12. SSRS jest kompletnym i precyzyjnym oświadczeniem przestrzegania zasad bezpieczeństwa oraz szczegółowych wymogów w zakresie bezpieczeństwa, które muszą zostać spełnione. Jest opracowane w oparciu o politykę Rady dotyczącą bezpieczeństwa i ocenę ryzyka, lub nałożony przez parametry środowiska operacyjnego, najniższy stopień poświadczenia bezpieczeństwa pracowników, najwyższa klauzula tajności przetwarzanych informacji, bezpieczny tryb działania lub wymagania użytkownika. SSRS stanowi integralną część dokumentacji projektu przedkładanej właściwym organom w celach zatwierdzenia odnoszącego się do aspektów technicznych, budżetowych i bezpieczeństwa. W swojej ostatecznej postaci, SSRS stanowi kompletne oświadczenie określające, czego potrzebuje SYSTEM, aby być zabezpieczony.

BEZPIECZNE TRYBY DZIAŁANIA

13. Wszystkie SYSTEMY przetwarzające informacje oznaczone klauzulą CONFIDENTIEL UE i wyższą, zostają akredytowane do działania w jednym, lub w przypadku gdy jest to uzasadnione przez wymagania podczas różnych okresów, w więcej niż jednym, z poniższych bezpiecznych trybów działania, lub ich krajowych odpowiednikach:

    a) tryb dedykowany;

    b) tryb wysokopoziomowy;

    c) tryb wielopoziomowy.

Rozdział II

Definicje

DODATKOWE OZNAKOWANIA

14. Stosuje się dodatkowe oznakowania, takie jak CRYPTO lub każde inne oznaczenia uznawane przez UE wskazujące na specjalne traktowanie, w przypadku gdy istnieje potrzeba ograniczonego rozpowszechniania i specjalnego traktowania, poza wynikającym z klauzuli tajności.

15. „DEDYKOWANY" BEZPIECZNY TRYB DZIAŁANIA oznacza: tryb działania, w którym WSZYSTKIE osoby posiadające dostęp do SYSTEMU są upoważnione do dostępu do informacji o najwyższym stopniu tajności, przetwarzanych w ramach SYSTEMU oraz posiadają powszechną potrzebę

▼B

niezbędnej wiedzy w odniesieniu do WSZYSTKICH informacji przetwarzanych w ramach tego SYSTEMU.

Uwagi:

1) Powszechna potrzeba niezbędnej wiedzy oznacza, że nie istnieje obowiązkowy wymóg dla zabezpieczającego oprogramowania komputerowego zapewniania podziału informacji w ramach SYSTEMU.

2) Pozostałe właściwości bezpieczeństwa (np. fizycznego, dotyczącego pracowników i proceduralnego) spełniają wymogi określone dla najwyższego stopnia tajności oraz wszystkich kategorii oznaczeń informacji przetwarzanych w ramach SYSTEMU.

16. „WYSOKOPOZIOMOWY" BEZPIECZNY TRYB DZIAŁANIA oznacza tryb działania, w którym WSZYSTKIE osoby posiadające dostęp do SYSTEMU są upoważnione do dostępu do informacji o najwyższym poziomie klasyfikacji przetwarzanych w ramach SYSTEMU, ale NIE WSZYSTKIE osoby upoważnione do dostępu do SYSTEMU mają powszechną potrzebę niezbędnej wiedzy w odniesieniu do informacji przetwarzanych w ramach SYSTEMU.

Uwagi:

1) Brak powszechnej potrzeby niezbędnej wiedzy oznacza, że istnieje wymóg w odniesieniu do zabezpieczającego oprogramowania komputerowego do zapewniania selektywnego dostępu do oraz podziału informacji w ramach SYSTEMU.

2) Pozostałe właściwości bezpieczeństwa (np. fizycznego, dotyczącego pracowników i proceduralnego) spełniają wymogi określone dla najwyższego stopnia tajności oraz wszystkich kategorii oznaczeń informacji przetwarzanych w ramach SYSTEMU.

3) Wszystkie informacje przetwarzane lub dostępne dla SYSTEMU w tym trybie działania wraz z odpowiednimi danymi podlegają takiej ochronie – tak długo, jak nie zostanie nic innego ustalone – jakby należały do kategorii i najwyższego poziomu zaklasyfikowania, chyba że istniejąca funkcja oznaczania jest w wystarczającej mierze godna zaufania

17. „WIELOPOZIOMOWY" BEZPIECZNY TRYB DZIAŁANIA oznacza tryb działania, w którym NIE WSZYSTKIE osoby posiadające dostęp do SYSTEMU są sprawdzane do najwyższego poziomu klauzuli tajności, przetwarzanych w ramach SYSTEMU i NIE WSZYSTKIE osoby upoważnione do dostępu do SYSTEMU mają powszechną potrzebę niezbędnej wiedzy w odniesieniu do informacji przetwarzanych w ramach SYSTEMU.

Uwagi:

1) Ten tryb działania umożliwia na bieżąco przetwarzanie informacji o różnych stopniach tajności i o mieszanych kategoriach oznaczeń informacji.

2) Fakt, że nie wszystkie osoby są upoważnione do dostępu do informacji o najwyższych stopniach tajności w połączeniu z brakiem powszechnej potrzeby niezbędnej wiedzy, oznacza, że istnieje wymóg dla zabezpieczającego oprogramowania komputerowego zapewniania selektywnego dostępu oraz podziału informacji w SYSTEMIE.

18. INFOSEC oznacza: stosowanie środków bezpieczeństwa w celu ochrony informacji przetwarzanych, przechowywanych i przekazywanych za pośrednictwem systemów łączności, informacji i innych systemów elektronicznych, przed przypadkową lub celową utratą poufności, integralności lub dostępności, oraz w celu zapobiegania utraty integralności i dostępności samych systemów. Środki stosowane w ramach INFOSEC obejmują środki bezpieczeństwa komputerowego, przekazu, nadawania oraz środki ochrony kryptograficznej, oraz wykrywania, dokumentowania i przeciwdziałania zagrożeniom w odniesieniu do informacji i SYSTEMÓW.

19. BEZPIECZEŃSTWO KOMPUTEROWE (COMPUSEC) oznacza: stosowanie właściwości sprzętu komputerowego, oprogramowania firmowego oraz oprogramowania odpowiedzialnego za bezpieczeństwo w systemie

▼B

komputerowym w celu ochrony przed lub zapobiegania nieuprawnionemu ujawnieniu, manipulacji, modyfikacji/usunięciu informacji lub blokadzie obsługi.

20. PRODUKT BEZPIECZEŃSTWA KOMPUTEROWEGO oznacza: element ogólnego bezpieczeństwa komputerowego, który ma zostać włączony do systemu IT w celu wykorzystania do wzmocnienia lub zapewnienia poufności, integralności lub dostępności przetwarzanych informacji.

21. BEZPIECZEŃSTWO SYSTEMÓW ŁĄCZNOŚCI (COMSEC) oznacza: stosowanie środków bezpieczeństwa w telekomunikacji, w celu uniemożliwienia osobom nieupoważnionym dostępu do informacji, które można uzyskać dzięki posiadaniu lub analizie takich systemów telekomunikacyjnych, lub w celu zapewnienia autentyczności takiej telekomunikacji.

Uwaga:

Takie środki obejmują ochronę kryptograficzną, przekazywania i nadawania, oraz bezpieczeństwo proceduralne, fizyczne, dotyczące pracowników, dokumentów i komputerowe.

22. OCENA oznacza: szczegółowe badanie techniczne aspektów bezpieczeństwa SYSTEMU lub aspektów kryptograficznych lub produktu bezpieczeństwa komputerowego, wykonywane przez właściwy organ.

Uwagi:

1) Ocena polega na zbadaniu, czy istnieje wymagana funkcjonalność środków bezpieczeństwa oraz czy nie istnieją niepożądane skutki uboczne takiej funkcjonalności oraz na ocenie niezawodności takiej funkcjonalności.

2) Ocena określa zakres, w jakim wymagania bezpieczeństwa SYSTEMU lub wymogi bezpieczeństwa produktu bezpieczeństwa komputerowego, zostają spełnione oraz ustanawia poziom zapewnienia SYSTEMU lub ochrony kryptograficznej lub powierzonej funkcji produktu bezpieczeństwa komputerowego.

23. CERTYFIKACJA oznacza: wydawanie, na podstawie niezależnych badań i oceny, formalnego oświadczenia o zakresie, w jakim SYSTEM spełnia wymogi bezpieczeństwa, lub że produkt bezpieczeństwa komputerowego spełnia uprzednio określone wymogi bezpieczeństwa.

24. AKREDYTACJA oznacza: autoryzację i zatwierdzenie przyznane SYSTEMOWI w celu przetwarzania informacji niejawnych UE w jego środowisku operacyjnym.

Uwaga:

Taka akredytacja powinna być przyznana po wykonaniu wszystkich właściwych procedur bezpieczeństwa i po osiągnięciu wystarczającego poziomu ochrony zasobów systemu. Akredytacji zwykle udziela się na podstawie SSRS, włącznie z:

a) oświadczeniem dotyczącym celu akredytacji systemu; w szczególności, z informacji jakiego stopnia (stopni) tajności będzie się korzystać i jaki system oraz jaki bezpieczny tryb(-y) działania sieci się proponuje;

b) dokonaniem przeglądu zarządzania ryzykiem, w celu określenia zagrożeń, słabych punktów i środków przeciwdziałania;

c) procedurami bezpieczeństwa operacyjnego (SecOP), ze szczegółowym opisem proponowanych działań (tzn. trybów, usług jakie mają być realizowane) oraz wraz z opisem podaniem właściwości bezpieczeństwa SYSTEMU, stanowiących podstawę akredytacji;

d) planem wykonania i utrzymania właściwości bezpieczeństwa systemu;

e) planem początkowej i dalszej kontroli, oceny i certyfikacji bezpieczeństwa systemu lub sieci; oraz

f) certyfikacją, jeśli wymagane wraz z innymi elementami akredytacji.

▼B

25. SYSTEM IT oznacza: zespół urządzeń, metod i procedur oraz, jeżeli to niezbędne, pracowników, zorganizowanych w celu realizacji funkcji przetwarzania informacji.

Uwagi:

1) Powyższe oznacza zespół instalacji, skonfigurowanych w celu korzystania z informacji w ramach systemu.

2) Takie systemy mogą mieć zastosowanie we wspieraniu działań konsultacyjnych, dowodzenia, kontrolnych, łącznościowych, naukowych lub administracyjnych, wraz z przetwarzaniem tekstów;

3) Granice systemu będą zwykle ustalane jako elementy podlegające kontroli jednego ITSOA.

4) System IT może zawierać podsystemy, z których niektóre same mogą być systemami IT.

26. Na CECHY BEZPIECZEŃSTWA SYSTEMU IT składają się wszystkie funkcje, cechy charakterystyczne i właściwości sprzętu komputerowego/oprogramowania firmowego/oprogramowania odpowiedzialnego za bezpieczeństwo; procedur działania, procedur odpowiedzialności oraz kontroli dostępu, obszaru sieci IT, obszaru odległego terminalu/stacji roboczej, ograniczenia zarządzania, struktury fizycznej i urządzeń, kontroli pracowników i łączności, niezbędnych w celu zapewnienia wystarczającego poziomu ochrony informacji niejawnych, które mają być przetwarzane w systemie IT.

27. SIEĆ IT oznacza: organizację, o dużym zasięgu geograficznym, systemów IT wzajemnie połączonych w celu wymiany danych i obejmującą części składowe wzajemnie połączonych systemów IT oraz ich interfejsu z danymi wspomagającymi lub sieciami łączności.

Uwagi:

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

2) Sieć IT nazywana jest „lokalną” jeśli łączy kilka komputerów w tym samym miejscu.

28. WŁAŚCIWOŚCI BEZPIECZEŃSTWA SIECI IT obejmują właściwości systemu bezpieczeństwa IT poszczególnych systemów IT, zawierających sieć łącznie z takimi dodatkowymi częściami składowymi i właściwościami związanymi z siecią (na przykład, sieci łączności, identyfikacja bezpieczeństwa, mechanizmy i procedury oznaczania, kontrole dostępu, programy i rejestracja śladów audytu) niezbędnych w celu osiągnięcia wymaganego poziomu ochrony informacji niejawnych.

29. OBSZAR IT oznacza; obszar zawierający jeden lub kilka komputerów, ich lokalne jednostki peryferyjne i składowania, jednostki kontrolne i sieci dedykowane oraz urządzenia służące do łączności.

Uwaga:

Nie dotyczy to oddzielnego obszaru, w którym znajdują się odległe urządzenia peryferyjne lub terminale/stacje robocze, nawet pomimo, iż są one połączone z urządzeniami z obszaru IT.

30. OBSZAR ODLEGŁEGO TERMINALU/STACJI ROBOCZEJ oznacza: obszar zawierający niektóre urządzenia komputerowe, ich lokalne urządzenia peryferyjne lub terminale/stacje robocze oraz wszelkie związane z nimi urządzenia służące do łączności, wyodrębnione z obszaru IT.

31. Środki przeciwdziałania TEMPEST: środki bezpieczeństwa przeznaczone do ochrony urządzeń i infrastruktury łączności przed ujawnieniem informacji niejawnych poprzez nieumyślną emisję elektromagnetyczną.

▼B

Rozdział III

Odpowiedzialność w zakresie bezpieczeństwa

OGÓLNE

32. Obowiązki Komitetu ds. Bezpieczeństwa, określone w sekcji I ust. 4, obejmują również kwestie dotyczące INFOSEC. Komitet ds. Bezpieczeństwa organizuje swoją działalność w taki sposób, aby mógł zapewnić doradztwo ekspertów w powyższych kwestiach.

33. W przypadku wystąpienia problemów dotyczących bezpieczeństwa (incydenty, naruszenie itp.), odpowiedzialne organy krajowe i/lub Biuro ds. Bezpieczeństwa SGR niezwłocznie podejmują działania. Wszystkie problemy zgłasza się do Biura ds. Bezpieczeństwa SGR.

34. Sekretarz Generalny/Wysoki Przedstawiciel lub, gdzie właściwe, szef zdecentralizowanej agencji UE, ustanawia biuro INFOSEC w celu zapewnienia organowi bezpieczeństwa informacji w sprawie wykonywania i kontroli specjalnych właściwości bezpieczeństwa zaprojektowanych jako część SYSTEMÓW.

URZĄD BEZPIECZEŃSTWA DS. AKREDYTACJI (SAA)

35. Urzędem Bezpieczeństwa ds. Akredytacji mogą być:

— OBN,

— organ wyznaczony przez Sekretarza Generalnego/Wysokiego Przedstawiciela,

— organ bezpieczeństwa zdecentralizowanej agencji UE, lub

— ich delegowani/nominowanych przedstawiciele, w zależności od SYSTEMU podlegającego akredytacji.

36. Urząd Bezpieczeństwa ds. Akredytacji jest odpowiedzialny za zapewnienie zgodności SYSTEMÓW z polityką bezpieczeństwa Rady. Jednym z jego zadań jest zatwierdzanie SYSTEMU w zakresie korzystania z informacji niejawnych do określonego stopnia tajności w jego środowisku operacyjnym. W odniesieniu do Sekretariatu Generalnego Rady i odpowiednio, zdecentralizowanych agencjach UE, Urząd Bezpieczeństwa ds. Akredytacji ponosi odpowiedzialność za bezpieczeństwo w imieniu Sekretarza Generalnego/Wysokiego Przedstawiciela lub szefów zdecentralizowanych agencji.

Jurysdykcja Urzędu Bezpieczeństwa ds. Akredytacji SGR obejmuje wszystkie SYSTEMY działające na terenie siedzib SGR. SYSTEMY i części składowe SYSTEMÓW działających w ramach Państwa Członkowskiego pozostają pod jurysdykcją tego Państwa Członkowskiego. Jeżeli różne części składowe SYSTEMU podlegają jurysdykcji Urzędu Bezpieczeństwa ds. Akredytacji SGR oraz innych Urzędów Bezpieczeństwa ds. Akredytacji, wszystkie strony powołają wspólny zarząd do spraw, koordynowany przez Urząd Bezpieczeństwa ds. Akredytacji SGR.

ORGAN INFOSEC (IA)

37. Organ INFOSEC jest odpowiedzialny za działalność biura INFOSEC. W odniesieniu do SGR i odpowiednio zdecentralizowanych agencji UE, organ INFOSEC jest odpowiedzialny za:

— udzielanie porad i pomocy technicznej Urzędowi Bezpieczeństwa ds. Akredytacji,

— pomoc w opracowywaniu SSRS,

— przegląd SSRS w celu zapewnienia spójności z niniejszymi przepisami dotyczącymi bezpieczeństwa, polityką INFOSEC oraz z dokumentacją techniczną,

— uczestnictwo, gdzie właściwe, w zespołach/zarządach do spraw akredytacji oraz przedkładanie Urzędowi Bezpieczeństwa ds. Akredytacji zaleceń INFOSEC w sprawach akredytacji,

▼B

— zapewnianie wsparcia prowadzonej przez INFOSEC działalności szkoleniowej i edukacyjnej,

— udzielanie porad technicznych w dochodzeniach prowadzonych w związku z incydentami dotyczącymi INFOSEC,

— ustanowienie informacji technicznych dotyczących polityki zapewniającej stosowanie wyłącznie legalnego oprogramowania.

ORGAN OPERACYJNY SYSTEMU IT (ITSOA)

38. Organ INFOSEC, na możliwie najwcześniejszym etapie, przekazuje ORGANOWI OPERACYJNEMU SYSTEMU IT odpowiedzialność za wykonywanie i działania kontrolne specjalnych właściwości bezpieczeństwa SYSTEMU. Odpowiedzialność ta obejmuje cały okres funkcjonowania SYSTEMU, od fazy projektowania do ostatecznej likwidacji.

39. ORGAN OPERACYJNY SYSTEMU IT jest odpowiedzialny za wszystkie środki bezpieczeństwa określone jako część całego SYSTEMU. Odpowiedzialność ta obejmuje przygotowanie SecOP. ORGAN OPERACYJNY SYSTEMU IT określa normy i praktyki dotyczące bezpieczeństwa, które muszą spełniać dostawcy SYSTEMU.

40. ORGAN OPERACYJNY SYSTEMU IT może przekazać część swoich obowiązków, gdzie właściwe, na przykład urzędnikowi ds. bezpieczeństwa INFOSEC i urzędnikowi ds. bezpieczeństwa terenu INFOSEC. Różne funkcje INFOSEC mogą być wykonywane przez pojedynczą osobę.

UŻYTKOWNICY

41. Wszyscy użytkownicy są odpowiedzialni za zapewnienie, że ich działania nie wpływają negatywnie na bezpieczeństwo SYSTEMU, z którego korzystają.

SZKOLENIA INFOSEC

42. Działalność szkoleniowa i edukacyjna INFOSEC jest dostępna na różnych poziomach, oraz dla różnych pracowników zatrudnionych, gdzie właściwe, w ramach SGR, zdecentralizowanych agencji UE lub służb rządowych Państw Członkowskich.

Rozdział IV

Nietechniczne środki bezpieczeństwa

BEZPIECZEŃSTWO PRACOWNIKÓW

43. Użytkownicy SYSTEMU podlegają postępowaniu sprawdzającemu oraz posiadają potrzebę niezbędnej wiedzy, odpowiednio do stopnia tajności i zawartości informacji przetwarzanych w ich konkretnym SYSTEMIE. Dostęp do niektórych urządzeń lub informacji szczególnych ze względu na bezpieczeństwo SYSTEMÓW będzie wymagać specjalnego poświadczenia wydanego zgodnie z procedurami Rady.

44. Urząd Bezpieczeństwa ds. Akredytacji wyznacza wszystkie sensytywne stanowiska oraz określa poziom poświadczenia i nadzoru, wymagany od pracowników, którzy je zajmują.

45. SYSTEMY są określone i zaprojektowane w sposób ułatwiający przydział obowiązków i odpowiedzialności pracownikom tak, aby zapobiec posiadaniu przez jedną osobę całkowitej wiedzy na temat kluczowych punktów bezpieczeństwa systemu lub wyłącznej kontroli nad nimi. Celem powinna być konieczność współdziałania między dwoma lub więcej osobami w celu dokonania zmiany lub celowej degradacji systemu lub sieci.

BEZPIECZEŃSTWO FIZYCZNE

46. IT oraz odległe obszary terminalu/stacji roboczej (jak określono w ust. 29 i 30), w obrębie których informacje oznaczone klauzulą CONFIDENTIEL UE i wyższą są wykorzystywane przez środki IT, lub w przypadku gdy istnieje potencjalna możliwość dostępu do takich informacji, są traktowane jak strefy bezpieczeństwa klasy I i II UE lub, gdzie właściwe, ich krajowe odpowiedniki.

▼B

47. IT oraz odległe obszary terminalu/stacji roboczej, w których bezpieczeństwo SYSTEMU może być zmieniane nie może być pod opieką wyłącznie jednego upoważnionego urzędnika/innego pracownika.

KONTROLA DOSTĘPU DO SYSTEMU

48. Wszystkie informacje i materiały, pozwalające na kontrolę dostępu do SYSTEMU, podlegają ochronie na mocy uzgodnień współmiernych informacjom o najwyższym stopniu tajności i kategorii oznaczeń, do których mogą umożliwiać dostęp.

49. Informacje i materiały dotyczące kontroli dostępu, które nie są już wykorzystywane w tym celu, zostają zniszczone w zastosowaniu ust. 61–63.

Rozdział V

Techniczne środki bezpieczeństwa

BEZPIECZEŃSTWO INFORMACJI

50. Obowiązkiem autora informacji jest określanie oraz klasyfikowanie wszystkich dokumentów zawierających informacje, niezależnie czy występują one w postaci wydruku z dysku twardego czy zapisu na komputerowym nośniku. Dół i góra każdej strony wydruku zawiera oznaczenie klauzuli. Wydruk, niezależnie czy występuje w postaci zapisu na dysku twardym czy zapisu na komputerowym nośniku, oznaczony zostaje taką samą klauzulą jak najwyższy stopień tajności informacji wykorzystanych przy jego sporządzaniu. Sposób, w jaki SYSTEM funkcjonuje również może wpływać na stopień tajności wydruków z tego systemu.

51. Obowiązkiem organizacji i posiadaczy jej informacji jest rozpatrywanie problemów powstałych w związku z nagromadzeniem pojedynczych elementów informacji oraz wniosków, jakie można wyciągnąć na podstawie powiązanych elementów oraz ustalanie czy przyznanie wyższego stopnia tajności jest właściwe w odniesieniu do całości informacji.

52. Fakt, że informacja może być zwięzłym kodem, kodem transmisyjnym lub przedstawiona w innej podwójnej formie, nie zapewnia żadnej ochrony bezpieczeństwa i dlatego nie powinna wpływać na klasyfikację informacji.

53. Jeżeli informacja jest przekazywana z jednego SYSTEMU do innego, podczas przekazywania oraz w SYSTEMIE docelowym jest ona chroniona w sposób współmierny do oryginalnej klauzuli i kategorii informacji.

54. Ze wszystkich komputerowych nośników informacji korzysta się w sposób współmierny do klauzuli najwyżej sklasyfikowanej przechowywanej informacji lub oznaczenia nośnika, i przez cały czas poddaje się odpowiedniej ochronie.

55. Komputerowe nośniki informacji wielokrotnego użycia stosowane w celu rejestracji informacji niejawnych UE zachowują najwyższy stopień tajności informacji, do której były kiedykolwiek użyte, do czasu odpowiedniego obniżenia lub zniesienia stopnia tajności tych informacji i następującego przeklasyfikowania nośników lub zniesienia stopnia tajności lub zniszczenia nośników zgodnie z procedurami zatwierdzonymi przez SGR lub procedurami krajowymi (patrz ust. 61–63).

KONTROLA I EWIDENCJA INFORMACJI

56. Prowadzone są, automatyczne (fiszki audytu) lub ręczne dzienniki ewidencji w celu rejestracji dostępu do informacji niejawnych oznaczonych klauzulą SECRET UE i wyższą. Rejestry te przechowywane są zgodnie z niniejszymi przepisami dotyczącymi bezpieczeństwa.

57. Niejawne wydruki UE, przechowywane w obszarze IT, mogą być traktowane jako jeden niejawny element i nie muszą być rejestrowane, pod warunkiem że materiał jest określony, oznaczony klauzulą oraz poddawany kontroli we właściwy sposób.

58. W przypadku gdy wydruk zostaje otrzymany z SYSTEMU korzystającego z informacji niejawnych UE, i zostaje przekazany do odległego terminalu/obszaru stacji roboczej z obszaru IT, ustanawia się procedury, za zgodą

▼B

Urzędu Bezpieczeństwa ds. Akredytacji w celu kontrolowania tego wydruku. Takie procedury, w odniesieniu do informacji oznaczonych klauzulą SECRET UE i wyższą, zawierają specjalne instrukcje dotyczące ewidencjonowania informacji.

TRAKTOWANIE I KONTROLA WYMIENIALNYCH KOMPUTEROWYCH NOŚNIKÓW INFORMACJI

59. Wszystkie wymienialne komputerowe nośniki informacji niejawnych oznaczonych klauzulą CONFIDENTIEL UE i wyższą, są traktowane tak jako materiały i będzie się stosować w odniesieniu do nich ogólne reguły. Właściwe oznaczenia identyfikacyjne i klasyfikacyjne muszą zostać dostosowane do szczególnej fizycznej formy nośników w celu umożliwienia ich łatwego rozpoznania.

60. Użytkownicy ponoszą odpowiedzialność za zapewnienie, że informacje niejawne UE są przechowywane na nośnikach z właściwymi oznaczeniami klasyfikacyjnymi i podlegają ochronie. Ustanawia się procedury w celu zapewnienia, że w odniesieniu do wszystkich poziomów informacji UE, przechowywanie informacji na komputerowych nośnikach informacji odbywa się zgodnie z niniejszymi przepisami dotyczącymi bezpieczeństwa.

DEKLASYFIKACJA I ZNISZCZENIE KOMPUTEROWYCH NOŚNIKÓW INFORMACJI

61. Komputerowe nośniki informacji, używane do rejestracji informacji niejawnych UE mogą być obniżone lub zdeklasyfikowane, jeżeli stosuje się procedury zatwierdzone przez SGR lub procedury krajowe.

62. Komputerowe nośniki informacji, na których były przechowywane informacje oznaczone klauzulą TRÈS SECRET UE/EU TOP SECRET lub informacje specjalnych kategorii nie są deklasyfikowane ani ponownie wykorzystywane.

63. Jeżeli komputerowe nośniki informacji nie mogą być zdeklasyfikowane lub nie są ponownie wykorzystane, nośniki te zostają zniszczone zgodnie z procedurami zatwierdzonymi przez SGR lub procedurami krajowymi.

BEZPIECZEŃSTWO ŁĄCZNOŚCI

64. Jeżeli informacje niejawne UE są przekazywane drogą elektromagnetyczną, stosuje się specjalne środki w celu ochrony poufności, integralności oraz dostępności takich przekazów. Urząd Bezpieczeństwa ds. Akredytacji ustala wymogi dotyczące ochrony przekazów przed wykryciem i przejęciem. Informacje przekazywane za pomocą systemu łączności podlegają ochronie opartej na wymogach poufności, integralności oraz dostępności.

65. Jeśli w celu zapewnienia ochrony poufności, integralności i dostępności wymagane są metody kryptograficzne, takie metody lub powiązane produkty zostają specjalnie zatwierdzone do tego celu przez Urząd Bezpieczeństwa ds. Akredytacji.

66. Podczas przekazu, poufność informacji niejawnych oznaczonych klauzulą SECRET UE i wyższą, podlega ochronie za pośrednictwem metod kryptograficznych lub produktów zatwierdzonych przez Radę na podstawie zalecenia Komitetu ds. Bezpieczeństwa Rady. Podczas przekazu, poufność informacji niejawnych oznaczonych klauzulą CONFIDENTIEL UE lub RESTREINT UE podlega ochronie za pośrednictwem metod kryptograficznych lub produktów zatwierdzonych albo przez Sekretarza Generalnego/ Wysokiego Przedstawiciela na podstawie zalecenia Komitetu ds. Bezpieczeństwa Rady, albo przez Państwo Członkowskie.

67. Szczegółowe reguły mające zastosowanie do przekazu informacji niejawnych UE zostają wymienione w specjalnych instrukcjach bezpieczeństwa, zatwierdzonych przez Radę na podstawie zalecenia Komitetu ds. Bezpieczeństwa Rady.

68. W wyjątkowych okolicznościach operacyjnych, informacje niejawne oznaczone klauzulami RESTREINT UE, CONFIDENTIEL UE oraz SECRET UE mogą być przekazywane w formie nieszyfrowanego tekstu, pod warun-

▼B

kiem każdorazowego wyraźnego upoważnienia. Za takie wyjątkowe okoliczności uważa się:

a) stany zbliżającego się lub trwającego kryzysu, konfliktu lub stanów wojny; oraz

b) sytuacje, w których czas doręczenia ma kluczowe znaczenie, środki szyfrowania nie są dostępne i ocenia się, że przekazane informacje nie mogą zostać wykorzystane w czasie tak, aby negatywnie wpłynąć na operacje.

69. SYSTEM posiada zdolność do skutecznej odmowy dostępu do informacji niejawnych UE w każdej lub we wszystkich odległych stacjach roboczych lub terminalach, jeżeli jest to wymagane albo poprzez fizyczne przerwanie połączenia lub poprzez specjalne właściwości oprogramowania zatwierdzone przez Urząd Bezpieczeństwa ds. Akredytacji.

BEZPIECZEŃSTWO INSTALACJI I PROMIENIOWANIA

70. Początkowa instalacja SYSTEMÓW oraz zasadnicze w nich zmiany zostają tak określone, aby instalacja była wykonywana przez monterów, którzy zostali poddani postępowaniu sprawdzającemu, oraz pod stałym nadzorem wykwalifikowanych pracowników technicznych upoważnionych do dostępu do informacji niejawnych UE o stopniu tajności równemu informacjom o najwyższej klauzuli, jakie będą przechowywane i przetwarzane w SYSTEMIE.

71. Wszystkie urządzenia są instalowane zgodnie z obecną polityką bezpieczeństwa Rady.

72. SYSTEMY wykorzystujące informacje niejawne oznaczone klauzulą CONFIDENTIEL UE i wyższą, są chronione w taki sposób, aby ich bezpieczeństwo nie mogło zostać zagrożone przez ujawnienie poprzez emisję, którego badanie i kontrola jest określona jako „TEMPEST".

73. Środki przeciwdziałania TEMPEST w odniesieniu do instalacji SGR lub zdecentralizowanych agencji UE są analizowane i zatwierdzone przez organ TEMPEST wyznaczony przez Organ ds. Bezpieczeństwa SGR. W odniesieniu do instalacji krajowych, które korzystają z informacji niejawnych UE, organem zatwierdzającym jest uznany krajowy organ zatwierdzający TEMPEST.

Rozdział VI

Bezpieczeństwo podczas przetwarzania

PROCEDURY BEZPIECZEŃSTWA OPERACYJNEGO

74. SecOP określają zasady, jakie mają zostać przyjęte w odniesieniu do kwestii bezpieczeństwa, procedur operacyjnych, jakie mają być przestrzegane oraz obowiązków pracowników. Opracowanie SecOP należy do obowiązków ITSOA.

OCHRONA OPROGRAMOWANIA/ZARZĄDZANIE KONFIGURACJĄ

75. Zakres ochrony bezpieczeństwa programów użytkowych zostaje ustalony na podstawie oceny klauzuli tajności samego programu, niż klauzuli informacji, które ma przetwarzać. Wykorzystywane wersje oprogramowania powinny być weryfikowane w regularnych odstępach czasu w celu zapewnienia ich integralności i właściwego funkcjonowania.

76. Nowe lub zmienione wersje oprogramowania nie powinny być używane do przetwarzania informacji niejawnych UE do czasu weryfikacji przez ITSOA.

WYKRYWANIE OBECNOŚCI OPROGRAMOWANIA DESTRUKCYJNEGO/ WIRUSÓW KOMPUTEROWYCH

77. Wykrywanie obecności oprogramowania destrukcyjnego/wirusów komputerowych jest przeprowadzane okresowo, zgodnie z wymogami Urzędu Bezpieczeństwa ds. Akredytacji.

78. Wszystkie komputerowe nośniki informacji wpływające do SGR lub zdecentralizowanych agencji UE lub Państw Członkowskich przed wprowa-

▼B

dzeniem do SYSTEMU, powinny zostać sprawdzone pod kątem wykrycia obecności oprogramowania destrukcyjnego lub wirusów komputerowych,

KONSERWACJA

79. Umowy i procedury dotyczące regularnej i doraźnej konserwacji SYSTEMÓW, w odniesieniu do których zostały sporządzone SSRS, określają wymogi i uzgodnienia dotyczące pracowników przeprowadzających konserwacje oraz ich wyposażenia wchodzących na teren obszaru IT.

80. Wymogi zostają wyraźnie określone w SSRS, a procedury zostają wyraźnie określone w SecOP. Wykonawcy usług konserwacyjnych wymagającemu zdalnego dostępu do celów procedur diagnostycznych uzyskuje na to pozwolenie jedynie w wyjątkowych okolicznościach, pod ścisłą kontrolą bezpieczeństwa i wyłącznie za zgodą Urzędu Bezpieczeństwa ds. Akredytacji.

Rozdział VII

Zakup

81. Każdy produkt bezpieczeństwa, który ma być stosowany w ramach SYSTEMU, który ma zostać zakupiony powinien albo zostać oceniony i certyfikowany, albo być na bieżąco oceniany i certyfikowany przez właściwy organ oceniający lub certyfikujący zgodnie z międzynarodowymi potwierdzonymi kryteriami (takimi jak wspólne kryteria oceny bezpieczeństwa technologii informacyjnych, patrz ISO 154 08).

82. Przy podejmowaniu decyzji, czy sprzęt, szczególnie komputerowe nośniki informacji, powinien być raczej wydzierżawiony niż zakupiony, należy wziąć pod uwagę fakt, że sprzęt taki, raz użyty do przetwarzania informacji niejawnych UE, nie może być udostępniony poza odpowiednio zabezpieczonym środowiskiem, bez uprzedniego zniesienia stopnia tajności za zgodą Urzędu Bezpieczeństwa ds. Akredytacji, przy czym zgoda taka nie zawsze jest możliwa.

AKREDYTACJA

83. Wszystkie SYSTEMY, w odniesieniu do których zostaje sporządzone SSRS, przed przetwarzaniem informacji niejawnych UE, podlegają akredytacji Urzędu Bezpieczeństwa ds. Akredytacji, w oparciu o informacje zawarte w SSRS, SecOP oraz w innej właściwej dokumentacji. Podsystemy oraz odległe terminale/stacje robocze są akredytowane jako część wszystkich SYSTEMÓW, z którymi są połączone. W przypadku gdy SYSTEM wspomaga działania zarówno Rady jak i innych organizacji, zostaje akredytowany za wspólną zgodą SGR oraz właściwych organów bezpieczeństwa.

84. Proces akredytacji może być prowadzony zgodnie ze strategią akredytacji właściwą dla danego SYSTEMU i określoną przez Urząd Bezpieczeństwa ds. Akredytacji.

OCENA I CERTYFIKACJA

85. Przed akredytacją, w niektórych przypadkach, właściwości sprzętu komputerowego, oprogramowania firmowego i oprogramowania odpowiedzialnego za bezpieczeństwo SYSTEMU podlegają ocenie i certyfikacji w celu potwierdzenia ich zdolności do ochrony informacji na zakładanym poziomie klasyfikacji.

86. Wymogi dotyczące oceny i certyfikacji zostają zawarte w planie systemu i wyraźnie określone w SSRS.

87. Proces oceny i certyfikacji prowadzony jest, zgodnie z zatwierdzonymi wytycznymi, oraz przez wykwalifikowanych i właściwie upoważnionych pracowników technicznych działających w imieniu ORGANU OPERACYJNEGO SYSTEMU IT.

88. Zespoły pracowników mogą być zapewniane przez wyznaczone przez Państwa Członkowskie organy oceniające i certyfikujące lub ich wyznaczonych przedstawicieli, na przykład, przez posiadającego odpowiednie kompetencje i właściwie upoważnionego wykonawcę.

▼B

89. Zakres danych procesów oceny i certyfikacji może zostać ograniczony (na przykład, tylko do aspektów integracji), w przypadku gdy SYSTEMY działają na bazie istniejących produktów bezpieczeństwa komputerowego ocenionych i certyfikowanych na szczeblu krajowym.

RUTYNOWA KONTROLA WŁAŚCIWOŚCI BEZPIECZEŃSTWA W CELU PRZEDŁUŻENIA OKRESU AKREDYTACJI

90. ORGAN OPERACYJNY SYSTEMU IT ustanawia rutynowe procedury kontrolne, które zapewniają, że wszystkie właściwości bezpieczeństwa SYSTEMU są nadal ważne.

91. Rodzaje zmian, które mogłyby spowodować ponowną akredytację lub które wymagają uprzedniej zgody Urzędu Bezpieczeństwa ds. Akredytacji są wyraźnie określone i wskazane w SSRS. Po każdej zmianie, naprawie lub awarii, która mogłaby mieć wpływ na właściwości bezpieczeństwa SYSTEMU, ORGAN OPERACYJNY SYSTEMU IT zapewnia przeprowadzenie kontroli w celu zapewnienia poprawnego funkcjonowania właściwości bezpieczeństwa. Przedłużenie okresu akredytacji SYSTEMU zwykle zależy od przeprowadzenia kontroli zakończonej zadowalającym wynikiem.

92. Wszystkie SYSTEMY, w których zastosowano właściwości bezpieczeństwa, są okresowo kontrolowane i przeglądane przez Urząd Bezpieczeństwa ds. Akredytacji. W odniesieniu do SYSTEMÓW przetwarzających informacje oznaczone klauzulą TRÈS SECRET UE/EU TOP SECRET lub informacji posiadających dodatkowe oznaczenia, kontrole są przeprowadzane nie rzadziej niż raz na rok.

Rozdział VIII

Korzystanie tymczasowe lub sporadyczne

BEZPIECZEŃSTWO MIKROKOMPUTERÓW/KOMPUTERÓW OSOBISTYCH

93. Mikrokomputery/komputery osobiste (PC) z dyskami stałymi (lub innymi trwałymi nośnikami informacji) działające albo w trybie niezależnym lub w ramach skonfigurowanej sieci, oraz przenośne urządzenia komputerowe (np. przenośne komputery osobiste i elektroniczne notatniki) z trwałymi dyskami twardymi uważa się za nośniki informacji w takim samum sensie jak dyskietki lub inne wymienialne komputerowe nośniki informacji.

94. Takiemu sprzętowi zapewnia się poziom bezpieczeństwa, w kwestii dostępu, korzystania, przechowywania i transportu współmierny do najwyższego stopnia tajności informacji kiedykolwiek przechowywanej lub przetwarzanej (do czasu obniżenia lub zniesienia stopnia tajności zgodnie z zatwierdzonymi procedurami).

KORZYSTANIE Z PRYWATNEGO SPRZĘTU IT DO URZĘDOWEJ PRACY RADY

95. Korzystanie z prywatnych wymienialnych komputerowych nośników informacji, oprogramowania oraz sprzętu komputerowego IT (na przykład z komputerów osobistych i przenośnych urządzeń komputerowych) z możliwością przechowywania jest zakazane w odniesieniu do korzystania z informacji niejawnych UE.

96. Prywatny sprzęt komputerowy, oprogramowanie oraz nośniki nie mogą zostać wniesione na teren którejkolwiek ze stref klasy I lub II, na terenie których są przetwarzane informacje niejawne UE, bez zezwolenia szefa Biura ds. Bezpieczeństwa SGR lub organu administracyjnego Państwa Członkowskiego lub danej zdecentralizowanej agencji UE.

KORZYSTANIE ZE SPRZĘTU IT BĘDĄCEGO WŁASNOŚCIĄ WYKONAWCY LUB POCHODZĄCEGO ZE ŹRÓDŁA KRAJOWEGO DO URZĘDOWEJ PRACY RADY

97. Szef Biura ds. Bezpieczeństwa SGR lub urząd Państwa Członkowskiego lub odpowiednia zdecentralizowana agencja UE może zezwolić na korzystanie ze sprzętu IT oraz oprogramowania, będących własnością wykonawcy, w organizacjach w celu wspierania prac urzędowych Rady. Korzystanie ze sprzętu IT i oprogramowania, pochodzących ze źródeł krajowych, przez

▼B

pracowników SGR lub zdecentralizowanej agencji UE może również być dozwolone; w takim przypadku sprzęt IT zostaje wpisany na właściwy wykaz SGR. W każdym przypadku, jeżeli sprzęt IT ma być używany do przetwarzania informacji niejawnych UE, zasięga się opinii właściwego Urzędu Bezpieczeństwa ds. Akredytacji w celu, aby elementy INFOSEC, które mają zastosowanie przy korzystaniu z tego sprzętu zostały właściwie uwzględnione i zastosowane.

▼B

SEKCJA XII

UDOSTĘPNIANIE INFORMACJI NIEJAWNYCH PAŃSTWOM TRZECIM ORAZ ORGANIZACJOM MIĘDZYNARODOWYM

ZASADY REGULUJĄCE UDOSTĘPNIANIE INFORMACJI NIEJAWNYCH UE

1. Udostępnienie informacji niejawnych UE państwom trzecim lub organizacjom międzynarodowym będzie podlegać decyzji Rady, podejmowanej na podstawie:

   — charakteru i treści takich informacji,

   — zasady „niezbędnej wiedzy" otrzymującego,

   — skali korzyści dla UE.

   Państwo Członkowskie będące autorem informacji niejawnej UE zostanie poproszone o wyrażenie zgody na jej udostępnienie.

2. Decyzje te będą podejmowane indywidualnie w każdym przypadku, w zależności od:

   — pożądanego poziomu współpracy z danymi państwami trzecimi lub organizacjami międzynarodowymi,

   — zaufania, jakim można je obdarzyć, które wynika z poziomu ochrony, który byłby stosowany w odniesieniu do informacji niejawnych UE powierzonych tym państwom lub organizacjom oraz od poziomu spójności przepisów dotyczących bezpieczeństwa stosowanych tam oraz w UE; Komitet ds. Bezpieczeństwa Rady przedstawi Radzie swoją opinię techniczną w tym względzie.

3. Przyjęcie przez państwa trzecie lub organizacje międzynarodowe informacji niejawnych UE spowoduje zobowiązanie, że informacje nie będą wykorzystywane w celach innych niż te uzasadniające udostępnienie lub wymianę informacji, oraz że zapewnią one ochronę zgodną z wymogami Rady.

POZIOMY

4. Po podjęciu decyzji o możliwości udostępnienia lub wymiany informacji niejawnych z danym państwem lub organizacją międzynarodową, Rada zdecyduje o możliwym poziomie współpracy. Będzie to zależało w szczególności od polityki i przepisów dotyczących bezpieczeństwa stosowanych przez to państwo lub organizację.

5. Istnieją trzy poziomy współpracy:

   Poziom 1 Współpraca z państwami trzecimi lub organizacjami międzynarodowymi, których polityka i przepisy dotyczące bezpieczeństwa są bardzo zbliżone do obowiązujących w UE.

   Poziom 2 Współpraca z państwami trzecimi lub organizacjami międzynarodowymi, których polityka i przepisy dotyczące bezpieczeństwa znacznie różnią się od obowiązujących w UE.

   Poziom 3 Okazjonalna współpraca z państwami trzecimi lub organizacjami międzynarodowymi, których polityka i przepisy dotyczące bezpieczeństwa nie mogą zostać ocenione.

6. W odniesieniu do każdego poziomu współpracy ustali się przepisy dotyczące bezpieczeństwa, przeredagowane w poszczególnych przypadkach w świetle opinii technicznej Komitetu ds. Bezpieczeństwa Rady, które otrzymujący informacje niejawne zobowiążą się zastosować w celu ochrony informacji im udostępnionych. Takie procedury i przepisy dotyczące bezpieczeństwa są wyszczególnione w dodatkach 4, 5 i 6.

UMOWY

7. Z chwilą, gdy Rada stwierdza, że istnieje stała i długoterminowa potrzeba wymiany informacji niejawnych między UE a państwami trzecimi lub innymi organizacjami międzynarodowymi, sporządzi z nimi „umowy

▼B

w sprawie procedur bezpieczeństwa w odniesieniu do wymiany informacji niejawnych", określające cel współpracy oraz wzajemne reguły dotyczące ochrony wymienianych informacji.

8. W przypadku okazjonalnej współpracy na poziomie 3, która z definicji jest ograniczona w czasie i co do celu, zamiast „umowy w sprawie procedur bezpieczeństwa w odniesieniu do wymiany informacji niejawnych" można zastosować zwykły protokół ustaleń, określający charakter informacji niejawnych będących przedmiotem wymiany oraz wzajemne zobowiązania dotyczące tych informacji, pod warunkiem że nie są one oznaczone klauzulą wyższą niż RESTREINT UE.

9. Projekty umów w sprawie procedur bezpieczeństwa lub protokołów ustaleń zostaną zatwierdzone przez Komitet ds. Bezpieczeństwa Rady, przed ich przedstawieniem, celem podjęcia decyzji, Radzie.

10. OBN udzielą wszelkiej niezbędnej pomocy Sekretarzowi Generalnemu/ Wysokiemu Przedstawicielowi w celu zapewnienia, że informacje, które mają zostać udostępnione, są wykorzystywane i chronione zgodnie z przepisami porozumień w sprawie procedur bezpieczeństwa lub Protokołów ustaleń.

▼M3

SEKCJA XIII

WSPÓLNE MINIMALNE NORMY W ZAKRESIE BEZPIECZEŃSTWA PRZEMYSŁOWEGO

1) Niniejsza sekcja dotyczy aspektów bezpieczeństwa działalności przemysłowej specyficznych dla negocjowania i zawierania umów, w których powierza się zadania obejmujące informacje niejawne UE, wiążące się z takimi informacjami lub je zawierające, oraz specyficznych dla wykonywania tych umów przez podmioty prowadzące działalność przemysłową lub inną, włącznie z udostępnianiem lub uzyskiwaniem dostępu do informacji niejawnych UE podczas przeprowadzania procedury zamówień publicznych (okres przetargowy oraz negocjacje poprzedzające zawarcie umowy).

DEFINICJE

2) Do celów niniejszych wspólnych minimalnych norm zastosowanie mają następujące definicje:

   a) „umowa niejawna”: każda umowa dotycząca dostawy towarów, wykonania prac lub świadczenia usług, której wykonanie wymaga dostępu do informacji niejawnych UE lub wytwarzania takich informacji bądź obejmuje dostęp do nich lub ich wytwarzanie;

   b) „niejawna umowa podwykonawcza”: umowa zawierana przez wykonawcę z innym wykonawcą (tj. podwykonawcą) na dostawę towarów, wykonanie prac lub świadczenie usług, której wykonanie wymaga dostępu do informacji niejawnych UE lub wytwarzania takich informacji bądź obejmuje dostęp do nich lub ich wytwarzanie;

   c) „wykonawca”: osoba fizyczna lub prawna posiadająca zdolność prawną do zawierania umów;

   d) „wyznaczona władza bezpieczeństwa (WWB)”: instytucja odpowiedzialna wobec krajowej władzy bezpieczeństwa (KWB) Państwa Członkowskiego UE, odpowiadająca za przekazywanie podmiotom prowadzącym działalność przemysłową lub inną informacji dotyczących krajowej polityki we wszelkich kwestiach związanych z bezpieczeństwem przemysłowym oraz za udzielanie wskazówek i pomocy w jej realizacji. Zadania WWB może wykonywać KWB;

   e) „świadectwo bezpieczeństwa przemysłowego (ŚBP)”: stwierdzenie przez KWB/WWB w drodze administracyjnej, że z punktu widzenia bezpieczeństwa dany podmiot jest w stanie zapewnić właściwą ochronę informacji niejawnych UE o określonej klauzuli tajności oraz że jego pracownicy, którzy mają uzyskać dostęp do informacji niejawnych UE, zostali właściwie sprawdzeni pod względem bezpieczeństwa oraz przeszkoleni w zakresie odpowiednich wymogów bezpieczeństwa niezbędnych do uzyskania dostępu do informacji niejawnych UE i do ich ochrony;

   f) „podmiot prowadzący działalność przemysłową lub inną”: podmiot zajmujący się dostawą towarów, wykonywaniem prac lub świadczeniem usług; pojęcie to może obejmować podmioty prowadzące działalność przemysłową, handlową, usługową, naukową, badawczą, edukacyjną lub rozwojową;

   g) „bezpieczeństwo przemysłowe”: stosowanie środków i procedur ochrony, w celu zapobiegania utracie informacji niejawnych UE bądź narażaniu na szwank ich bezpieczeństwa, wykrywania takich zdarzeń oraz likwidowania ich skutków w odniesieniu do informacji niejawnych znajdujących się w dyspozycji wykonawcy lub podwykonawcy w trakcie negocjacji poprzedzających zawarcie umowy oraz w trakcie wykonywania umowy;

   h) „krajowa władza bezpieczeństwa (KWB)”: instytucja rządowa Państwa Członkowskiego UE ostatecznie odpowiedzialna za ochronę informacji niejawnych UE;

   i) „ogólna klauzula tajności umowy”: określenie klauzuli tajności całej umowy na podstawie klauzuli tajności informacji lub materiałów, które mają lub mogą być wytwarzane, udostępniane lub do których może być uzyskany dostęp na mocy któregokolwiek elementu całej umowy.

▼M3

Ogólna klauzula tajności umowy nie może być niższa niż najwyższa klauzula tajności któregokolwiek z jej elementów, ale może ona być wyższa w związku z efektem kumulacji;

j) „dokument określający aspekty bezpieczeństwa (DAB)": zbiór specjalnych warunków dotyczących umowy, wydany przez instytucję zlecającą, stanowiący integralną część umowy niejawnej obejmującej dostęp do informacji niejawnych UE lub ich wytwarzanie, określający wymogi bezpieczeństwa lub wskazujący te elementy umowy, które wymagają ochrony;

k) „przewodnik nadawania klauzul (PNK)": dokument opisujący niejawne elementy programu lub umowy, określający mającą zastosowanie klauzulę tajności. PNK może być rozszerzany w okresie trwania programu lub umowy, a klauzule tajności dla części informacji mogą zostać zmienione lub obniżone. PNK musi stanowić część DAB.

ORGANIZACJA

3) Sekretariat Generalny Rady (SGR) może na podstawie umowy powierzyć zadania obejmujące informacje niejawne UE, wiążące się z takimi informacjami lub je zawierające, podmiotom prowadzącym działalność przemysłową lub inną, zarejestrowanym w Państwie Członkowskim.

4) SGR odpowiada za to, by wszystkie wymogi wynikające z niniejszych minimalnych norm były spełnione przy zawieraniu umów niejawnych.

5) Państwa Członkowskie odpowiadają za to, by ich KWB posiadała właściwe struktury umożliwiające stosowanie niniejszych minimalnych norm w zakresie bezpieczeństwa przemysłowego. Struktury te mogą obejmować jedną lub kilka WWB.

6) Ostateczna odpowiedzialność za ochronę informacji niejawnych UE w podmiotach prowadzących działalność przemysłową lub inną spoczywa na ich kierownictwie.

7) W przypadku zawierania umowy lub umowy podwykonawczej podlegającej niniejszym minimalnym normom SGR lub, w stosownych przypadkach, KWB/WWB niezwłocznie powiadomi o tym fakcie KWB/WWB Państwa Członkowskiego, w których wykonawca lub podwykonawca jest zarejestrowany.

UMOWY NIEJAWNE

8) Przy określaniu klauzuli tajności umów niejawnych muszą zostać uwzględnione następujące zasady:

a) SGR określa, w stosownych przypadkach, aspekty umowy, które wymagają ochrony, oraz odpowiednią klauzulę tajności; czyniąc to, musi brać pod uwagę oryginalną klauzulę tajności przyznaną przez wytwórcę informacji wytworzonej przed zawarciem umowy;

b) ogólna klauzula tajności umowy nie może być niższa niż najwyższa klauzula któregokolwiek z jej elementów;

c) informacjom niejawnym UE wytworzonym w ramach działalności objętej umową nadaje się klauzule tajności zgodnie z PNK;

d) w stosownych przypadkach SGR odpowiada za dokonanie zmiany, w porozumieniu z wytwórcą, ogólnej klauzuli tajności umowy lub klauzuli tajności któregokolwiek jej elementu oraz za poinformowanie o tym wszystkich zainteresowanych stron;

e) informacje niejawne udostępnione wykonawcy lub podwykonawcy lub wytworzone w ramach działalności objętej umową nie mogą być wykorzystywane w innych celach, niż cele określone w umowie niejawnej i nie mogą być ujawniane stronom trzecim bez uprzedniej pisemnej zgody wytwórcy.

9) KWB/WWB Państw Członkowskich odpowiadają za dopilnowanie, by wykonawcy lub podwykonawcy, z którymi zawarto umowy niejawne obejmujące informacje oznaczone klauzulą CONFIDENTIEL UE lub SECRET

▼M3

UE, stosowali wszelkie właściwe środki w celu zabezpieczania informacji niejawnych UE im udostępnianych lub wytwarzanych przez nich w toku wykonywania umowy niejawnej, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Niestosowanie się do wymogów bezpieczeństwa może skutkować rozwiązaniem umowy.

10) Wszystkie podmioty prowadzące działalność przemysłową lub inną będące stronami umów obejmujących dostęp do informacji oznaczonych klauzulą CONFIDENTIEL UE lub SECRET UE muszą posiadać krajowe ŚBP. ŚBP przyznawane jest przez KWB/WWB Państwa Członkowskiego w celu potwierdzenia, że dany podmiot jest w stanie zapewnić właściwą ochronę informacji niejawnych UE odpowiednio do określonego poziomu klauzuli tajności.

11) KWB/WWB odpowiada za wydawanie, zgodnie z przepisami krajowymi, poświadczenia bezpieczeństwa osobowego (PBO) wszystkim osobom zatrudnionym w podmiotach prowadzących działalność przemysłową lub inną, zarejestrowanych w tym Państwie Członkowskim, których obowiązki wymagają dostępu do informacji UE oznaczonych klauzulą CONFIDENTIEL UE lub SECRET UE objętych umową niejawną.

12) Umowy niejawne muszą zawierać DAB, jak określone w pkt 2 lit. j). DAB musi zawierać PNK.

13) Przed rozpoczęciem negocjacji umowy niejawnej SGR skontaktuje się z KWB/WWB Państwa Członkowskiego, w którym zarejestrowane są dane podmioty prowadzące działalność przemysłową lub inną, w celu otrzymania potwierdzenia, że posiadają one ważne ŚBP odpowiednie do klauzuli tajności umowy.

14) Instytucja zlecająca nie powinna zawierać umowy niejawnej z wybranym uczestnikiem przetargu przed uzyskaniem ważnego certyfikatu ŚBP.

15) Nie wymaga się ŚBP dla umów obejmujących informacje oznaczone klauzulą RESTREINT UE, chyba że wymagają tego krajowe przepisy ustawowe i wykonawcze Państw Członkowskich.

16) W przypadku przetargów dotyczących umów niejawnych zaproszenia do przetargu muszą zawierać klauzulę zastrzegającą, że uczestnik przetargu, który nie złoży oferty lub który nie zostanie wybrany, będzie zobowiązany do zwrotu w określonym terminie wszystkich dokumentów.

17) Istnieje możliwość, że wykonawca będzie musiał negocjować niejawne umowy podwykonawcze z podwykonawcami na różnych poziomach. Wykonawca odpowiada za zapewnienie, by wszystkie czynności podwykonawcze były podejmowane zgodnie ze wspólnymi minimalnymi normami zawartymi w niniejszej sekcji. Jednakże wykonawca nie może przekazywać podwykonawcy informacji lub materiałów niejawnych UE bez uprzedniej pisemnej zgody wytwórcy.

18) Warunki, na których wykonawca może zawrzeć umowę z podwykonawcą, muszą zostać określone w specyfikacji przetargowej oraz w umowie. Nie można zawrzeć żadnej umowy podwykonawczej z podmiotami zarejestrowanymi w państwie niebędącym członkiem UE bez wyraźnego pisemnego upoważnienia SGR.

19) W czasie trwania umowy odpowiednia KWB/WWB we współpracy z SGR będzie sprawowała kontrolę nad przestrzeganiem wszystkich przepisów bezpieczeństwa zawartych w umowie. Powiadamianie o wydarzeniach istotnych ze względu na bezpieczeństwo podlega raportowaniu zgodnie z przepisami określonymi w części II sekcji X niniejszych przepisów dotyczących bezpieczeństwa. SGR oraz każda KWB/WWB, którą powiadomiono o ŚBP, są natychmiast informowane o zmianie lub cofnięciu tego ŚBP.

20) W przypadku rozwiązania umowy niejawnej lub niejawnej umowy podwykonawczej SGR lub, w stosownym przypadku, KWB/WWB niezwłocznie powiadomi o tym fakcie KWB/WWB Państwa Członkowskiego, w którym zarejestrowany jest wykonawca lub podwykonawca.

▼M3

21) Po rozwiązaniu lub zakończeniu umowy niejawnej lub niejawnej umowy podwykonawczej w dalszym ciągu zastosowanie znajdują wspólne minimalne normy zawarte w niniejszej sekcji, a wykonawcy i podwykonawcy nadal utrzymują w tajemnicy informacje niejawne.

22) Przepisy szczególne dotyczące niszczenia informacji niejawnych po zakończeniu umowy określone zostaną w DAB lub innych odpowiednich przepisach określających wymogi bezpieczeństwa.

WIZYTY

23) Wizyty pracowników SGR w tych podmiotach prowadzących działalność przemysłową lub inną w Państwach Członkowskich, które wykonują umowy niejawne UE, muszą zostać uzgodnione z odpowiednią KWB/WWB. Wizyty pracowników podmiotów prowadzących działalność przemysłową lub inną w ramach umowy niejawnej UE muszą zostać uzgodnione pomiędzy właściwymi KWB/WWB. Jednakże KWB/WWB zaangażowane w umowę niejawną UE mogą wyrazić zgodę na procedurę, zgodnie z którą wizyty pracowników podmiotów prowadzących działalność przemysłową lub inną mogą być uzgadniane bezpośrednio.

PRZESYŁANIE I PRZEWÓZ INFORMACJI NIEJAWNYCH UE

24) W odniesieniu do przesyłania informacji niejawnych UE zastosowanie mają przepisy rozdziału II sekcji VII części II oraz w stosownych przypadkach przepisy sekcji XI niniejszych przepisów dotyczących bezpieczeństwa. Jako uzupełnienie tych przepisów zastosowanie będą miały wszelkie istniejące procedury obowiązujące między Państwami Członkowskimi.

25) Międzynarodowy przewóz materiałów niejawnych UE w ramach umów niejawnych odbywa się zgodnie z krajowymi procedurami Państw Członkowskich. Przy analizie uzgodnień dotyczących bezpieczeństwa przewozu międzynarodowego będą miały zastosowanie następujące zasady:

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

b) przesyłka podlega ochronie przewidzianej dla najwyższej klauzuli tajności materiału, który się w niej znajduje;

c) firmy świadczące usługę przewozu w stosownych przypadkach uzyskują ŚBP. W takich przypadkach pracownicy przewożący przesyłkę podlegają sprawdzeniu pod względem bezpieczeństwa zgodnie ze wspólnymi minimalnymi normami zawartymi w niniejszej sekcji;

d) przejazdy są w miarę możliwości bezpośrednie i trwają nie dłużej, niż jest to konieczne ze względu na okoliczności;

e) jeżeli jest to możliwe, trasy powinny przebiegać wyłącznie przez Państwa Członkowskie UE. Trasy przebiegające przez państwa niebędące członkami UE mogą zostać ustalone pod warunkiem zatwierdzenia przez KWB/WWB zarówno państwa nadawcy, jak i państwa odbiorcy;

f) przed jakimkolwiek przemieszczeniem materiałów niejawnych UE nadawca sporządza plan przewozu, podlegający zatwierdzeniu przez odpowiednie KWB/WWB.

▼B

Dodatek 1

Wykaz krajowych organów bezpieczeństwa

BELGIA

Service public fédéral des affaires étrangères, du commerce extérieur et de la coopération au développement
Autorité nationale de sécurité (ANS)
Direction du protocole et de la sécurité
Service de la sécurité P&S 6
Rue des Petits Carmes 15
B-1000 Bruxelles
Telephone Secretariat: + 32/2/519 05 74
Telephone Presidency: + 32/2/501 82 20
+ 32/2/501 87 10
Fax: + 32/2/519 05 96

REPUBLIKA CZESKA

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tel.: (420) 257 28 33 35
Fax: (420) 257 28 31 10

DANIA

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg
Telephone: (45) 33 14 88 88
Fax: (45) 33 43 01 90

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 København Ø
Telephone: (45) 33 32 55 66
Fax: (45) 33 93 13 20

NIEMCY

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101 D
D-11014 Berlin
Telefon: + 49-1-888 681 15 26
Fax: + 49-1-888 681 558 06

ESTONIA

Eesti Vabariigi Kaitseministeerium
(Ministry of Defence, Republic of Estonia, Department of Security National Security Authority)
Sakala 1
EE-15094 Tallinn
Telephone: + 372/717 00 30
+ 372/717 00 31
+ 372/717 00 77
Fax: + 372/717 00 01

GRECJA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)

▼**M2**

Διεύθυνση Ασφαλείας και Αντιπληροφοριών
GR-ΣΤΓ 1020 Χολαργός (Αθήνα)
Τηλέφωνα: (30-210) 657 20 09 (ώρες γραφείου)
(30-210) 657 20 10 (ώρες γραφείου)
Φαξ: (30-210) 642 64 32
(30-210) 652 76 12

[Hellenic National Defence General Staff (HNDGS)]
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens
Telephone: (30-210) 657 20 09 (office hours)
(30-210) 657 20 10 (office hours)
Fax: (30-210) 642 64 32
(30-210) 652 76 12

HISZPANIA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera nacional radial VI, km 8,5
E-28023 Madrid
Telephone: + 34/913 72 57 07
+ 34/913 72 50 27
Fax: + 34/913 72 58 08

FRANCJA

Secrétariat général de la défense nationale
Service de sécurité de défense (SGDN/SSD)
51, boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telephone: + 33/1/71 75 81 77
Fax: + 33/1/71 75 82 00

IRLANDIA

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
IRL-Dublin 2
Telephone (353-1) 478 08 22
Fax (353-1) 478 14 84

WŁOCHY

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Cesis III Reparto (UCSi)
Via di Santa Susanna, 15
I-00187 Roma
Telephone: + 39/06/611 742 66
Fax: + 39/06/488 52 73

CYPR

Υπουργείο Άμυνας
Στρατιωτικό επιτελείο του υπουργού
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
CY-1432 Λευκωσία
Τηλέφωνα:
(357-22) 80 75 69
(357-22) 80 75 19

▼M2

(357-22) 80 77 64
Φαξ: (357-22) 30 23 51

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi Street
CY-1432 Nicosia
Telephone: (357-22) 80 75 69
(357-22) 80 75 19
(357-22) 80 77 64
Fax: (357-22) 30 23 51

ŁOTWA

National Security Authority of Constitution Protection
Bureau of the Republic of Latvia
Miera iela 85 A
LV-1013 Riga
Telephone: + 371/702 54 18
Fax: + 371/702 54 54

LITWA

Lithuanian National Security Authority
Gedimino ave. 40/1
LT-01110 Vilnius
Telephone: + 370/5/266 32 01
Fax: + 370/5/266 32 00

LUKSEMBURG

Autorité nationale de sécurité
Ministère d'État
Boîte postale 23 79
L-1023 Luxembourg
Telephone: + 352/478 22 10 central
+ 352/478 22 35 direct
Fax: + 352/478 22 43
+ 352/478 22 71

WĘGRY

National Security Authority Republic of Hungary
Nemzeti Biztonsági Felügyelet
Pf.: 2
HU-1352 Budapest
Telephone: + 361/346 96 52
Fax: + 361/346 96 58

MALTA

Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta
Telephone: + 356/21 24 98 44
Fax: + 356/21 23 53 00

NIDERLANDY

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Nederland
Telephone: (31-70) 320 44 00
Fax: (31-70) 320 07 33

Ministerie van Defensie

▼M2

Beveiligingsautoriteit (BA)
Postbus 20701
2500 ES Den Haag
Nederland
Telephone: (31-70) 318 70 60
Fax: (31-70) 318 75 22

AUSTRIA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Telefon: + 43-1-531 15 23 96
Fax: + 43-1-531 15 25 08

POLSKA

Wojskowe Służby Informacyjne (Military Information Services
National Security Authority – Military Sphere)
PL-00-909 Warszawa 60
Telephone: + 48/22/684 13 62
Fax: + 48/22/684 10 76

Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency
National Security Authority – Civilian Sphere
Department for the Protection of Classified Information)
ul. Rakowiecka 2A
PL-00-993 Warszawa
Telephone: + 48/22/585 73 60
Fax: + 48/22/585 85 09

PORTUGALIA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1400-204 Lisboa
Tel.: (351) 21 301 17 10
Fax: (351) 21 303 17 11

SŁOWENIA

Office of the Government of the Republic of Slovenia
For the Protection of Classified Information – NSA
Slovenska cesta 5
SI-1000 Ljubljana
Tel.: (386-1) 426 91 20
Faks: (386-1) 426 91 21

SŁOWACJA

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
SK-851 05 Bratislava
Telephone: + 421/2/68 69 23 14
Fax: + 421/2/68 69 17 00

FINLANDIA

Ulkoasiainministeriö/Utrikesministeriet
Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Laivastokatu 22/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Telephone: (358-9) 16 05 53 38

▼**M2**

Fax: (358-9) 16 05 53 03

SZWECJA

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telephone: + 46/8/405 54 44
Fax: + 46/8/723 11 76

ZJEDNOCZONE KRÓLESTWO

UK National Security Authority
PO Box 49359
London, SW1P 1LU
United Kingdom
Telephone (44-207) 930 87 68
Fax (44-207) 821 86 04

▼M2

Dodatek 2

Porównanie klauzuli tajności

Klasyfikacja UE i Państw Członkowskich	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Euratom	*Eura — Top Secret*	*Eura — Secret*	*Eura — Confidential*	*Eura — Restricted*
Belgia	Très Secret Zeer geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte verspreiding
Republika Czeska	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dania	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Niemcy	Streng geheim	Geheim	VS (9) — Vertraulich	VS — Nur für den Dienstgebrauch
Estonia	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Grecja	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Hiszpania	Secreto	Reservado	Confidencial	Difusión Limitada
Francja	Très Secret Défense (10)	Secret Défense	Confidentiel Défense	nota (11)
Irlandia	Top Secret	Secret	Confidential	Restricted
Włochy	Segretissimo	Segreto	Riservatissimo	Riservato
Cypr	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Łotwa	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litwa	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luksemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte

▼M2

Klasyfikacja UE i Państw Członkowskich	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Węgry	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Niderlandy	Zeer geheim	Geheim	Confidentieel	Vertrouwelijk
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polska	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalia	Muito Secreto	Secreto	Confidencial	Reservado
Słowenia	Strogo tajno	Tajno	Zaupno	Interno
Słowacja	Prísne tajné	Tajné	Dôverné	Vyhradené
Finlandia	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Szwecja	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Zjednoczone Królestwo	Top Secret	Secret	Confidential	Restricted
Klasyfikacja Organizacji Międzynarodowej	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
WEU	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted

([9]) Niemcy: VS = Verschlusssache.
([10]) Francja: klasyfikacja „Très secret défense", obejmująca priorytetowe kwestie rządowe, może zostać zmieniona jedynie z upoważnienia premiera.
([11]) Francja nie stosuje kategorii klasyfikacji „DIFFUSION RESTREINTE" w swoim systemie krajowym. Francja traktuje i chroni dokumenty noszące oznaczenie „RESTREINT UE" zgodnie ze swoimi obowiązującymi przepisami krajowym; które nie mają charakteru mniej surowego niż przepisy Rady dotyczące bezpieczeństwa.

Dodatek 3

Praktyczny przewodnik po klauzulach tajności

Niniejszy przewodnik ma charakter orientacyjny i nie może być rozumiany jako wprowadzający zmiany do podstawowych przepisów ustanowionych w sekcjach II i III.

Klasyfikacja	Kiedy	Kto	Oznaczenia	Obniżanie/Deklasyfikacja/Niszczenie	
				Kto	Kiedy
TRÈS SECRET UE/EU TOP SECRET: Ta klauzula jest stosowana wyłącznie w odniesieniu do informacji i materiałów, których nieuprawnione ujawnienie może spowodować wyjątkowo poważną szkodę w podstawowych interesach UE lub jednego lub więcej jej Państw Członkowskich [SII(1)].	Nieuprawnione ujawnienie aktywów oznaczonych klauzulą TRÈS SECRET UE/EU TOP SECRET może: — bezpośrednio zagrażać wewnętrznej stabilności UE lub jednego z jej Państw Członkowskich lub państw zaprzyjaźnionych — spowodować wyjątkowo poważną szkodę w stosunkach z rządami państw zaprzyjaźnionych — bezpośrednio prowadzić do znacznych strat w ludziach — spowodować wyjątkowo poważną szkodę dla bezpieczeństwa lub skuteczności operacyjnej Państw Członkowskich lub innych sił przyczyniających się, lub utrzymaniu skuteczności bezpieczeństwa o niezwykle istotnym znaczeniu lub działalności wywiadu — spowodować dotkliwe długoterminowe straty w gospodarce UE lub Państw Członkowskich	Państwa Członkowskie: Osoby właściwie upoważnione (autorzy dokumentu) [SIII(4)]; SGR: Osoby właściwie upoważnione (autorzy dokumentu) [SIII(4)], Sekretarz Generalny/Wysoki Przedstawiciel i SDG. Autorzy określają datę lub okres, z upływem których można obniżyć lub znieść stopień tajności w odniesieniu do zawartości dokumentu. W przeciwnym razie, dokonują przeglądu dokumentów przynajmniej co pięć lat, w celu uzyskania pewności, że pierwotna klauzula tajności jest nadal niezbędna.[SII(10)].	Klauzulę TRÈS SECRET UE/EU TOP SECRET stosuje się do dokumentów TRÈS SECRET UE/EU TOP SECRET, i w przypadku gdy to stosowne, nanosi się oznaczenie ochronne ESDP, przy pomocy urządzeń mechanicznych oraz ręcznie [SII(8)]. Klauzule UE są umieszczane centralnie na dole i na górze każdej strony, a każda strona jest ponumerowana. Każdy dokument jest opatrzony numerem referencyjnym oraz datą; ten numer referencyjny umieszcza się na każdej stronie. Jeżeli dokument jest rozpowszechniany w kilku egzemplarzach, każdy z nich zawiera numer egzemplarza, który umieszcza się na pierwszej stronie, łącznie z całkowitą liczbą stron. Wszystkie załączniki i dołączenia są wymienione na pierwszej stronie [SVIII)].	Deklasyfikacja lub obniżenie może zostać dokonana jedynie przez autora dokumentu lub Sekretarza Generalnego/Wysokiego Przedstawiciela lub SDG, którzy powiadamiają o zmianie dalszych adresatów, którym przesłano dokument lub jego kopię [SIII(9)]. Dokumenty oznaczone klauzulą TRÈS SECRET UE/EU TOP SECRET są niszczone przez centralny rejestr lub rejestr pomocniczy, dla nich właściwy. Każdy zniszczony dokument jest wymieniony na świadectwie zniszczenia, podpisanym przez urzędnika ds. kontroli dokumentów oznaczonych klauzulą TRÈS SECRET UE/EU TOP SECRET oraz urzędnika będącego świadkiem zniszczenia, którymi są osoby upoważnione do dostępu do dokumentów oznaczonych klauzulą TRÈS SECRET UE/EU TOP SECRET. Adnotacji w tym celu dokonuje się w dzienniku. Świadectwa zniszczenia wraz z kartami obiegu przechowuje się w rejestrze przez okres 10 lat [SVII(31)].	Zgromadzone w nadmiernej liczbie kopie oraz dokumenty, które nie są już potrzebne muszą zostać zniszczone [SVII(31)]. Dokumenty oznaczone klauzulą TRÈS SECRET UE/EU TOP SECRET, łącznie z odpadami niejawnymi powstającymi podczas przygotowywania dokumentów TRÈS SECRET UE/EU TOP SECRET, jak np. uszkodzone kopie, wersje robocze, notatki maszynowe czy kalki, są niszczone pod nadzorem urzędnika ds. TRÈS SECRET UE/EU TOP SECRET przez spalenie, zmiażdżenie, pocięcie lub w inny sposób uniemożliwiający ich identyfikację bądź odtworzenie [SVII (31)].

Klasyfikacja	Kiedy	Kto	Oznaczenia	Obniżanie/Deklasyfikacja/Niszczenie	
				Kto	Kiedy
SECRET: Ta klauzula jest stosowana w odniesieniu do informacji i materiałów, których nieuprawnione ujawnienie może spowodować poważną szkodę w podstawowych interesach UE lub jednego lub więcej jej Państw Członkowskich [SII(2)].	Nieuprawnione ujawnienie aktywów oznaczonych klauzulą SECRET UE może: — podnieść napięcia międzynarodowe — znacznie pogorszyć stosunki z rządami państw zaprzyjaźnionych — bezpośrednio zagrażać życiu lub poważnie zaszkodzić w utrzymywaniu porządku publicznego lub bezpieczeństwa osobistego lub swobód — spowodować poważną szkodę w bezpieczeństwie lub skuteczności operacyjnej Państw Członkowskich lub innych sił przyczyniających się, lub utrzymaniu skuteczności bezpieczeństwa o bardzo istotnym znaczeniu lub działalności wywiadu — spowodować poważne straty materialne w interesach finansowych, monetarnych, gospodarczych i handlowych UE lub jednego z jej Państw Członkowskich.	Państwa Członkowskie: Upoważnione osoby (autorzy dokumentów) [SIII(2)]; SGR oraz zdecentralizowane agencje UE: Upoważnione osoby (autorzy dokumentów) [SIII(2)], dyrektorzy Generalni, Sekretarz Generalny/Wysoki Przedstawiciel i SDG. Autorzy określają datę lub okres, z upływem których można obniżyć lub znieść stopień tajności w odniesieniu do zawartości dokumentu. W przeciwnym razie, dokonują przeglądu dokumentów przynajmniej co pięć lat, w celu uzyskania pewności, że pierwotna klauzula tajności jest nadal niezbędna [SIII(l0)].	Klauzulę SECRET UE stosuje się do dokumentów SECRET UE i w przypadku gdy to stosowne, nanosi się oznaczenie ochronne - ESDP, przy pomocy urządzeń mechanicznych oraz ręcznie [SIII(8)]. Klauzule UE są umieszczane centralnie na dole i na górze każdej strony, a każda strona jest ponumerowana. Każdy dokument jest opatrzony numerem referencyjnym oraz datą; ten numer referencyjny umieszcza się na każdej stronie. Jeżeli dokument jest rozpowszechniany w kilku egzemplarzach, każdy z nich zawiera numer egzemplarza, który umieszcza się na pierwszej stronie, łącznie z całkowitą liczbą stron. Wszystkie załączniki i dołączenia są wymienione na pierwszej stronie [SVIII)].	Deklasyfikacji i obniżenia dokonuje jedynie autor dokumentu lub Sekretarz Generalny/Wysoki Przedstawiciel lub SDG, którzy powiadamiają o zmianie dalszych adresatów, którym przesłano dokument lub jego kopię [SIII(9)]. Dokumenty oznaczone klauzulą SECRET UE zostają zniszczone przez rejestr właściwy dla tych dokumentów pod nadzorem osoby upoważnionej do dostępu. Zniszczone dokumenty są wymienione na podpisanych świadectwach zniszczenia, przechowywanych w rejestrze wraz z kartami obiegu przez okres co najmniej 3 lat [SVII (32)].	Zgromadzone w nadmiernej liczbie kopie oraz dokumenty, które nie są już potrzebne muszą zostać zniszczone [SVII(31)]. Dokumenty oznaczone klauzulą SECRET UE, łącznie z odpadami niejawnymi powstającymi podczas przygotowywania dokumentów SECRET UE, jak np. uszkodzone kopie, wersje robocze, notatki maszynowe czy kalki, są niszczone przez spalenie, zmiażdżenie, pocięcie lub w inny sposób uniemożliwiający ich identyfikację bądź odtworzenie [SVII(31),(32)].

Klasyfikacja	Kiedy	Kto	Oznaczenia	Obniżanie/Deklasyfikacja/Niszczenie	
				Kto	Kiedy
CONFIDENTIEL UE: Ta klauzula jest stosowana w odniesieniu do informacji i materiałów, których nieuprawnione ujawnienie może zaszkodzić podstawowym interesom UE lub jednego lub więcej jej Państw Członkowskich [SII (3)].	Nieuprawnione ujawnienie aktywów oznaczonych klauzulą CONFIDENTIEL UE może: — materialnie zaszkodzić stosunkom dyplomatycznym, tzn. spowodować oficjalny protest lub inne sankcje — zaszkodzić osobistemu bezpieczeństwu lub swobodom — spowodować szkodę w bezpieczeństwie lub skuteczności operacyjnej Państw Członkowskich lub innych sił przyczyniających się, lub skuteczności bezpieczeństwa o istotnym znaczeniu lub działalności wywiadu — poważnie osłabić zdolność finansową najważniejszych organizacji — utrudniać prowadzenie dochodzeń i ułatwiać popełnianie poważnych przestępstw — działać w zasadzie na niekorzyść finansowych, monetarnych, gospodarczych i handlowych interesów UE lub Państw Członkowskich — poważnie utrudniać rozwój lub realizację głównych polityk UE — uniemożliwić lub inaczej zakłócić zasadniczo istotną działalność UE	Państwa Członkowskie: Upoważnione osoby (autorzy dokumentów) [SIII(2)]; SGR oraz zdecentralizowane agencje UE: Upoważnione osoby (autorzy dokumentów) [SIII(2)], dyrektorzy Generalni, Sekretarz Generalny/Wysoki Przedstawiciel i SDG. Autorzy określają datę lub okres, z upływem których można obniżyć lub znieść stopień tajności w odniesieniu do zawartości dokumentu. W przeciwnym razie, dokonują przeglądu dokumentów przynajmniej co pięć lat, w celu uzyskania pewności, że pierwotna klauzula tajności jest nadal niezbędna [SIII(10)].	Klauzulę CONFIDENTIEL UE stosuje się do dokumentów CONFIDENTIEL UE, i w przypadku gdy to stosowne, nanosi się oznaczenie ochronne - ESDP, przy pomocy urządzeń mechanicznych oraz ręcznie lub poprzez nadruk na zarejestrowanych drukach, uprzednio ostemplowanych [SII(8)]. Klauzule UE są umieszczane centralnie na dole i na górze każdej strony, a każda strona jest ponumerowana. Każdy dokument jest opatrzony numerem referencyjnym oraz datą. Wszystkie załączniki i dołączenia są wymienione na pierwszej stronie [SVIII)].	Deklasyfikacja i obniżenie może zostać dokonana jedynie przez autora dokumentu lub Sekretarza Generalnego/Wysokiego Przedstawiciela lub SDG, którzy powiadamiają o zmianie dalszych adresatów, którym przesłano dokument lub jego kopię [SIII(9)]. Dokumenty oznaczone klauzulą CONFIDENTIEL UE zostają zniszczone przez rejestr właściwy dla tych dokumentów pod nadzorem osoby upoważnionej do dostępu. Zniszczenie tych dokumentów ewidencjonuje się zgodnie z krajowymi przepisami, a w przypadku SGR lub zdecentralizowanej agencji UE, zgodnie z instrukcjami Sekretarza Generalnego/Wysokiego Przedstawiciela lub SDG [SVII(33)].	Zgromadzone w nadmiernej liczbie kopie oraz dokumenty, które nie są już potrzebne muszą zostać zniszczone [SVII(31)]. Dokumenty oznaczone klauzulą CONFIDENTIEL UE, łącznie z odpadami niejawnymi powstającymi podczas przygotowywania dokumentów CONFIDENTIEL UE, jak np. uszkodzone kopie, wersje robocze, notatki maszynowe czy kalki, są niszczone przez spalenie, zmiażdżenie, pocięcie lub w inny sposób uniemożliwiający ich identyfikację bądź odtworzenie [SVII(31),(33)].

Klasyfikacja	Kiedy	Kto	Oznaczenia	Obniżanie/Deklasyfikacja/Niszczenie	
				Kto	Kiedy
RESTREINT UE: Ta klauzula jest stosowana w odniesieniu do informacji i materiałów, których nieuprawnione ujawnienie może być niekorzystne dla interesów UE lub jednego lub więcej jej Państw Członkowskich [SII(4)].	Nieuprawnione ujawnienie aktywów oznaczonych klauzulą RESTREINT UE może: — niekorzystnie wpłynąć na stosunki dyplomatyczne — spowodować trudną sytuację konkretnych osób — utrudnić utrzymywanie bezpieczeństwa lub skuteczności operacyjnej Państw Członkowskich lub innych sił przyczyniających się — spowodować straty finansowe lub ułatwiać osiąganie nienależnego zysku bądź korzyści przez osoby lub spółki — naruszać właściwe zobowiązania dotyczące utrzymania poufności informacji dostarczanych przez strony trzecie — naruszać ograniczenia ustawowe dotyczące ujawniania informacji — utrudniać prowadzenie dochodzeń i ułatwiać popełnianie poważnych przestępstw — stawiać w niekorzystnej sytuacji UE lub Państwa Członkowskie w negocjacjach politycznych lub handlowych z innymi stronami — utrudniać skuteczny rozwój lub realizację polityki UE — osłabiać właściwe zarządzanie UE i jej działalności.	Państwa Członkowskie: Upoważnione osoby (autorzy dokumentów) [SIII(2)]; SGR oraz zdecentralizowane agencje UE: Upoważnione osoby (autorzy dokumentów) [SIII(2), dyrektorzy Generalni, Sekretarz Generalny/Wysoki Przedstawiciel i SDG. Autorzy określają datę lub okres, z upływem których można obniżyć lub znieść stopień tajności w odniesieniu do zawartości dokumentu. W przeciwnym razie, dokonują przeglądu dokumentów przynajmniej co pięć lat, w celu uzyskania pewności, że pierwotna klauzula tajności jest nadal niezbędna [SIII(10)].	Klauzulę RESTREINT UE stosuje się do dokumentów RESTREINT UE, i w przypadku gdy to stosowne, nanosi się oznaczenie ochronne - ESDP, przy pomocy urządzeń mechanicznych lub elektronicznych [SII(8)]. Klauzule UE są umieszczane centralnie na dole i na górze każdej strony, a każda strona jest ponumerowana. Każdy dokument jest opatrzony numerem referencyjnym oraz datą [SVIII)].	Deklasyfikacja i obniżenie może zostać dokonane jedynie przez autora dokumentu lub Sekretarza Generalnego/Wysokiego Przedstawiciela lub SDG, którzy powiadamiają o zmianie dalszych adresatów, którym przesłano dokument lub jego kopię [SIII(9)]. Dokumenty oznaczone klauzulą RESTREINT UE zostają zniszczone przez rejestr właściwy dla tych dokumentów, zgodnie z krajowymi przepisami, a w przypadku SGR lub zdecentralizowanej agencji UE, zgodnie z instrukcjami Sekretarza Generalnego/Wysokiego Przedstawiciela lub SDG [SVII(34)].	Zgromadzone w nadmiernej liczbie kopie oraz dokumenty, które nie są już potrzebne muszą zostać zniszczone [SVII(31)].

▼B

Dodatek 4

Wytyczne w sprawie udostępniania informacji niejawnych UE państwom trzecim lub organizacjom międzynarodowym

Współpraca na poziomie 1

PROCEDURY

1. Upoważnieniem do udostępniania informacji niejawnych UE państwom, które nie są sygnatariuszami Traktatu o Unii Europejskiej lub innym organizacjom międzynarodowym, których przepisy oraz polityka dotyczące bezpieczeństwa są porównywalne do obowiązujących w UE, dysponuje Rada.

2. Rada może delegować upoważnienie do podjęcia decyzji o udostępnieniu informacji niejawnych. Delegacja ta określi charakter informacji, które mogą zostać udostępnione oraz stopień ich tajności, który zwykle nie będzie wyższy od CONFIDENTIEL UE.

3. Z zastrzeżeniem zawarcia umowy w sprawie bezpieczeństwa, wnioski o udostępnienie informacji niejawnych UE będą przedkładane Sekretarzowi Generalnemu/Wysokiemu Przedstawicielowi przez organy bezpieczeństwa zainteresowanych państw lub organizacji międzynarodowych, określając cele, w jakich informacja ma zostać udostępniona oraz charakter informacji niejawnych do udostępnienia.

   Wnioski może również składać Państwo Członkowskie lub zdecentralizowana agencja UE, które uznają, że udostępnienie informacji niejawnych jest pożądane; określą one cele i korzyści dla UE wynikające z takiego udostępnienia, określając charakter i stopień tajności informacji do udostępnienia.

4. Wnioski będą rozpatrywane przez SGR, który:

   — zasięga opinii Państw Członkowskich lub odpowiednio, zdecentralizowanej agencji UE, będących autorami informacji, która ma zostać udostępniona,

   — ustanawia niezbędne kontakty z organami bezpieczeństwa otrzymującego państwa lub organizacji międzynarodowych, w celu stwierdzenia, czy ich polityka i przepisy dotyczące bezpieczeństwa są odpowiednie by zagwarantować, że udostępnione informacje niejawne będą chronione zgodnie z niniejszymi przepisami dotyczącymi bezpieczeństwa,

   — zasięga opinii technicznych Organów Bezpieczeństwa Narodowego Państw Członkowskich, w sprawie oceny poziomu zaufania, jakim można obdarzyć otrzymujące państwo lub organizację międzynarodową.

5. SGR prześle wniosek oraz zalecenie Biura ds. Bezpieczeństwa Radzie w celu podjęcia decyzji.

PRZEPISY DOTYCZĄCE BEZPIECZEŃSTWA, KTÓRE MAJĄ BYĆ STOSOWANE PRZEZ BENEFICJENTÓW

6. Sekretarz Generalny/Wysoki Przedstawiciel powiadomi otrzymujące państwa lub organizacje międzynarodowe, o decyzji Rady upoważniającej do udostępnienia informacji niejawnych UE, przesyłając taką liczbę egzemplarzy niniejszych przepisów dotyczących bezpieczeństwa, jaką uznaje się za niezbędną. Jeżeli wniosek został złożony przez Państwo Członkowskie, państwo to powiadomi otrzymującego o upoważnieniu do udostępnienia.

   Decyzja o udostępnieniu wejdzie w życie jedynie wtedy, gdy otrzymujący złoży pisemne zapewnienie, że będzie:

   — wykorzystywać informacje wyłącznie w uzgodnionym celu,

   — chronić informacje zgodnie z niniejszymi przepisami dotyczącymi bezpieczeństwa, w szczególności ze specjalnymi przepisami określonymi poniżej.

7. *Pracownicy*

▼B

a) Liczba urzędników posiadających dostęp do informacji niejawnych UE będzie ściśle ograniczona, na podstawie zasady niezbędnej wiedzy, do osób, których zakres obowiązków wymaga takiego dostępu.

b) Wszyscy urzędnicy lub obywatele upoważnieni do posiadania dostępu do informacji niejawnych oznaczonych klauzulą CONFIDENTIEL UE lub wyższą, posiadają albo poświadczenie bezpieczeństwa upoważniające do dostępu do odpowiedniego poziomu albo równoważne poświadczenie bezpieczeństwa oba wydane przez rząd ich państwa.

8. *Przekazywanie dokumentów*

a) Praktyczne procedury dotyczące przekazywania dokumentów zostaną określone w drodze porozumienia na podstawie sekcji VII przepisów Rady dotyczących bezpieczeństwa. W szczególności określą one rejestry, do których będą przekazywane informacje niejawne UE.

b) Jeżeli informacje niejawne, które zostają udostępnione na mocy upoważnienia Rady, obejmują informacje oznaczone klauzulą TRÈS SECRET UE/EU TOP SECRET, otrzymujące państwo lub organizacja międzynarodowa tworzą centralny rejestr UE oraz, jeżeli jest to niezbędne, rejestry pomocnicze UE. Rejestry te będą podlegać sekcji VIII niniejszych przepisów dotyczących bezpieczeństwa.

9. *Ewidencja*

Z chwilą otrzymania przez rejestr dokumentów niejawnych UE oznaczonych klauzulą CONFIDENTIEL UE lub wyższą, rejestr odnotuje je w specjalnym dzienniku ewidencyjnym, prowadzonym przez organizację, który posiada kolumny przeznaczone do wpisania daty otrzymania, dane szczegółowe dokumentu (data, numer referencyjny i numer egzemplarza), jego klauzulę, tytuł, nazwisko odbiorcy lub jego stanowisko, datę zwrotu potwierdzenia odbioru oraz datę zwrotu dokumentu do jego autora w UE lub jego zniszczenia.

10. *Niszczenie*

a) Dokumenty niejawne UE zostaną zniszczone zgodnie z instrukcjami określonymi w sekcji VI niniejszych przepisów dotyczących bezpieczeństwa. Kopie protokołów zniszczenia dokumentów oznaczonych klauzulą SECRET UE oraz TRÈS SECRET UE/EU TOP SECRET będę przesyłane do rejestru UE, który przekazał te dokumenty.

b) Dokumenty niejawne UE zostaną ujęte w awaryjnych planach niszczenia dokumentów, dotyczących własnych dokumentów niejawnych otrzymujących organów.

11. *Ochrona dokumentów*

Zostaną podjęte wszelkie kroki w celu uniemożliwienia nieupoważnionym osobom dostępu do informacji niejawnych UE.

12. *Kopie, tłumaczenia i wyciągi*

Nie można sporządzać fotokopii, dokonywać tłumaczeń dokumentów niejawnych oznaczonych klauzulą CONFIDENTIEL UE lub SECRET UE, lub dokonywać wyciągów, bez zezwolenia szefa danej organizacji ds. bezpieczeństwa, który będzie rejestrował i sprawdzał te kopie, tłumaczenia lub wyciągi oraz stemplował je w razie potrzeby.

Na wykonanie kopii lub tłumaczenia dokumentów oznaczonych klauzulą TRÈS SECRET UE/EU TOP SECRET zgodę może wydać jedynie organ będący autorem informacji, który określi liczbę kopii, jaką można wykonać; jeżeli nie można ustalić autora dokumentu, wniosek zostanie przekazany do Biura ds. Bezpieczeństwa SGR.

13. *Naruszenie bezpieczeństwa*

Jeżeli w odniesieniu do informacji niejawnych UE miało miejsce naruszenie bezpieczeństwa lub podejrzewa się takie naruszenie, należy, z zastrzeżeniem zawarcia porozumienia dotyczącego bezpieczeństwa, niezwłocznie podjąć następujące działania:

▼B

a) przeprowadzić dochodzenie w celu ustalenia okoliczności naruszenia bezpieczeństwa;

b) powiadomić Biuro ds. Bezpieczeństwa SGR, Organy Bezpieczeństwa Narodowego oraz organ wystawiający dokument lub wyraźnie zaznaczyć, że ten ostatni nie został powiadomiony, jeśli tego nie dokonano;

c) podjąć działania w celu zminimalizowania skutków naruszenia bezpieczeństwa;

d) ponownie rozważyć i zastosować środki w celu niedopuszczenia do zaistnienia takiego samego naruszenia w przyszłości;

e) zastosować wszelkie środki zalecane przez Biuro ds. Bezpieczeństwa SGR w celu niedopuszczenia do zaistnienia takiego samego naruszenia w przyszłości.

14. *Kontrole*

Biuro ds. Bezpieczeństwa SGR, na podstawie porozumienia z zainteresowanymi państwami lub organizacjami międzynarodowymi, otrzyma zezwolenie na dokonywanie oceny skuteczności środków ochrony udostępnionych informacji niejawnych UE.

15. *Składanie sprawozdań*

Z zastrzeżeniem zawarcia umowy w sprawie bezpieczeństwa, tak długo jak informacje niejawne UE znajdują się w posiadaniu państwa lub organizacji międzynarodowej, powinny one przedkładać roczne sprawozdanie, w terminie określonym wraz z udzieleniem upoważnienia na udostępnienie informacji, potwierdzające przestrzeganie niniejszych przepisów dotyczących bezpieczeństwa.

▼B

Dodatek 5

Wytyczne w sprawie udostępniania informacji niejawnych UE państwom trzecim lub organizacjom międzynarodowym

Współpraca na poziomie 2

PROCEDURA

1. Upoważnieniem do udostępniania informacji niejawnych UE państwom trzecim lub organizacjom międzynarodowym, których polityka i przepisy dotyczące bezpieczeństwa znacznie różnią się od obowiązujących w UE, dysponuje Rada. W zasadzie, ogranicza się to do informacji oznaczonych klauzulami od RESTRICTED UE do SECRET UE włącznie; nie dotyczy to informacji państwowych specjalnie zastrzeżonych dla Państw Członkowskich i kategorii informacji niejawnych UE chronionych za pomocą specjalnych oznaczeń.

2. Rada może delegować upoważnienie do podjęcia tej decyzji; przy delegowaniu upoważnienia, w ramach ograniczeń określonych w ust. 1, określi charakter informacji, które mogą zostać udostępnione oraz poziom ich zaklasyfikowania, który zwykle nie będzie wyższy od RESTREINT UE.

3. Z zastrzeżeniem zawarcia umowy w sprawie bezpieczeństwa, wnioski o udostępnienie informacji niejawnych UE będą przedkładane Sekretarzowi Generalnemu/Wysokiemu Przedstawicielowi przez organy bezpieczeństwa zainteresowanych państw lub organizacji międzynarodowych, określając cele, w jakich informacja ma zostać udostępniona oraz charakter informacji niejawnych do udostępnienia.

   Wnioski może również składać Państwo Członkowskie lub zdecentralizowana agencja UE, które uznają, że udostępnienie informacji niejawnych jest pożądane; określą one cele i korzyści dla UE wynikające z takiego udostępnienia, określając charakter i stopień tajności informacji do udostępnienia.

4. Wnioski będą rozpatrywane przez SGR, który:

   — zasięga opinii Państw Członkowskich lub odpowiednio, zdecentralizowanej agencji UE, będących autorami informacji, która ma zostać udostępniona,

   — ustanawia wstępne kontakty z organami bezpieczeństwa otrzymującego państwa lub organizacji międzynarodowych, w celu uzyskania informacji dotyczących ich temat polityki i przepisów dotyczących bezpieczeństwa, w szczególności w celu sporządzenia tabeli porównującej klasyfikacje stosowane w UE i zainteresowanym państwie lub organizacji,

   — organizuje posiedzenie Komitetu ds. Bezpieczeństwa Rady lub jeżeli jest to niezbędne, w drodze cichej procedury, zwraca się do Organów Bezpieczeństwa Narodowego Państw Członkowskich, w celu uzyskania technicznej opinii Komitetu ds. Bezpieczeństwa.

5. Techniczna opinia Komitetu ds. Bezpieczeństwa będzie dotyczyć następujących kwestii:

   — zaufania, jakim można obdarzyć otrzymujące państwa lub organizacje międzynarodowe, w celu oceny zagrożeń dotyczących bezpieczeństwa, na które jest narażona UE lub jej Państwa Członkowskie,

   — oceny możliwości otrzymujących w zakresie ochrony informacji niejawnych udostępnionych przez UE,

   — propozycji dotyczących praktycznych procedur odnoszących się do korzystania z informacji niejawnych (na przykład: dostarczanie niepełnych wersji tekstu) i przekazywania dokumentów (zachowywania lub usuwania nagłówków informujących o stopniu tajności, specjalnych oznaczeń itd.),

▼B

— obniżenia lub deklasyfikacji przez organy wytwarzające dokument, przed udostępnieniem informacji państwom beneficjentom lub organizacjom międzynarodowym ([1]).

6. Sekretarz Generalny/Wysoki Przedstawiciel prześle Radzie, w celu podjęcia decyzji, wniosek oraz techniczną opinię Komitetu ds. Bezpieczeństwa Rady uzyskaną przez Biuro ds. Bezpieczeństwa SGR.

PRZEPISY DOTYCZĄCE BEZPIECZEŃSTWA, KTÓRE MAJĄ BYĆ STOSOWANE PRZEZ BENEFICJENTÓW

7. Sekretarz Generalny/Wysoki Przedstawiciel powiadomi Państwa Członkowskie lub organizacje międzynarodowe o decyzji Rady upoważniającej do udostępnienia informacji niejawnych UE wraz z tabelą porównującą klasyfikację stosowaną w UE i zainteresowanych państwach lub organizacjach. Jeżeli wniosek został złożony przez Państwo Członkowskie, państwo to powiadomi beneficjenta o upoważnieniu do udostępnienia.

   Decyzja o udostępnieniu wejdzie w życie jedynie wtedy, gdy otrzymujący złoży pisemne zapewnienie, że będzie:

   — wykorzystywać informacje wyłącznie w uzgodnionym celu,

   — chronić informacje zgodnie z przepisami ustanowionymi przez Radę.

8. Następujące reguły dotyczące ochrony zostaną ustanowione, o ile Rada, po otrzymaniu technicznej opinii Komitetu ds. Bezpieczeństwa Rady, zdecyduje w sprawie szczególnej procedury dotyczącej korzystania z dokumentów niejawnych UE (usunięcie wzmianki o klauzuli UE, specjalnego oznaczenia itd.).

   W tym przypadku reguły zostaną dostosowane.

9. *Pracownicy*

   a) Liczba urzędników posiadających dostęp do informacji niejawnych UE musi zostać ściśle ograniczona, na podstawie zasady niezbędnej wiedzy, do osób, których zakres obowiązków wymaga takiego dostępu.

   b) Wszyscy urzędnicy lub obywatele upoważnieni do posiadania dostępu do informacji niejawnych udostępnionych przez UE posiadają krajowe poświadczenie bezpieczeństwa lub upoważnienie do dostępu, w przypadku krajowych informacji niejawnych o odpowiednim poziomie równoważnym z poziomem UE, zgodnie z tabelą porównawczą.

   c) Te krajowe poświadczenia bezpieczeństwa lub upoważnienia zostaną przekazane, w celu informacyjnym Sekretarzowi Generalnemu/Wysokiemu Przedstawicielowi.

10. *Przekazywanie dokumentów*

   a) Praktyczne procedury dotyczące przekazywania dokumentów zostaną uzgodnione w drodze porozumienia między Biurem ds. Bezpieczeństwa SGR a organami bezpieczeństwa otrzymujących państw lub organizacji międzynarodowych, na podstawie reguł określonych w sekcji VII niniejszych przepisów. W szczególności określą one adresy, pod które dokumenty muszą zostać przekazane oraz kuriera lub usługi pocztowe wykorzystywane do przekazywania informacji niejawnych UE.

   b) Dokumenty oznaczone klauzulą CONFIDENTIEL UE lub wyższą, będą przekazywane w podwójnej kopercie. Wewnętrzna koperta zostanie oznaczona „UE” wraz z klauzulą tajności. Formularz potwierdzenia odbioru będzie załączony do każdego dokumentu niejawnego. Formularz potwierdzenia odbioru, który sam nie będzie oznaczony klauzulą, będzie określał jedynie dane szczegółowe dokumentu (numer referencyjny, datę, liczbę egzemplarzy) oraz język dokumentu, ale nie tytuł.

([1]) To pociąga za sobą zastosowanie przez organy będące autorem dokumentu procedury określonej w ust. 9 sekcji III, w odniesieniu do wszystkich egzemplarzy znajdujących się w obiegu na terytorium UE.

▼B

c) Wewnętrzna koperta zostanie następnie umieszczona w kopercie zewnętrznej, która zostanie oznaczona numerem przesyłki do celów potwierdzenia odbioru. Zewnętrzna koperta nie będzie oznaczona klauzulą tajności.

d) Potwierdzenie odbioru, zawierające numer przesyłki, zawsze będzie przekazywane kurierom.

11. *Ewidencja przy odbiorze*

OBN państwa adresata lub ich odpowiednik w państwie, otrzymującym w imieniu jego rządu informacje niejawne przekazane przez UE, lub biuro bezpieczeństwa otrzymującej organizacji międzynarodowej, założą specjalny rejestr w celu ewidencjonowania informacje niejawne UE, w chwili ich odbioru. Rejestr będzie zawierał kolumny przeznaczone do wpisania daty wpływu, danych szczegółowych dokumentu (data, numer referencyjny i numer egzemplarza), jego klauzuli, tytułu, nazwiska adresata lub jego stanowiska, daty zwrotu potwierdzenia odbioru oraz daty zwrotu dokumentu do UE lub jego zniszczenia.

12. *Zwrot dokumentów*

Jeżeli odbiorca zwraca dokument niejawny Radzie lub Państwu Członkowskiemu, które go udostępniły, będzie on postępował zgodnie z przepisami określonymi w ust. 10.

13. *Ochrona*

a) Jeżeli dokumenty nie są w użyciu, będą przechowywane w pojemnikach bezpieczeństwa, które są zatwierdzone do przechowywania krajowych dokumentów niejawnych o takim samym stopniu tajności. Pojemnik nie będzie nosił oznaczeń dotyczących jego zawartości, które będą dostępne wyłącznie osobom upoważnionym do korzystania z informacji niejawnych UE. W przypadku gdy używa się zamków szyfrowych, kombinacja szyfrowa będzie znana tylko tym urzędnikom w państwie lub organizacji, którzy posiadają upoważnienie do dostępu do informacji niejawnych UE przechowywanych w pojemniku i będzie zmieniana co sześć miesięcy, lub wcześniej, w przypadku przeniesienia urzędnika lub wycofania upoważnienia do dostępu jednego z urzędników znających kombinację szyfrową, lub jeżeli występuje ryzyko nieuprawnionego ujawnienia.

b) Dokumenty niejawne UE będą wyjmowane z pojemnika bezpieczeństwa jedynie przez tych urzędników, którzy posiadają upoważnienie do dostępu do dokumentów niejawnych UE oraz potrzebę niezbędnej wiedzy. Urzędnicy ci będą odpowiedzialni za bezpieczne przechowywanie tych dokumentów tak długo, jak długo są w ich posiadaniu oraz, w szczególności, będą odpowiedzialni za zapewnienie, że nikt nieupoważniony nie będzie miał dostępu do dokumentów. Będą oni również zapewniać, że dokumenty są przechowywane w pojemniku bezpieczeństwa, po tym jak skończyli ich konsultację a także po godzinach pracy.

c) Nie można sporządzać fotokopii dokumentów niejawnych oznaczonych klauzulą CONFIDENTIEL UE lub wyższą, ani dokonywać wyciągów, bez zezwolenia Biura ds. Bezpieczeństwa SGR.

d) Procedurę na wypadek nagłej potrzeby szybkiego i całkowitego zniszczenia dokumentów, powinno się ustanowić i przedstawić do zatwierdzenia do Biura ds. Bezpieczeństwa SGR.

14. *Bezpieczeństwo fizyczne*

a) Jeżeli się z nich nie korzysta, pojemniki bezpieczeństwa używane do przechowywania dokumentów niejawnych UE są przez cały czas zamknięte.

b) Jeżeli niezbędne jest dopuszczenie do pracy lub wejścia do pomieszczenia, gdzie znajdują się takie pojemniki bezpieczeństwa, osób zajmujących się konserwacją lub sprzątaniem, przez cały czas towarzyszy im członek służb bezpieczeństwa państwa lub organizacji lub urzędnik

▼B

przede wszystkim odpowiedzialny za nadzór nad bezpieczeństwem pomieszczenia.

c) Poza normalnymi godzinami pracy (w nocy, w czasie weekendów i dni ustawowo wolnych od pracy) pojemniki bezpieczeństwa zawierające dokumenty niejawne UE są chronione albo przez strażników albo przez automatyczny system alarmowy.

15. *Naruszenie bezpieczeństwa*

Jeżeli w odniesieniu do informacji niejawnych UE miało miejsce naruszenie bezpieczeństwa lub podejrzewa się takie naruszenie, należy niezwłocznie podjąć następujące działania:

a) niezwłocznie przesłać sprawozdanie do Biura ds. Bezpieczeństwa SGR lub OBN Państwa Członkowskiego, które podjęło inicjatywę przesyłania dokumentów (wraz z kopią dla Biura ds. Bezpieczeństwa SGR);

b) przeprowadzić dochodzenie, po zakończeniu którego należy przedłożyć kompletne sprawozdanie organowi bezpieczeństwa (patrz lit. a) powyżej). Należy przyjąć niezbędne środki w celu zaradzenia zaistniałej sytuacji.

16. *Kontrole*

Zezwoli się Biurze ds. Bezpieczeństwa SGR, na podstawie porozumienia z zainteresowanymi państwami lub organizacjami międzynarodowymi, na dokonywanie oceny skuteczności środków ochrony w odniesieniu do udostępnionych informacji niejawnych UE.

17. *Zdawanie sprawozdania*

Tak długo jak państwo lub organizacja międzynarodowa posiada informacje niejawne UE, przedkładają one roczne sprawozdanie, w terminie określonym wraz z udzieleniem upoważnienia na udostępnienie informacji, potwierdzające przestrzeganie niniejszych przepisów dotyczących bezpieczeństwa.

▼B

Dodatek 6

Wytyczne w sprawie udostępniania informacji niejawnych UE państwom trzecim lub organizacjom międzynarodowym

Współpraca na poziomie 3

PROCEDURA

1. Od czasu do czasu, w pewnych szczególnych okolicznościach, Rada może wyrazić chęć podjęcia współpracy z państwami lub organizacjami, które nie są w stanie udzielić zapewnień wymaganych przez niniejsze przepisy bezpieczeństwa, jednakże względy współpracy mogą wymagać udostępnienia informacji niejawnych UE. Takie udostępnienie będzie wyłączne w odniesieniu do informacji krajowych specjalnie zastrzeżonych dla Państw Członkowskich.

2. W takich szczególnych okolicznościach, wnioski dotyczące współpracy z UE, zarówno od państw trzecich lub organizacji międzynarodowych, jak i złożone przez Państwa Członkowskie, lub, gdzie stosowne, przez zdecentralizowane agencje UE, będą najpierw rozważane co do swej istoty przez Radę, która będzie, w miarę potrzeby, zasięgać opinii Państw Członkowskich lub zdecentralizowane agencji wytwarzającej informacje. Rada rozważy zasadność udostępnienia informacji niejawnych, oceni potrzebę „niezbędnej wiedzy" otrzymujących oraz zdecyduje o charakterze informacji niejawnych, które mogą być podane do wiadomości.

3. Jeżeli Rada przychyla się do udostępnienia, Sekretarz Generalny/Wysoki Przedstawiciel będzie odpowiedzialny za zwołanie Komitetu ds. Bezpieczeństwa Rady lub zwrócenie się do Organów Bezpieczeństwa Narodowego Państw Członkowskich, jeżeli jest to niezbędne, w drodze cichej procedury, w celu uzyskania technicznej opinii Komitetu ds. Bezpieczeństwa.

4. Techniczna opinia Komitetu ds. Bezpieczeństwa będzie dotyczyć następujących kwestii:

   a) oceny zagrożeń dla bezpieczeństwa, na jakie narażona jest UE lub jej Państw Członkowskich;

   b) stopnia tajności informacji, które mogą zostać udostępnione, w odpowiednim przypadku, ze względu na charakter informacji;

   c) obniżenia lub deklasyfikacji informacji przez organy wystawiające dokument, przed udostępnieniem informacji zainteresowanym państwom lub organizacjom międzynarodowym ([1]);

   d) procedur dotyczących korzystania z dokumentów, które mają zostać udostępnione (patrz ust. 5 poniżej);

   e) możliwych metod przekazywania dokumentów (korzystanie z publicznych usług pocztowych, publicznych lub zabezpieczonych systemów telekomunikacji, poczty dyplomatycznej, upoważnionych kurierów itd.).

5. Dokumenty udostępniane państwom lub organizacjom objętym niniejszym dodatkiem, w zasadzie będą przygotowywane bez odniesienia do źródła lub klauzuli UE. Komitet ds. Bezpieczeństwa Rady może zalecić zastosowanie:

   — specjalnego oznaczenia lub kodu,

   — specjalnego systemu klasyfikacji łączącego sensytywność informacji ze środkami kontroli wymaganymi w metodach przekazywania dokumentów przez otrzymującego (patrz przykłady w ust. 14).

([1]) To pociąga za sobą zastosowanie przez organ wytwarzający procedury określonej w ust. 9 sekcji III, w odniesieniu do wszystkich egzemplarzy znajdujących się w obiegu na terytorium UE.

▼B

6. Biuro ds. Bezpieczeństwa SGR przedstawi Radzie techniczną opinię Komitetu ds. Bezpieczeństwa Rady, załączając w miarę potrzeby proponowane delegacje uprawnień wymaganych do wykonania zadania, szczególnie w nagłych przypadkach.

7. Wraz z zatwierdzeniem przez Radę udostępnienia informacji niejawnych UE i praktycznych procedur wykonania powyższego, Biuro ds. Bezpieczeństwa SGR nawiąże niezbędny kontakt z organem bezpieczeństwa zainteresowanego państwa lub organizacji w celu ułatwienia zastosowania przewidzianych środków bezpieczeństwa.

8. Jako odniesienie, Biuro ds. Bezpieczeństwa SGR rozpowszechni wśród Państw Członkowskich i, gdzie stosowne, wśród zainteresowanych zdecentralizowanych agencji UE, tabelę podsumowującą charakter i klauzule informacji oraz zawierającą wykaz organizacji i państw, którym można je udostępnić, zgodnie z decyzją Rady.

9. OBN Państwa Członkowskiego dokonującego udostępnienia lub Biuro ds. Bezpieczeństwa SGR podejmą wszelkie niezbędne środki w celu ułatwienie dokonania oceny jakichkolwiek następstw szkody oraz przeglądu procedur.

10. W każdym przypadku gdy warunki współpracy zostają zmienione, należy ponownie zwrócić się do Rady.

PRZEPISY DOTYCZĄCE BEZPIECZEŃSTWA, KTÓRE MAJĄ BYĆ STOSOWANE PRZEZ BENEFICJENTÓW

11. Sekretarz Generalny/Wysoki Przedstawiciel powiadomi Państwa Członkowskie lub organizacje międzynarodowe o decyzji Rady upoważniającej do udostępnienia informacji niejawnych UE wraz ze szczegółowymi regułami w zakresie ochrony, zaproponowanymi przez Komitet ds. Bezpieczeństwa Rady i zatwierdzonymi przez Radę. Jeżeli wniosek został złożony przez Państwo Członkowskie, państwo to powiadomi otrzymującego o upoważnieniu do udostępnienia.

    Decyzja o udostępnieniu wejdzie w życie jedynie wtedy, gdy otrzymujący złoży pisemne zapewnienie, że będzie:

    — wykorzystywać informacje wyłącznie w celu współpracy określonym przez Radę,

    — zapewnienia informacji dotyczących ochrony wymaganej przez Radę.

12. *Przekazywanie dokumentów*

    a) Praktyczne procedury dotyczące przekazywania dokumentów zostaną uzgodnione w drodze porozumienia między Biurem ds. Bezpieczeństwa SGR a organami bezpieczeństwa otrzymujących państw lub organizacji międzynarodowych. W szczególności określą one dokładne adresy, pod które dokumenty muszą zostać przekazane.

    b) Dokumenty oznaczone klauzulą CONFIDENTIEL UE lub wyższą, zostaną przekazane w podwójnej kopercie. Wewnętrzna koperta będzie oznaczona szczególną pieczęcią lub kodem uprzednio określonym oraz wzmianką o specjalnej klauzuli zatwierdzonej w odniesieniu do dokumentu. Formularz potwierdzenia odbioru będzie załączony do każdego dokumentu niejawnego. Formularz potwierdzenia odbioru, który sam nie będzie oznaczony klauzulą, będzie określał jedynie dane szczegółowe dokumentu (numer referencyjny, datę, liczbę egzemplarzy) oraz język dokumentu, ale nie tytuł.

    c) Wewnętrzna koperta zostanie następnie umieszczona w kopercie zewnętrznej, która zostanie oznaczona numerem przesyłki do celów potwierdzenia odbioru. Zewnętrzna koperta nie będzie oznaczona klauzulą tajności.

    d) Potwierdzenie odbioru, zawierające numer przesyłki, zawsze będzie przekazywane kurierom.

13. *Ewidencja przy odbiorze*

▼B

OBN państwa adresata lub ich odpowiednik w państwie, otrzymującym w imieniu jego rządu informacje niejawne przekazane przez UE, lub biuro bezpieczeństwa otrzymującej organizacji międzynarodowej, założą specjalny rejestr w celu ewidencjonowania informacji niejawnych UE, w chwili ich odbioru. Rejestr będzie zawierał kolumny przeznaczone do wpisania daty wpływu, danych szczegółowych dokumentu (data, numer referencyjny i numer egzemplarza), jego klauzuli, tytułu, nazwiska adresata lub jego stanowiska, daty zwrotu potwierdzenia odbioru oraz daty zwrotu dokumentu do UE lub jego zniszczenia.

14. *Korzystanie z wymienionych dokumentów niejawnych i ochrona*

a) Informacje oznaczone klauzulą SECRET UE będą przetwarzane przez specjalnie wyznaczonych urzędników upoważnionych do posiadania dostępu do informacji oznaczonych taką klauzulą. Będą one przechowywane bezpiecznych szafach dobrej jakości, które mogą być otwarte jedynie przez osoby upoważnione do posiadania dostępu do mieszczących się w nich informacji. Strefy, w których znajdują się te szafy, są stale strzeżone oraz zostanie zainstalowany system kontroli zapewniający, że jedynie należycie upoważnione osoby mogą wejść na ich teren. Informacje oznaczone klauzulą SECRET UE będą przekazywane w przesyłkach dyplomatycznych, za pomocą bezpiecznych usług pocztowych lub bezpiecznej telekomunikacji. Dokumenty oznaczone klauzulą SECRET UE mogą być kopiowane wyłącznie za pisemną zgodą organu wytwarzającego, który je wystawił. Wszystkie egzemplarze będą rejestrowane i monitorowane. Potwierdzenia odbioru będą wystawiane w odniesieniu do wszystkich operacji związanych z dokumentami oznaczonymi klauzulą SECRET UE.

b) Informacje oznaczone klauzulą CONFIDENTIEL UE będą przetwarzane przez należycie wyznaczonych urzędników upoważnionych do posiadania informacji w nich zawartych. Dokumenty będą przechowywane w bezpiecznych zamykanych szafach w kontrolowanych strefach.

Informacje oznaczone klauzulą CONFIDENTIEL UE będą przekazywane w formie przesyłek dyplomatycznych, za pomocą usług poczty wojskowej i bezpiecznej telekomunikacji. Organ otrzymujący może wykonywać kopie, odnotowując ich ilość i dane dotyczące dystrybucji w specjalnym rejestrze.

c) Informacje oznaczone klauzulą RESTREINT UE będą przetwarzane w pomieszczeniach, do których nie mają dostępu nieupoważnieni pracownicy oraz przechowywane w zamykanych pojemnikach. Dokumenty mogą być przekazywane za pośrednictwem publicznych usług pocztowych w formie przesyłek poleconych w podwójnej kopercie oraz w sytuacjach nagłych podczas operacji, za pomocą niechronionych publicznych systemów telekomunikacyjnych. Odbiorcy mogą wykonywać kopie.

d) Informacje nieoznaczone klauzulą nie wymagają podejmowania specjalnych środków ochronnych i mogą być przekazywane za pośrednictwem poczty i za pomocą publicznych systemów telekomunikacyjnych. Adresaci mogą wykonywać kopie.

15. *Niszczenie dokumentów*

Dokumenty, które nie są dłużej potrzebne muszą zostać zniszczone. W przypadku dokumentów oznaczonych klauzulą RESTREINT UE i CONFIDENTIEL UE, należy umieścić właściwą adnotację w specjalnych rejestrach. W przypadku dokumentów oznaczonych klauzulą SECRET UE, świadectwa zniszczenia zostaną wydane i podpisane przez dwie osoby, będące świadkami zniszczenia.

16. *Naruszenie bezpieczeństwa*

Jeżeli informacje oznaczone klauzulą CONFIDENTIEL UE lub SECRET UE zostają w sposób nieuprawniony ujawnione lub istnieje podejrzenie takiego ujawnienia, OBN państwa lub szef bezpieczeństwa organizacji przeprowadzi dochodzenie dotyczące okoliczności nieuprawnionego ujawnienia.

▼B

Jeżeli dochodzenie przynosi pozytywne wyniki, powiadamia się organy, które wystawiły dokument. Podjęte zostaną niezbędne kroki w celu udoskonalenie nieodpowiednich procedur lub metod przechowywania, jeżeli to one spowodowały nieuprawnione ujawnienie. Sekretarz Generalny/Wysoki Przedstawiciel Rady lub OBN Państwa Członkowskiego, który udostępnił ujawnioną w sposób nieuprawniony informację może zwrócić się do beneficjenta w sprawie szczegółów dotyczących dochodzenia.