

IV

*(Informacje)*INFORMACJE INSTYTUCJI, ORGANÓW I JEDNOSTEK ORGANIZACYJNYCH
UNII EUROPEJSKIEJ

EUROPEJSKA SŁUŻBA DZIAŁAŃ ZEWNĘTRZNYCH

**Decyzja Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa
z dnia 19 września 2017 r. w sprawie przepisów bezpieczeństwa mających zastosowanie do
Europejskiej Służby Działań Zewnętrznych**

ADMIN(2017) 10

(2018/C 126/01)

WYSOKI PRZEDSTAWICIEL UNII DO SPRAW ZAGRANICZNYCH I POLITYKI BEZPIECZEŃSTWA,

uwzględniając decyzję Rady 2010/427/UE z dnia 26 lipca 2010 r. określającą organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych ⁽¹⁾ („ESDZ”),

uwzględniając opinię Komitetu, o którym mowa w art. 9 ust. 6 decyzji Wysokiego Przedstawiciela z dnia 15 czerwca 2011 r. w sprawie przepisów bezpieczeństwa mających zastosowanie do Europejskiej Służby Działań Zewnętrznych ⁽²⁾,

a także mając na uwadze, co następuje:

- (1) W ESDZ, jako funkcjonalnie autonomicznym organie Unii Europejskiej (UE), powinny obowiązywać przepisy bezpieczeństwa, o których mowa w art. 10 ust. 1 decyzji Rady 2010/427/UE.
- (2) Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (dalej zwany „Wysokim Przedstawicielem”) powinien w drodze decyzji określić przepisy bezpieczeństwa mające zastosowanie do ESDZ, obejmujące wszystkie aspekty bezpieczeństwa w zakresie funkcjonowania ESDZ, aby umożliwić jej skuteczne zarządzanie ryzykiem, na jakie narażony jest personel podlegający odpowiedzialności ESDZ, jego majątek rzeczowy, informacje i osoby odwiedzające, a także aby umożliwić jej wypełnianie w tym względzie jej zadań wynikających z obowiązku dochowania należytej staranności.
- (3) W szczególności personelowi podlegającemu odpowiedzialności ESDZ, majątkowi rzeczowemu ESDZ, w tym systemom teleinformatycznym, informacjom i osobom odwiedzającym należy zapewnić poziom ochrony zgodny z najlepszymi praktykami stosowanymi w Radzie, Komisji, państwach członkowskich oraz w stosownych przypadkach w organizacjach międzynarodowych.
- (4) Przepisy bezpieczeństwa mające zastosowanie do ESDZ powinny przyczynić się do stworzenia w UE bardziej spójnych kompleksowych ogólnych ram ochrony informacji niejawnych UE (dalej zwanych „EUCI”) w oparciu o przepisy bezpieczeństwa przyjęte przez Radę Unii Europejskiej (dalej zwaną „Radą”) oraz przez Komisję Europejską i przy zachowaniu możliwie jak największej spójności z tymi przepisami.
- (5) ESDZ, Rada i Komisja zobowiązują się stosować równoważne normy bezpieczeństwa w celu ochrony EUCI.
- (6) Niniejsza decyzja zostaje przyjęta, nie naruszając art. 15 i 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) oraz aktów prawnych służących wykonaniu tych artykułów.

⁽¹⁾ Dz.U. L 201 z 3.8.2010, s. 30.

⁽²⁾ Dz.U. C 304 z 15.10.2011, s. 7.

- (7) Konieczne jest określenie zasad organizacji bezpieczeństwa w ESDZ oraz przydzielenie zadań w zakresie bezpieczeństwa w ramach struktur ESDZ.
- (8) Wysoki Przedstawiciel powinien w razie potrzeby korzystać z odnośnej wiedzy fachowej w państwach członkowskich, Sekretariacie Generalnym Rady oraz Komisji Europejskiej.
- (9) Wysoki Przedstawiciel powinien podjąć wszelkie niezbędne środki w celu wprowadzenia w życie niniejszych przepisów przy wsparciu państw członkowskich, Sekretariatu Generalnego Rady i Komisji Europejskiej.
- (10) Sekretarz Generalny ESDZ jest organem ESDZ ds. bezpieczeństwa i art. 1 decyzji Sekretarza Generalnego Europejskiej Służby Działań Zewnętrznych ADMIN(2015) 34 z dnia 14 września 2015 r. stanowi, że funkcje w zakresie bezpieczeństwa organu ds. bezpieczeństwa, przewidziane przepisami bezpieczeństwa ESDZ, wykonuje dyrektor generalny ds. budżetu i administracji,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Cel i zakres stosowania

W niniejszej decyzji ustanawia się przepisy bezpieczeństwa mające zastosowanie do Europejskiej Służby Działań Zewnętrznych (dalej zwane „przepisami bezpieczeństwa ESDZ”).

Zgodnie z art. 10 ust. 1 decyzji Rady 2010/427/UE z dnia 26 lipca 2010 r. określającej organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych przepisy te mają zastosowanie do wszystkich członków personelu ESDZ oraz wszystkich członków personelu w delegaturach Unii, niezależnie od ich statusu administracyjnego lub pochodzenia; określają one ogólne ramy regulacyjne skutecznego zarządzania ryzykiem, na jakie narażony jest personel podlegający odpowiedzialności ESDZ, zgodnie z jego definicją w art. 2, a także lokale, majątek rzeczowy, informacje i osoby odwiedzające ESDZ.

Artykuł 2

Definicje

Do celów niniejszej decyzji stosuje się następujące definicje:

- a) „personel ESDZ” oznacza urzędników i innych pracowników ESDZ, w tym pracowników służb dyplomatycznych państw członkowskich mianowanych na czas określony oraz oddelegowanych ekspertów krajowych w rozumieniu art. 6 decyzji Rady 2010/427/UE z dnia 26 lipca 2010 r. określającej organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych;
- b) „personel podlegający odpowiedzialności ESDZ” oznacza personel ESDZ w siedzibie głównej i w delegaturach Unii oraz wszystkich pozostałych członków personelu w delegaturach Unii, niezależnie od ich statusu administracyjnego lub pochodzenia, a także, w kontekście niniejszej decyzji, Wysokiego Przedstawiciela i w stosownych przypadkach innych członków personelu znajdujących się w siedzibie głównej ESDZ;
- c) „osoby na utrzymaniu” oznaczają członków rodziny członków personelu podlegającego odpowiedzialności ESDZ w delegaturach Unii, zamieszkujących w tym samym gospodarstwie domowym, co dany członek personelu, zgodnie z informacją przekazaną ministerstwu spraw zagranicznych państwa przyjmującego;
- d) „lokale ESDZ” oznaczają wszelkie obiekty ESDZ, w tym budynki, biura, pomieszczenia i inne miejsca, a także pomieszczenia, w których znajdują się systemy teleinformatyczne (w tym systemy, w których przetwarzane są EUCI), w których ESDZ stale lub czasowo prowadzi działalność;
- e) „interesy bezpieczeństwa ESDZ” obejmują personel podlegający odpowiedzialności ESDZ i osoby będące na ich utrzymaniu, a także lokale ESDZ, jej majątek rzeczowy, w tym systemy teleinformatyczne, oraz informacje i osoby odwiedzające;
- f) „informacje niejawne UE” („EUCI”) oznaczają wszelkie informacje lub materiały objęte klauzulą tajności UE, których nieuprawnione ujawnienie mogłoby w różnym stopniu wyrządzić szkodę interesom Unii Europejskiej lub interesom co najmniej jednego państwa członkowskiego;

- g) „delegatury Unii” oznaczają delegatury w państwach trzecich i organizacjach międzynarodowych, o których mowa w art. 1 ust. 4 decyzji Rady 2010/427/UE z dnia 26 lipca 2010 r. określającej organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych.

Pozostałe definicje zawarto w odpowiednich załącznikach oraz w dodatku A.

Artykuł 3

Obowiązek dochowania należytej staranności

1. Przepisy bezpieczeństwa ESDZ mają na celu realizację przez ESDZ jej zadań wynikających z obowiązku dochowania należytej staranności.
2. Obowiązek dochowania należytej staranności obejmuje podjęcie wszelkich racjonalnych kroków w zakresie wdrożenia środków bezpieczeństwa mających zapobiec dającej się racjonalnie przewidzieć szkodzie dla interesów bezpieczeństwa ESDZ.

Obejmuje to aspekty bezpieczeństwa i ochrony, w tym wynikające z wszelkiego rodzaju sytuacji nagłych lub kryzysowych.
3. Biorąc pod uwagę obowiązek dochowania należytej staranności spoczywający na państwach członkowskich, instytucjach i organach UE oraz innych stronach, których personel znajduje się w delegaturach Unii lub ich lokalach, bądź obowiązek taki spoczywający na ESDZ w sytuacji, gdy delegatury Unii korzystają z lokali wyżej wymienionych innych stron, ESDZ zawiera porozumienia administracyjne z poszczególnymi wyżej wymienionymi podmiotami, określając role, zakresy odpowiedzialności i zadania poszczególnych stron i mechanizmy współpracy.

Artykuł 4

Bezpieczeństwo fizyczne i bezpieczeństwo infrastruktury

1. W celu ochrony interesów bezpieczeństwa ESDZ wprowadza ona wszelkie właściwe środki bezpieczeństwa (o charakterze stałym lub tymczasowym), w tym w zakresie kontroli dostępu, we wszystkich lokalach ESDZ. Takie środki uwzględnia się przy projektowaniu i planowaniu nowych lokali lub przed wynajęciem lokali istniejących.
2. Ze względów bezpieczeństwa możliwe jest nakładanie na określony czas i na określonych obszarach szczególnych obowiązków lub ograniczeń na personel podlegający odpowiedzialności ESDZ i na osoby będące na jego utrzymaniu.
3. Środki, o których mowa w ust. 1 i 2, są współmierne do oszacowanego ryzyka.

Artykuł 5

Stopnie alarmowe i zarządzanie sytuacjami kryzysowymi

1. Organ ESDZ ds. bezpieczeństwa, zdefiniowany w art. 13 ust. 1 sekcji I, jest odpowiedzialny za wdrożenie odpowiednich środków w zakresie stopni alarmowych w przewidywaniu zagrożeń i incydentów mających wpływ na bezpieczeństwo w ESDZ lub w odpowiedzi na takie zagrożenia i incydenty oraz jest odpowiedzialny za środki wymagane do zarządzania sytuacjami kryzysowymi.
2. Środki w zakresie stopni alarmowych, o których mowa w ust. 1, są współmierne do poziomu zagrożenia dla bezpieczeństwa. Poziomy stopni alarmowych określa się w ściślejszej współpracy z właściwymi służbami innych instytucji, agencji i organów Unii oraz służbami państwa członkowskiego lub państw członkowskich, w których znajdują się lokale ESDZ.
3. Organ ESDZ ds. bezpieczeństwa jest punktem kontaktowym w sprawach dotyczących stopni alarmowych i zarządzania sytuacjami kryzysowymi.

Artykuł 6

Ochrona informacji niejawnych

1. Ochrona EUCI podlega wymogom określonym w niniejszej decyzji, a w szczególności w załączniku A. Posiadacz jakiegokolwiek EUCI jest odpowiedzialny za ich należyłą ochronę.
2. ESDZ zapewnia, aby dostępu do informacji niejawnych udzielano wyłącznie osobom, które spełniają warunki określone w art. 5 załącznika A.
3. Warunki udzielania dostępu do EUCI pracownikom miejscowym są określane również przez Wysokiego Przedstawiciela zgodnie z zasadami ochrony EUCI określonymi w załączniku A do niniejszej decyzji.
4. Dyrekcja odpowiedzialna za bezpieczeństwo w ESDZ prowadzi bazę danych dotyczącą statusu wszystkich członków personelu podlegającego odpowiedzialności ESDZ oraz wykonawców ESDZ pod względem poświadczenia bezpieczeństwa.
5. W przypadku gdy państwa członkowskie wprowadzają do struktur lub sieci ESDZ informacje niejawne opatrzone oznaczeniem krajowej klauzuli tajności, ESDZ obejmuje te informacje ochroną zgodnie z wymogami, które mają zastosowanie do EUCI o równorzędnej klauzuli tajności – zgodnie z tabelą odpowiedników klauzul tajności zawartą w dodatku B do niniejszej decyzji.
6. W miejscach, w których w ESDZ przechowuje się informacje o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, bądź klauzuli jej równoważnej, tworzy się strefy zabezpieczone zgodnie z przepisami obowiązującymi na podstawie załącznika AII do niniejszej decyzji, a strefy te zatwierdza organ ESDZ ds. bezpieczeństwa.
7. Procedury wykonywania przez Wysokiego Przedstawiciela obowiązków w ramach umów lub porozumień administracyjnych dotyczących wymiany EUCI z państwami trzecimi lub organizacjami międzynarodowymi określono w załącznikach A i AVI do niniejszej decyzji.
8. Sekretarz Generalny określa warunki, na jakich ESDZ może wymieniać znajdujące się w jej posiadaniu EUCI z innymi instytucjami, organami lub jednostkami organizacyjnymi Unii. W tym celu ustanowione zostaną właściwe ramy, w tym przez przystępowanie do umów międzyinstytucjonalnych lub w razie potrzeby innych temu służących ustaleń.
9. Wszelkie takie ramy zapewniają, aby EUCI były chronione stosownie do ich klauzuli tajności i zgodnie z podstawowymi zasadami i minimalnymi normami, które są równoważne z określonymi w niniejszej decyzji.

Artykuł 7

Incydenty bezpieczeństwa i sytuacje nadzwyczajne

1. Aby zapewnić szybkie i skuteczne reagowanie na incydenty bezpieczeństwa, ESDZ wprowadza proces zgłaszania takich incydentów i sytuacji nadzwyczajnych, działający całą dobę we wszystkie dni tygodnia i obejmujący wszelkiego rodzaju incydenty bezpieczeństwa lub sytuacje powodujące zagrożenie dla interesów bezpieczeństwa ESDZ (np. wypadki, konflikty, czyny dokonane w złym zamiarze, działania przestępcze, porwania oraz przetrzymywanie zakładników, nagłe przypadki medyczne, incydenty dotyczące systemów teleinformatycznych, ataki cybernetyczne itp.).
2. Pomiędzy główną siedzibą ESDZ, delegaturami Unii, Radą, Komisją, specjalnymi przedstawicielami UE i państwami członkowskimi tworzy się kanały łączności kryzysowej, aby wspierać je w zarządzaniu incydentami bezpieczeństwa z udziałem personelu oraz ich skutkami, w tym w planowaniu ewentualnościowym.
3. Zarządzanie incydentami bezpieczeństwa obejmuje między innymi:
 - procedury skutecznego wspierania procesu decyzyjnego w odniesieniu do incydentu bezpieczeństwa z udziałem personelu, w tym decyzji dotyczących ewakuacji lub zawieszenia misji, oraz
 - strategie i procedury ewakuacji personelu, np. w wypadku zaginięcia, porwania lub przetrzymywania zakładników, z uwzględnieniem szczegółowych zakresów odpowiedzialności państw członkowskich, instytucji UE i ESDZ w tym zakresie. W zarządzaniu tego rodzaju operacjami bierze się pod uwagę potrzeby w zakresie szczególnych zdolności z uwzględnieniem zasobów, jakie mogą udostępnić państwa członkowskie.

4. ESDZ wprowadza odpowiednie rozwiązania administracyjne na potrzeby zgłaszania incydentów związanych z bezpieczeństwem w delegaturach Unii. W stosownych przypadkach informuje się państwa członkowskie, Komisję, wszelkie inne właściwe organy oraz odpowiednie komitety ds. bezpieczeństwa.
5. Przeprowadza się regularne ćwiczenia i przeglądy procesów zarządzania incydentami.

Artykuł 8

Bezpieczeństwo systemów teleinformatycznych

1. ESDZ chroni informacje przetwarzane w systemach teleinformatycznych („CIS”) przed zagrożeniami dla ich poufności, integralności, dostępności, autentyczności i niezaprzeczalności.
2. Zasady, wytyczne dotyczące bezpieczeństwa oraz program bezpieczeństwa służące ochronie wszelkich CIS należących do ESDZ lub przez nią użytkowanych zatwierdza organ ESDZ ds. bezpieczeństwa.
3. Treść wyżej wspomnianych zasad, polityki i programu jest zgodna, a ich wdrażanie ściśle skoordynowane z zasadami, polityką i programami bezpieczeństwa Rady i Komisji, a w stosownych przypadkach z polityką bezpieczeństwa stosowaną przez państwa członkowskie.
4. Wszystkie CIS, w których przetwarza się informacje niejawne, przechodzą proces akredytacji. ESDZ stosuje system zarządzania akredytacją bezpieczeństwa w porozumieniu z Sekretariatem Generalnym Rady oraz Komisją.
5. W przypadkach gdy EUCI przetwarzane przez ESDZ podlegają ochronie przy użyciu produktów kryptograficznych, produkty te są zatwierdzane przez organ ds. zatwierdzania produktów kryptograficznych ESDZ na podstawie zalecenia Komitetu ds. Bezpieczeństwa w Radzie.
6. W zakresie, w jakim jest to niezbędne, organ ESDZ ds. bezpieczeństwa ustanawia następujące funkcje zabezpieczania informacji:
 - a) organ ds. zabezpieczania informacji;
 - b) organ ds. TEMPEST;
 - c) organ ds. zatwierdzania produktów kryptograficznych;
 - d) organ ds. dystrybucji produktów kryptograficznych.
7. Organ ESDZ ds. bezpieczeństwa ustanawia dla każdego systemu następujące funkcje:
 - a) organ ds. akredytacji bezpieczeństwa;
 - b) organ operacyjny ds. zabezpieczania informacji.
8. Przepisy dotyczące wprowadzania w życie niniejszego artykułu w zakresie ochrony EUCI określono w załącznikach A i A IV.

Artykuł 9

Naruszenie bezpieczeństwa oraz narażenie na szwank informacji niejawnych

1. Naruszenie bezpieczeństwa następuje w wyniku działania lub zaniechania działania w sposób sprzeczny z przepisami bezpieczeństwa ustanowionymi w niniejszej decyzji lub z polityką bezpieczeństwa bądź wytycznymi określającymi środki niezbędne do wdrożenia tej decyzji, zatwierdzonymi zgodnie z art. 21 ust. 1.
2. Narażenie na szwank informacji niejawnych następuje wówczas, gdy informacje niejawne zostają w całości lub częściowo ujawnione nieupoważnionym osobom lub podmiotom.
3. Wszelkie naruszenie bezpieczeństwa lub narażenie na szwank informacji niejawnych bądź podejrzenie takiego naruszenia lub narażenia na szwank niezwłocznie zgłasza się dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo, która podejmuje odpowiednie działania określone w art. 11 załącznika A.
4. Każda osoba odpowiedzialna za naruszenie przepisów bezpieczeństwa określonych w niniejszej decyzji lub za nieuprawnione ujawnienie informacji niejawnych może podlegać postępowaniu dyscyplinarnemu lub sądowemu zgodnie z mającymi zastosowanie zasadami oraz przepisami ustawowymi i wykonawczymi, wymienionymi w art. 11 ust. 3 załącznika A.

Artykuł 10

Dochodzenie w przypadku incydentów bezpieczeństwa, naruszeń bezpieczeństwa lub narażenia na szwank informacji niejawnych oraz działania naprawcze

1. Nie naruszając art. 86 (środki dyscyplinarne) i załącznika IX regulaminu pracowniczego ⁽¹⁾, dyrekcja ESDZ odpowiedzialna za bezpieczeństwo może prowadzić postępowania sprawdzające:
 - a) w przypadku potencjalnego wycieku, nieostrożnego przetwarzania lub narażenia na szwank EUCI, informacji niejawnych Euratom lub szczególnie chronionych informacji jawnych;
 - b) w celu przeciwdziałania atakom wrogich służb wywiadu wymierzonym w ESDZ i jej personel;
 - c) w celu przeciwdziałania atakom terrorystycznym wymierzonym w ESDZ i jej personel;
 - d) w przypadku cyberincydentów;
 - e) w przypadku innych incydentów, które mają wpływ lub mogą wpływać na ogólne bezpieczeństwo w ESDZ, w tym w przypadku podejrzenia o popełnienie przestępstwa.
2. Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo, w stosownych przypadkach przy wsparciu ekspertów z państw członkowskich lub innych instytucji UE i w razie potrzeby za zezwoleniem organu ESDZ ds. bezpieczeństwa, podejmuje – w stosownym czasie i w stosownych przypadkach – wszelkie niezbędne działania naprawcze wynikające z dochodzeń.

Jedynie pracownikom upoważnionym na podstawie imiennych uprawnień przyznanych przez organ ESDZ ds. bezpieczeństwa, z uwagi na ich bieżące obowiązki, można nadać uprawnienia do przeprowadzania i koordynowania postępowań sprawdzających w ESDZ.

3. Osobom prowadzącym dochodzenia zapewnia się dostęp do wszelkich informacji niezbędnych do ich prowadzenia oraz pełne wsparcie wszelkich służb i personelu ESDZ w tym zakresie.

Osoby prowadzące dochodzenia mogą podejmować odpowiednie działania w celu zabezpieczenia materiału dowodowego w sposób proporcjonalny do wagi kwestii będącej przedmiotem dochodzenia.

4. W przypadku gdy dostęp do informacji dotyczy danych osobowych, w tym danych znajdujących się w systemach teleinformatycznych, dostępu takiego udziela się zgodnie z rozporządzeniem (WE) nr 45/2001 Parlamentu Europejskiego i Rady ⁽²⁾.
5. W przypadkach gdy na potrzeby dochodzenia konieczne jest stworzenie bazy danych zawierającej dane osobowe, powiadamia się Europejskiego Inspektora Ochrony Danych (EIOD) zgodnie z wyżej wspomnianym rozporządzeniem.

Artykuł 11

Zarządzanie ryzykiem dla bezpieczeństwa

1. W celu określenia swoich potrzeb w zakresie zapewnienia bezpieczeństwa ESDZ w ścisłej współpracy z Dyrekcją ds. Bezpieczeństwa w Komisji oraz w stosownych przypadkach z Biurem Bezpieczeństwa w Sekretariacie Generalnym Rady opracowuje metodykę kompleksowego szacowania ryzyka dla bezpieczeństwa.
2. Zarządzanie ryzykiem dla interesów bezpieczeństwa ESDZ przebiega w ramach określonego procesu. Celem tego procesu jest ustalenie znanych rodzajów ryzyka dla bezpieczeństwa, określenie środków bezpieczeństwa mających ograniczać to ryzyko do dopuszczalnego poziomu oraz stosowanie środków zgodnie z koncepcją ochrony w głąb. Skuteczność takich środków i poziom ryzyka podlega ciągłej ocenie.

⁽¹⁾ Regulamin pracowniczy urzędników Unii Europejskiej i warunki zatrudnienia innych pracowników Unii Europejskiej, określone w rozporządzeniu Rady (EWG, Euratom, EWWiS) nr 259/68 (Dz.U. L 56 z 4.3.1968, s. 1), zwane dalej „regulaminem pracowniczym i warunkami zatrudnienia”.

⁽²⁾ Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1).

3. Role, zakresy odpowiedzialności i zadania określone w niniejszej decyzji pozostają bez uszczerbku dla odpowiedzialności każdego członka personelu podlegającego odpowiedzialności ESDZ; w szczególności personel UE przebywający na misjach w państwach trzecich musi wykazywać zdrowy rozsądek i właściwą ocenę sytuacji w zakresie własnego bezpieczeństwa oraz przestrzegać wszelkich obowiązujących przepisów, zasad, procedur i instrukcji dotyczących bezpieczeństwa.
4. Aby zapobiegać ryzyku związanemu z bezpieczeństwem i je kontrolować, upoważniony personel może dokonywać podstawowego sprawdzenia osób objętych zakresem niniejszej decyzji w celu ustalenia, czy przyznanie takim osobom dostępu do obiektów ESDZ lub informacji nie stanowi zagrożenia dla bezpieczeństwa. W tym celu i zgodnie z rozporządzeniem (WE) nr 45/2001 upoważniony personel może: a) korzystać z wszelkich źródeł informacji dostępnych ESDZ, uwzględniając wiarygodność źródła informacji; b) uzyskać dostęp do akt personalnych lub danych ESDZ na temat osób, które zatrudnia lub planuje zatrudnić, lub na temat pracowników wykonawców, gdy jest to należycie uzasadnione.
5. ESDZ podejmuje wszelkie racjonalne środki dla zapewnienia ochrony swoich interesów bezpieczeństwa i dla zapobieżenia dającej się racjonalnie przewidzieć szkodzie dla tych interesów.
6. Środki bezpieczeństwa w ESDZ dotyczące ochrony EUCI w całym ich cyklu życia ustala się w sposób współmierny w szczególności do ich klauzuli tajności, do formy i ilości informacji lub materiału, do lokalizacji i konstrukcji obiektów, w których przechowywane są EUCI, oraz do zagrożenia (w tym oszacowanego na poziomie lokalnym) ze strony działań realizowanych w złych zamiarach lub działalności przestępczej, w tym szpiegostwa, sabotażu lub terroryzmu.

Artykuł 12

Świadomość w kwestiach związanych z bezpieczeństwem i szkolenie

1. Organ ESDZ ds. bezpieczeństwa zapewnia opracowanie i wdrożenie odpowiednich programów podnoszenia świadomości i szkolenia w dziedzinie bezpieczeństwa oraz dba o to, by członkowie personelu podlegającego odpowiedzialności ESDZ, a w stosownych przypadkach również osoby na ich utrzymaniu, otrzymali niezbędne instrukcje i szkolenia w zakresie bezpieczeństwa, współmierne do ryzyka w ich miejscu pracy lub zamieszkania.
2. Przed uzyskaniem dostępu do EUCI, a po jego uzyskaniu – w regularnych odstępach czasu – członkowie personelu informowani są o obowiązku ochrony EUCI zgodnie z przepisami określonymi w art. 6 i potwierdzają przyjęcie tego obowiązku do wiadomości.

Artykuł 13

Organizacja bezpieczeństwa w ESDZ

Sekcja 1

Przepisy ogólne

1. Organem ESDZ ds. bezpieczeństwa jest Sekretarz Generalny. Pełniąc tę funkcję, Sekretarz Generalny zapewnia, aby:
 - a) środki bezpieczeństwa koordynowano w miarę potrzeb z właściwymi organami państw członkowskich, Sekretariatem Generalnym Rady i Komisją, a w stosownych przypadkach z państwami trzecimi lub organizacjami międzynarodowymi, w odniesieniu do wszelkich kwestii związanych z bezpieczeństwem, które są istotne dla działań ESDZ, w tym w odniesieniu do charakteru ryzyka dla interesów bezpieczeństwa ESDZ oraz sposobów ochrony przed tym ryzykiem;
 - b) we wszystkich działaniach ESDZ od samego początku w pełni uwzględniano aspekty bezpieczeństwa;
 - c) dostęp do informacji niejawnych był udzielany wyłącznie osobom, które spełniają warunki określone w art. 5 załącznika A;
 - d) ustanowiono system kancelarii tajnych gwarantujący, że sposób przetwarzania informacji opatrzonej klauzulą CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą jest zgodny z niniejszą decyzją zarówno w ESDZ, jak i przy przekazywaniu ich państwom członkowskim UE, instytucjom, organom lub agencjom UE lub innym upoważnionym odbiorcom. Osobno prowadzi się rejestr wszystkich EUCI przekazywanych przez ESDZ państwom trzecim lub organizacjom międzynarodowym oraz wszystkich informacji niejawnych otrzymanych od państw trzecich lub organizacji międzynarodowych;
 - e) przeprowadzono inspekcje bezpieczeństwa, o których mowa w art. 16;

- f) w każdym przypadku zaistniałego lub domniemanego naruszenia zasad bezpieczeństwa oraz zaistniałego lub domniemanego narażenia na szwank lub utraty informacji niejawnych będących w posiadaniu ESDZ lub pochodzących z ESDZ przeprowadzono postępowanie wyjaśniające oraz by o pomoc w takich postępowaniach zwracano się do odpowiednich organów ds. bezpieczeństwa;
- g) wprowadzono odpowiednie plany i mechanizmy postępowania na wypadek incydentów oraz plany i mechanizmy zarządzania ich skutkami w celu zapewnienia szybkiego i skutecznego reagowania na incydenty bezpieczeństwa;
- h) podejmowano odpowiednie środki w razie nieprzestrzegania przez poszczególne osoby przepisów niniejszej decyzji;
- i) wprowadzono odpowiednie środki fizyczne i organizacyjne w celu ochrony interesów bezpieczeństwa ESDZ.

W tym względzie organ ESDZ ds. bezpieczeństwa:

- ustala kategorię bezpieczeństwa delegatur Unii, w porozumieniu z Komisją,
- podejmuje, w stosownych przypadkach po konsultacji z Wysokim Przedstawicielem, decyzję o ewentualnej ewakuacji delegatury Unii, jeżeli wymaga tego sytuacja pod względem bezpieczeństwa,
- podejmuje decyzję o środkach, jakie należy podjąć w stosownych przypadkach w celu ochrony osób na utrzymaniu, z uwzględnieniem uzgodnień z instytucjami UE, o których mowa w art. 3 ust. 3,
- zatwierdza strategię przekazywania informacji kryptograficznych, w szczególności program instalacji mechanizmu i produktów kryptograficznych.

2. W wykonywaniu tych zadań organowi ESDZ ds. bezpieczeństwa pomagają dyrektor generalny ds. budżetu i administracji, dyrektor ESDZ odpowiedzialny za bezpieczeństwo oraz w stosownych przypadkach zastępca Sekretarza Generalnego ds. wspólnej polityki bezpieczeństwa i obrony oraz reagowania w sytuacjach kryzysowych.

3. Sekretarz Generalny jako organ ESDZ ds. bezpieczeństwa może w stosownych przypadkach delegować swoje zadania w tym zakresie.

4. Każdy kierownik departamentu lub działu jest odpowiedzialny za wdrażanie zasad ochrony EUCI w podległym mu departamencie lub dziale.

Bez uszczerbku dla odpowiedzialności za powyższe zadania każdy kierownik departamentu lub działu wyznacza pracownika do pełnienia funkcji departamentalnego koordynatora ds. bezpieczeństwa, dysponującego zasobami proporcjonalnymi do ilości EUCI, które są przetwarzane przez dany departament lub dział.

Departamentalni koordynatorzy ds. bezpieczeństwa w stosownych przypadkach służą pomocą i wsparciem kierownikom departamentów lub działów, którym podlegają, w wykonywaniu zadań związanych z bezpieczeństwem, takich jak:

- a) opracowywanie ewentualnych dodatkowych wymogów bezpieczeństwa odpowiednich do konkretnych potrzeb danego departamentu lub działu;
- b) prowadzenie okresowych instruktaży dotyczących bezpieczeństwa dla pracowników danego departamentu lub działu;
- c) zapewnianie przestrzegania w danym departamencie lub dziale zasady ograniczonego dostępu;
- d) prowadzenie i aktualizowanie listy bezpiecznych kodów i kluczy;
- e) utrzymywanie procedur i środków bezpieczeństwa;
- f) zgłaszanie wszelkich przypadków naruszenia bezpieczeństwa lub narażenia na szwank EUCI dyrektorowi, któremu podlegają, oraz dyrekcji odpowiedzialnej za bezpieczeństwo;
- g) przeprowadzanie rozmów z pracownikami odchodzącymi z pracy w ESDZ;
- h) regularne przedstawianie sprawozdań dotyczących kwestii bezpieczeństwa w departamencie lub dziale za pośrednictwem hierarchii;
- i) utrzymywanie kontaktów z dyrekcją ESDZ odpowiedzialną za bezpieczeństwo w sprawach dotyczących bezpieczeństwa.

Wszelkie działania lub kwestie, które mogą mieć wpływ na bezpieczeństwo, należy bez zbędnej zwłoki zgłaszać dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo.

5. Każdy szef delegatury jest odpowiedzialny za wdrażanie wszystkich środków dotyczących bezpieczeństwa danej delegatury Unii.

Sekcja 2

Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo

1. W ESDZ istnieje dyrekcja odpowiedzialna za bezpieczeństwo. Dyrekcja ta:
 - a) zajmuje się zarządzaniem, koordynacją, nadzorem lub wdrażaniem w odniesieniu do wszystkich środków bezpieczeństwa w siedzibie głównej oraz we wszystkich lokalach podlegających odpowiedzialności ESDZ, w UE i w państwach trzecich;
 - b) zapewnia spójność i zgodność wszelkich działań, które mogą wpływać na ochronę interesów bezpieczeństwa ESDZ, z niniejszą decyzją i przepisami wykonawczymi;
 - c) pełni funkcję głównego doradcy Wysokiego Przedstawiciela, organu ESDZ ds. bezpieczeństwa oraz zastępcy Sekretarza Generalnego we wszystkich kwestiach dotyczących bezpieczeństwa;
 - d) korzysta z pomocy właściwych służb państw członkowskich zgodnie z art. 10 ust. 3 decyzji Rady 2010/427/UE określającej organizację i zasady funkcjonowania ESDZ;
 - e) wspiera działania organu ESDZ ds. akredytacji bezpieczeństwa przez prowadzenie ocen bezpieczeństwa fizycznego ogólnego i lokalnego środowiska bezpieczeństwa systemów teleinformatycznych, w których przetwarzane są EUCI, oraz lokali, które mają zostać dopuszczone do przetwarzania i przechowywania EUCI.
2. Dyrektor ESDZ odpowiedzialny za bezpieczeństwo odpowiada za:
 - a) zapewnienie ogólnej ochrony interesów bezpieczeństwa ESDZ;
 - b) opracowywanie, przeglądy i aktualizacje przepisów bezpieczeństwa oraz koordynację środków bezpieczeństwa z właściwymi organami państw członkowskich oraz w stosownych przypadkach z właściwymi organami państw trzecich i organizacjami międzynarodowymi, które są związane z UE umowami lub uzgodnieniami dotyczącymi bezpieczeństwa;
 - c) wspieranie prac Komitetu ds. Bezpieczeństwa ESDZ, o którym mowa w art. 15 ust. 1 niniejszej decyzji;
 - d) kontaktowanie się w kwestiach bezpieczeństwa z wszelkimi partnerami lub organami niewymienionymi w lit. b) powyżej – w stosownych przypadkach;
 - e) ustalanie priorytetów i przedstawianie wniosków dotyczących zarządzania budżetem na cele bezpieczeństwa w siedzibie głównej i w delegaturach Unii.
3. Kierownik dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo:
 - a) dopilnowuje, aby przypadki naruszenia bezpieczeństwa i narażenia na szwank informacji były rejestrowane oraz aby w stosownych przypadkach wszczynano i przeprowadzono dochodzenia;
 - b) odbywa zarówno regularne, jak i zwoływane w razie konieczności spotkania z dyrektorem ds. bezpieczeństwa Sekretariatu Generalnego Rady oraz dyrektorem Dyrekcji ds. Bezpieczeństwa w Komisji Europejskiej w celu omówienia kwestii stanowiących przedmiot wspólnego zainteresowania.
4. Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo nawiązuje kontakt i utrzymuje ścisłą współpracę z:
 - departamentami odpowiedzialnymi za bezpieczeństwo w ministerstwach spraw zagranicznych państw członkowskich,
 - krajowymi władzami bezpieczeństwa (KWB) lub innymi właściwymi organami ds. bezpieczeństwa w państwach członkowskich w celu uzyskiwania od nich pomocy w zakresie informacji potrzebnych do oceny niebezpieczeństwa i zagrożeń, jakie mogą grozić ESDZ, jej personelowi, działalności, majątkowi i zasobom oraz jej informacjom niejawnym w miejscu, w którym zwykle prowadzi ona działalność,
 - właściwymi organami ds. bezpieczeństwa państw członkowskich lub państw przyjmujących, na których terytorium ESDZ może prowadzić działalność, we wszelkich kwestiach dotyczących ochrony personelu ESDZ, jej działalności, majątku i zasobów oraz jej informacji niejawnych na terytorium tych państw,
 - Biurem Bezpieczeństwa Sekretariatu Generalnego Rady oraz Dyrekcją ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji, a w stosownych przypadkach również departamentami ds. bezpieczeństwa innych instytucji, organów i agencji UE,
 - departamentami ds. bezpieczeństwa państw trzecich lub organizacji międzynarodowych w celu prowadzenia użytecznej koordynacji,
 - krajowymi władzami bezpieczeństwa państw członkowskich w zakresie wszelkich kwestii dotyczących ochrony EUCI.

Sekcja 3

Delegatury Unii

1. Każdy szef delegatury jest odpowiedzialny za lokalne wdrażanie wszystkich środków służących ochronie interesów bezpieczeństwa ESDZ w lokalach danej delegatury Unii i w zakresie jej kompetencji oraz za zarządzanie tymi środkami.

W porozumieniu z właściwymi organami państwa przyjmującego podejmuje on w razie konieczności wszystkie racjonalnie wykonalne działania dla zapewnienia, aby wprowadzono odpowiednie środki fizyczne i organizacyjne służące osiągnięciu tego celu.

Szef delegatury opracowuje w stosownych przypadkach procedury bezpieczeństwa służące ochronie osób na utrzymaniu w rozumieniu art. 2 lit. c) z uwzględnieniem wszelkich porozumień administracyjnych, o których mowa w art. 3 ust. 3. Szef delegatury składa sprawozdania dotyczące wszystkich kwestii bezpieczeństwa wchodzących w zakres jego kompetencji na ręce kierownika dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo.

W wykonywaniu tych zadań wspierają go: dyrekcja ESDZ odpowiedzialna za bezpieczeństwo, zespół ds. zarządzania bezpieczeństwem w delegaturze Unii, w skład którego wchodzi personel wykonujący zadania i pełniący funkcje związane z bezpieczeństwem, oraz w stosownych przypadkach oddelegowani pracownicy ochrony.

Delegatura Unii nawiązuje regularny kontakt i utrzymuje ścisłą współpracę w kwestiach bezpieczeństwa z misjami dyplomatycznymi państw członkowskich.

2. Ponadto szef delegatury:

- ustala szczegółowe plany bezpieczeństwa i plany awaryjne delegatury Unii na podstawie ogólnych obowiązujących procedur działania,
- zapewnia skuteczne działanie przez całą dobę i wszystkie dni tygodnia systemu zarządzania incydentami bezpieczeństwa i sytuacjami nadzwyczajnymi w zakresie działania delegatury Unii,
- zapewnia, aby wszyscy członkowie personelu pracujący w delegaturze Unii byli objęci ubezpieczeniem zgodnie z wymogami obowiązującymi na danym obszarze,
- zapewnia, aby kwestie bezpieczeństwa były uwzględniane w szkoleniach przygotowawczych delegatury Unii organizowanych dla wszystkich członków personelu przydzielonych do pracy w delegaturze Unii w momencie ich przybycia do delegatury Unii, oraz
- zapewnia wdrożenie wszelkich zaleceń wydanych na podstawie ocen bezpieczeństwa oraz regularnie przekazuje organowi ESDZ ds. bezpieczeństwa pisemne sprawozdania dotyczące wdrożenia tych zaleceń oraz innych kwestii bezpieczeństwa.

3. Bez uszczerbku dla odpowiedzialności i rozliczalności za zapewnienie zarządzania kwestiami bezpieczeństwa oraz odporności organizacji, szef delegatury może delegować wykonanie swoich zadań w zakresie bezpieczeństwa koordynatorowi delegatury ds. bezpieczeństwa, który jest zastępcą szefa delegatury, lub – jeżeli nie został on powołany – innej odpowiedniej osobie.

Koordinatorowi delegatury ds. bezpieczeństwa można powierzyć w szczególności następujące działania:

- koordynowanie funkcji związanych z bezpieczeństwem w delegaturze Unii,
- utrzymywanie kontaktów w kwestiach bezpieczeństwa z właściwymi organami państwa przyjmującego oraz odpowiednimi osobami w ambasadach i misjach dyplomatycznych państw członkowskich,
- wdrażanie odpowiednich procedur zarządzania bezpieczeństwem związanych z interesami bezpieczeństwa ESDZ, w tym z ochroną EUCI,
- zapewnianie zgodności z przepisami i instrukcjami bezpieczeństwa,
- instruowanie personelu na temat obowiązujących przepisów bezpieczeństwa oraz szczególnych zagrożeń w danym państwie przyjmującym,
- składanie wniosków do dyrekcji ESDZ odpowiedzialnej za poświadczenia bezpieczeństwa w sprawie stanowisk, które wymagają poświadczenia bezpieczeństwa osobowego, oraz
- informowanie szefa delegatury, regionalnego pełnomocnika ds. ochrony oraz dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo o incydentach lub wydarzeniach na danym obszarze, mających znaczenie dla ochrony interesów bezpieczeństwa ESDZ.

4. Szef delegatury może delegować zadania związane z bezpieczeństwem o charakterze administracyjnym lub technicznym kierownikowi administracyjnemu oraz innym członkom personelu delegatury Unii.

5. Delegaturę Unii wspomaga regionalny pełnomocnik ds. ochrony. Regionalni pełnomocnicy ds. ochrony pełnią niżej opisane role w delegaturach Unii w swoich odpowiednich geograficznych zakresach kompetencji.

W pewnych okolicznościach, jeżeli wymaga tego aktualna sytuacja pod względem bezpieczeństwa, do konkretnej delegatury Unii może zostać oddelegowany w pełnym wymiarze czasu pracy specjalny regionalny pełnomocnik ds. ochrony.

Regionalny pełnomocnik ds. ochrony może być zobowiązany do przeniesienia się poza swój obecny obszar kompetencji, w tym do głównej siedziby, lub nawet do objęcia stanowiska na miejscu w dowolnym państwie w zależności od sytuacji w zakresie bezpieczeństwa i zgodnie z wymogami dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo.

6. Regionalni pełnomocnicy ds. ochrony podlegają bezpośredniej kontroli operacyjnej służb w siedzibie głównej ESDZ odpowiedzialnych za bezpieczeństwo w terenie, ale dzielonej kontroli administracyjnej szefa delegatury w miejscu zatrudnienia i służb w siedzibie głównej odpowiedzialnych za bezpieczeństwo w terenie. Zapewniają oni doradztwo i pomoc szefowi oraz personelowi delegatury Unii w organizowaniu i wdrażaniu wszystkich środków fizycznych, organizacyjnych i proceduralnych dotyczących bezpieczeństwa delegatury Unii.

7. Regionalni pełnomocnicy ds. ochrony służą szefowi i personelowi delegatury Unii radą i wsparciem. W stosownych przypadkach, zwłaszcza jeżeli dany regionalny pełnomocnik ds. ochrony pracuje na miejscu w pełnym wymiarze czasu, powinien on wspomagać delegaturę Unii w zarządzaniu środkami bezpieczeństwa i ich wdrażaniu, w tym w przygotowywaniu umów w dziedzinie bezpieczeństwa oraz zarządzaniu akredytacjami i poświadczeniami.

Artykuł 14

Działania w ramach WPBiO i specjaliści przedstawiciele UE

Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo doradza dyrektorowi Dyrekcji ds. Zarządzania Kryzysowego i Planowania, dyrektorowi generalnemu Sztabu Wojskowego UE, dowódcy operacji cywilnych, kierującemu Komórką Planowania i Prowadzenia Operacji Cywilnych oraz dowódcom operacji wojskowych UE w dziedzinie aspektów bezpieczeństwa operacji w ramach WPBiO, zaś specjalnym przedstawicielem UE – w dziedzinie aspektów bezpieczeństwa pełnionych przez nich funkcji, w uzupełnieniu szczegółowych przepisów w tym zakresie, przewidzianych w odpowiednich politykach przyjętych przez Radę.

Artykuł 15

Komitet ds. Bezpieczeństwa ESDZ

1. Niniejszym ustanawia się Komitet ds. Bezpieczeństwa ESDZ.

Komitetowi przewodniczy organ ESDZ ds. operacyjnych lub wyznaczona przez niego osoba, a posiedzenia Komitetu odbywają się na polecenie przewodniczącego lub na wniosek jednego z członków. Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo wspiera przewodniczącego w pełnieniu funkcji i w razie konieczności zapewnia wsparcie administracyjne dla prac Komitetu.

2. Komitet ds. Bezpieczeństwa ESDZ składa się z przedstawicieli:

- każdego z państw członkowskich,
- Biura Bezpieczeństwa Sekretariatu Generalnego Rady,
- Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa Komisji.

Delegacja państwa członkowskiego w Komitecie ds. Bezpieczeństwa ESDZ może składać się z członków:

- krajowej władzy bezpieczeństwa lub wyznaczonej władzy bezpieczeństwa,
- departamentów odpowiedzialnych za bezpieczeństwo w ministerstwie spraw zagranicznych.

3. Przedstawicielom Komitetu w razie konieczności mogą towarzyszyć i służyć radą eksperci. Przedstawiciele innych instytucji, agencji lub organów UE mogą być zapraszani do udziału w dyskusjach dotyczących kwestii istotnych dla ich bezpieczeństwa.

4. Nie naruszając przepisów ust. 5 poniżej Komitet ds. Bezpieczeństwa ESDZ wspiera ESDZ w formie konsultacji we wszystkich kwestiach bezpieczeństwa istotnych dla działalności ESDZ oraz dla siedziby głównej i delegatur Unii.

W szczególności, nie naruszając przepisów ust. 5 poniżej:

a) zasięga się opinii Komitetu ds. Bezpieczeństwa ESDZ w sprawie:

- polityki bezpieczeństwa, wytycznych, pojęć lub innych dokumentów metodycznych dotyczących bezpieczeństwa, w szczególności w zakresie ochrony informacji niejawnych oraz środków, jakie należy zastosować w przypadku nieprzestrzegania przepisów bezpieczeństwa przez personel ESDZ,
- technicznych aspektów bezpieczeństwa, które mogą mieć wpływ na decyzję Wysokiego Przedstawiciela o przedstawieniu Radzie zalecenia dotyczącego podjęcia rokowań w sprawie umów o bezpieczeństwie informacji, o których mowa w art. 10 ust. 1 lit. a) załącznika A,
- wszelkich zmian do niniejszej decyzji;

b) w stosownych przypadkach zasięga się opinii Komitetu ds. Bezpieczeństwa ESDZ lub go informuje w sprawach dotyczących bezpieczeństwa personelu i majątku w siedzibie głównej ESDZ i w delegaturach Unii, nie naruszając przepisów art. 3 ust. 3;

c) informuje się Komitet ds. Bezpieczeństwa ESDZ o każdym przypadku narażenia na szwank lub utraty EUCI, jaki miał miejsce w ESDZ.

5. Wszelkie zmiany zasad dotyczących ochrony EUCI określonych w niniejszej decyzji i w załączniku A wymagają jednogłośnej pozytywnej opinii państw członkowskich reprezentowanych w Komitecie ds. Bezpieczeństwa ESDZ. Taka jednogłośna pozytywna opinia jest wymagana również przed:

- podjęciem rokowań na temat porozumień administracyjnych, o których mowa w art. 10 ust. 1 lit. b) załącznika A,
- ujawnieniem informacji niejawnych w wyjątkowych okolicznościach, o których mowa w pkt 9, 11 i 12 załącznika A VI,
- przyjęciem odpowiedzialności wytwórcy informacji w okolicznościach, o których mowa w art. 10 ust. 6 zdanie ostatnie załącznika A.

W przypadku gdy wymagana jest jednogłośna pozytywna opinia, warunek ten jest spełniony, jeżeli żadna z delegacji państw członkowskich nie wyraża sprzeciwu w czasie obrad Komitetu.

6. Komitet ds. Bezpieczeństwa ESDZ w pełni uwzględnia polityki i wytyczne w zakresie bezpieczeństwa obowiązujące w Radzie i Komisji.

7. Komitet ds. Bezpieczeństwa ESDZ otrzymuje wykaz corocznych inspekcji ESDZ oraz sprawozdania z inspekcji po ich zakończeniu.

8. Organizacja posiedzeń:

- Komitet ds. Bezpieczeństwa ESDZ spotyka się co najmniej dwa razy w roku. Przewodniczący może zorganizować dodatkowe posiedzenia w pełnym składzie bądź w formie bezpieczeństwa z udziałem przedstawicieli krajowych władz bezpieczeństwa, wyznaczonych władz bezpieczeństwa lub ministerstw spraw zagranicznych; o zorganizowanie takich posiedzeń mogą też zwrócić się członkowie Komitetu.
- Komitet ds. Bezpieczeństwa ESDZ organizuje swoją działalność w taki sposób, aby móc przedstawiać zalecenia w określonych dziedzinach dotyczących bezpieczeństwa. Może on w razie potrzeby powoływać inne podgrupy eksperckie. Komitet wyznacza zakres zadań takich podgrup eksperckich i otrzymuje od nich sprawozdania z działalności.
- Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo odpowiada za przygotowywanie punktów do dyskusji. Przewodniczący sporządza wstępny porządek obrad każdego posiedzenia. Członkowie Komitetu mogą proponować dodatkowe punkty do dyskusji.

*Artykuł 16***Inspekcje w zakresie bezpieczeństwa**

1. Organ ESDZ ds. bezpieczeństwa zapewnia regularne przeprowadzanie w siedzibie głównej ESDZ i w delegaturach Unii inspekcji w zakresie bezpieczeństwa, których celem jest ocena adekwatności środków bezpieczeństwa i ich zgodności z niniejszą decyzją. Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo może w stosownych przypadkach wyznaczać ekspertów do udziału w inspekcjach w zakresie bezpieczeństwa w agencjach i organach UE powoływanych na mocy tytułu V rozdział 2 TUE.

2. Inspekcje ESDZ w zakresie bezpieczeństwa odbywają się pod kierunkiem dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo, w stosownych przypadkach przy wsparciu ekspertów w dziedzinie bezpieczeństwa reprezentujących inne instytucje UE lub państwa członkowskie, w szczególności w kontekście uzgodnień, o których mowa w art. 3 ust. 3.

3. ESDZ może w razie potrzeby korzystać z wiedzy fachowej w państwach członkowskich, Sekretariacie Generalnym Rady oraz w Komisji.

W razie potrzeby do udziału w inspekcji w zakresie bezpieczeństwa w delegaturze Unii mogą być zaproszeni odpowiedni eksperci w dziedzinie bezpieczeństwa pracujący w misjach państw członkowskich w państwach trzecich lub przedstawiciele departamentów ds. bezpieczeństwa dyplomatycznego w państwach członkowskich.

4. Przepisy dotyczące wprowadzania w życie niniejszego artykułu w zakresie ochrony EUCI określono w załączniku A III.

*Artykuł 17***Wizyty oceniające**

Aby stwierdzić skuteczność środków bezpieczeństwa stosowanych w państwie trzecim lub organizacji międzynarodowej w celu ochrony EUCI wymienianych na podstawie porozumienia administracyjnego, o którym mowa w art. 10 ust. 1 lit. b) załącznika A, przeprowadzane są wizyty oceniające.

Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo może wyznaczyć ekspertów do udziału w wizytach oceniających w państwach trzecich lub organizacjach międzynarodowych, z którymi UE zawarła umowę o bezpieczeństwie informacji, o której mowa w art. 10 ust. 1 lit. a) załącznika A.

*Artykuł 18***Planowanie ciągłości działania**

W ramach ogólnego planowania ciągłości działania ESDZ dyrekcja ESDZ odpowiedzialna za bezpieczeństwo wspiera organ ESDZ ds. bezpieczeństwa w zarządzaniu aspektami procesów ciągłości działania ESDZ związanymi z bezpieczeństwem.

*Artykuł 19***Porady dla osób wyjeżdżających na misje poza UE**

Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo zapewnia dostępność informacji dotyczących misji personelu podlegającego odpowiedzialności ESDZ, wyjeżdżającego poza UE, z wykorzystaniem zasobów wszystkich właściwych służb ESDZ, w szczególności SITROOM, INTCEN, departamentów geograficznych i delegatur Unii.

Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo przedstawia, na wniosek i na podstawie wyżej wymienionych zasobów, szczegółowe porady dla członków personelu podlegającego odpowiedzialności ESDZ, wyjeżdżającego na misje do państw trzecich o wysokim lub podwyższonym poziomie ryzyka.

*Artykuł 20***Zdrowie i bezpieczeństwo**

Przepisy bezpieczeństwa ESDZ stanowią uzupełnienie przyjętych przez Wysokiego Przedstawiciela przepisów ESDZ dotyczących ochrony zdrowia i bezpieczeństwa.

*Artykuł 21***Wdrożenie i przegląd**

1. Organ ESDZ ds. bezpieczeństwa, w stosownych przypadkach po konsultacji z Komitetem ds. Bezpieczeństwa ESDZ, zatwierdza wytyczne dotyczące bezpieczeństwa, określające wszelkie środki konieczne do wdrożenia niniejszych przepisów w ESDZ, oraz tworzy niezbędne zdolności obejmujące wszystkie aspekty bezpieczeństwa w ścisłej współpracy z właściwymi organami do spraw bezpieczeństwa w państwach członkowskich oraz przy wsparciu odpowiednich służb instytucji UE.
2. Zgodnie z art. 4 ust. 5 decyzji Rady 2010/427/UE z dnia 26 lipca 2010 r. określającej organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych w razie potrzeby mogą być stosowane rozwiązania przejściowe z wykorzystaniem porozumień o gwarantowanym poziomie usług z odpowiednimi służbami Sekretariatu Generalnego Rady i Komisji.
3. Wysoki Przedstawiciel zapewnia ogólną spójność stosowania niniejszej decyzji i prowadzi przeglądy niniejszych przepisów bezpieczeństwa.
4. Przepisy bezpieczeństwa ESDZ wdraża się w ścisłej współpracy z właściwymi organami ds. bezpieczeństwa w państwach członkowskich.
5. ESDZ zapewnia uwzględnianie wszystkich aspektów procesu bezpieczeństwa w ramach systemu reagowania kryzysowego ESDZ.
6. Wdrożenie niniejszej decyzji zapewniają Sekretarz Generalny jako organ ds. bezpieczeństwa oraz kierownik dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo.

*Artykuł 22***Zastąpienie poprzednich decyzji**

Niniejsza decyzja uchyla i zastępuje decyzję Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 19 kwietnia 2013 r. w sprawie przepisów bezpieczeństwa mających zastosowanie do Europejskiej Służby Działań Zewnętrznych ⁽¹⁾.

*Artykuł 23***Postanowienia końcowe**

Niniejsza decyzja wchodzi w życie w dniu jej podpisania.

Zostaje ona opublikowana w Dzienniku Urzędowym Unii Europejskiej.

Właściwe organy ESDZ w odpowiednim terminie należycie informują wszystkich członków personelu objętych zakresem niniejszej decyzji i jej załączników o ich treści, wejściu w życie i wszelkich ewentualnych późniejszych zmianach.

Sporządzono w Brukseli dnia 19 września 2017 r.

Federica MOGHERINI

*Wysoka Przedstawiciel Unii do Spraw Zagranicznych i Polityki
Bezpieczeństwa*

⁽¹⁾ Dz.U. C 190 z 29.6.2013, s. 1

ZAŁĄCZNIK A

ZASADY I NORMY OCHRONY EUCI

Artykuł 1

Cel, zakres stosowania i definicje

1. W niniejszym załączniku określa się podstawowe zasady i minimalne normy bezpieczeństwa służące ochronie EUCI.
2. Podstawowe zasady i minimalne normy mają zastosowanie do ESDZ w rozumieniu art. 1 niniejszej decyzji oraz do personelu podlegającego odpowiedzialności ESDZ w rozumieniu definicji zawartej w art. 2 niniejszej decyzji.

Artykuł 2

Definicja EUCI, klauzule tajności i oznaczenia

1. „Informacje niejawne UE” (EUCI) oznaczają wszelkie informacje lub materiały objęte klauzulą tajności UE, których nieuprawnione ujawnienie mogłoby w różnym stopniu wyrządzić szkodę interesom Unii Europejskiej lub interesom co najmniej jednego państwa członkowskiego.
2. EUCI otrzymują jedną z następujących klauzul tajności:
 - a) TRES SECRET UE/EU TOP SECRET: informacje i materiały, których nieuprawnione ujawnienie mogłoby wyrządzić wyjątkowo poważną szkodę podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;
 - b) SECRET UE/EU SECRET: informacje i materiały, których nieuprawnione ujawnienie mogłoby poważnie zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;
 - c) CONFIDENTIEL UE/EU CONFIDENTIAL: informacje i materiały, których nieuprawnione ujawnienie mogłoby zaszkodzić podstawowym interesom Unii Europejskiej lub co najmniej jednego państwa członkowskiego;
 - d) RESTREINT UE/EU RESTRICTED: informacje i materiały, których nieuprawnione ujawnienie mogłoby być niekorzystne dla interesów Unii Europejskiej lub co najmniej jednego państwa członkowskiego.
3. EUCI opatruje się klauzulą tajności zgodnie z ust. 2. Można nadać im dodatkowe oznaczenie wskazujące dziedzinę działalności, do której się odnoszą, wytwórcę, ograniczenia dystrybucji, ograniczenia wykorzystania lub możliwość ujawnienia.

Artykuł 3

Zarządzanie klauzulami tajności

1. ESDZ zapewnia, by EUCI nadawano odpowiednie klauzule tajności, by informacje takie były wyraźnie oznaczone jako informacje niejawne, a także by były one objęte danym poziomem klauzuli tajności nie dłużej, niż jest to konieczne.
2. Obniżenie lub zniesienie klauzuli tajności nadanej EUCI bądź zmiana lub usunięcie oznaczeń, o których mowa w art. 2 ust. 3, wymagają uprzedniej pisemnej zgody wytwórcy.
3. Organ ESDZ ds. bezpieczeństwa, po konsultacji z Komitetem ds. Bezpieczeństwa ESDZ zgodnie z art. 15 ust. 5 niniejszej decyzji, zatwierdza wytyczne bezpieczeństwa w zakresie wytwarzania EUCI, które obejmują praktyczny przewodnik nadawania klauzul tajności.

Artykuł 4

Ochrona informacji niejawnych

1. EUCI podlegają ochronie zgodnie z niniejszą decyzją.
2. Posiadacz jakichkolwiek EUCI jest odpowiedzialny za ich ochronę zgodnie z niniejszą decyzją.

3. W przypadku gdy państwa członkowskie wprowadzają do struktur lub sieci ESDZ informacje niejawnne opatrzone krajową klauzulą tajności, ESDZ obejmuje te informacje ochroną zgodnie z wymogami, które mają zastosowanie do EUCI o równorzędnej klauzuli tajności – zgodnie z tabelą odpowiedników klauzul tajności zawartą w dodatku B.

ESDZ ustanawia odpowiednie procedury w celu prowadzenia dokładnych rejestrów dotyczących wytwórcy:

- informacji niejawnnych otrzymywanych przez ESDZ, oraz
- materiałów źródłowych zawartych w informacjach niejawnnych wytworzonych przez ESDZ.

O procedurach tych informuje się Komitet ds. Bezpieczeństwa ESDZ.

4. Uzasadnione może być objęcie dużych ilości lub kompilacji EUCI ochroną na poziomie właściwym dla wyższej klauzuli tajności niż klauzula, którą objęto ich części składowe.

Artykuł 5

Bezpieczeństwo osobowe w kontekście przetwarzania informacji niejawnnych UE

1. Bezpieczeństwo osobowe oznacza stosowanie środków zapewniających, aby dostęp do EUCI był przyznawany tylko osobom, które:

- muszą mieć dostęp w ramach zasady ograniczonego dostępu,
- w odniesieniu do dostępu do informacji o klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej – otrzymały poświadczenie bezpieczeństwa do odpowiedniego poziomu lub ze względu na pełnione przez siebie funkcje otrzymały inne odpowiednie uprawnienie zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, oraz
- zostały poinformowane o swoich obowiązkach.

2. W ramach procedur wydawania poświadczenia bezpieczeństwa osobowego (PBO) stwierdza się, czy daną osobę, ze względu na jej lojalność, wiarygodność i rzetelność, można uprawnnić do dostępu do EUCI.

3. Przed uzyskaniem dostępu do EUCI, a następnie w regularnych odstępach czasu po jego uzyskaniu, wszystkie osoby informowane są o obowiązku ochrony EUCI zgodnie z niniejszą decyzją i potwierdzają na piśmie przyjęcie do wiadomości tego obowiązku.

4. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A I.

Artykuł 6

Bezpieczeństwo fizyczne informacji niejawnnych UE

1. Bezpieczeństwo fizyczne oznacza stosowanie fizycznych i technicznych środków ochrony w celu powstrzymania nieuprawnionego dostępu do EUCI.

2. Środki bezpieczeństwa fizycznego mają na celu zapobieżenie wtargnięciu osoby nieupoważnionej, w sposób niezauważony lub z użyciem siły, powstrzymanie od podjęcia nieuprawnionych działań, udaremnianie i wykrywanie takich działań oraz umożliwienie podziału personelu pod względem dostępu do EUCI zgodnie z zasadą ograniczonego dostępu. Środki te określone są na podstawie procesu zarządzania ryzykiem.

3. Środki bezpieczeństwa fizycznego wprowadza się we wszystkich obiektach, budynkach, biurach, pomieszczeniach i innych strefach, w których EUCI są przetwarzane lub przechowywane, w tym w strefach, w których znajdują się systemy teleinformatyczne określone w art. 8 ust. 2 załącznika A.

4. Strefy, w których przechowywane są EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, ustanawiane są strefami bezpieczeństwa zgodnie z załącznikiem A II; strefy takie zatwierdza organ ESDZ ds. bezpieczeństwa.

5. Do ochrony EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej wykorzystuje się wyłącznie zatwierdzony sprzęt lub zatwierdzone urządzenia.

6. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A II.

Artykuł 7

Zarządzanie informacjami niejawnymi

1. Zarządzanie informacjami niejawnymi polega na stosowaniu środków administracyjnych służących kontroli EUCI na wszystkich etapach ich cyklu życia w celu uzupełnienia środków przewidzianych w art. 5, 6 i 8 i przyczynienia się w ten sposób do powstrzymania zamierzonego lub przypadkowego narażenia na szwank lub utraty tych informacji, wykrywania takich przypadków i usuwania ich skutków. Środki takie dotyczą w szczególności wytwarzania, rejestracji, kopiowania, tłumaczenia, przenoszenia, przetwarzania, przechowywania i niszczenia EUCI.
2. Informacje niejawne opatrzone klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą są ze względów bezpieczeństwa rejestrowane przed dystrybucją i w momencie wpłynięcia. Właściwe organy ESDZ ustanawiają do tego celu system kancelarii tajnych. Informacje niejawne opatrzone klauzulą tajności TRES SECRET UE/EU TOP SECRET rejestruje się w wyznaczonych kancelariach tajnych.
3. Jednostki organizacyjne i lokale, w których EUCI są przetwarzane lub przechowywane, poddawane są regularnym inspekcjom przeprowadzanym przez organ ESDZ ds. bezpieczeństwa.
4. Poza strefami chronionymi fizycznie EUCI są przekazywane między jednostkami organizacyjnymi i lokalami w sposób następujący:
 - a) zgodnie z ogólną zasadą EUCI są przekazywane drogą elektroniczną chronioną przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 7 ust. 5 niniejszej decyzji oraz zgodnie z jasno zdefiniowanymi operacyjnymi procedurami bezpieczeństwa;
 - b) jeżeli nie stosuje się sposobu, o którym mowa w lit. a), EUCI są przekazywane:
 - (i) za pomocą środków elektronicznych (jak np. pamięć USB, płyty kompaktowe, twarde dyski) chronionych przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 8 ust. 5 niniejszej decyzji; lub
 - (ii) we wszystkich pozostałych przypadkach – jak zalecono w wytycznych organu ESDZ ds. bezpieczeństwa zgodnie z odpowiednimi środkami ochrony określonymi w załączniku A III sekcja V.
5. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A III.

Artykuł 8

Ochrona EUCI przetwarzanych w systemach teleinformatycznych

1. Zabezpieczanie informacji w ramach systemów teleinformatycznych oznacza pewność, że systemy te będą chronić informacje, które są w nich przetwarzane, i będą działać tak, jak powinny i kiedy powinny pod kontrolą uprawnionych użytkowników. Skuteczne zabezpieczanie informacji zapewnia odpowiedni poziom poufności, integralności, dostępności, niezaprzeczalności i autentyczności. Zabezpieczanie informacji opiera się na procesie zarządzania ryzykiem.
2. „System teleinformatyczny” (CIS) oznacza każdy system umożliwiający przetwarzanie informacji w formie elektronicznej. System teleinformatyczny obejmuje wszystkie zasoby niezbędne do jego funkcjonowania, w tym infrastrukturę, organizację, personel oraz zasoby informatyczne. Niniejszy załącznik ma zastosowanie do wszelkich systemów teleinformatycznych ESDZ, w których przetwarzane są EUCI.
3. CIS przetwarza EUCI zgodnie z koncepcją zabezpieczania informacji.
4. Wszystkie CIS, w których przetwarzane są EUCI, poddawane są procedurze akredytacji. Celem akredytacji jest upewnienie się, że zastosowano wszystkie odpowiednie środki bezpieczeństwa i że osiągnięto wystarczający poziom ochrony EUCI i CIS zgodnie z niniejszą decyzją. W świadectwie akredytacji określa się najwyższą klauzulę tajności informacji, które może przetwarzać dany CIS, oraz odnośne zasady i warunki.
5. CIS, w którym przetwarzane są informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i wyższej jest chroniony w taki sposób, by wykluczyć narażenie na szwank informacji z powodu niezamierzonych emisji elektromagnetycznych („środki bezpieczeństwa TEMPEST”).
6. W przypadku gdy EUCI podlegają ochronie przy użyciu produktów kryptograficznych, produkty te są zatwierdzane zgodnie z art. 8 ust. 5 niniejszej decyzji.

7. Podczas transmisji EUCI drogą elektroniczną stosuje się zatwierdzone produkty kryptograficzne. Niezależnie od tego wymogu w nadzwyczajnych okolicznościach mogą mieć zastosowanie szczególne procedury lub specjalne konfiguracje techniczne określone w załączniku A IV.

8. Zgodnie z art. 8 ust. 6 niniejszej decyzji ustanawia się, w koniecznym zakresie, następujące funkcje zabezpieczenia informacji:

- a) organ ds. zabezpieczania informacji (IAA);
- b) organ ds. TEMPEST (TA);
- c) organ ds. zatwierdzania produktów kryptograficznych (CAA);
- d) organ ds. dystrybucji produktów kryptograficznych (CDA).

9. Zgodnie z art. 8 ust. 7 niniejszej decyzji w odniesieniu do każdego systemu ustanawia się:

- a) organ ds. akredytacji bezpieczeństwa (SAA);
- b) organ operacyjny ds. zabezpieczania informacji.

10. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A IV.

Artykuł 9

Bezpieczeństwo przemysłowe

1. Bezpieczeństwo przemysłowe oznacza stosowanie środków mających zapewnić ochronę EUCI przez wykonawców lub podwykonawców podczas negocjacji poprzedzających zawarcie umów i na wszystkich etapach cyklu życia umów niejawnych. Umowy takie co do zasady nie obejmują dostępu do informacji niejawnych o klauzuli tajności TRES SECRET UE/EU TOP SECRET.

2. ESDZ może na podstawie umowy powierzyć zadania obejmujące dostęp do EUCI bądź ich przetwarzanie lub przechowywanie przez podmioty gospodarcze lub inne, zarejestrowane w państwie członkowskim lub w państwie trzecim, z którym zawarto umowę o bezpieczeństwie informacji lub porozumienie administracyjne, o których mowa w art. 10 ust. 1 załącznika A.

3. Jako instytucja zamawiająca ESDZ zapewnia, by w przypadku zawierania umów niejawnych z podmiotami gospodarczymi lub innymi spełnione były minimalne normy bezpieczeństwa przemysłowego określone w niniejszej decyzji i wymienione w danej umowie. ESDZ zapewnia zgodność ze wspomnianymi minimalnymi normami za pośrednictwem odpowiednich KWB lub WWB.

4. Wykonawcy lub podwykonawcy, którzy są zarejestrowani w państwie członkowskim i są stronami umów niejawnych lub niejawnych umów o podwykonawstwo i od których wymaga się przetwarzania i przechowywania informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET w należących do nich obiektach, czy to podczas wykonywania takich umów czy też na etapie poprzedzającym ich zawarcie, posiadają świadectwo bezpieczeństwa przemysłowego (SBP) na odpowiednim poziomie klauzuli tajności, wydane przez KWB, WWB lub jakikolwiek inny właściwy organ ds. bezpieczeństwa danego państwa członkowskiego.

5. Personel wykonawcy lub podwykonawcy, któremu do celów wykonania umowy niejawnej potrzebny jest dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, posiada poświadczenie bezpieczeństwa osobowego (PBO) wydane przez odpowiednią krajową władzę bezpieczeństwa (KWB), wyznaczoną władzę bezpieczeństwa (WWB) lub jakikolwiek inny właściwy organ bezpieczeństwa zgodnie z krajowymi przepisami ustawowymi i wykonawczymi oraz minimalnymi normami bezpieczeństwa określonymi w załączniku A I.

6. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A V.

Artykuł 10

Wymiana informacji niejawnych z państwami trzecimi i organizacjami międzynarodowymi

1. ESDZ może wymieniać EUCI z państwem trzecim lub organizacją międzynarodową wyłącznie w przypadku, gdy:
- a) obowiązuje umowa o bezpieczeństwie informacji zawarta między UE a tym państwem trzecim lub organizacją międzynarodową zgodnie z art. 37 TUE i art. 218 TFUE; lub

- b) obowiązuje porozumienie administracyjne między Wysokim Przedstawicielem a właściwymi organami ds. bezpieczeństwa tego państwa trzeciego lub organizacji międzynarodowej, regulujące wymianę informacji niejawnych opatrzonej klauzulą tajności co do zasady nie wyższą niż RESTREINT UE/EU RESTRICTED, zawarte zgodnie z procedurą określoną w art. 15 ust. 5 niniejszej decyzji; lub
- c) obowiązuje umowa ramowa lub umowa ad hoc w sprawie udziału zawarta między UE a tym państwem trzecim w kontekście operacji zarządzania kryzysowego WPBiO, zawarta zgodnie z art. 37 TUE i art. 218 TFUE;

i spełniono warunki określone w tym instrumencie.

Wyjątki od ogólnej zasady opisanej powyżej określono w załączniku A VI sekcja V.

2. Porozumienia administracyjne, o których mowa w ust. 1 lit. b), zawierają postanowienia zapewniające, by w przypadku gdy państwa trzecie lub organizacje międzynarodowe otrzymają EUCI, informacje te były chronione w sposób odpowiadający ich klauzuli tajności i zgodny z minimalnymi normami, które są nie mniej rygorystyczne niż normy określone w niniejszej decyzji.

Wymiana informacji na podstawie umów, o których mowa w ust. 1 lit. c), ogranicza się do informacji dotyczących operacji WPBiO, w których dane państwo trzecie uczestniczy na podstawie tych umów i zgodnie z ich postanowieniami.

3. Jeżeli uczestniczące państwo trzecie lub organizacja międzynarodowa zawrze następnie z Unią umowę o bezpieczeństwie informacji, umowa ta zastępuje przepisy dotyczące wymiany informacji niejawnych zawarte we wszelkich umowach ramowych w sprawie udziału, umowach ad hoc w sprawie udziału lub porozumieniach administracyjnych ad hoc w odniesieniu do wymiany i przetwarzania EUCI.

4. EUCI wytworzone do celów operacji WPBiO mogą być ujawnione personelowi oddelegowanemu do tej operacji przez państwa trzecie lub organizacje międzynarodowe zgodnie z ust. 1–3 i załącznikiem A VI. Upoważniając taki personel do dostępu do EUCI w obiektach lub w CIS w ramach operacji WPBiO, stosuje się środki (w tym rejestrację ujawnianych EUCI) służące złagodzeniu ryzyka utraty lub narażenia na szwank bezpieczeństwa informacji. Środki te są określane w odpowiednich dokumentach dotyczących planowania lub misji.

5. Aby stwierdzić skuteczność środków bezpieczeństwa służących ochronie wymienianych EUCI organizuje się w państwach trzecich lub organizacjach międzynarodowych wizyty oceniające, o których mowa w art. 17 niniejszej decyzji.

6. Decyzję o udostępnieniu EUCI, którymi dysponuje ESDZ, państwu trzeciemu lub organizacji międzynarodowej podejmuje się po rozpatrzeniu każdego przypadku z osobna, w zależności od charakteru i treści takich informacji, oraz od tego, czy odbiorca spełnia zasadę ograniczonego dostępu i w jakim stopniu jest to korzystne dla UE.

Dla upewnienia się, że nie ma przeciwwskazań do udostępnienia informacji, ESDZ zwraca się o pisemną zgodę do każdego podmiotu, który przekazał informację niejawną stanowiącą materiał źródłowy EUCI wytworzonej przez ESDZ.

Jeżeli wytwórcą informacji niejawnej, o której udostępnienie wystąpiono, nie jest ESDZ, to ESDZ najpierw zwraca się o pisemną zgodę wytwórcy na jej udostępnienie.

Jeśli jednak ESDZ nie jest w stanie ustalić wytwórcy informacji, to organ ESDZ ds. bezpieczeństwa przyjmuje na siebie odpowiedzialność wytwórcy po uzyskaniu jednogłośnej pozytywnej opinii państw członkowskich reprezentowanych w Komitecie ds. Bezpieczeństwa ESDZ.

- 7. Przepisy dotyczące wprowadzania w życie niniejszego artykułu znajdują się w załączniku A VI.

Artykuł 11

Naruszenia zasad bezpieczeństwa oraz narażenie na szwank informacji niejawnych

1. Wszelkie naruszenie bezpieczeństwa lub narażenie na szwank informacji niejawnych bądź podejrzenie takiego naruszenia lub narażenia na szwank niezwłocznie zgłasza się dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo, która informuje w stosownych przypadkach dane państwo lub państwa członkowskie lub wszelkie inne podmioty.

2. Jeżeli wiadomo lub jeżeli istnieją uzasadnione przesłanki, by podejrzewać, że doszło do narażenia na szwank lub utraty informacji niejawnych, dykcja ESDZ odpowiedzialna za bezpieczeństwo informuje KWB danego państwa lub państw członkowskich i podejmuje wszelkie właściwe środki zgodnie z odpowiednimi przepisami ustawowymi i wykonawczymi, w celu:

- a) zabezpieczenia dowodów;
 - b) zapewnienia, by sprawa została zbadana przez personel niezwiązany bezpośrednio z danym przypadkiem naruszenia lub narażenia na szwank informacji niejawnych w celu ustalenia faktów;
 - c) bezzwłocznego powiadomienia wytwórcy informacji lub wszelkich innych podmiotów, których sprawa dotyczy;
 - d) podjęcia właściwych środków, aby zapobiec powtórzeniu się podobnego przypadku;
 - e) oceny potencjalnych szkód dla interesów UE lub państw członkowskich; oraz
 - f) powiadomienia właściwych organów o skutkach zaistniałego lub domniemanego narażenia na szwank informacji niejawnych i o podjętych działaniach.
3. Każdy członek personelu podlegającego odpowiedzialności ESDZ, odpowiedzialny za naruszenie przepisów bezpieczeństwa określonych w niniejszej decyzji, może podlegać postępowaniu dyscyplinarnemu zgodnie z mającymi zastosowanie zasadami i przepisami wykonawczymi.

Każda osoba odpowiedzialna za narażenie na szwank lub utratę informacji niejawnych podlega postępowaniu dyscyplinarnemu lub sądowemu zgodnie z mającymi zastosowanie przepisami ustawowymi, zasadami i przepisami wykonawczymi.

4. Na czas trwania dochodzenia dotyczącego danego naruszenia lub narażenia na szwank kierownik dykcji ESDZ odpowiedzialnej za bezpieczeństwo może zawiesić dostęp danej osoby do EUCI i do lokali ESDZ. O podjęciu takiej decyzji informuje się niezwłocznie Dykcję ds. Bezpieczeństwa w Dykcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji, Biuro ds. Bezpieczeństwa w Sekretariacie Generalnym Rady lub KWB państwa lub państw członkowskich bądź inne podmioty, których sprawa dotyczy.

ZAŁĄCZNIK A I

BEZPIECZEŃSTWO OSOBOWE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 5 załącznika A. Określa się w nim w szczególności kryteria, które powinna stosować ESDZ do oceny, czy daną osobę ze względu na jej lojalność, wiarygodność i rzetelność można uprawnić do dostępu do EUCI, a także procedury sprawdzające i administracyjne, które należy stosować w tym celu.
2. „Poświadczenie bezpieczeństwa osobowego” (PBO) w zakresie dostępu do EUCI to oświadczenie właściwego organu państwa członkowskiego, wydawane po zakończeniu postępowania sprawdzającego dotyczącego bezpieczeństwa, prowadzonego przez właściwe organy państwa członkowskiego; stanowi ono poświadczenie, że dana osoba – o ile stwierdzono, że spełnia ona zasadę ograniczonego dostępu – może uzyskać dostęp do EUCI opatrzonych klauzulą tajności do określonego poziomu (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) do określonej daty; osobę taką określa się jako „posiadającą poświadczenie bezpieczeństwa”.
3. „Zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego” (ZPBO) to zaświadczenie wydane przez organ ESDZ ds. bezpieczeństwa, potwierdzające, że dana osoba posiada poświadczenie bezpieczeństwa, oraz zawierające informację o poziomie klauzuli tajności EUCI, do których dana osoba może uzyskać dostęp, o terminie ważności odpowiedniego PBO oraz o terminie ważności samego zaświadczenia.
4. „Uprawnienie do dostępu do EUCI” to uprawnienie wydawane zgodnie z niniejszą decyzją przez organ ESDZ ds. bezpieczeństwa po wydaniu PBO przez właściwe organy państwa członkowskiego, które stanowi poświadczenie, że dana osoba – o ile stwierdzono, że spełnia ona zasadę ograniczonego dostępu – może uzyskać dostęp do EUCI opatrzonych klauzulą tajności do określonego poziomu (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) do określonego terminu; osobę taką określa się jako „posiadającą poświadczenie bezpieczeństwa”.

II. PRYZNAWANIE UPRAWNIEŃ DO DOSTĘPU DO EUCI

5. Uprawnienie do dostępu do informacji o klauzuli tajności RESTREINT UE/EU RESTRICTED nie wymaga poświadczenia bezpieczeństwa i jest przyznawane po:
 - a) ustaleniu związku statutowego lub umownego danej osoby z ESDZ;
 - b) stwierdzeniu, że osoba ta spełnia zasadę ograniczonego dostępu;
 - c) poinformowaniu tej osoby o przepisach i procedurach bezpieczeństwa służących ochronie EUCI i uzyskaniu od niej pisemnego potwierdzenia, że jest ona świadoma swoich obowiązków w zakresie ochrony EUCI zgodnie z niniejszą decyzją.
6. Daną osobę można uprawnić do dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej wyłącznie po:
 - a) ustaleniu związku statutowego lub umownego danej osoby z ESDZ;
 - b) określeniu jej potrzeb w ramach zasady ograniczonego dostępu;
 - c) przyznaniu jej PBO do odpowiedniego poziomu lub innego należytego upoważnienia ze względu na pełnione funkcje, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi; oraz
 - d) poinformowaniu jej o przepisach i procedurach bezpieczeństwa służących ochronie EUCI i uzyskaniu od niej potwierdzenia na piśmie, że jest świadoma swoich obowiązków w zakresie ochrony takich informacji.
7. ESDZ określa, które stanowiska w jej strukturach wymagają dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej i w związku z tym wymagają uzyskania PBO do odpowiedniego poziomu zgodnie z ust. 4 powyżej.
8. Członkowie personelu ESDZ składają oświadczenia, w których informują, czy posiadają obywatelstwo więcej niż jednego państwa.

Procedury związane z ubieganiem się o PBO w ESDZ

9. W przypadku personelu ESDZ organ ESDZ ds. bezpieczeństwa przekazuje wypełnioną ankietę bezpieczeństwa osobowego do KWB w państwie członkowskim, którego obywatelem jest dana osoba, z wnioskiem o przeprowadzenie postępowania sprawdzającego do poziomu EUCI, do którego dostęp będzie tej osobie niezbędny.
10. W przypadku osoby posiadającej obywatelstwo więcej niż jednego państwa wniosek o postępowanie sprawdzające kieruje się do KWB w tym państwie, którego obywatelstwem legitymowała się dana osoba przy przyjmowaniu jej do pracy.
11. Jeżeli ESDZ uzyska istotną dla postępowania sprawdzającego informację dotyczącą osoby, która złożyła wniosek o PBO, powiadamia o tym odpowiednią KWB, działając zgodnie z odpowiednimi zasadami i przepisami wykonawczymi.
12. Po zakończeniu postępowania sprawdzającego odpowiednia KWB powiadamia dyrekcję ESDZ odpowiedzialną za bezpieczeństwo o wyniku takiego postępowania.
 - a) Jeżeli w wyniku postępowania sprawdzającego uzyska się pewność, że nie istnieją żadne niekorzystne okoliczności, które mogłyby podważyć lojalność, wiarygodność i rzetelność danej osoby, organ ESDZ ds. bezpieczeństwa może wydać tej osobie uprawnienie do dostępu do EUCI do odpowiedniego poziomu i do określonego terminu.
 - b) ESDZ podejmuje wszystkie właściwe środki dla zapewnienia należytego wdrożenia warunków lub ograniczeń nałożonych przez KWB. KWB jest informowana o wyniku tych działań.
 - c) Jeżeli w wyniku postępowania sprawdzającego nie uzyskuje się takiej pewności, organ ESDZ ds. bezpieczeństwa powiadamia o tym fakcie daną osobę, a ona może się do niego zwrócić z prośbą o wysłuchanie. Organ ESDZ ds. bezpieczeństwa może zwrócić się do właściwej KWB o przedstawienie wszelkich dalszych wyjaśnień, których może ona udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli wynik zostanie potwierdzony, nie wydaje się uprawnienia do dostępu do EUCI. W takim wypadku ESDZ podejmuje wszystkie właściwe środki w celu uniemożliwienia takiej osobie wszelkiego dostępu do EUCI.
13. Postępowanie sprawdzające oraz jego wyniki, stanowiące dla ESDZ podstawę do decyzji o przyznaniu lub odmowie przyznania uprawnienia do dostępu do EUCI, podlegają odpowiednim przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim, w tym także przepisom dotyczącym środków odwoławczych. Decyzje organu ESDZ ds. bezpieczeństwa podlegają środkom odwoławczym zgodnie z regulaminem pracowniczym.
14. Pewność, na podstawie której wydaje się PBO, o ile jest ono nadal ważne, odnosi się do każdego zadania powierzonego danej osobie w ESDZ, Sekretariacie Generalnym Rady lub Komisji.
15. Komisja akceptuje uprawnienie do dostępu do EUCI wydane przez każdą inną instytucję, organ lub jednostkę organizacyjną Unii Europejskiej, o ile jest ono nadal ważne. Uprawnienia te dotyczą każdego zadania powierzonego danej osobie w obrębie ESDZ. Instytucja, organ lub jednostka organizacyjna Unii Europejskiej, w której dana osoba zostaje zatrudniona, poinformuje odpowiednią KWB o tej zmianie pracodawcy.
16. Jeżeli okres wykonywania przez daną osobę obowiązków służbowych nie rozpocznie się w terminie 12 miesięcy od powiadomienia organu ESDZ ds. bezpieczeństwa o wyniku postępowania sprawdzającego lub jeżeli w pełnieniu obowiązków przez daną osobę występuje przerwa trwająca 12 miesięcy lub dłużej, w czasie której osoba ta nie jest zatrudniona w ESDZ, ani w innych instytucjach, agencjach czy organach UE, ani też na żadnym stanowisku w administracji krajowej państwa członkowskiego wymagającym dostępu do informacji niejawnych, wynik postępowania sprawdzającego jest przekazywany odpowiedniej KWB w celu potwierdzenia, czy nadal pozostaje ważny i właściwy.
17. Jeżeli ESDZ znajdzie się w posiadaniu informacji o ryzyku naruszenia zasad bezpieczeństwa przez osobę, która posiada ważne PBO, ESDZ – działając zgodnie z odpowiednimi zasadami i przepisami wykonawczymi – powiadamia o tym odpowiednią KWB i może zawiesić dostęp do EUCI lub wycofać uprawnienie do dostępu do EUCI. Jeżeli KWB powiadomi ESDZ o utracie pewności uzyskanej zgodnie z pkt 12 lit. a) w odniesieniu do osoby posiadającej ważne uprawnienie do dostępu do EUCI, organ ESDZ ds. bezpieczeństwa może zwrócić się o przedstawienie wszelkich dalszych wyjaśnień, których KWB może udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli niekorzystne informacje zostaną potwierdzone, wspomniane uprawnienie zostaje cofnięte, a osobie takiej odbiera się prawo dostępu do EUCI i odsuwa się ją od stanowisk, na których taki dostęp jest możliwy lub na których osoba ta mogłaby zagrażać bezpieczeństwu.

18. O każdej decyzji w sprawie cofnięcia członkowi personelu ESDZ uprawnienia do dostępu do EUCI, a także w stosownych przypadkach o przyczynach tego cofnięcia, powiadamia się daną osobę, a ona może zwrócić się do organu ESDZ ds. bezpieczeństwa z prośbą o wysłuchanie. Informacje przedstawione przez KWB podlegają odpowiednim przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim, w tym także przepisom dotyczącym środków odwoławczych. Decyzje organu ESDZ ds. bezpieczeństwa podlegają środkom odwoławczym zgodnie z regulaminem pracowniczym.
19. Eksperti krajowi oddelegowani do ESDZ na stanowisko wymagające dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej przedstawiają organowi ESDZ ds. bezpieczeństwa – przed rozpoczęciem wykonywania swoich zadań – ważne PBO uprawniające do dostępu do EUCI. Wyżej opisanym procesem zarządza wysyłające państwo członkowskie.

Rejestr PBO

20. ESDZ prowadzi bazę danych dotyczącą statusu wszystkich członków personelu podlegającego odpowiedzialności ESDZ oraz personelu wykonawców ESDZ pod względem poświadczenia bezpieczeństwa. Rejestr ten zawiera informacje o poziomie klauzuli tajności EUCI, do których dana osoba może mieć dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższy), dacie wydania PBO i okresie jego ważności.
21. Wprowadza się odpowiednie procedury koordynacji z państwami członkowskimi oraz innymi instytucjami, agencjami i organami UE w celu zapewnienia, aby ESDZ posiadała zgodny z prawdą i wyczerpujący wykaz statusu wszystkich członków personelu podlegającego odpowiedzialności ESDZ oraz personelu wykonawców ESDZ pod względem poświadczenia bezpieczeństwa.
22. Organ ESDZ ds. bezpieczeństwa może wydać zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego (ZPBO) zawierające informacje o poziomie klauzuli tajności EUCI, do których dana osoba może mieć dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższy), terminie ważności odpowiedniego PBO lub uprawnienia do dostępu oraz terminie ważności samego zaświadczenia.

Zwolnienia z wymogu posiadania PBO

23. Osobom uprawnionym do dostępu do EUCI ze względu na pełnione przez siebie funkcje zgodnie z krajowymi przepisami ustawowymi i wykonawczymi dyrekcja ESDZ odpowiedzialna za bezpieczeństwo udziela w stosownych przypadkach instrukcji na temat ich obowiązków w zakresie bezpieczeństwa dotyczących ochrony EUCI.

III. SZKOLENIA I UPOWSZECHNIANIE WIEDZY W ZAKRESIE BEZPIECZEŃSTWA

24. Wszystkie osoby, które mają otrzymać uprawnienie do dostępu do EUCI, oświadczają uprzednio na piśmie, że zrozumiały spoczywające na nich obowiązki w zakresie ochrony EUCI i konsekwencje ewentualnego narażenia na szwank EUCI. ESDZ zachowuje takie pisemne oświadczenia w aktach.
25. Wszystkie osoby, które są uprawnione do dostępu do EUCI lub od których wymaga się przetwarzania EUCI, są na początku informowane o zagrożeniach bezpieczeństwa, a następnie regularnie instruowane w zakresie tych zagrożeń; osoby te muszą bezzwłocznie zgłaszać właściwym organom bezpieczeństwa wszelkie kontakty lub działania, które uznają za podejrzane lub nietypowe.
26. Wszystkie osoby, które uzyskały uprawnienie do dostępu do EUCI, podlegają stałym środkom bezpieczeństwa osobowego (tj. stałej opiece) przez cały okres przetwarzania EUCI. Stałe bezpieczeństwo osobowe wchodzi w zakres odpowiedzialności:
 - a) osób, którym udzielono dostępu do EUCI: osoby te są osobiście odpowiedzialne za własne postępowanie w zakresie bezpieczeństwa i muszą bezzwłocznie zgłaszać właściwym organom bezpieczeństwa wszelkie kontakty lub działania, które uznają za podejrzane lub nietypowe, a także wszelkie zmiany własnej sytuacji osobistej, które mogą mieć znaczenie dla ich PBO lub uprawnienia do dostępu do EUCI;
 - b) bezpośrednich przełożonych: odpowiadają oni za to, aby ich personel był zaznajomiony ze środkami bezpieczeństwa i własnymi obowiązkami w zakresie ochrony EUCI, a także za monitorowanie postępowania personelu w zakresie bezpieczeństwa oraz za rozwiązywanie we własnym zakresie wszelkich problemów związanych z bezpieczeństwem lub przekazywanie właściwym organom ds. bezpieczeństwa wszelkich niekorzystnych informacji, które mogą mieć wpływ na PBO podlegającego im personelu lub na ich uprawnienia do dostępu do EUCI;

- c) osób odpowiedzialnych za bezpieczeństwo w ramach organizacji bezpieczeństwa ESDZ, o której mowa w art. 12 niniejszej decyzji: osoby te odpowiadają za organizowanie szkoleń dla zapewnienia, by personel na ich obszarze był okresowo informowany na temat bezpieczeństwa; za kształtowanie silnej kultury bezpieczeństwa w ich obszarze odpowiedzialności, za wprowadzenie środków monitorowania postępowania personelu w zakresie bezpieczeństwa oraz za zgłaszanie właściwym organom ds. bezpieczeństwa wszelkich niekorzystnych informacji, które mogą mieć znaczenie dla PBO którejkolwiek osoby;
 - d) ESDZ i państw członkowskich: uruchamiają one specjalne kanały przekazywania informacji, które mogą mieć znaczenie dla PBO którejkolwiek osoby lub jej uprawnienie do dostępu do EUCI.
27. Wszystkie osoby, które przestają wykonywać obowiązki wymagające dostępu do EUCI, informowane są o obowiązku stałej ochrony EUCI, a w stosownych przypadkach świadomość tego obowiązku potwierdzają na piśmie.

IV. WYJĄTKOWE OKOLICZNOŚCI

28. W nagłych przypadkach, jeżeli jest to należycie uzasadnione interesami ESDZ, w oczekiwaniu na zakończenie pełnego postępowania sprawdzającego organ ESDZ ds. bezpieczeństwa może, po konsultacji z KWB państwa członkowskiego, którego obywatelem jest dana osoba, oraz z zastrzeżeniem, że wynik wstępnego sprawdzenia nie wykazał niekorzystnych informacji, wydać urzędnikom i innym pracownikom ESDZ tymczasowe uprawnienie do dostępu do EUCI, by mogli wykonywać określone zadania. Pełne postępowanie sprawdzające należy przeprowadzić w najbliższym możliwym terminie. Takie tymczasowe uprawnienia zachowują ważność przez okres nieprzekraczający sześciu miesięcy i nie uprawniają do dostępu do informacji niejawnych o klauzuli tajności TRES SECRET UE/EU TOP SECRET. Wszystkie osoby, którym przyznano tymczasowe uprawnienie, oświadczają na piśmie, że rozumiały spoczywające na nich obowiązki w zakresie ochrony EUCI i konsekwencje ewentualnego narażenia na szwank EUCI. ESDZ zachowuje takie pisemne oświadczenia w aktach.
29. Jeżeli dana osoba ma objąć stanowisko, które wymaga PBO na poziomie o jeden stopień wyższym niż aktualnie przez nią posiadany, może ona tymczasowo pełnić obowiązki związane z tym stanowiskiem, pod warunkiem że:
- a) bezwzględna potrzeba dostępu do EUCI o wyższej klauzuli tajności jest uzasadniona na piśmie przez przełożonego tej osoby;
 - b) dostęp jest ograniczony do konkretnych EUCI, które są potrzebne do pracy na tym stanowisku;
 - c) osoba ta posiada ważne PBO;
 - d) podjęto czynności w celu uzyskania uprawnienia do dostępu do EUCI na poziomie wymaganym na tym stanowisku;
 - e) właściwy organ dokonał sprawdzenia, które potwierdziło, że dana osoba nie naruszyła poważnie ani wielokrotnie przepisów dotyczących bezpieczeństwa;
 - f) objęcie tego stanowiska przez daną osobę zatwierdził właściwy organ ESDZ;
 - g) zasięgnięto opinii właściwej KWB lub WWB, która wydała PBO danej osoby, i władza ta nie wyraziła sprzeciwu; oraz
 - h) dokumentacja dotycząca przyznania dostępu w drodze wyjątku, wraz z opisem informacji, do których zatwierdzono dostęp, przechowywana jest w odpowiedzialnej kancelarii tajnej lub podległej kancelarii tajnej.
30. Powyższa procedura jest stosowana, by przyznać danej osobie jednorazowy dostęp do EUCI o klauzuli tajności o jeden poziom wyższej niż klauzula, do której odnosi się poświadczenie bezpieczeństwa danej osoby. Z procedury tej nie korzysta się w sposób wielokrotny.
31. W szczególnie wyjątkowych okolicznościach, takich jak misje prowadzone we wrogim środowisku lub w okresie rosnącego napięcia międzynarodowego, i gdy wymagają tego środki nadzwyczajne, w szczególności w celu ratowania życia ludzkiego, Wysoki Przedstawiciel, organ ESDZ ds. bezpieczeństwa lub dyrektor generalny ds. budżetu i administracji mogą udzielić, w miarę możliwości na piśmie, dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET osobom, które nie posiadają wymaganego PBO, pod warunkiem że takie zezwolenie jest absolutnie niezbędne. Zachowuje się dokumentację takiego zezwolenia zawierającą opis informacji, do których dostęp zatwierdzono.

32. Taki nadzwyczajny dostęp do informacji niejawnych o klauzuli tajności TRES SECRET UE/EU TOP SECRET przysługuje tylko obywatelom UE, których upoważniono do dostępu do informacji niejawnych o klauzuli krajowej odpowiadającej klauzuli tajności TRES SECRET UE/EU TOP SECRET albo do informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET.
 33. O przypadkach skorzystania z procedury przedstawionej w pkt 31 i 32 informuje się Komitet ds. Bezpieczeństwa ESDZ.
 34. Komitet ds. Bezpieczeństwa ESDZ otrzymuje roczne sprawozdanie na temat korzystania z procedur określonych w niniejszej sekcji.
- V. UDZIAŁ W POSIEDZENIACH W SIEDZIBIE GŁÓWNEJ ESDZ I W DELEGATURACH UNII
35. Osoby wyznaczone do udziału w posiedzeniach w siedzibie głównej ESDZ i w delegaturach Unii, podczas których omawiane są informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, mogą brać w nich udział tylko po potwierdzeniu statusu ich PBO. W przypadku przedstawicieli państw członkowskich i urzędników Sekretariatu Generalnego Rady oraz Komisji ich ZPBO lub inny dowód posiadania przez nich PBO przesyłany jest przez właściwe organy do dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo lub do koordynatora delegatury Unii ds. bezpieczeństwa bądź – w sytuacjach wyjątkowych – przedstawiany jest przez osobę, której dotyczy. W stosownych przypadkach można zastosować zbiorczy wykaz nazwisk, przedstawiając odpowiednie dowody posiadania PBO.
 36. W przypadku cofnięcia PBO uprawniającego do dostępu do EUCI osobie, której obowiązki obejmują uczestnictwo w posiedzeniach w siedzibie głównej ESDZ i w delegaturach Unii, podczas których omawiane są informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, właściwy organ informuje o tym ESDZ.
- VI. POTENCJALNY DOSTĘP DO EUCI
37. Osoby, które mają zostać zatrudnione w warunkach stwarzających potencjalny dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, posiadają odpowiednie poświadczenie bezpieczeństwa lub przez cały czas towarzyszy im eskorta.
 38. Kurierzy, strażnicy i eskorta posiadają poświadczenie bezpieczeństwa do odpowiedniego poziomu lub są w inny sposób odpowiednio sprawdzani zgodnie z krajowymi przepisami ustawowymi i wykonawczymi oraz są regularnie informowani na temat procedur bezpieczeństwa w zakresie ochrony EUCI i obowiązku ochrony informacji, które im powierzono lub do których mogą mimowolnie mieć dostęp.
-

ZAŁĄCZNIK A II

BEZPIECZEŃSTWO FIZYCZNE INFORMACJI NIEJAWNYCH UE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 6 załącznika A. Określa się w nim minimalne wymogi w zakresie fizycznej ochrony lokali, budynków, biur, pomieszczeń i innych stref, w których ma miejsce przetwarzanie i przechowywanie EUCI, w tym stref, w których znajdują się CIS.
2. Środki bezpieczeństwa fizycznego mają zapobiegać nieuprawnionemu dostępowi do EUCI przez:
 - a) zapewnienie, by EUCI były przetwarzane i przechowywane we właściwy sposób;
 - b) umożliwienie podziału pracowników pod względem dostępu do EUCI zgodnie z zasadą ograniczonego dostępu, a w stosownych przypadkach na podstawie posiadanego przez nich poświadczenia bezpieczeństwa;
 - c) powstrzymywanie, udaremnianie i wykrywanie nieuprawnionych działań; oraz
 - d) uniemożliwienie lub opóźnienie wtargnięcia osób nieupoważnionych w sposób niezauważony lub z użyciem siły.

II. WYMOGI I ŚRODKI BEZPIECZEŃSTWA FIZYCZNEGO

3. ESDZ stosuje w swoich lokalach proces zarządzania ryzykiem służący ochronie EUCI, aby zapewnić poziom ochrony fizycznej proporcjonalny do szacowanego ryzyka. Proces zarządzania ryzykiem uwzględnia wszelkie istotne czynniki, a w szczególności:
 - a) klauzulę tajności EUCI;
 - b) postać i ilość EUCI z uwzględnieniem faktu, że duża ilość EUCI lub ich kompilacja mogą wymagać zastosowania bardziej rygorystycznych środków ochronnych;
 - c) otoczenie i strukturę budynków lub stref, w których znajdują się EUCI;
 - d) ocenę zagrożenia w danym państwie trzecim, opracowaną przez INTCEN w szczególności na podstawie sprawozdań delegatur Unii; oraz
 - e) szacowane zagrożenie ze strony służb wywiadowczych, których celem jest UE lub państwa członkowskie, oraz zagrożenie sabotażem, terroryzmem, działalnością wywrotową lub inną działalnością przestępczą.
4. Stosując koncepcję ochrony w głąb, organ ESDZ ds. bezpieczeństwa określa właściwą kombinację środków bezpieczeństwa fizycznego, które należy zastosować. Mogą one obejmować jeden z poniższych środków lub większą ich liczbę:
 - a) ogrodzenie: fizyczne ogrodzenie, które chroni granice strefy wymagającej ochrony;
 - b) systemy sygnalizacji włamania i napadu (SSWiN): SSWiN można stosować w celu podwyższenia poziomu bezpieczeństwa zapewnianego przez ogrodzenie, zaś w pomieszczeniach i budynkach w celu zastąpienia lub wsparcia pracowników ochrony;
 - c) kontrola dostępu: kontrola dostępu może obejmować teren, budynek lub budynki znajdujące się na danym terenie bądź też strefy lub pomieszczenia wewnątrz budynku. Kontrolę można prowadzić za pomocą środków elektronicznych lub środków elektromechanicznych, za pośrednictwem pracowników ochrony lub pracowników recepcji, bądź za pomocą wszelkich innych środków fizycznych;
 - d) pracownicy ochrony: przeszkoleni, nadzorowani, a w razie konieczności posiadający odpowiednie poświadczenie bezpieczeństwa pracownicy ochrony mogą być zatrudniani m.in. w celu powstrzymania osób planujących niezauważone wejście na dany teren;
 - e) telewizja przemysłowa (CCTV): CCTV może być stosowana przez pracowników ochrony w celu sprawdzania incydentów i sygnałów alarmowych pochodzących z SSWiN na rozległych terenach lub na ich granicach;

- f) oświetlenie ochronne: oświetlenie ochronne może być stosowane w celu powstrzymania potencjalnych osób nieupoważnionych, a ponadto w celu zapewnienia oświetlenia koniecznego do prowadzenia skutecznego nadzoru bezpośrednio przez pracowników ochrony lub pośrednio za pomocą systemu CCTV; oraz
 - g) wszelkie inne stosowne środki fizyczne służące powstrzymaniu lub wykryciu przypadków nieuprawnionego dostępu bądź zapobieganiu utracie lub uszkodzeniu EUCI.
5. Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo może przeprowadzać przeszukania osób wchodzących i wychodzących jako środek odstraszający przed nieuprawnionym wnoszeniem materiałów lub nieuprawnionym wynoszeniem EUCI z lokali lub budynków.
6. Jeżeli istnieje ryzyko podglądu EUCI, także przypadkowego, podejmuje się stosowne środki w celu zlikwidowania takiego ryzyka.
7. W przypadku nowych obiektów wymogi dotyczące bezpieczeństwa fizycznego i specyfikacje dotyczące ich stosowania określone są w ramach planowania i projektowania tych obiektów. W przypadku obiektów już istniejących wymogi dotyczące bezpieczeństwa fizycznego stosowane są w największym możliwym zakresie.

III. SPRZĘT SŁUŻĄCY DO FIZYCZNEJ OCHRONY EUCI

8. Przy zakupie sprzętu służącego do fizycznej ochrony EUCI (takiego jak zabezpieczone szafy, niszcarki, zamki do drzwi, elektroniczne systemy kontroli dostępu, SSWiN, systemy alarmowe) organ ESDZ ds. bezpieczeństwa zapewnia, by sprzęt ten spełniał zatwierdzone normy techniczne i minimalne wymogi.
9. Specyfikacje techniczne sprzętu, który ma być wykorzystywany do fizycznej ochrony EUCI, określone są w wytycznych dotyczących bezpieczeństwa, które zatwierdza Komitet ds. Bezpieczeństwa ESDZ.
10. Systemy bezpieczeństwa są poddawane regularnym inspekcjom, a sprzęt – regularnej konserwacji. Podczas konserwacji uwzględnia się wyniki inspekcji, aby zapewnić dalsze optymalne działanie sprzętu.
11. Podczas każdej inspekcji przeprowadza się ocenę skuteczności poszczególnych środków bezpieczeństwa oraz całego systemu bezpieczeństwa.

IV. STREFY CHRONIONE FIZYCZNIE

12. Ustanawia się dwa rodzaje stref chronionych fizycznie lub ich krajowych odpowiedników, służących fizycznej ochronie EUCI:
- a) strefy administracyjne; oraz
 - b) strefy bezpieczeństwa (w tym strefy technicznie zabezpieczone).
13. Organ ESDZ ds. bezpieczeństwa stwierdza, czy dana strefa spełnia wymogi potrzebne do uznania jej za strefę administracyjną, strefę bezpieczeństwa lub strefę technicznie zabezpieczoną.
14. W przypadku stref administracyjnych:
- a) wyraźnie określa się granicę umożliwiającą kontrolę osób, a jeżeli to możliwe – pojazdów;
 - b) dostęp bez eskorty umożliwia się tylko osobom odpowiednio upoważnionym przez dyrekcję ESDZ odpowiedzialną za bezpieczeństwo; oraz
 - c) wszystkim innym osobom przez cały czas towarzyszy eskorta lub poddaje się je równorzędnej kontroli.
15. W przypadku stref bezpieczeństwa:
- a) wyraźnie określa się i chroni granicę, na której wszelkie wejścia i wyjścia kontrolowane są za pomocą przepustki lub systemu rozpoznawania osób;

- b) dostęp bez eskorty umożliwia się tylko osobom posiadającym poświadczenie bezpieczeństwa do odpowiedniego poziomu i wyraźnie upoważnionym do wejścia do danej strefy zgodnie z zasadą ograniczonego dostępu;
 - c) wszystkim innym osobom przez cały czas towarzyszy eskorta lub poddaje się je równorzędnej kontroli.
16. Jeżeli wejście do strefy bezpieczeństwa jest w praktyce równoznaczne z bezpośrednim dostępem do informacji niejawnych znajdujących się w tej strefie, zastosowanie mają następujące dodatkowe wymogi:
- a) wyraźnie wskazuje się najwyższą klauzulę tajności, którą przyznano informacjom zwykle przechowywanym w tej strefie;
 - b) wszystkie osoby wchodzące do tej strefy muszą posiadać specjalne upoważnienie do wejścia, przez cały czas towarzyszy im eskorta i muszą one posiadać odpowiednie poświadczenie bezpieczeństwa, chyba że podjęto kroki zapewniające, aby dostęp do EUCI nie był możliwy;
 - c) urządzenia elektroniczne pozostawia się poza tą strefą.
17. Strefy bezpieczeństwa chronione przed podsłuchem uznawane są za strefy technicznie zabezpieczone. Zastosowanie mają następujące dodatkowe wymogi:
- a) strefy takie wyposażone są w SSWiN, są zamknięte na klucz, gdy nikt w nich nie przebywa, i chronione, gdy ktoś w nich przebywa. Wszystkie klucze podlegają kontroli zgodnie z sekcją VI niniejszego załącznika;
 - b) wszystkie osoby wchodzące do takich stref lub materiały tam wnoszone podlegają kontroli;
 - c) strefy takie podlegają regularnym inspekcjom fizycznym lub technicznym zgodnie z wymogami organu ESDZ ds. bezpieczeństwa. Inspekcje takie przeprowadza się także po każdorazowym nieuprawnionym wejściu do strefy lub podejrzeniu, że takie wejście miało miejsce; oraz
 - d) w strefach takich nie mogą się znajdować niezatwierdzone linie telekomunikacyjne, niezatwierdzone telefony, inne niezatwierdzone urządzenia komunikacyjne ani sprzęt elektryczny lub elektroniczny.
18. Niezależnie od pkt 17 lit. d), zanim urządzenia komunikacyjne i sprzęt elektryczny lub elektroniczny zostaną użyte w strefach, w których odbywają się posiedzenia lub prowadzone są prace związane z wykorzystaniem informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET i wyższej, a także jeżeli ocenia się, że istnieje wysokie zagrożenie dla EUCI, urządzenia i sprzęt taki zostają najpierw sprawdzone przez organ ESDZ ds. bezpieczeństwa w celu zapewnienia, aby żadne zrozumiałe informacje nie mogły zostać nieumyślnie lub nielegalnie przekazane przez taki sprzęt poza granicę strefy bezpieczeństwa.
19. Strefy bezpieczeństwa, w których nie pracują w systemie całodobowym pracownicy pełniący dyżur, są w razie potrzeby poddawane inspekcji na koniec normalnych godzin pracy i w przypadkowych odstępach czasu poza tymi godzinami, chyba że znajdują się tam SSWiN.
20. Strefy bezpieczeństwa oraz strefy technicznie zabezpieczone mogą być tworzone tymczasowo na terenie stref administracyjnych w celu zorganizowania niejawnego posiedzenia lub w jakimkolwiek innym podobnym celu.
21. Dla każdej strefy bezpieczeństwa opracowywane są procedury bezpiecznej eksploatacji określające:
- a) poziom klauzuli tajności EUCI, które można przetwarzać i przechowywać w tej strefie;
 - b) środki nadzoru i ochrony, które należy stosować;
 - c) osoby upoważnione do wejścia do strefy bez eskorty ze względu na zasadę ograniczonego dostępu i posiadane poświadczenie bezpieczeństwa;
 - d) w odpowiednich przypadkach procedury dotyczące eskort lub ochrony EUCI, jeżeli zezwala się na wejście do strefy innym osobom;
 - e) wszelkie inne odpowiednie środki i procedury.
22. W obrębie stref bezpieczeństwa są budowane wzmocnione pomieszczenia. Ściany, podłogi, sufity, okna i wyposażone w zamek drzwi zatwierdzone są przez organ ds. bezpieczeństwa ESDZ i zapewniają ochronę równoważną zabezpieczonym szafom zatwierdzonym do celów przechowywania EUCI z taką samą klauzulą tajności.

V. FIZYCZNE ŚRODKI OCHRONY NA POTRZEBY PRZETWARZANIA I PRZECHOWYWANIA EUCI

23. EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED mogą być przetwarzane:

- a) w strefie bezpieczeństwa;
- b) w strefie administracyjnej, pod warunkiem że EUCI są chronione przed dostępem osób nieupoważnionych; lub
- c) poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz przenosi EUCI zgodnie z załącznikiem A III pkt 30–42 i zobowiązał się do zastosowania środków zastępczych określonych w instrukcjach bezpieczeństwa, wydanych przez organ ESDZ ds. bezpieczeństwa, służących zapewnieniu, aby nieupoważnione osoby nie miały dostępu do EUCI.

24. EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED przechowywane są w odpowiednim do tego celu zamkniętym meblu biurowym w strefie administracyjnej lub strefie bezpieczeństwa. Mogą być one tymczasowo przechowywane poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz zobowiązał się do zastosowania środków zastępczych określonych w instrukcjach bezpieczeństwa wydanych przez organ ESDZ ds. bezpieczeństwa.

25. EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET mogą być przetwarzane:

- a) w strefie bezpieczeństwa;
- b) w strefie administracyjnej, pod warunkiem że EUCI są chronione przed dostępem osób nieupoważnionych; lub
- c) poza strefą bezpieczeństwa lub strefą administracyjną, pod warunkiem że posiadacz:
 - (i) przenosi EUCI zgodnie z załącznikiem A III pkt 30–42;
 - (ii) zobowiązał się do zastosowania środków zastępczych określonych w instrukcjach bezpieczeństwa wydanych przez organ ESDZ ds. bezpieczeństwa, służących zapewnieniu, aby nieupoważnione osoby nie miały dostępu do EUCI;
 - (iii) przechowuje EUCI przez cały czas pod swoją kontrolą; oraz
 - (iv) w przypadku dokumentów w formie papierowej – powiadomił o tym fakcie właściwą kancelarię tajną.

26. EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET przechowywane są w strefie bezpieczeństwa w zabezpieczonej szafie lub wzmocnionym pomieszczeniu.

27. Przetwarzanie EUCI o klauzuli tajności TRES SECRET UE/EU TOP SECRET odbywa się w strefie bezpieczeństwa.

28. EUCI o klauzuli tajności TRES SECRET UE/EU TOP SECRET przechowywane są w strefie bezpieczeństwa w siedzibie głównej, przy spełnieniu jednego z następujących warunków:

- a) są one przechowywane w zabezpieczonej szafie zgodnej z pkt 8, z co najmniej jednym z następujących zabezpieczeń dodatkowych:
 - (i) stała ochrona lub kontrola przez posiadających poświadczenie bezpieczeństwa pracowników ochrony lub pracowników pełniących dyżur;
 - (ii) zatwierdzony SSWiN w połączeniu z obecnością pracowników odpowiedzialnych za bezpieczeństwo;
- lub
- b) są one przechowywane we wzmocnionym pomieszczeniu wyposażonym w SSWiN w połączeniu z obecnością pracowników odpowiedzialnych za bezpieczeństwo.

29. Przepisy regulujące przenoszenie EUCI poza strefy chronione fizycznie znajdują się w załączniku A III.

VI. KONTROLA KLUCZY I KODÓW WYKORZYSTYWANYCH DO OCHRONY EUCI

30. Organ ESDZ ds. bezpieczeństwa określa procedury zarządzania kluczami i kodami do biur, pomieszczeń, wzmocnionych pomieszczeń i zabezpieczonych szaf. Procedury te chronią przed nieuprawnionym dostępem.

31. Kody zostają powierzone do zapamiętania jak najmniejszej liczbie osób, dla których znajomość tych kodów jest niezbędna. Kody do zabezpieczonych szaf i wzmocnionych pomieszczeń, w których przechowywane są EUCI, zostają zmienione:
- a) w przypadku otrzymania nowej szafy;
 - b) przy każdej zmianie pracowników znających kod;
 - c) w każdym przypadku, gdy następuje rzeczywiste lub domniemane narażenie na szwank bezpieczeństwa informacji;
 - d) gdy zamek poddano konserwacji lub naprawie; oraz
 - e) co najmniej raz na 12 miesięcy.
-

ZAŁĄCZNIK A III

ZARZĄDZANIE INFORMACJAMI NIEJAWNymi

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 7 załącznika A. Określa się w nim środki administracyjne służące kontroli EUCI na wszystkich etapach ich cyklu życia, w celu przyczynienia się w ten sposób do powstrzymania zamierzonego lub przypadkowego narażenia na szwank lub utraty tych informacji, wykrywania takich przypadków i usuwania ich skutków.

II. ZARZĄDZANIE KLAUZULAMI TAJNOŚCI

Klauzule tajności i oznaczenia

2. Informacjom nadaje się klauzulę tajności, jeżeli należy chronić ich poufność.
3. Za określenie poziomu klauzuli tajności, zgodnie z odpowiednimi wytycznymi w zakresie nadawania klauzul, i za dystrybucję informacji odpowiada wytwórca EUCI.
4. Poziom klauzuli tajności EUCI określa się zgodnie z art. 2 ust. 2 załącznika A i przez odniesienie do wytycznych bezpieczeństwa, które mają być zatwierdzone zgodnie z art. 3 ust. 3 załącznika A.
5. Informacjom niejawnym pochodzącym z państw członkowskich, przekazywanym ESDZ, zapewnia się taki sam poziom ochrony jak EUCI opatrzonym równorzędną klauzulą tajności. Tabela równorzędnych odpowiedników klauzul tajności znajduje się w dodatku B do niniejszej decyzji.
6. Klauzulę tajności, w stosownych przypadkach wraz z datą lub określeniem konkretnego wydarzenia, po którym klauzulę można obniżyć lub znieść, nanosi się wyraźnie i poprawnie, niezależnie od tego, czy dana EUCI ma formę pisemną, ustną, elektroniczną czy jakkolwiek inną.
7. Poszczególne części danego dokumentu (np. strony, punkty, sekcje, załączniki, dodatki, załączone dokumenty i uzupełnienia) mogą wymagać nadania różnych klauzul tajności i zostają odpowiednio oznaczone, w tym także wówczas, gdy są przechowywane w formie elektronicznej.
8. Na ile jest to możliwe, dokumenty, których częściom nadaje się różne klauzule tajności, mają taką strukturę, aby części oznaczone różnymi klauzulami można było łatwo zidentyfikować i w razie potrzeby oddzielić.
9. Ogólna klauzula tajności dokumentu lub pliku jest co najmniej tak wysoka jak klauzula tajności tej części dokumentu, która została oznaczona najwyższą klauzulą tajności. W przypadku zebrania informacji pochodzących z różnych źródeł sprawdza się ostateczną wersję dokumentu w celu określenia jego ogólnej klauzuli tajności, gdyż może istnieć konieczność nadania mu klauzuli tajności wyższej niż klauzule jego poszczególnych części.
10. Klauzula tajności pisma lub noty zawierających załączniki ma taki poziom jak najwyższa klauzula tajności nadana załącznikom. Wytwórca wyraźnie wskazuje, jaki poziom klauzuli tajności ma być nadany takiemu pismu lub nocie po ich odłączeniu od załączników, stosując w tym celu odpowiednie oznaczenie, np.:

CONFIDENTIEL UE/EU CONFIDENTIAL:

RESTREINT UE/EU RESTRICTED bez załącznika(-ów)

Oznaczenia

11. Oprócz jednej z klauzul tajności określonych w art. 2 ust. 2 załącznika A EUCI mogą być opatrzone dodatkowymi oznaczeniami, takimi jak:
 - a) dane identyfikujące wytwórcę;
 - b) wszelkie oznaczenia zastrzegające, kody słowne lub akronimy określające obszar działalności, do którego odnosi się dany dokument, szczególnie sposób dystrybucji dokumentu zgodnie z zasadą ograniczonego dostępu lub ograniczenia w zakresie wykorzystania;
 - c) oznaczenia dotyczące możliwości udostępnienia.

12. W następstwie decyzji o udostępnieniu EUCI państwu trzeciemu lub organizacji międzynarodowej dyrekcja ESDZ odpowiedzialna za bezpieczeństwo przekazuje daną informację niejawną, która jest opatrzona oznaczeniem dotyczącym możliwości udostępnienia, wskazującym państwo trzecie lub organizację międzynarodową, którym ma zostać udostępniona.
13. Organ ESDZ ds. bezpieczeństwa przechowuje wykaz takich zatwierdzonych oznaczeń.

Skrócone oznaczenia klauzul tajności

14. W celu nadania poziomu klauzuli tajności pojedynczym ustępom tekstu można stosować standardowe skrócone oznaczenia klauzul tajności. Skróty nie zastępują pełnych nazw klauzul tajności.
15. W celu wskazania poziomu klauzuli tajności sekcji lub ciągłych fragmentów tekstu krótszych niż jedna strona w dokumentach niejawnych UE można stosować następujące standardowe skróty:

| | |
|---------------------------------|-------------|
| TRES SECRET UE/EU TOP SECRET | TS-UE/EU-TS |
| SECRET UE/EU SECRET | S-UE/EU-S |
| CONFIDENTIEL UE/EU CONFIDENTIAL | C-UE/EU-C |
| RESTREINT UE/EU RESTRICTED | R-UE/EU-R |

Wytwarzanie EUCI

16. Przy wytwarzaniu dokumentu niejawnego UE:
 - a) każdą stronę wyraźnie oznacza się klauzulą tajności;
 - b) numeruje się każdą stronę;
 - c) na dokumencie umieszcza się numer referencyjny i temat, który nie stanowi informacji niejawnej, chyba że z jego oznaczenia wynika inaczej;
 - d) na dokumencie umieszcza się datę;
 - e) na każdej stronie dokumentów o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, które mają zostać rozpowszechnione w kilku kopiach, umieszcza się numer kopii.
17. Jeżeli do EUCI nie można zastosować pkt 16, podejmowane są inne odpowiednie środki zgodnie z wytycznymi dotyczącymi bezpieczeństwa, które należy ustalić na mocy niniejszej decyzji.

Obniżanie i znoszenie klauzul tajności EUCI

18. W momencie wytwarzania EUCI wytwórca wskazuje, o ile to możliwe, a w szczególności w odniesieniu do informacji niejawnych o klauzuli tajności RESTREINT UE/EU RESTRICTED, czy klauzula tajności EUCI może zostać obniżona lub zniesiona z daną datą lub w następstwie konkretnego wydarzenia.
19. ESDZ przeprowadza regularne przeglądy EUCI znajdujących się w jej posiadaniu, by stwierdzić, czy dana klauzula tajności ma nadal zastosowanie. ESDZ tworzy system służący do przeglądu klauzul tajności nadanych zarejestrowanym EUCI, których jest wytwórcą, nie rzadziej niż co pięć lat. Taki przegląd nie jest konieczny, jeżeli wytwórca określił na samym początku czas, po upływie którego klauzula tajności nadana danym informacjom zostanie automatycznie obniżona lub zniesiona, a informacje te zostały odpowiednio oznaczone.

III. REJESTRACJA EUCI ZE WZGLĘDÓW BEZPIECZEŃSTWA

20. W siedzibie głównej ustanawia się główną kancelarię tajną. Dla każdej jednostki organizacyjnej w ESDZ, w której przetwarza się EUCI, ustanawia się odpowiedzialną kancelarię tajną, podlegającą głównej kancelarii tajnej, w celu zapewnienia przetwarzania EUCI w sposób zgodny z niniejszą decyzją. Kancelarie tajne uznaje się za strefy bezpieczeństwa zgodnie z definicją w załączniku A.

Każda delegatura Unii ustanawia własną kancelarię tajną na potrzeby EUCI.

Organ ESDZ ds. bezpieczeństwa wyznacza dyrektora ds. kancelarii tajnych.

21. Do celów niniejszej decyzji rejestracja ze względów bezpieczeństwa (zwana dalej „rejestracją”) oznacza stosowanie procedur rejestrowania etapów cyklu życia informacji, w tym jej dystrybucji i zniszczenia. W przypadku CIS procedury rejestracji mogą być stosowane w ramach działań samego CIS.
22. Wszystkie materiały o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i wyższej rejestruje się w momencie ich wpłynięcia do jednostki organizacyjnej, w również delegatury Unii, lub wysłania z tej jednostki. Informacje niejawne opatrzone klauzulą tajności TRES SECRET UE/EU TOP SECRET rejestruje się w wyznaczonych kancelariach tajnych.
23. Główna kancelaria tajna stanowi w głównej siedzibie ESDZ główny punkt, do którego wpływają i z którego przekazywane są informacje niejawne wymieniane z państwami trzecimi i organizacjami międzynarodowymi. Główna kancelaria tajna rejestruje wszystkie takie wymiany informacji.
24. Organ ESDZ ds. bezpieczeństwa zatwierdza wytyczne bezpieczeństwa dotyczące rejestrowania EUCI do celów bezpieczeństwa, zgodnie z art. 14 niniejszej decyzji.

Kancelarie tajne TRES SECRET UE/EU TOP SECRET

25. W głównej siedzibie ESDZ wyznacza się główną kancelarię tajną będącą głównym organem otrzymującym i wysyłającym informacje niejawne o klauzuli tajności TRES SECRET UE/EU TOP SECRET. W razie potrzeby można wyznaczyć podległe kancelarie tajne do przetwarzania takich informacji do celów rejestracji.
26. Takie podległe kancelarie tajne nie mogą przekazywać dokumentów o klauzuli tajności TRES SECRET UE/EU TOP SECRET bezpośrednio innym podległym kancelariom tajnym podlegającym tej samej głównej kancelarii tajnej TRES SECRET UE/EU TOP SECRET ani na zewnątrz bez wyraźnego pisemnego upoważnienia tej głównej kancelarii tajnej.

IV. KOPIOWANIE I TŁUMACZENIE DOKUMENTÓW NIEJAWNYCH UE

27. Dokumenty o klauzuli tajności TRES SECRET UE/EU TOP SECRET nie mogą być kopiowane ani tłumaczone bez wcześniejszej pisemnej zgody ich wytwórcy.
28. Jeżeli wytwórca dokumentów o klauzuli tajności SECRET UE/EU SECRET i niższej nie zgłosił zastrzeżeń co do ich kopiowania lub tłumaczenia, dokumenty takie można kopiować lub tłumaczyć na zlecenie posiadacza.
29. Środki bezpieczeństwa, które mają zastosowanie do oryginalnego dokumentu, mają zastosowanie do jego kopii i tłumaczeń. Kopie dokumentów o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej wykonuje wyłącznie właściwa kancelaria lub podległa kancelaria tajna za pomocą zabezpieczonej kopiarki. Kopie muszą być rejestrowane.

V. PRZENOSZENIE EUCI

30. Przenoszenie EUCI podlega środkom ochrony określonym w pkt 32–42. Gdy EUCI przenosi się na nośnikach elektronicznych, niezależnie od przepisów art. 7 ust. 4 załącznika A, poniższe środki ochrony mogą być uzupełnione odpowiednimi technicznymi środkami zaradczymi zgodnie z wytycznymi organu ESDZ ds. bezpieczeństwa, tak aby zminimalizować ryzyko utraty lub nieuprawnionego ujawnienia informacji.
31. Organ ESDZ ds. bezpieczeństwa wydaje instrukcje dotyczące przenoszenia EUCI zgodnie z niniejszą decyzją.

W obrębie budynku lub grupy budynków stanowiącej zamkniętą całość

32. EUCI przenoszone w ramach budynku lub grupy budynków stanowiącej zamkniętą całość zakrywa się, aby nie można było zobaczyć ich treści.
33. W ramach budynku lub grupy budynków stanowiącej zamkniętą całość informacje niejawne o klauzuli tajności TRES SECRET UE/EU TOP SECRET przenoszą osoby o odpowiednim poświadczeniu bezpieczeństwa w zabezpieczonej kopercie, na której znajduje się jedynie nazwisko adresata.

Na terytorium UE

34. EUCI przenoszone między budynkami lub obiektami na terytorium UE są opakowane w sposób zabezpieczający je przed nieuprawnionym ujawnieniem.

35. Przenoszenie informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET na terytorium UE odbywa się za pomocą jednego z następujących środków:
- a) za pośrednictwem, w stosownych przypadkach, kurierów wojskowych, rządowych lub dyplomatycznych;
 - b) osobiście, pod warunkiem że:
 - (i) EUCI przez cały czas znajdują się w posiadaniu osoby przynoszącej, chyba że są przechowywane zgodnie z wymogami określonymi w załączniku A II;
 - (ii) EUCI nie są po drodze otwierane ani czytane w miejscach publicznych;
 - (iii) osoby przynoszące posiadają poświadczenie bezpieczeństwa do odpowiedniego poziomu i zostają poinformowane o obowiązkach w zakresie bezpieczeństwa;
 - (iv) w razie potrzeby osobom przynoszącym wydaje się list kurierski;
 - c) za pośrednictwem usług pocztowych lub prywatnych służb kurierskich, pod warunkiem że:
 - (i) są one zatwierdzone przez odpowiednią KWB zgodnie z krajowymi przepisami ustawowymi i wykonawczymi;
 - (ii) stosują one odpowiednie środki ochrony zgodnie z minimalnymi wymogami, które mają być ustalone w wytycznych dotyczących bezpieczeństwa zgodnie z art. 21 ust. 1 niniejszej decyzji.

W przypadku przewozu z jednego państwa członkowskiego do drugiego przepisy lit. c) są ograniczone do informacji niejawnych o klauzuli tajności do poziomu CONFIDENTIEL UE/EU CONFIDENTIAL.

36. Materiał oznaczony klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET (np. sprzęt lub urządzenia), który nie może być przewożony środkami, o których mowa w pkt 34, transportuje się jako ładunek przez prywatne firmy przewozowe zgodnie z załącznikiem A V.
37. Przenoszenie informacji niejawnych o klauzuli tajności TRES SECRET UE/EU TOP SECRET między budynkami lub obiektami na terytorium UE odbywa się za pośrednictwem, w stosownych przypadkach, kurierów wojskowych, rządowych lub dyplomatycznych.

Z terytorium UE na terytorium państwa trzeciego lub pomiędzy jednostkami organizacyjnymi UE w państwach trzecich

38. EUCI przewożone z terytorium UE na terytorium państwa trzeciego lub pomiędzy jednostkami organizacyjnymi UE w państwach trzecich są opakowane w sposób zabezpieczający je przed nieuprawnionym ujawnieniem.
39. Przewóz informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET z terytorium UE na terytorium państwa trzeciego oraz przenoszenie wszelkich EUCI o klauzuli tajności do poziomu SECRET UE/EU SECRET pomiędzy jednostkami organizacyjnymi UE w państwach trzecich odbywa się za pomocą jednego z następujących środków:
- a) za pośrednictwem kurierów wojskowych lub dyplomatycznych;
 - b) osobiście, pod warunkiem że:
 - (i) przesyłka opatrzona jest urzędową pieczęcią lub sposób zapakowania wskazuje na to, że jest to przesyłka urzędowa i nie powinna podlegać kontroli celnej ani kontroli bezpieczeństwa;
 - (ii) osoba przynosząca posiada list kurierski zawierający informacje o przesyłce i upoważniający ją do przenoszenia tej przesyłki;
 - (iii) EUCI przez cały czas znajdują się w posiadaniu osoby przynoszącej, chyba że są przechowywane zgodnie z wymogami określonymi w załączniku A II;
 - (iv) EUCI nie są po drodze otwierane ani czytane w miejscach publicznych; oraz
 - (v) osoby przynoszące posiadają poświadczenie bezpieczeństwa do odpowiedniego poziomu oraz informuje się je o ich obowiązkach w zakresie bezpieczeństwa.
40. Przewóz informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET udostępnionych przez UE państwu trzeciemu lub organizacji międzynarodowej odbywa się w sposób zgodny z odpowiednimi przepisami umowy o bezpieczeństwie informacji lub porozumienia administracyjnego zgodnie z art. 10 ust. 2 załącznika A.
41. Informacje niejawne o klauzuli tajności RESTREINT UE/EU RESTRICTED mogą być przewożone z terytorium UE na terytorium państwa trzeciego także za pośrednictwem usług pocztowych lub prywatnych służb kurierskich.

42. Przewóz informacji niejawnych o klauzuli tajności TRES SECRET UE/EU TOP SECRET z terytorium UE na terytorium państwa trzeciego lub pomiędzy jednostkami organizacyjnymi UE w państwach trzecich odbywa się za pośrednictwem kurierów wojskowych lub dyplomatycznych.

VI. NISZCZENIE EUCI

43. Dokumenty niejawne UE, które nie są już potrzebne, mogą zostać zniszczone, bez uszczerbku dla odpowiednich zasad i przepisów wykonawczych dotyczących archiwizowania.
44. Dokumenty podlegające rejestracji zgodnie z art. 7 ust. 2 załącznika A są niszczone przez odpowiedzialną kancelarię tajną na polecenie posiadacza lub właściwego organu. Rejestry i inne informacje dotyczące rejestracji są odpowiednio uaktualniane.
45. W przypadku dokumentów niejawnych o klauzuli tajności SECRET UE/EU SECRET lub TRES SECRET UE/EU TOP SECRET niszczenie przebiega w obecności świadka, który posiada poświadczenie bezpieczeństwa co najmniej do poziomu klauzuli tajności niszczonego dokumentu.
46. Osoba dokonująca rejestracji oraz świadek, jeżeli jego obecność jest wymagana, podpisują protokół zniszczenia, który zostaje umieszczony w dokumentacji kancelarii tajnej. Protokoły zniszczenia dokumentów o klauzuli tajności TRES SECRET UE/EU TOP SECRET przechowywane są w kancelarii tajnej przez okres co najmniej dziesięciu lat, a dokumentów o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET – przez okres co najmniej pięciu lat.
47. Dokumenty niejawne, w tym dokumenty o klauzuli tajności RESTREINT UE/EU RESTRICTED, są niszczone przy zastosowaniu metod, które spełniają odpowiednie normy UE lub normy równoważne lub które zostały zatwierdzone przez państwa członkowskie zgodnie z krajowymi normami technicznymi, tak by nie mogły zostać całkowicie lub częściowo odtworzone.
48. Niszczenie komputerowych nośników EUCI odbywa się zgodnie z procedurami zatwierdzonymi przez organ ESDZ ds. bezpieczeństwa.

VII. INSPEKCJE W ZAKRESIE BEZPIECZEŃSTWA

Inspekcje ESDZ w zakresie bezpieczeństwa

49. Zgodnie z art. 16 niniejszej decyzji inspekcje ESDZ w zakresie bezpieczeństwa obejmują:
- ogólne inspekcje w zakresie bezpieczeństwa, mające na celu ocenę ogólnego poziomu bezpieczeństwa siedziby głównej ESDZ, delegatur Unii i wszelkich lokali zależnych lub powiązanych, w szczególności w celu oceny skuteczności środków bezpieczeństwa wdrożonych dla ochrony interesów bezpieczeństwa ESDZ;
 - inspekcje w zakresie bezpieczeństwa EUCI, mające na celu ocenę, ogólnie pod kątem akredytacji, skuteczności środków podjętych w celu ochrony EUCI w siedzibie głównej ESDZ i w delegaturach Unii.
- W szczególności inspekcje takie przeprowadza się m.in. aby:
- zapewnić przestrzeganie określonych w niniejszej decyzji wymaganych norm minimalnych w zakresie ochrony EUCI;
 - podkreślić znaczenie bezpieczeństwa i skutecznego zarządzania ryzykiem wewnątrz kontrolowanych podmiotów;
 - zalecić środki zaradcze mające złagodzić konkretne skutki, jakie może powodować utrata poufności, integralności lub dostępności informacji niejawnych; oraz
 - ulepszyć istniejące, opracowane przez organy bezpieczeństwa, programy szkoleń i upowszechniania wiedzy w dziedzinie bezpieczeństwa.

Przeprowadzanie inspekcji ESDZ w zakresie bezpieczeństwa i sprawozdawczość

50. Inspekcje ESDZ w zakresie bezpieczeństwa przeprowadza zespół kontrolny dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo, w razie potrzeby ze wsparciem ekspertów w dziedzinie bezpieczeństwa z innych instytucji UE lub państw członkowskich.

Zespół kontrolny ma dostęp do wszystkich miejsc, w których przetwarzane są EUCI, w szczególności do kancelarii tajnych i punktów, w których znajdują się CIS.

51. Inspekcje ESDZ w zakresie bezpieczeństwa w delegaturach Unii można przeprowadzać w razie potrzeby ze wsparciem urzędników ds. bezpieczeństwa ambasad państw członkowskich znajdujących się w danych państwach trzecich.
52. Przed końcem każdego roku kalendarzowego organ ESDZ ds. bezpieczeństwa przyjmuje program inspekcji na następny rok.
53. W razie potrzeby organ ESDZ ds. bezpieczeństwa może zorganizować inspekcje w zakresie bezpieczeństwa, które nie zostały przewidziane w wyżej wspomnianym programie.
54. Pod koniec inspekcji w zakresie bezpieczeństwa kontrolowanemu podmiotowi przedstawiane są główne wnioski i zalecenia. Następnie zespół kontrolny sporządza sprawozdanie z inspekcji. W przypadku gdy zostały zaproponowane działania naprawcze i zalecenia, w sprawozdaniu zamieszcza się odpowiednio szczegółowe dane uzasadniające sformułowane wnioski. Sprawozdanie przekazuje się organowi ESDZ ds. bezpieczeństwa oraz kierownikowi kontrolowanego podmiotu.

Pod nadzorem dyrekcji ESDZ odpowiedzialnej za bezpieczeństwo opracowuje się okresowe sprawozdanie mające na celu uwypuklenie doświadczeń nabytych w wyniku inspekcji przeprowadzonych w danym okresie; sprawozdanie to podlega analizie Komitetu ds. Bezpieczeństwa ESDZ.

Przeprowadzanie inspekcji w zakresie bezpieczeństwa w agencjach i organach UE ustanowionych na mocy tytułu V rozdział 2 TUE oraz sprawozdawczość.

55. Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo może w stosownych przypadkach wyznaczać ekspertów, którzy będą członkami wspólnych zespołów kontrolnych przeprowadzających inspekcje w agencjach i organach UE ustanowionych na mocy tytułu V rozdział 2 TUE.

Lista kontrolna na potrzeby inspekcji ESDZ w zakresie bezpieczeństwa

56. Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo sporządza i uaktualnia listę kontrolną, zawierającą kwestie, które należy sprawdzić w trakcie inspekcji ESDZ w zakresie bezpieczeństwa. Wspomniana lista kontrolna przekazywana jest Komitetowi ds. Bezpieczeństwa ESDZ.
57. Informacji służących uzupełnieniu listy kontrolnej udziela, w szczególności podczas inspekcji, personel odpowiedzialny za bezpieczeństwo w jednostce, w której przeprowadzana jest inspekcja. Po wypełnieniu listy kontrolnej szczegółowymi odpowiedziami nadaje się jej klauzulę tajności w porozumieniu z kontrolowaną jednostką. Lista ta nie jest częścią sprawozdania z inspekcji.

ZAŁĄCZNIK A IV

OCHRONA EUCI PRZETWARZANYCH W CIS

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 8 załącznika A.
2. Następujące cechy i koncepcje zabezpieczania informacji są niezbędne dla bezpieczeństwa i prawidłowego funkcjonowania operacji dokonywanych w ramach systemów teleinformatycznych (CIS):

| | |
|--------------------|---|
| Autentyczność: | gwarancja, że informacje są prawdziwe i pochodzą z rzetelnych źródeł; |
| Dostępność: | cecha polegająca na tym, że informacje są dostępne i gotowe do wykorzystania na wniosek uprawnionego podmiotu; |
| Poufność: | cecha polegająca na tym, że informacje nie są ujawniane nieupoważnionym osobom, podmiotom ani do celów nieuprawnionego przetwarzania; |
| Integralność: | cecha polegająca na zachowywaniu dokładności i kompletności informacji i zasobów; |
| Niezaprzeczalność: | możliwość udowodnienia, że działanie lub wydarzenie miało miejsce, aby następnie nie można było zaprzeczyć wystąpieniu tego działania lub wydarzenia. |

II. ZASADY ZABEZPIECZANIA INFORMACJI

3. Przedstawione poniżej przepisy stanowią podstawę bezpieczeństwa wszelkich systemów CIS, w których przetwarzane są EUCI. Szczegółowe wymogi dotyczące wdrażania tych przepisów określa się w wytycznych bezpieczeństwa dotyczących zabezpieczania informacji.

Zarządzanie ryzykiem dla bezpieczeństwa

4. Zarządzanie ryzykiem dla bezpieczeństwa stanowi integralną część opracowywania, tworzenia, eksploatacji i konserwacji CIS. Zarządzanie ryzykiem (ocena, zmniejszanie, akceptacja i powiadamianie) jest prowadzone jako proces iteracyjny wspólnie przez przedstawicieli właścicieli systemu, organy odpowiedzialne za projekt, organy operacyjne oraz organy zatwierdzające bezpieczeństwo, w ramach sprawdzonego, przejrzystego i w pełni zrozumiałego procesu oceny ryzyka. Zakres stosowania CIS oraz jego zasobów jest jasno definiowany na początku procesu zarządzania ryzykiem.
5. Właściwe organy ESDZ dokonują przeglądu potencjalnych zagrożeń dla CIS i prowadzą aktualne i dokładne oceny zagrożeń, odzwierciedlające aktualne środowisko operacyjne. Stale uaktualniają swoją wiedzę na temat podatności na zagrożenia i dokonują okresowych przeglądów oceny podatności, aby dostosować się do zmieniających się technologii informatycznych (IT).
6. Celem zarządzania ryzykiem dla bezpieczeństwa jest zastosowanie zestawu środków bezpieczeństwa prowadzących do osiągnięcia zadowalającej równowagi między wymaganiami użytkownika a szacunkowym ryzykiem dla bezpieczeństwa.
7. Szczególne wymogi, skala i stopień szczegółowości określone przez właściwy organ ds. akredytacji bezpieczeństwa (SAA) do celów przyznania akredytacji CIS są proporcjonalne do szacowanego ryzyka z uwzględnieniem wszystkich odpowiednich czynników, w tym poziomu klauzuli tajności EUCI przetwarzanych w danym CIS. Akredytacja obejmuje oficjalne oświadczenie o ryzyku szacunkowym oraz akceptację ryzyka szacunkowego przez odpowiedzialny organ.

Bezpieczeństwo w całym cyklu życia CIS

8. Zapewnianie bezpieczeństwa jest wymogiem obowiązującym w całym cyklu życia CIS, od jego uruchomienia do wycofania z użytkowania.

9. Dla każdego etapu cyklu życia CIS określana jest rola i interakcja każdego z podmiotów związanych z CIS w odniesieniu do jego bezpieczeństwa.
10. Wszystkie CIS wraz z technicznymi i innymi środkami bezpieczeństwa są podczas procedury akredytacji poddawane testom bezpieczeństwa, aby zapewnić osiągnięcie odpowiedniego stopnia zabezpieczenia wdrożonych środków bezpieczeństwa oraz sprawdzić, czy są one prawidłowo wdrożone, zintegrowane i skonfigurowane.
11. Oceny bezpieczeństwa, inspekcje i przeglądy przeprowadzane są okresowo w fazie operacyjnej oraz podczas konserwacji CIS, jak również przy pojawieniu się nadzwyczajnych okoliczności.
12. Dokumentacja bezpieczeństwa CIS ewoluuje podczas wszystkich etapów jego cyklu życia na zasadzie integralnej części procesu zmian i zarządzania konfiguracjami.

Najlepsze praktyki

13. ESDZ współpracuje z Sekretariatem Generalnym Rady, Komisją i państwami członkowskimi, aby opracować najlepsze praktyki ochrony EUCI przetwarzanych w CIS. Wytyczne w zakresie dobrych praktyk obejmują techniczne, fizyczne, organizacyjne i proceduralne środki bezpieczeństwa dotyczące CIS o sprawdzonej skuteczności w zapobieganiu danym zagrożeniom i podatności.
14. Ochrona EUCI przetwarzanych w CIS opiera się na doświadczeniach podmiotów zaangażowanych w zabezpieczanie informacji, zarówno w UE, jak i poza nią.
15. Rozpowszechnianie, a następnie wdrażanie dobrych praktyk pomaga w osiągnięciu równoważnego poziomu zabezpieczenia różnych CIS eksploatowanych przez ESDZ i przetwarzających EUCI.

Ochrona w głąb

16. Aby zmniejszyć ryzyko zagrażające CIS, wdraża się szereg technicznych i innych środków bezpieczeństwa o strukturze różnych poziomów ochrony. Poziomy te obejmują:
 - a) *powstrzymanie*: środki bezpieczeństwa ukierunkowane na zniechęcenie osób planujących atak na CIS;
 - b) *zapobieganie*: środki bezpieczeństwa ukierunkowane na udaremnienie lub powstrzymanie ataku na CIS;
 - c) *wykrywanie*: środki bezpieczeństwa ukierunkowane na ujawnienie ataku na CIS;
 - d) *odporność*: środki bezpieczeństwa ukierunkowane na ograniczenie skutków ataku, tak by dotknęły one jak najmniejszą ilość informacji lub zasobów CIS, oraz na zapobieżenie dalszym szkodom; oraz
 - e) *usuwanie skutków*: środki bezpieczeństwa ukierunkowane na odzyskanie bezpiecznego statusu CIS.

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

17. ESDZ dba o to, by była w stanie reagować na incydenty, które mogą przekraczać granice poszczególnych organizacji i państw, koordynować reakcje i dzielić się informacjami o tych incydentach i związanym z nimi ryzyku (zdolności do reagowania na sytuacje nadzwyczajne w ramach systemów komputerowych).

Zasada minimalizmu i najmniejszych uprawnień

18. Aby zapobiec niepotrzebnemu ryzyku, stosowane są wyłącznie funkcje, urządzenia i usługi służące spełnieniu wymogów operacyjnych.

19. Aby ograniczyć szkody wynikające z wypadków, błędów lub nieuprawnionego korzystania z zasobów CIS, użytkownicy CIS oraz procesy zautomatyzowane otrzymują wyłącznie taki dostęp i takie przywileje i upoważnienia, jakie są im niezbędne do wykonywania ich zadań.
20. Procedury rejestracji stosowane w razie konieczności w ramach CIS sprawdzane są jako element procedury akredytacji.

Świadomość zabezpieczania informacji

21. Świadomość ryzyka i dostępnych środków bezpieczeństwa stanowi pierwszą linię obrony bezpieczeństwa CIS. W szczególności wszyscy członkowie personelu związani z CIS na poszczególnych etapach jego cyklu życia, w tym użytkownicy, powinni:
 - a) zdawać sobie sprawę, że niedopatrzona w zakresie bezpieczeństwa mogą znacznie zaszkodzić CIS i całej organizacji;
 - b) rozumieć potencjalne szkody, jakie mogą ponieść inne podmioty w związku z podłączeniem do systemów lub sieci i współzależnością; oraz
 - c) być świadomi, że osobiście ponoszą odpowiedzialność i są rozliczani za bezpieczeństwo CIS zgodnie z pełnionymi przez siebie funkcjami w tych systemach i procesach.
22. Aby zapewnić zrozumienie obowiązków związanych z bezpieczeństwem, wszyscy członkowie personelu związani z CIS, w tym wyższe kierownictwo i użytkownicy CIS, przechodzą obowiązkowe szkolenia mające na celu edukację i zdobycie wiedzy w zakresie zabezpieczania informacji.

Ocena i zatwierdzanie produktów służących bezpieczeństwu systemów informatycznych

23. Wymagany stopień zabezpieczenia, jaki zapewniają środki bezpieczeństwa, określony jako poziom zabezpieczenia, określa się zgodnie z wynikami procesu zarządzania ryzykiem i zgodnie z odpowiednimi politykami i wytycznymi dotyczącymi bezpieczeństwa.
24. Poziom zabezpieczenia sprawdzany jest przy użyciu uznanych na szczeblu międzynarodowym lub zatwierdzonych na szczeblu krajowym procesów i metod. Obejmują one przede wszystkim ocenę, kontrole i audyt.
25. Produkty kryptograficzne służące ochronie EUCI są oceniane i zatwierdzane przez krajowy organ ds. zatwierdzania produktów kryptograficznych (CAA) państwa członkowskiego.
26. Przed zaleceniem do zatwierdzenia produktów kryptograficznych (CAA ESDZ) organowi ESDZ ds. zatwierdzania, zgodnie z art. 8 ust. 5 niniejszej decyzji, wspomniane produkty kryptograficzne muszą uzyskać pozytywny wynik podczas zewnętrznej oceny dokonywanej przez wykwalifikowany organ oceny produktów kryptograficznych (AQUA) państwa członkowskiego, które nie jest zaangażowane w projektowanie ani wytwarzanie tego sprzętu. Wymagany stopień szczegółowości oceny wewnętrznej zależy od przewidywanego najwyższego poziomu klauzuli tajności EUCI, które mają być chronione za pomocą tych produktów.
27. Jeżeli uzasadniają to określone względy operacyjne, CAA ESDZ może na zalecenie Komitetu ds. Bezpieczeństwa Rady znieść wymogi wynikające z pkt 25 lub 26 i udzielić tymczasowego zatwierdzenia na dany okres zgodnie z art. 8 ust. 5 niniejszej decyzji.
28. AQUA jest organem ds. zatwierdzania produktów kryptograficznych (CAA) państwa członkowskiego, który na podstawie kryteriów ustalonych przez Radę otrzymał akredytację, aby przeprowadzić ocenę zewnętrzną produktów kryptograficznych służących ochronie EUCI.
29. Wysoki Przedstawiciel zatwierdza politykę bezpieczeństwa dotyczącą kwalifikowania i zatwierdzania niekryptograficznych produktów służących bezpieczeństwu systemów informatycznych.

Transmisja w strefach bezpieczeństwa

30. Niezależnie od przepisów niniejszej decyzji, gdy transmisja EUCI ogranicza się do stref bezpieczeństwa lub stref administracyjnych, można je rozpowszechnić w postaci niezasyfrowanej lub zaszyfrować je na niższym poziomie na podstawie wyników procesu zarządzania ryzykiem i z zastrzeżeniem zatwierdzenia przez SAA.

Bezpieczne połączenia międzysystemowe CIS

31. Do celów niniejszej decyzji połączenie międzysystemowe oznacza bezpośrednie połączenie co najmniej dwóch systemów informatycznych w celu wspólnego korzystania z danych i innych zasobów informacyjnych (np. łączności) w sposób jednokierunkowy lub wielokierunkowy.
32. CIS traktuje każdy system informatyczny przyłączony połączeniem międzysystemowym jako niewzbudzający zaufania i stosuje środki ochrony, aby kontrolować wymianę informacji niejawnych.
33. Wszystkie połączenia międzysystemowe CIS z innym systemem informatycznym spełniają następujące podstawowe wymogi:
 - a) właściwe organy określają i zatwierdzają wymogi biznesowe i operacyjne dla takich połączeń;
 - b) połączenie międzysystemowe przechodzi proces zarządzania ryzykiem i akredytacji oraz wymaga zatwierdzenia przez właściwe organy akredytacji bezpieczeństwa (SAA); oraz
 - c) na granicach wszystkich CIS stosowane są usługi ochrony na granicy systemów (BPS).
34. Pomędzy CIS posiadającym akredytację a siecią niezabezpieczoną lub publiczną brak jest połączeń międzysystemowych z wyjątkiem sytuacji, w których w ramach CIS zainstalowano w tym celu zatwierdzone BPS między CIS a siecią niezabezpieczoną lub publiczną. Środki bezpieczeństwa dotyczące takich połączeń międzysystemowych są poddawane przeglądowi przez właściwy organ ds. zabezpieczania informacji (IAA) i zatwierdzane przez właściwy SAA.

Gdy sieć niezabezpieczona lub publiczna wykorzystywana jest wyłącznie jako nośnik, a dane zostały zaszyfrowane przy wykorzystaniu produktu kryptograficznego zatwierdzonego zgodnie z art. 8 ust. 5 niniejszej decyzji, takiego połączenia nie uznaje się za połączenie międzysystemowe.

35. Bezpośrednie lub kaskadowe połączenie międzysystemowe CIS posiadającego akredytację do przetwarzania informacji o klauzuli tajności TRES SECRET UE/EU TOP SECRET z siecią niezabezpieczoną lub publiczną jest zakazane.

Komputerowe nośniki informacji

36. Komputerowe nośniki informacji są niszczone zgodnie z procedurami zatwierdzonymi przez organ ESDZ ds. bezpieczeństwa.
37. Ponowne użycie komputerowych nośników informacji bądź obniżenie lub zniesienie ich klauzuli tajności odbywa się zgodnie z wytycznymi bezpieczeństwa, które są określone na mocy art. 8 ust. 2 niniejszej decyzji.

Okoliczności nadzwyczajne

38. Niezależnie od przepisów niniejszej decyzji w okolicznościach nadzwyczajnych, takich jak zbliżający się lub trwający kryzys, konflikt, stan wojny, lub w wyjątkowych sytuacjach operacyjnych można przez ograniczony czas stosować specjalne procedury opisane poniżej.
39. EUCI można transmitować z wykorzystaniem produktów kryptograficznych zatwierdzonych dla niższego poziomu klauzuli tajności lub w postaci niezasyfrowanej za zgodą właściwego organu, jeżeli jakakolwiek zwłoka spowodowałaby szkody wyraźnie większe od szkód, które mogłyby spowodować ujawnienie materiałów niejawnych, oraz jeżeli:
 - a) nadawca i odbiorca nie posiadają wymaganego urządzenia szyfrującego lub też nie posiadają żadnego urządzenia szyfrującego; oraz
 - b) materiały niejawne nie mogą być dostarczone na czas w inny sposób.
40. Informacje niejawne transmitowane w okolicznościach przedstawionych w pkt 39 nie są opatrzone żadnymi oznaczeniami ani wskazaniem odróżniającymi je od informacji jawnych lub informacji, które mogą być chronione przy pomocy dostępnego urządzenia szyfrującego. Odbiorcy są bezzwłocznie powiadamiani za pomocą innych środków o poziomie klauzuli tajności.

41. W przypadku stosowania przepisów pkt 39 należy następnie sporządzić sprawozdanie dla Dyrekcji ds. Bezpieczeństwa ESDZ i za jej pośrednictwem przekazać je Komitetowi ds. Bezpieczeństwa ESDZ. W sprawozdaniu określa się przynajmniej nadawcę, odbiorcę oraz wytwórcę każdej EUCI.

III. FUNKCJE I ORGANY ZABEZPIECZANIA INFORMACJI

42. W ESDZ ustanawia się następujące funkcje w zakresie zabezpieczania informacji. Funkcje te nie muszą być skupione w tych samych jednostkach organizacyjnych. Są one objęte oddzielnymi mandatami. Funkcje te, oraz związana z nimi odpowiedzialność, mogą być jednak połączone lub zintegrowane w tej samej jednostce organizacyjnej, bądź podzielone na różne jednostki organizacyjne, pod warunkiem że unika się wewnętrznych konfliktów interesów lub zadań.

Organ ds. zabezpieczania informacji (IAA)

43. Organ ds. zabezpieczania informacji (IAA) odpowiada za:
- opracowywanie wytycznych dotyczących bezpieczeństwa w zakresie zabezpieczania informacji oraz za monitorowanie ich skuteczności i adekwatności;
 - zabezpieczanie informacji technicznych związanych z produktami kryptograficznymi i zarządzanie tymi informacjami;
 - zapewnianie, by środki zabezpieczania informacji wybrane do ochrony EUCI były zgodne z odpowiednimi wytycznymi dotyczącymi kryteriów ich przydatności i wyboru;
 - zapewnianie, by wybór produktów kryptograficznych odbywał się zgodnie z wytycznymi dotyczącymi kryteriów ich przydatności i wyboru;
 - koordynowanie szkoleń i upowszechniania wiedzy na temat zabezpieczania informacji;
 - konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników co do wytycznych dotyczących bezpieczeństwa w zakresie zabezpieczania informacji; oraz
 - zapewnianie odpowiedniej wiedzy fachowej na temat zabezpieczania informacji w podgrupie eksperckiej Komitetu ds. Bezpieczeństwa ESDZ.

Organ ds. TEMPEST

44. Organ ds. TEMPEST (TA) odpowiada za zapewnienie zgodności CIS z politykami i wytycznymi TEMPEST. Zatwierdza on środki zaradcze TEMPEST dla instalacji i produktów, służące ochronie EUCI do określonego poziomu klauzuli tajności w środowisku operacyjnym.

Organ ds. zatwierdzania produktów kryptograficznych (CAA)

45. CAA odpowiada za zapewnienie zgodności produktów kryptograficznych z odpowiednimi wytycznymi kryptograficznymi. Wydaje on zgodę na to, by dany produkt kryptograficzny chronił EUCI do określonego poziomu klauzuli tajności w swoim środowisku operacyjnym.

Organ ds. dystrybucji produktów kryptograficznych (CDA)

46. CDA odpowiada za:
- zarządzanie materiałami kryptograficznymi UE i odpowiedzialność za nie;
 - zapewnianie stosowania odpowiednich procedur i stworzenia kanałów umożliwiających odpowiedzialność za wszystkie materiały kryptograficzne UE, ich bezpieczne przetwarzanie, przechowywanie i rozpowszechnianie; oraz
 - zapewnianie przekazywania materiałów kryptograficznych UE między osobami lub służbami korzystającymi z tych materiałów.

Organ ds. akredytacji bezpieczeństwa (SAA)

47. SAA jest w każdym systemie odpowiedzialny za:
- zapewnianie zgodności CIS z odpowiednimi wytycznymi dotyczącymi bezpieczeństwa, dostarczając poświadczenie zatwierdzenia CIS do celów przetwarzania EUCI do określonego poziomu klauzuli tajności w jego środowisku operacyjnym; w poświadczeniu określa się warunki akredytacji oraz kryteria, przy spełnieniu których konieczne jest ponowne zatwierdzenie;

- b) stworzenie procesu akredytacji bezpieczeństwa, zgodnie z odpowiednimi wytycznymi, z wyraźnie określonymi warunkami zatwierdzenia CIS pod nadzorem tego organu;
 - c) określanie strategii akredytacji bezpieczeństwa przez ustalenie stopnia szczegółowości procedury akredytacji – proporcjonalnego do wymaganego poziomu zabezpieczenia;
 - d) analizowanie i zatwierdzanie dokumentacji związanej z bezpieczeństwem, w tym oświadczeń o zarządzaniu ryzykiem i o ryzyku szczątkowym, oświadczeń o szczególnych wymaganiach bezpieczeństwa systemu (zwanym dalej „SSRS”), dokumentacji związanej z weryfikacją zapewnienia bezpieczeństwa oraz procedur bezpiecznej eksploatacji systemu (zwanym dalej „SecOP”), jak również zapewnianie zgodności tej dokumentacji z przepisami i wytycznymi w zakresie bezpieczeństwa ESDZ;
 - e) sprawdzanie wdrażania środków bezpieczeństwa w odniesieniu do CIS przez dokonywanie ocen, inspekcji lub przeglądów bezpieczeństwa czy też wspieranie takich działań;
 - f) określanie wymogów bezpieczeństwa (np. poziomów poświadczeń bezpieczeństwa personelu) w przypadku stanowisk o szczególnie wrażliwym charakterze w odniesieniu do CIS;
 - g) zatwierdzanie wyboru produktów kryptograficznych i produktów klasy TEMPEST wykorzystywanych do zapewnienia bezpieczeństwa CIS;
 - h) zatwierdzanie lub w odpowiednich przypadkach uczestniczenie we wspólnym zatwierdzaniu międzysystemowego połączenia CIS z innymi CIS; oraz
 - i) konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w związku z zarządzaniem ryzykiem dla bezpieczeństwa, w szczególności ryzykiem szczątkowym, jak również z warunkami i okolicznościami poświadczenia zatwierdzenia.
48. SAA ESDZ jest odpowiedzialny za przyznawanie akredytacji wszystkim CIS działającym w zakresie właściwości ESDZ.

Rada Akredytacji w zakresie Bezpieczeństwa (SAB)

49. Wspólna Rada Akredytacji w zakresie Bezpieczeństwa (SAB) jest odpowiedzialna za przyznawanie akredytacji CIS działającym w zakresie właściwości SAA ESDZ, jak i SAA państw członkowskich. W skład tej rady wchodzi po jednym przedstawicielu SAA z każdego państwa członkowskiego, a w jej obradach uczestniczy przedstawiciel SAA Sekretariatu Generalnego Rady oraz Komisji. Inne podmioty posiadające połączenia z danym CIS są zapraszane do uczestnictwa w obradach, gdy omawiany jest ten system.

Obradom SAB przewodniczy przedstawiciel SAA ESDZ. SAB podejmuje decyzje na zasadzie konsensusu przedstawicieli SAA z instytucji, państw członkowskich i innych podmiotów posiadających połączenia z danym CIS. SAB sporządza okresowe sprawozdania ze swojej działalności i przedstawia je Komitetowi ds. Bezpieczeństwa ESDZ oraz informuje Komitet o wszystkich świadectwach akredytacji.

Organ operacyjny ds. zabezpieczania informacji

50. Organ operacyjny ds. zabezpieczania informacji odpowiada w każdym systemie za:
- a) opracowanie dokumentacji bezpieczeństwa zgodnie z wytycznymi dotyczącymi bezpieczeństwa, zwłaszcza oświadczenia o szczególnych wymaganiach bezpieczeństwa systemu (SSRS), w tym oświadczenia o ryzyku szczątkowym, procedur bezpiecznej eksploatacji systemu (SecOP) i planu kryptograficznego w ramach procesu akredytacji CIS;
 - b) uczestnictwo w wyborze i testowaniu technicznych środków bezpieczeństwa, urządzeń i oprogramowania dla poszczególnych systemów, nadzorowanie ich wdrażania i zapewnianie, by były one w bezpieczny sposób instalowane, konfigurowane i konserwowane zgodnie z odpowiednią dokumentacją bezpieczeństwa;
 - c) uczestnictwo w wyborze środków bezpieczeństwa i urządzeń klasy TEMPEST, jeżeli jest to wymagane na podstawie SSRS, i zapewnianie, by były one w bezpieczny sposób instalowane i konserwowane we współpracy z TA;
 - d) monitorowanie wdrażania i stosowania SecOP, a w odpowiednich przypadkach zlecenie właścicielowi systemu obowiązków operacyjnych w zakresie bezpieczeństwa;

- e) zarządzanie produktami kryptograficznymi i ich przetwarzanie, zapewnianie nadzoru nad obiektami kryptograficznymi i kontrolowanymi oraz, jeżeli jest to wymagane, zapewnienie wytwarzania zmiennych kryptograficznych;
 - f) przeprowadzanie przeglądów i testów analizy bezpieczeństwa, w szczególności w celu sporządzenia odpowiednich sprawozdań o ryzyku, zgodnie z wymogami SAA;
 - g) zapewnianie szkolenia w zakresie zabezpieczania informacji w odniesieniu do poszczególnych CIS;
 - h) wdrażanie środków bezpieczeństwa w odniesieniu do poszczególnych CIS i stosowanie tych środków.
-

ZAŁĄCZNIK A V

BEZPIECZEŃSTWO PRZEMYSŁOWE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 9 załącznika A. Ustanawia się w nim ogólne przepisy w zakresie bezpieczeństwa mające zastosowanie do podmiotów gospodarczych lub innych podczas negocjacji poprzedzających zawarcie umowy oraz na wszystkich etapach cyklu życia umów niejawnych zawartych przez ESDZ.
2. Organ ESDZ ds. bezpieczeństwa zatwierdza wytyczne dotyczące bezpieczeństwa przemysłowego, określające zwłaszcza szczegółowe wymogi w odniesieniu do świadectw bezpieczeństwa przemysłowego (SBP), dokumentów określających aspekty bezpieczeństwa (DOAB), wizyt, transmisji i przenoszenia EUCL.

II. ELEMENTY DOTYCZĄCE BEZPIECZEŃSTWA W UMOWIE NIEJAWNEJ

Przewodnik nadawania klauzul (PNK)

3. Przed zamieszczeniem ogłoszenia o przetargu lub zawarciem umowy niejawnej ESDZ jako instytucja zamawiająca określa klauzulę tajności wszelkich informacji, które należy dostarczyć oferentom i wykonawcom, jak również klauzulę tajności wszelkich informacji, które mają być wytworzone przez wykonawcę. W tym celu ESDZ opracowuje PNK, który należy stosować podczas wykonywania umów.
4. Do określania klauzuli tajności różnych elementów umowy niejawnej zastosowanie mają następujące zasady:
 - a) podczas opracowywania PNK ESDZ uwzględnia wszystkie odpowiednie aspekty bezpieczeństwa, w tym klauzulę tajności nadaną informacjom, które ich wytwórca przekazał i których wykorzystanie do celów umowy zatwierdził;
 - b) ogólna klauzula tajności umowy nie może być niższa od najwyższej klauzuli tajności któregośkolwiek z jej elementów; oraz
 - c) w stosownych przypadkach ESDZ działa w porozumieniu z KWB/WWB państw członkowskich lub jakimkolwiek innym właściwym organem bezpieczeństwa na wypadek jakichkolwiek zmian klauzul tajności informacji wytworzonych przez wykonawców lub przekazanych im podczas wykonywania umowy oraz w przypadku wprowadzania jakichkolwiek późniejszych zmian do PNK.

Dokument określający aspekty bezpieczeństwa (DOAB)

5. Wymogi bezpieczeństwa dotyczące poszczególnych umów opisane są w DOAB. DOAB w stosownych przypadkach zawiera PNK i stanowi integralną część umowy niejawnej lub niejawnej umowy o podwykonawstwo.
6. DOAB zawiera przepisy zobowiązujące wykonawcę lub podwykonawcę do przestrzegania minimalnych norm określonych w niniejszej decyzji. Nieprzestrzeganie tych minimalnych norm może stanowić wystarczający powód do rozwiązania umowy.

Instrukcje bezpieczeństwa programu/projektu (IBP)

7. W zależności od zakresu programów lub projektów obejmujących dostęp do EUCL, ich przetwarzanie lub przechowywanie instytucja zarządzająca wyznaczona do zarządzania danym programem lub projektem może sporządzić specjalne instrukcje bezpieczeństwa programu/projektu (IBP). IBP wymagają zatwierdzenia przez KWB/WWB państw członkowskich lub jakimkolwiek inny właściwy organ bezpieczeństwa uczestniczący w programie/projekcie i mogą zawierać dodatkowe wymogi bezpieczeństwa.

III. ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO (SBP)

8. Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo zwraca się do KWB lub WWB lub innego właściwego organu bezpieczeństwa danego państwa członkowskiego o wydanie SBP w celu zaświadczenia, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, że dany podmiot gospodarczy lub inny jest w stanie zapewnić w swoich obiektach ochronę EUCI odpowiadającą określonemu poziomowi klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET). Do czasu przekazania SBP do ESDZ żadnemu rzeczywistemu ani potencjalnemu wykonawcy ani podwykonawcy nie udziela się ani nie umożliwia się dostępu do EUCI.
9. W stosownych przypadkach ESDZ jako instytucja zamawiająca powiadamia odpowiednią KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa o tym, że na etapie poprzedzającym zawarcie umowy lub do wykonywania umowy wymagane jest SBP. SBP lub PBO są wymagane na etapie poprzedzającym zawarcie umowy, jeżeli podczas składania ofert mają być dostarczone EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET.
10. ESDZ jako instytucja zamawiająca nie zawiera umowy niejawniej z wybranym oferentem, zanim nie otrzyma od KWB/WWB lub jakiegokolwiek innego właściwego organu bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest dany wykonawca lub podwykonawca, potwierdzenia, że wydane zostało, jeśli istnieje taki wymóg, odpowiednie SBP.
11. ESDZ jako instytucja zamawiająca zwraca się do KWB/WWB lub jakiegokolwiek innego właściwego organu bezpieczeństwa, który wydał SBP, o przekazywanie ESDZ wszelkich niekorzystnych informacji dotyczących SBP. W przypadku umowy o podwykonawstwo informuje się o tym odpowiednio KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa.
12. Cofnięcie SBP przez odpowiednią KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa stanowią dla ESDZ jako instytucji zamawiającej wystarczający powód do rozwiązania umowy niejawniej lub wykluczenia oferenta z postępowania.

IV. POŚWIADCZENIA BEZPIECZEŃSTWA OSOBOWEGO (PBO) DLA PRACOWNIKÓW WYKONAWCY

13. Wszyscy zatrudnieni przez wykonawcę pracownicy, którym niezbędny jest dostęp do EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej, muszą przed uzyskaniem dostępu do tych informacji uzyskać odpowiednie poświadczenie bezpieczeństwa i spełniać zasadę ograniczonego dostępu. Dostęp do EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED nie wymaga PBO, ale wymaga spełnienia zasady ograniczonego dostępu.
14. Wnioski o PBO dla pracowników wykonawcy składa się do KWB/WWB odpowiedzialnej za dany podmiot.
15. ESDZ informuje wykonawców, którzy zamierzają zatrudnić obywatela państwa trzeciego na stanowisku wymagającym dostępu do EUCI, że za ustalenie zgodnie z niniejszą decyzją, czy tej osobie można udzielić dostępu do takich informacji, odpowiada KWB/WWB państwa członkowskiego, w którym znajduje się siedziba podmiotu zatrudniającego; do jej obowiązków należy również potwierdzenie, że przed udzieleniem takiego dostępu uzyskano zgodę wytwórcy informacji.

V. UMOWY NIEJAWNE I NIEJAWNE UMOWY O PODWYKONAWSTWO

16. Jeżeli EUCI przekazywane są oferentowi na etapie poprzedzającym zawarcie umowy, ogłoszenie o przetargu zawiera przepis zobowiązujący oferenta, który nie złoży oferty lub który nie zostanie wybrany, do zwrotu wszystkich dokumentów niejawnych w określonym terminie.
17. Po zawarciu umowy niejawniej lub niejawniej umowy o podwykonawstwo ESDZ jako instytucja zamawiająca powiadamia KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa wykonawcy lub podwykonawcy o zawartych w tej umowie przepisach bezpieczeństwa.
18. W przypadku rozwiązania lub wygaśnięcia takich umów ESDZ jako instytucja zamawiająca (lub – w przypadku umowy o podwykonawstwo – KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa, w zależności od przypadku) niezwłocznie powiadamia o tym fakcie KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest wykonawca lub podwykonawca.

19. Co do zasady, od wykonawcy lub podwykonawcy wymaga się zwrotu do instytucji zamawiającej wszelkich posiadanych przez niego EUCI po rozwiązaniu lub wygaśnięciu umowy niejawnego lub niejawnego umowy o podwykonawstwo.
20. Szczegółowe przepisy dotyczące pozbywania się EUCI podczas wykonywania umowy lub po jej rozwiązaniu bądź wygaśnięciu określa się w DOAB.
21. Jeżeli wykonawca lub podwykonawca są upoważnieni do zachowania EUCI po rozwiązaniu lub wygaśnięciu umowy, nadal przestrzegają oni minimalnych norm zawartych w niniejszej decyzji i nadal chronią poufność EUCI.
22. Warunki, na których wykonawca może zlecić podwykonawstwo, są określone w ogłoszeniu o przetargu oraz w umowie.
23. Przed zleceniem podwykonawstwa części umowy niejawnego wykonawca uzyskuje zgodę ESDZ jako instytucji zamawiającej. Nie można zawrzeć umowy o podwykonawstwo z podmiotami gospodarczymi ani innymi, zarejestrowanymi w państwie, które nie jest państwem członkowskim UE i nie zawarło z UE umowy o bezpieczeństwie informacji.
24. Wykonawca odpowiada za zapewnienie zgodności wszystkich podejmowanych czynności podwykonawczych z minimalnymi normami określonymi w niniejszej decyzji i nie dostarcza EUCI podwykonawcy bez uprzedniej pisemnej zgody instytucji zamawiającej.
25. W odniesieniu do EUCI wytworzonych lub przetwarzanych przez wykonawcę lub podwykonawcę prawa przysługujące wytwórcy są wykonywane przez instytucję zamawiającą.

VI. WIZYTY ZWIĄZANE Z UMOWAMI NIEJAWNYMI

26. Jeżeli do celów wykonania umowy niejawnego ESDZ, wykonawcy lub podwykonawcy niezbędny jest dostęp do informacji niejawnego o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET w obiektach innej z wymienionych stron, organizuje się wizyty w porozumieniu z KWB/WWB lub jakimkolwiek innym właściwym organem bezpieczeństwa. Pozostaje to bez uszczerbku dla uprawnienia KWB/WWB do uzgodnienia, w kontekście konkretnych projektów, procedury umożliwiającej bezpośrednie organizowanie wizyt.
27. W odniesieniu do dostępu do EUCI związanych z umową zawartą przez ESDZ wszystkie osoby wizytujące muszą posiadać odpowiednie PBO i podlegają zasadzie ograniczonego dostępu.
28. Osobom wizytującym umożliwia się dostęp wyłącznie do EUCI związanych z celem wizyty.

VII. TRANSMISJA I PRZENOSZENIE EUCI

29. Do transmisji EUCI drogą elektroniczną zastosowanie mają odpowiednie przepisy art. 8 załącznika A oraz załącznika A IV.
30. Do przenoszenia EUCI zastosowanie mają odpowiednie przepisy załącznika A III zgodnie z krajowymi przepisami ustawowymi i wykonawczymi.
31. Jeżeli materiały niejawnego są przewożone jako ładunek, do określania zabezpieczeń stosuje się następujące zasady:
 - a) bezpieczeństwo zapewnia się na wszystkich etapach przewozu, począwszy od miejsca wyjazdu do miejsca przeznaczenia;
 - b) stopień ochrony, jakim objęto przesyłkę, określa się według najwyższego poziomu klauzuli tajności materiału zawartego w przesyłce;
 - c) firmy dokonujące przewozu muszą uzyskać SBP na stosownym poziomie, jeśli przewóz wymaga również przechowywania informacji niejawnego w obiektach wykonawcy. W każdym przypadku pracownicy obsługujący się z przesyłką muszą posiadać odpowiednie poświadczenie bezpieczeństwa zgodnie z załącznikiem A I;

- d) przed wszelkim transgranicznym przemieszczeniem materiałów o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET nadawca sporządza plan przewozu, który jest zatwierdzany przez ESDZ, w stosownych przypadkach w porozumieniu z KWB/WWB nadawcy i odbiorcy lub jakimkolwiek innym właściwym organem bezpieczeństwa;
- e) przejazdy odbywają się w miarę możliwości bezpośrednio między dwoma punktami i w najkrótszym czasie, na jaki pozwalają okoliczności;
- f) jeżeli jest to możliwe, trasy powinny przebiegać wyłącznie przez terytoria państw członkowskich. Transport trasami przebiegającymi przez terytoria państw innych niż państwa członkowskie powinien się odbywać wyłącznie pod warunkiem zatwierdzenia przez ESDZ lub jakikolwiek inny właściwy organ bezpieczeństwa zarówno państwa nadawcy, jak i państwa odbiorcy.

VIII. PRZEKAZYWANIE EUCI WYKONAWCOM ZNAJDUJĄCYM SIĘ W PAŃSTWACH TRZECICH

- 32. EUCI są przekazywane wykonawcom i podwykonawcom znajdującym się w państwach trzecich, które zawarły z UE ważną umowę dotyczącą bezpieczeństwa, zgodnie ze środkami bezpieczeństwa uzgodnionymi przez ESDZ, jako instytucję zamawiającą, z KWB/WWB państwa trzeciego, w którym zarejestrowany jest wykonawca.

IX. PRZETWARZANIE I PRZECHOWYWANIE INFORMACJI NIEJAWNYCH O KLAUZULI TAJNOŚCI RESTREINT UE/EU RESTRICTED

- 33. ESDZ jako instytucja zamawiająca, w stosownych przypadkach w porozumieniu z KWB/WWB w państwie członkowskim, jest upoważniona na podstawie przepisów umownych do przeprowadzania wizyt w obiektach wykonawców/podwykonawców w celu sprawdzenia, czy wprowadzone zostały odpowiednie środki bezpieczeństwa służące ochronie EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED zgodnie z wymogami umowy.
- 34. W zakresie zgodnym z wymogami krajowych przepisów ustawowych i wykonawczych ESDZ jako instytucja zamawiająca powiadamia KWB/WWB lub jakikolwiek inny właściwy organ bezpieczeństwa o umowach niejawnych lub niejawnym umowach o podwykonawstwo zawierających informacje niejawne o klauzuli tajności RESTREINT UE/EU RESTRICTED.
- 35. W przypadku umów zawartych przez ESDZ zawierających informacje niejawne o klauzuli tajności RESTREINT UE/EU RESTRICTED od wykonawców, podwykonawców ani ich personelu nie wymaga się posiadania SBP ani PBO.
- 36. ESDZ jako instytucja zamawiająca analizuje odpowiedzi na zaproszenia do składania ofert w przypadku umów, które wymagają dostępu do informacji niejawnych o klauzuli tajności RESTREINT UE/EU RESTRICTED, niezależnie od wszelkich ewentualnych wymogów związanych z SBP lub PBO określonych w krajowych przepisach ustawowych i wykonawczych.
- 37. Warunki, na których wykonawca może zlecić podwykonawstwo, są zgodne z pkt 22–24.
- 38. Jeżeli umowa obejmuje przetwarzanie informacji niejawnych o klauzuli tajności RESTREINT UE/EU RESTRICTED w ramach CIS, który eksploatuje wykonawca, ESDZ jako instytucja zamawiająca zapewnia, aby umowa ta lub jakakolwiek umowa o podwykonawstwo określała niezbędne wymogi techniczne i administracyjne dotyczące akredytacji CIS, które są proporcjonalne do szacowanego ryzyka z uwzględnieniem wszystkich odpowiednich czynników. Zakres akredytacji dla takiego CIS jest uzgadniany między instytucją zamawiającą a odpowiednią KWB/WWB.

ZAŁĄCZNIK A VI

WYMIANA INFORMACJI NIEJAWNYCH Z PAŃSTWAMI TRZECIMI I ORGANIZACJAMI MIĘDZYNARODOWYMI

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wprowadzania w życie art. 10 załącznika A.

II. RAMY REGULUJĄCE WYMIANĘ INFORMACJI NIEJAWNYCH

2. ESDZ może wymieniać EUCI z państwami trzecimi lub organizacjami międzynarodowymi zgodnie z art. 10 ust. 1 załącznika A.

W celu wsparcia Wysokiego Przedstawiciela w wykonywaniu jego obowiązków określonych w art. 218 TFUE:

- a) odpowiedni departament geograficzny lub tematyczny ESDZ, w porozumieniu z dyrekcją ESDZ odpowiedzialną za bezpieczeństwo, w stosownych przypadkach stwierdza potrzebę długoterminowej wymiany EUCI z danym państwem trzecim lub organizacją międzynarodową;
 - b) dyrekcja ESDZ odpowiedzialna za bezpieczeństwo, w porozumieniu z właściwym departamentem geograficznym ESDZ, w stosownych przypadkach przedstawia Wysokiemu Przedstawicielowi projekty tekstów, które mają zostać przedstawione Radzie jako wnioski na podstawie art. 218 ust. 3, 5 i 6 TFUE;
 - c) dyrekcja ESDZ odpowiedzialna za bezpieczeństwo wspiera Wysokiego Przedstawiciela w prowadzeniu negocjacji w koordynacji z właściwymi służbami Komisji i Sekretariatu Generalnego Rady;
 - d) w odniesieniu do umów lub uzgodnień z państwami trzecimi dotyczących ich uczestnictwa w operacjach zarządzania kryzysowego WPBiO, o których mowa w art. 10 ust. 1 lit. c) załącznika A, Dyrekcja ds. Zarządzania Kryzysowego i Planowania ESDZ w porozumieniu z właściwymi służbami ESDZ w stosownych przypadkach przedstawia Wysokiemu Przedstawicielowi projekty tekstów, które mają zostać przedstawione Radzie jako wnioski na podstawie art. 218 ust. 3, 5 i 6 TFUE i wspiera Wysokiego Przedstawiciela w prowadzeniu negocjacji w koordynacji z właściwymi służbami ESDZ i Sekretariatu Generalnego Rady.
3. W przypadkach, w których umowy o bezpieczeństwie informacji przewidują dokonywanie technicznych uzgodnień wykonawczych pomiędzy dyrekcją ESDZ odpowiedzialną za bezpieczeństwo (w koordynacji z Dyrekcją ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji oraz Biurem Bezpieczeństwa w Sekretariacie Generalnym Rady) a właściwym organem bezpieczeństwa w danym państwie trzecim lub organizacji międzynarodowej, w uzgodnieniach takich uwzględnia się poziom ochrony przewidziany w przepisach, strukturach i procedurach dotyczących bezpieczeństwa istniejących w danym państwie trzecim lub danej organizacji międzynarodowej.
 4. Jeżeli istnieje długoterminowa potrzeba wymiany przez ESDZ z państwem trzecim lub organizacją międzynarodową informacji niejawnych o klauzuli tajności co do zasady nie wyższej niż RESTREINT UE/EU RESTRICTED i jeżeli ustalono, że dana strona nie dysponuje systemem bezpieczeństwa wystarczająco rozwiniętym, aby być w stanie zawrzeć umowę o bezpieczeństwie informacji, Wysoki Przedstawiciel może, po uzyskaniu jednomyślnej przychylniej opinii Komitetu ds. Bezpieczeństwa ESDZ wyrażonej zgodnie z art. 15 ust. 5 niniejszej decyzji, zawrzeć porozumienie administracyjne z właściwymi organami bezpieczeństwa danego państwa trzeciego lub organizacji międzynarodowej.
 5. Nie wymienia się z państwem trzecim ani organizacją międzynarodową żadnych EUCI drogą elektroniczną, o ile nie zostało to wyraźnie przewidziane w umowie o bezpieczeństwie informacji lub porozumieniu administracyjnym.
 6. W ramach porozumienia administracyjnego o wymianie informacji niejawnych ESDZ i dane państwo trzecie lub organizacja międzynarodowa wyznaczają, każde we własnym zakresie, kancelarię tajną, do której – jako głównego punktu – będą wpływać i z której będą przekazywane informacje niejawne podlegające wymianie. W przypadku ESDZ będzie to główna kancelaria tajna ESDZ.
 7. Porozumienia administracyjne co do zasady przyjmują postać wymiany listów.

III WIZYTY OCENIAJĄCE

8. Wizyty oceniające, o których mowa w art. 17 niniejszej decyzji, przeprowadza się w porozumieniu z danym państwem trzecim lub organizacją międzynarodową i służą one ocenie:
- ram prawnych mających zastosowanie do ochrony informacji niejawnych;
 - wszelkich cech charakterystycznych przepisów ustawowych i wykonawczych, polityk i procedur danego państwa trzeciego lub organizacji międzynarodowej w zakresie bezpieczeństwa, które mogą mieć wpływ na to, jaką najwyższą klauzulę tajności mogą mieć wymieniane informacje niejawne;
 - stosowanych w danym czasie środków i procedur bezpieczeństwa dotyczących ochrony informacji niejawnych; oraz
 - procedur sprawdzających w zakresie poświadczenia bezpieczeństwa odpowiadających klauzuli tajności EUCI, które mają być udostępniane.
9. Nie dokonuje się wymiany EUCI przed przeprowadzeniem wizyty oceniającej i ustaleniem poziomu, na jakim dane strony mogą wymieniać informacje niejawne, na podstawie równoważności poziomu ochrony przypisanego tym informacjom.

Jeśli przed wizytą oceniającą Wysoki Przedstawiciel uzyska wiedzę na temat jakichkolwiek wyjątkowych lub pilnych powodów, dla których konieczna jest wymiana informacji niejawnych, wówczas ESDZ:

- zwraca się najpierw o pisemną zgodę wytwórcy informacji w celu ustalenia, że nie ma przeciwwskazań dla udostępnienia informacji;
- zwraca się do organu ESDZ ds. bezpieczeństwa, który może postanowić o udostępnieniu informacji pod warunkiem uzyskania jednogłośnej przychyłnej opinii państw członkowskich reprezentowanych w Komitecie ds. Bezpieczeństwa ESDZ.

Jeśli ESDZ nie jest w stanie ustalić wytwórcy informacji, to organ ESDZ ds. bezpieczeństwa przyjmuje na siebie odpowiedzialność wytwórcy po uzyskaniu jednogłośnej przychyłnej opinii Komitetu ds. Bezpieczeństwa ESDZ.

IV. UPOWAŻNIENIE DO UDOSTĘPNIANIA EUCI PAŃSTWOM TRZECIM LUB ORGANIZACJOM MIĘDZYNARODOWYM

10. W przypadku gdy zgodnie z art. 10 ust. 1 załącznika A istnieją ramy wymiany informacji niejawnych z państwem trzecim lub organizacją międzynarodową, decyzję o udostępnieniu EUCI przez ESDZ państwu trzeciemu lub organizacji międzynarodowej podejmuje organ ESDZ ds. bezpieczeństwa, który może delegować udzielanie takiego upoważnienia urzędnikom ESDZ wysokiego szczebla bądź innym podlegającym mu osobom.
11. Jeżeli ESDZ nie jest wytwórcą informacji niejawnej, która ma zostać udostępniona, ani wytwórcą materiału źródłowego, który może ona zawierać, to ESDZ najpierw zwraca się o pisemną zgodę wytwórcy w celu ustalenia, że nie ma przeciwwskazań dla udostępnienia tej informacji. Jeśli ESDZ nie jest w stanie ustalić wytwórcy informacji, to organ ESDZ ds. bezpieczeństwa przyjmuje na siebie odpowiedzialność wytwórcy po uzyskaniu jednogłośnej przychyłnej opinii państw członkowskich reprezentowanych w Komitecie ds. Bezpieczeństwa ESDZ.

V. WYJĄTKOWE UDOSTĘPNIANIE EUCI AD HOC

12. W przypadku braku ram, o których mowa w art. 10 ust. 1 załącznika A, i jeśli interes UE lub co najmniej jednego z jej państw członkowskich wymaga udostępnienia EUCI z przyczyn politycznych, operacyjnych lub z innych pilnych powodów, w drodze wyjątku można udostępnić EUCI państwu trzeciemu lub organizacji międzynarodowej po podjęciu opisanych poniżej działań.

Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo, po zapewnieniu spełnienia warunków określonych w pkt 11:

- w miarę możliwości sprawdza z organami bezpieczeństwa w danym państwie trzecim lub danej organizacji międzynarodowej, czy ich przepisy, struktury i procedury dotyczące bezpieczeństwa gwarantują ochronę udostępnianych EUCI zgodnie z normami nie mniej rygorystycznymi niż normy określone w niniejszej decyzji;

- b) zwraca się do Komitetu ds. Bezpieczeństwa, by na podstawie dostępnych informacji wydał opinię dotyczącą zaufania, jakie można mieć do przepisów, struktur i procedur dotyczących bezpieczeństwa w państwie trzecim lub organizacji międzynarodowej, którym mają zostać udostępnione EUCI;
 - c) zwraca się do organu ESDZ ds. bezpieczeństwa, który może postanowić o udostępnieniu informacji pod warunkiem uzyskania jednogłośnej przychylniej opinii państw członkowskich reprezentowanych w Komitecie ds. Bezpieczeństwa ESDZ.
13. W przypadku braku ram, o których mowa w art. 10 ust. 1 załącznika A, dana strona trzecia zobowiązuje się na piśmie do odpowiedniej ochrony EUCI.
-

Dodatek A

Definicje

Do celów niniejszej decyzji stosuje się następujące definicje:

„akredytacja” oznacza proces prowadzący do formalnego stwierdzenia przez organ ds. akredytacji bezpieczeństwa (SAA), że określony system jest zatwierdzony do celów działania na zdefiniowanym poziomie klauzuli tajności, w konkretnym trybie bezpiecznej pracy systemu w swoim środowisku operacyjnym oraz na poziomie ryzyka możliwym do zaakceptowania, przy założeniu, że wdrożono zatwierdzony zestaw technicznych, fizycznych, organizacyjnych i proceduralnych środków bezpieczeństwa;

„zasoby” oznaczają wszystkie elementy, które mają wartość dla danej organizacji, prowadzenia przez nią działań i ich ciągłości, w tym zasoby informacyjne, które wspierają misję organizacji;

„uprawnienie do dostępu do EUCI” oznacza uprawnienie wydawane zgodnie z niniejszą decyzją przez organ ESDZ ds. bezpieczeństwa po wydaniu PBO przez odpowiednie organy państwa członkowskiego, stanowiące poświadczenie, że dana osoba – o ile stwierdzono, że spełnia ona zasadę ograniczonego dostępu – może uzyskać dostęp do EUCI opatrzonego klauzulą tajności do określonego poziomu (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) do określonego terminu (zob. art. 2 załącznika A I);

„naruszenie” oznacza działanie określonej osoby lub zaniechanie przez nią działania w sposób sprzeczny z zasadami bezpieczeństwa ustanowionymi w niniejszej decyzji lub z polityką bądź wytycznymi dotyczącymi bezpieczeństwa, określającymi środki niezbędne do ich wdrożenia;

„cykl życia CIS” oznacza cały okres istnienia CIS, który obejmuje powstanie pomysłu, opracowanie koncepcji, zaplanowanie, analizę wymogów, zaprojektowanie, utworzenie, testowanie, wdrożenie, działanie, konserwację i wycofanie z działania;

„umowa niejawna” oznacza umowę zawieraną przez ESDZ z wykonawcą na dostawę towarów, wykonanie robót lub świadczenie usług, której wykonanie wymaga dostępu do EUCI lub wytwarzania takich informacji bądź wiąże się z dostępem do nich lub ich wytwarzaniem;

„niejawna umowa o podwykonawstwo” oznacza umowę zawieraną przez wykonawcę ESDZ z innym wykonawcą (tj. podwykonawcą) na dostawę towarów, wykonanie robót lub świadczenie usług, której wykonanie wymaga dostępu do EUCI lub wytwarzania takich informacji bądź wiąże się z dostępem do nich lub ich wytwarzaniem;

„system teleinformatyczny” (CIS) oznacza każdy system umożliwiający przetwarzanie informacji w formie elektronicznej; system teleinformatyczny obejmuje wszystkie zasoby niezbędne do jego funkcjonowania, w tym infrastrukturę, organizację, personel oraz zasoby informatyczne; – zob. art. 8 ust. 2 załącznika A;

„narażenie na szwank EUCI” oznacza ujawnienie EUCI w całości lub częściowo nieupoważnionym osobom lub podmiotom (zob. art. 9 ust. 2);

„wykonawca” oznacza osobę fizyczną lub prawną posiadającą zdolność prawną do zawierania umów;

„produkty kryptograficzne” oznaczają algorytmy kryptograficzne, sprzęt i oprogramowanie kryptograficzne, a także produkty zawierające szczegółły stosowania i związaną z nim dokumentację oraz klucze;

„operacja WPBiO” oznacza wojskową lub cywilną operację zarządzania kryzysowego prowadzoną na mocy tytułu V rozdział 2 TUE;

„zniesienie klauzuli tajności” oznacza zniesienie wszelkiej klauzuli tajności;

„ochrona w głąb” oznacza stosowanie szeregu środków bezpieczeństwa w formie wielu warstw zabezpieczeń;

„wyznaczona władza bezpieczeństwa” (WWB) oznacza instytucję podlegającą krajowej władzy bezpieczeństwa (KWB) w państwie członkowskim, odpowiedzialną za przekazywanie podmiotom gospodarczym lub innym informacjom dotyczącym polityki we wszelkich sprawach związanych z bezpieczeństwem przemysłowym oraz za udzielanie wskazówek i pomocy w jej realizacji; zadania WWB może wykonywać KWB lub dowolny inny właściwy organ;

„dokument” oznacza każdą zapisaną informację, niezależnie od jej postaci fizycznej lub cech;

„obniżenie klauzuli tajności” oznacza obniżenie poziomu klauzuli tajności;

„informacje niejawne UE” (EUCI) oznaczają wszelkie informacje lub materiały objęte klauzulą tajności UE, których nieuprawnione ujawnienie mogłoby w różnym stopniu wyrządzić szkodę interesom Unii Europejskiej lub interesom co najmniej jednego państwa członkowskiego (zob. art. 2 lit. f));

„świadcstwo bezpieczeństwa przemysłowego” oznacza stwierdzenie przez KWB lub WWB w wyniku procedur administracyjnych, że z punktu widzenia bezpieczeństwa dany obiekt jest w stanie zapewnić odpowiednią ochronę EUCI opatrzoną określoną klauzulą tajności, a personel tego obiektu, któremu niezbędny jest dostęp do EUCI, posiada odpowiednie poświadczenie bezpieczeństwa i odebrał instruktaż dotyczący odpowiednich wymogów bezpieczeństwa niezbędnych do uzyskania dostępu do EUCI i do ochrony EUCI;

„przetwarzanie” EUCI oznacza wszelkie możliwe działania, jakim mogą być poddawane EUCI w całym cyklu ich życia; pojęcie to obejmuje wytwarzanie, modyfikowanie i przenoszenie EUCI, obniżanie lub znoszenie ich klauzul tajności oraz ich zniszczenie. W odniesieniu do CIS pojęcie to obejmuje również gromadzenie, wyświetlanie, przesyłanie i przechowywanie EUCI;

„posiadacz” oznacza odpowiednio uprawnioną osobę, której potrzeby w ramach ograniczonego dostępu zostały ustalone i w której posiadaniu znajduje się EUCI, w związku z czym odpowiada ona za ochronę przedmiotowych informacji;

„podmiot gospodarczy lub inny” oznacza podmiot zaangażowany w dostawę towarów, wykonanie robót lub świadczenie usług; może to być podmiot przemysłowy, gospodarczy, usługowy, naukowy, badawczy, edukacyjny lub rozwojowy bądź osoba prowadząca działalność gospodarczą;

„bezpieczeństwo przemysłowe” oznacza stosowanie środków mających zapewnić ochronę EUCI przez wykonawców lub podwykonawców podczas negocjacji poprzedzających zawarcie umów i na wszystkich etapach cyklu życia umów niejawnych – zob. art. 9 ust. 1 załącznika A;

„zabezpieczanie informacji” w ramach systemów teleinformatycznych oznacza pewność, że systemy te będą chronić przetwarzane informacje i będą działać zgodnie z potrzebami i w każdej sytuacji, w której będzie to potrzebne, pod kontrolą uprawnionych użytkowników; skuteczne zabezpieczanie informacji zapewnia odpowiedni poziom poufności, integralności, dostępności, niezaprzeczalności i autentyczności; zabezpieczanie informacji opiera się na procesie zarządzania ryzykiem – zob. art. 8 ust. 1 załącznika A;

„połączenie międzysystemowe” oznacza, do celów niniejszej decyzji, bezpośrednie połączenie co najmniej dwóch systemów informatycznych w celu wspólnego korzystania z danych i innych zasobów informacyjnych (np. łączności) w sposób jednokierunkowy lub wielokierunkowy (zob. załącznik A IV, pkt 31);

„zarządzanie informacjami niejawnymi” polega na stosowaniu środków administracyjnych służących kontroli EUCI na wszystkich etapach ich cyklu życia w uzupełnieniu środków przewidzianych w art. 5, 6 i 8, co ma pomóc w powstrzymaniu od zamierzonego lub przypadkowego nieuprawnionego ujawnienia tych informacji lub ich utraty, w wykrywaniu takich przypadków i usuwaniu ich skutków; środki takie dotyczą w szczególności wytwarzania, rejestracji, kopiowania, tłumaczenia, przenoszenia, przetwarzania, przechowywania i niszczenia EUCI – zob. art. 7 ust. 1 załącznika A;

„materiały” oznaczają jakikolwiek dokument lub dowolne urządzenia lub sprzęt, już wytworzone lub będące w trakcie wytwarzania;

„wytwórca” oznacza instytucję, agencję lub organ UE, państwo członkowskie, państwo trzecie lub organizację międzynarodową, w ramach właściwości której wytworzono informacje niejawne lub wprowadzono je do struktur UE;

„bezpieczeństwo osobowe” oznacza stosowanie środków gwarantujących, że dostęp do EUCI jest przyznawany tylko osobom, które:

- muszą mieć dostęp w ramach zasady ograniczonego dostępu,
- w odniesieniu do dostępu do informacji o klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej – otrzymały poświadczenie bezpieczeństwa do odpowiedniego poziomu lub ze względu na pełnione przez siebie funkcje otrzymały inne odpowiednie uprawnienie zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, oraz
- zostały poinformowane o swojej odpowiedzialności –

zob. art. 5 ust. 1 załącznika A;

„poświadczenie bezpieczeństwa osobowego” (PBO) w zakresie dostępu do EUCI oznacza oświadczenie właściwego organu państwa członkowskiego, wydawane po zakończeniu postępowania sprawdzającego prowadzonego przez właściwe organy państwa członkowskiego; stanowi ono poświadczenie, że dana osoba – o ile stwierdzono, że spełnia ona zasadę ograniczonego dostępu – może uzyskać dostęp do EUCI opatrzonej klauzulą tajności do określonego poziomu (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) do określonej daty; osobę taką określa się jako „posiadającą poświadczenie bezpieczeństwa”;

„zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego” oznacza zaświadczenie wydane przez właściwy organ, potwierdzające, że dana osoba posiada poświadczenie bezpieczeństwa lub uprawnienie do dostępu do EUCI wydane przez kierownika dysektu ESDZ odpowiedzialnej za bezpieczeństwo, oraz zawierające informację o poziomie klauzuli tajności EUCI, do których dana osoba może uzyskać dostęp (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższym), dacie ważności odpowiedniego PBO oraz dacie ważności samego zaświadczenia;

„bezpieczeństwo fizyczne” oznacza stosowanie fizycznych i technicznych środków ochrony w celu powstrzymania nieuprawnionego dostępu do EUCI – zob. art. 6 załącznika A;

„instrukcje bezpieczeństwa programu/projektu (IBP)” oznaczają wykaz procedur bezpieczeństwa stosowanych do określonego programu/projektu w celu ujednoczenia procedur bezpieczeństwa; instrukcje mogą być zmieniane podczas trwania programu/projektu;

„rejestracja” oznacza stosowanie procedur rejestrowania etapów cyklu życia informacji, w tym jej dystrybucji i zniszczenia – zob. pkt 21 załącznika A III;

„ryzyko szczątkowe” oznacza ryzyko, które pozostaje po wdrożeniu środków bezpieczeństwa, z uwagi na to, że nie przeciwdziała się wszystkim zagrożeniom i że nie każdą podatność można wyeliminować;

„ryzyko” oznacza prawdopodobieństwo, że dane zagrożenie wykorzysta wewnętrzną i zewnętrzną podatność danej organizacji lub jakiegokolwiek systemu przez nią używanego i przez to wyrządzi szkodę tej organizacji i jej zasobom materialnym lub niematerialnym; ryzyko mierzone jest jako połączenie prawdopodobieństwa wystąpienia zagrożeń oraz ich skutków;

„akceptacja ryzyka” jest decyzją o zaakceptowaniu dalszego występowania określonego ryzyka szczątkowego po zmniejszeniu ryzyka;

„ocena ryzyka” polega na określaniu zagrożeń i podatności oraz przeprowadzeniu odpowiedniej analizy ryzyka, tj. analizy prawdopodobieństwa i skutków;

„powiadamianie o ryzyku” polega na upowszechnianiu wiedzy o ryzyku wśród społeczności korzystających z CIS, na informowaniu o takim ryzyku organów zatwierdzających i na składaniu sprawozdań z nich organom operacyjnym;

„proces zarządzania ryzykiem” oznacza cały proces określania, kontrolowania i minimalizacji niepewnych zdarzeń, które mogą wpłynąć na bezpieczeństwo danej organizacji lub jakiegokolwiek systemu przez nią używanego; obejmuje on wszystkie działania związane z ryzykiem, w tym ocenę, zmniejszanie ryzyka, akceptację i powiadamianie;

„zmniejszanie ryzyka” polega na łagodzeniu, usuwaniu lub redukowaniu ryzyka (przy pomocy odpowiedniego połączenia środków technicznych, fizycznych, organizacyjnych lub proceduralnych), jego przenoszeniu lub monitorowaniu;

„dokument określający aspekty bezpieczeństwa” (DOAB) oznacza zbiór specjalnych warunków umownych, wydany przez instytucję zamawiającą, stanowiący integralną część każdej umowy niejawniej obejmującej dostęp do EUCI lub ich wytwarzanie, określający wymogi bezpieczeństwa lub wskazujący te elementy umowy, których bezpieczeństwo wymaga ochrony – zob. sekcja II załącznika A V;

„przewodnik nadawania klauzul” (PNK) oznacza dokument opisujący niejawne elementy programu lub umowy i określający mające zastosowanie poziomy klauzul tajności; PNK może być rozszerzany podczas trwania programu lub umowy, a klauzule tajności dla części informacji mogą być zmieniane lub obniżane; jeżeli PNK jest opracowany, to powinien być częścią SAL – zob. sekcja II załącznika A V;

„postępowanie sprawdzające” oznacza procedury sprawdzające przeprowadzane przez właściwy organ państwa członkowskiego zgodnie z jego przepisami ustawowymi i wykonawczymi w celu uzyskania pewności, że nie istnieją żadne znane niekorzystne okoliczności, które mogłyby stanowić przeszkodę w wydaniu danej osobie krajowego PBO lub PBO UE do dostępu do EUCI do określonego poziomu klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej);

„procedury bezpiecznej eksploatacji systemu” (SecOP) oznaczają opis sposobu wdrożenia polityki bezpieczeństwa, który należy przyjąć, procedur operacyjnych, których należy przestrzegać, oraz obowiązków personelu;

„szczególnie chronione informacje jawne” to informacje lub materiały, które ESDZ musi chronić z powodu zobowiązań prawnych określonych w Traktatach lub aktach prawnych przyjętych w celu ich wykonania lub ze względu na ich szczególną ochronę; szczególnie chronione informacje jawne obejmują między innymi informacje lub materiały objęte ze względu na swój charakter obowiązkiem tajemnicy zawodowej, o którym mowa w art. 339 TFUE, informacje objęte interesami chronionymi na mocy art. 4 rozporządzenia (WE) nr 1049/2001 Parlamentu Europejskiego i Rady ⁽¹⁾ w związku z odpowiednim orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej lub dane osobowe objęte zakresem rozporządzenia (WE) nr 45/2001.

„oświadczenie o szczególnych wymaganiach bezpieczeństwa” (SSRS) oznacza wiążący zestaw zasad bezpieczeństwa, których należy przestrzegać, oraz szczegółowych wymogów bezpieczeństwa, które należy wdrożyć, stanowiący podstawę procesu certyfikacji i akredytacji CIS;

„TEMPEST” oznacza sprawdzanie, analizę i kontrolę emisji elektromagnetycznych umożliwiających przechwycenie danych oraz środki służące tłumieniu takich emisji;

„zagrożenie” oznacza potencjalną przyczynę niepożądanego incydentu, który może skutkować szkodą dla organizacji lub jakiegokolwiek systemu przez nią używanego; zagrożenia takie mogą być przypadkowe lub zamierzone (rozmyślne) i obejmują elementy zagrażające, potencjalne cele i metody ataku;

„podatność” oznacza każdego rodzaju słaby punkt, który może zostać wykorzystany przez jedno zagrożenie lub większą ich liczbę; podatność może być zaniechaniem lub może odnosić się do słabego punktu środków kontroli, jeżeli chodzi o ich solidność, wszechstronność lub spójność; może mieć charakter techniczny, proceduralny, fizyczny, organizacyjny lub operacyjny.

⁽¹⁾ Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz.U. L 145 z 31.5.2001, s. 43).

Dodatek B

Odpowiedniki klauzul tajności

| EU | TRES SECRET UE/EU TOP SECRET | SECRET UE/EU SECRET | CONFIDENTIEL UE/EU CONFIDENTIAL | RESTREINT UE/EU RESTRICTED |
|------------------|--|--|---|-------------------------------------|
| EURATOM | EURATOM TOP SECRET | EURATOM SECRET | EURATOM CONFIDENTIAL | EURATOM RESTRICTED |
| Belgia | Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998) | Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998) | Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998) | Przypis ⁽¹⁾ poniżej |
| Bułgaria | Строго секретно | Секретно | Поверително | За служебно ползване |
| Republika Czeska | Prísne tajné | Tajné | Důvěrné | Vyhrazené |
| Dania | Yderst hemmeligt | Hemmeligt | Fortroligt | Til tjenestebrug |
| Niemcy | STRENG GEHEIM | GEHEIM | VS ⁽²⁾ — VERTRAULICH | VS — NUR FÜR DEN DIENSTGEBRAUCH |
| Estonia | Täiesti salajane | Salajane | Konfidentsiaalne | Piiratud |
| Irlandia | Top Secret | Secret | Confidential | Restricted |
| Grecja | Άκρως Απόρρητο Skrót: ΑΑΠ | Απόρρητο Skrót: (ΑΠ) | Εμπιστευτικό Skrót: (ΕΜ) | Περιορισμένης Χρήσης Skrót: (ΠΧ) |
| Hiszpania | SECRETO | RESERVADO | CONFIDENCIAL | DIFUSIÓN LIMITADA |
| Francja | Très Secret Défense | Secret Défense | Confidentiel Défense | Przypis ⁽³⁾ poniżej |
| Chorwacja | VRLO TAJNO | TAJNO | POVJERLJIVO | OGRANIČENO |
| Włochy | Segretissimo | Segreto | Riservatissimo | Riservato |
| Cypr | Άκρως Απόρρητο Skrót: (ΑΑΠ) | Απόρρητο Skrót: (ΑΠ) | Εμπιστευτικό Skrót: (ΕΜ) | Περιορισμένης Χρήσης Skrót: (ΠΧ) |
| Łotwa | Sevišķi slepeni | Slepeni | Konfidenciāli | Dienesta vajadzībām |
| Litwa | Visiškai slaptai | Slaptai | Konfidencialiai | Riboto naudojimo |
| Luksemburg | Très Secret Lux | Secret Lux | Confidentiel Lux | Restreint Lux |
| Węgry | „Szigorúan titkos!” | „Titkos!” | „Bizalmas!” | „Korlátozott terjesztésű!” |
| Malta | L-Ogħla Segretezza | Sigriet | Kunfidenzjali | Ristrett |
| Niderlandy | Stg. ZEER GEHEIM | Stg. GEHEIM | Stg. CONFIDENTIEEL | Dep. VERTROUWELIJK |
| Austria | Streng Geheim | Geheim | Vertraulich | Eingeschränkt |
| Polska | Ścisłe Tajne | Tajne | Poufne | Zastrzeżone |
| Portugalia | Muito Secreto | Secreto | Confidencial | Reservado |

| EU | TRES SECRET UE/EU TOP SECRET | SECRET UE/EU SECRET | CONFIDENTIEL UE/EU CONFIDENTIAL | RESTREINT UE/EU RESTRICTED |
|------------------------|--|-------------------------|------------------------------------|---|
| Rumunia | Strict secret de importanță deosebită | Strict secret | Secret | Secret de serviciu |
| Słowenia | Strogo tajno | Tajno | Zaupno | Interno |
| Słowacja | Prísne tajné | Tajné | Dôverné | Vyhradené |
| Finlandia | ERITTÄIN SALAINEN YTTERST HEMLIG | SALAINEN HEMLIG | LUOTTAMUKSELLINEN KONFIDENTIELL | KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG |
| Szwecja ⁽⁴⁾ | HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET | HEMLIG/SECRET HEMLIG | HEMLIG/CONFIDENTIAL HEMLIG | HEMLIG/RESTRICTED HEMLIG |
| Zjednoczone Królestwo | UK TOP SECRET | UK SECRET | Brak odpowiednika ⁽⁵⁾ | UK OFFICIAL - SENSITIVE |

⁽¹⁾ Oznaczenie Restreinte/Beperkte Verspreiding nie jest w Belgii uznawane za klauzulę tajności. W Belgii przetwarza się i chroni informacje oznaczone „RESTREINT UE/EU RESTRICTED” w sposób nie mniej rygorystyczny, niż przewidują to normy i procedury opisane w przepisach bezpieczeństwa Rady Unii Europejskiej.

⁽²⁾ Niemcy: VS = Verschlussache.

⁽³⁾ Francja nie stosuje klauzuli „RESTREINT” w swoim systemie krajowym. We Francji przetwarza się i chroni informacje oznaczone „RESTREINT UE/EU RESTRICTED” w sposób nie mniej rygorystyczny, niż przewidują to standardy i procedury opisane w przepisach bezpieczeństwa Rady Unii Europejskiej.

⁽⁴⁾ W Szwecji: oznaczenia klauzuli tajności w górnym rządzie są używane przez organy obrony, zaś oznaczenia w dolnym rządzie – przez inne organy.

⁽⁵⁾ W Zjednoczonym Królestwie przetwarza się i chroni EUCI oznaczone CONFIDENTIEL UE/EU CONFIDENTIAL zgodnie z wymaganiami bezpieczeństwa dla informacji oznaczonych UK SECRET.