EUROPEJSKA SŁUŻBA DZIAŁAŃ ZEWNĘTRZNYCH

DECYZJA WYSOKIEGO PRZEDSTAWICIELA UNII DO SPRAW ZAGRANICZNYCH I POLITYKI BEZPIECZEŃSTWA

z dnia 19 czerwca 2023 r.

w sprawie przepisów bezpieczeństwa dla Europejskiej Służby Działań Zewnętrznych

(2023/C 263/04)

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] (zwaną dalej „decyzją Rady 2010/427/UE"), w szczególności jej art. 10 ust. 1,

a także mając na uwadze, co następuje:

1) Europejska Służba Działań Zewnętrznych (zwana dalej „ESDZ"), jako funkcjonalnie autonomiczny organ Unii Europejskiej (UE), ma posiadać przepisy bezpieczeństwa przewidziane w art. 10 ust. 1 decyzji Rady 2010/427/UE.

2) Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa (zwany dalej „Wysokim Przedstawicielem" lub „WP") ma podejmować decyzje w sprawie przepisów bezpieczeństwa dla ESDZ obejmujących wszystkie aspekty bezpieczeństwa dotyczące funkcjonowania ESDZ, tak aby mogła ona skutecznie zarządzać ryzykiem dla podlegającego jej personelu, jej mienia fizycznego, informacji i gości oraz wypełniać swój obowiązek staranności i odpowiedzialności w tym zakresie.

3) W szczególności należy zapewnić poziom ochrony pracownikom podlegającym ESDZ, majątkowi ESDZ, w tym systemom teleinformatycznym, informacjom i gościom, co jest zgodne z optymalnymi rozwiązaniami stosowanymi w Radzie, Komisji, państwach członkowskich oraz, w stosownych przypadkach, w organizacjach międzynarodowych.

4) Przepisy bezpieczeństwa ESDZ powinny pomóc w uzyskaniu bardziej spójnych, kompleksowych ogólnych ram ochrony informacji niejawnych UE, w oparciu o przepisy bezpieczeństwa Rady Unii Europejskiej (zwanej dalej „Radą") i przepisy Komisji Europejskiej dotyczące bezpieczeństwa oraz przy zachowaniu jak największej zgodności z przepisami bezpieczeństwa Unii Europejskiej.

5) ESDZ, Rada i Komisja są zdecydowane stosować równoważne normy bezpieczeństwa w celu ochrony EUCI.

6) Niniejsza decyzja jest przyjmowana bez uszczerbku dla art. 15 i 16 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) oraz aktów prawnych służących wykonaniu tych artykułów.

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 odpowiedniej wiedzy fachowej w państwach członkowskich, w Sekretariacie Generalnym Rady i w Komisji.

9) Wysoki Przedstawiciel powinien podjąć wszelkie niezbędne środki w celu wprowadzenia w życie tych przepisów przy wsparciu państw członkowskich, Sekretariatu Generalnego Rady oraz Komisji.

[1] Dz.U. L 201 z 3.8.2010, s. 30.

10) Chociaż sekretarz generalny ESDZ jest organem bezpieczeństwa ESDZ, należy dokonać przeglądu przepisów bezpieczeństwa ESDZ, w szczególności w celu uwzględnienia utworzenia centrum reagowania kryzysowego i w tym celu uchylić i zastąpić decyzję Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa ADMIN(2017)10 z dnia 19 września 2017 r. ([2])

11) Zgodnie z art. 15 ust. 4 lit. a) decyzji Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa ADMIN(2017) 10 z dnia 19 września 2017 r. w sprawie przepisów bezpieczeństwa dla Europejskiej Służby Działań Zewnętrznych przeprowadzono konsultacje z Komitetem ESDZ ds. Bezpieczeństwa w sprawie planowanych zmian przepisów bezpieczeństwa ESDZ.

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Przedmiot i zakres stosowania

W niniejszej decyzji określa się przepisy dotyczące bezpieczeństwa Europejskiej Służby Działań Zewnętrznych (dalej zwane „przepisami bezpieczeństwa ESDZ").

Zgodnie z art. 10 ust. 1 decyzji Rady 2010/427/UE ma ona zastosowanie do całego personelu ESDZ i całego personelu w delegaturach Unii, niezależnie od ich statusu administracyjnego lub pochodzenia, oraz ustanawia ogólne ramy regulacyjne służące skutecznemu zarządzaniu ryzykiem dla personelu podlegającego ESDZ, o którym mowa w art. 2, w odniesieniu do pomieszczeń, majątku, informacji i gości ESDZ.

Artykuł 2

Definicje

Do celów niniejszej decyzji stosuje się następujące definicje:

a) „personel ESDZ" oznacza urzędników ESDZ i innych pracowników Unii Europejskiej, w tym personel wywodzący się ze służb dyplomatycznych państw członkowskich zatrudniony na czas określony, oraz oddelegowanych ekspertów krajowych, zgodnie z definicją zawartą odpowiednio w art. 6 ust. 2 i 3 decyzji Rady 2010/427/UE.

b) „personel podlegający ESDZ" oznacza personel ESDZ w siedzibie i w delegaturach Unii oraz wszystkich pozostałych członków personelu w delegaturach Unii, niezależnie od ich statusu administracyjnego lub pochodzenia, a także, w rozumieniu niniejszej decyzji, Wysokiego Przedstawiciela i w stosownych przypadkach innych członków personelu znajdujących się w pomieszczeniach siedziby ESDZ.

c) „kwalifikujące się osoby pozostające na utrzymaniu" oznaczają członków rodziny członka personelu podlegającego ESDZ w delegaturach Unii należących do ich gospodarstwa domowego, co zostało notyfikowane Ministerstwu Spraw Zagranicznych państwa przyjmującego, którzy faktycznie zamieszkują z nim w miejscu zatrudnienia w momencie ewakuacji z kraju.

d) „obiekty ESDZ" oznaczają wszystkie placówki ESDZ, w tym budynki, biura, pomieszczenia i inne strefy, a także obszary, w których znajdują się systemy teleinformatyczne (w tym te, w których przetwarza się EUCI), w których ESDZ prowadzi stałą lub tymczasową działalność.

e) „interesy ESDZ w zakresie bezpieczeństwa" oznaczają personel podlegający ESDZ, pomieszczenia ESDZ, osoby pozostające na utrzymaniu ESDZ, majątek, w tym systemy teleinformatyczne, informacje i goście.

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) „delegatura Unii" oznacza delegatury w państwach trzecich i organizacjach międzynarodowych, o których mowa w art. 1 ust. 4 decyzji Rady 2010/427/UE, oraz urzędy UE zgodnie z art. 5 decyzji Rady 2010/427/UE.

Pozostałe definicje do celów niniejszej decyzji są określone w odpowiednich załącznikach i w dodatku A.

([2]) Dz.U. C 126 z 10.04.2018, s. 1.

Artykuł 3

Należyta staranność

1. Przepisy bezpieczeństwa ESDZ mają na celu wypełnienie spoczywającego na ESDZ obowiązku dochowania należytej staranności i wypełniania jej obowiązków w tym zakresie.

2. Obowiązek dochowania należytej staranności obejmuje podejmowanie wszelkich uzasadnionych działań w celu wdrożenia środków bezpieczeństwa mających zapobiec dającej się racjonalnie przewidzieć szkodzie dla interesów ESDZ w zakresie bezpieczeństwa.

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 lub organach UE i innych stronach posiadających personel w delegaturach Unii lub w pomieszczeniach należących do tych delegatur oraz obowiązek dochowania należytej staranności spoczywający na ESDZ w odniesieniu do delegatur Unii, które znajdują się w wyżej wymienionych pomieszczeniach należących do innych stron, ESDZ dokonuje z każdym z wyżej wymienionych podmiotów uzgodnień administracyjnych dotyczących odpowiednich ról i obowiązków, zadań i mechanizmów 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 pomieszczeniach ESDZ. Takie środki uwzględnia się przy projektowaniu i planowaniu nowych pomieszczeń lub przed wynajęciem istniejących pomieszczeń.

2. Ze względów bezpieczeństwa możliwe jest nakładanie na określony czas i na określonych obszarach szczególnych obowiązków lub ograniczeń na personel podlegający ESDZ i na osoby pozostające na jego utrzymaniu.

3. Środki, o których mowa w ust. 1 i 2, są współmierne do szacowanego ryzyka.

Artykuł 5

Stany alarmowe i sytuacje kryzysowe

1. Organ ESDZ ds. bezpieczeństwa określony w art. 13 ust. 1 sekcja I jest odpowiedzialny za określenie poziomów stanów alarmowych oraz za wprowadzenie odpowiednich środków w zakresie stanu alarmowego na wypadek zagrożeń i incydentów mających wpływ na bezpieczeństwo w ESDZ lub w odpowiedzi na te zagrożenia lub incydenty.

2. Środki w zakresie stanów alarmowych, o których mowa w ust. 1, są współmierne do poziomu zagrożenia dla bezpieczeństwa. Organ ESDZ ds. bezpieczeństwa określa poziomy stanów alarmowych w ścisłej współpracy z właściwymi służbami innych instytucji, agencji i organów unijnych oraz służbami państwa członkowskiego lub państw członkowskich, w których znajdują się obiekty ESDZ.

3. Organ ESDZ ds. bezpieczeństwa jest punktem kontaktowym w odniesieniu do stanów alarmowych i do reagowania na sytuacje kryzysowe. Może on podzlecać powiązane zadania odpowiednio dyrektorowi generalnemu ds. zarządzania zasobami, o którym mowa w art. 4 ust. 3 lit. a) tiret drugie decyzji Rady 2010/427/UE, w przypadku siedziby ESDZ, oraz dyrektorowi centrum reagowania kryzysowego w delegaturach Unii.

Artykuł 6

Ochrona informacji niejawnych

1. Ochronę EUCI regulują wymogi określone w niniejszej decyzji, a w szczególności w załączniku A. Posiadacz jakichkolwiek EUCI jest odpowiedzialny za ich należytą 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 również określane przez Wysokiego Przedstawiciela zgodnie z zasadami ochrony EUCI określonymi w załączniku A do niniejszej decyzji.

4. ESDZ *zapewnia zarządzanie* statusem poświadczenia bezpieczeństwa wszystkich pracowników podlegających ESDZ i wykonawców pracujących dla ESDZ.

5. Jeżeli państwa członkowskie wprowadzają do struktur lub sieci ESDZ informacje niejawne, którym nadano krajową klauzulę tajności, ESDZ obejmuje te informacje ochroną zgodnie z wymogami, które mają zastosowanie do EUCI o równorzędnej klauzuli tajności – zgodnie z tabelą równoważności klauzul tajności zamieszczoną 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 na podstawie załącznika AII do niniejszej decyzji, a strefy te zatwierdza organ ds. bezpieczeństwa ESDZ.

7. Procedury wykonywania obowiązków Wysokiego Przedstawiciela w ramach umów lub ustaleń administracyjnych dotyczących wymiany EUCI z państwami trzecimi lub organizacjami międzynarodowymi opisano w załącznikach A i A *VI* do niniejszej decyzji.

8. Sekretarz generalny określa warunki, na jakich może wymieniać EUCI znajdujące się w posiadaniu ESDZ z innymi instytucjami, organami, urzędami lub agencjami Unii. W tym celu można przewidzieć właściwe ramy, w tym poprzez przystępowanie, w razie potrzeby, do *międzyinstytucjonalnych* umów lub innych ustaleń temu służących.

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 do tych określonych w niniejszej decyzji.

Artykuł 7

Incydenty związane z bezpieczeństwem, sytuacje nadzwyczajne i reagowanie kryzysowe

1. Aby zapewnić terminową i skuteczną reakcję na incydenty związane z bezpieczeństwem, ESDZ tworzy procedurę zgłaszania takich incydentów i sytuacji nadzwyczajnych, która będzie działać dwadzieścia cztery godziny na dobę, siedem dni w tygodniu i będzie obejmować wszelkiego rodzaju incydenty dotyczące bezpieczeństwa lub zagrożenia dla interesów ESDZ w zakresie bezpieczeństwa (np. wypadki, konflikty, czyny dokonane w złym zamiarze, czyny przestępcze, porwania i wzięcia zakładników, nagłe przypadki medyczne, incydenty dotyczące systemów teleinformatycznych, cyberataki itp.).

2. Tworzy się kanały łącznikowe w sytuacjach nadzwyczajnych między siedzibą ESDZ, delegaturami Unii, Radą, Komisją, specjalnymi przedstawicielami UE i państwami członkowskimi w celu wspierania ich w reagowaniu na sytuacje kryzysowe, incydenty związane z bezpieczeństwem i sytuacje nadzwyczajne z udziałem personelu i ich następstwa, w tym w planowaniu ewentualnościowym.

3. Taka reakcja na incydenty dotyczące bezpieczeństwa/sytuacje nadzwyczajne/kryzysy obejmuje między innymi:

— procedury skutecznego wspierania procesu decyzyjnego w związku z zagrożeniami, incydentami dotyczącymi bezpieczeństwa i sytuacjami nadzwyczajnymi z udziałem personelu, w tym decyzje dotyczące ewakuacji lub zawieszenia misji; oraz

— kierunek polityki i procedury poszukiwania i uwalniania personelu, np. w wypadku zaginięcia lub porwania i przetrzymywania zakładników, z uwzględnieniem szczegółowych zakresów odpowiedzialności państw członkowskich, instytucji UE oraz ESDZ w tym względzie. 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 procedury zgłaszania incydentów dotyczących bezpieczeństwa w delegaturach Unii. W stosownych przypadkach informuje się państwa członkowskie, Komisję, wszelkie inne właściwe organy oraz odpowiednie komitety ds. bezpieczeństwa.

5. Należy regularnie przeprowadzać i poddawać przeglądowi procesy reagowania na incydenty, sytuacje nadzwyczajne i sytuacje kryzysowe.

Artykuł 8

Bezpieczeństwo systemów teleinformatycznych

1. ESDZ chroni informacje przetwarzane w systemach teleinformatycznych określone w załączniku A do niniejszej decyzji przed zagrożeniami dla ich poufności, integralności, dostępności, autentyczności i niezaprzeczalności.

2. Zasady, wytyczne bezpieczeństwa i program służący ochronie wszystkich systemów teleinformatycznych będących własnością ESDZ lub przez nią eksploatowanych są zatwierdzane przez 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 systemy teleinformatyczne, 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 ESDZ ds. zatwierdzania produktów kryptograficznych 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) operacyjny organ ds. zabezpieczania informacji.

8. Przepisy dotyczące wykonania niniejszego artykułu w zakresie ochrony EUCI znajdują się w załącznikach A i A IV.

Artykuł 9

Naruszenia zasad bezpieczeństwa oraz narażenie na szwank informacji niejawnych

1. Naruszenie bezpieczeństwa następuje w wyniku działania lub zaniechania, które jest sprzeczne z zasadami bezpieczeństwa określonymi w niniejszej decyzji lub z polityką lub wytycznymi w zakresie bezpieczeństwa określającymi wszelkie środki niezbędne do jej wdrożenia, zatwierdzone 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. O każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa, a także o wszelkich przypadkach narażenia na szwank lub podejrzeń narażenia na szwank informacji niejawnych powiadamia się niezwłocznie dyrektora ds. bezpieczeństwa siedziby i dyrektora ds. bezpieczeństwa informacji ESDZ, który podejmuje odpowiednie środki określone w art. 11 załącznika A.

4. Każda osoba odpowiedzialna za naruszenie przepisów bezpieczeństwa określonych w niniejszej decyzji kub za narażenie na szwank informacji niejawnych może podlegać postępowaniu dyscyplinarnemu lub sądowemu zgodnie z mającymi zastosowanie przepisami prawa, zasadami i przepisami wykonawczymi określonymi w art. 11 ust. 3 w załączniku A.

Artykuł 10

Dochodzenie w przypadku incydentów związanych z bezpieczeństwem, naruszeń bezpieczeństwa lub narażenia na szwank bezpieczeństwa oraz działania naprawcze

1. Bez uszczerbku dla art. 86 i załącznika IX do regulaminu pracowniczego ([3]), dochodzenia w sprawie bezpieczeństwa mogą być wszczynane i prowadzone przez dyrekcję odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ:

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. Organ ESDZ ds. bezpieczeństwa , wspomagany przez dyrekcję odpowiedzialną za bezpieczeństwo siedziby, [...] ESDZ i bezpieczeństwo informacji, przez dyrekcję odpowiedzialną za Centrum Reagowania Kryzysowego (CRC) oraz, w stosownych przypadkach, przez ekspertów z państw członkowskich lub innych instytucji UE, w stosownych przypadkach wdraża 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 postępowania zapewnia się dostęp do wszelkich informacji niezbędnych do ich prowadzenia oraz pełne wsparcie wszelkich służb i personelu ESDZ w tym zakresie.

Prowadzący postępowania mogą podjąć odpowiednie działania w celu zabezpieczenia śladu dowodowego w sposób proporcjonalny do powagi sprawy będącej przedmiotem postępowania.

4. Jeżeli dostęp do informacji dotyczy danych osobowych, w tym danych zawartych w systemach teleinformatycznych, dostęp taki przetwarza się zgodnie z rozporządzeniem (UE) 2018/1725 ([4]).

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 potrzeb ESDZ w zakresie bezpieczeństwa dotyczących ochrony dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ oraz dyrekcja odpowiedzialna za centrum reagowania kryzysowego opracowują i aktualizują, w ścisłej współpracy z Dyrekcją ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa Komisji oraz, w stosownych przypadkach, z Dyrekcją Bezpieczeństwa i Ochrony Sekretariatu Generalnego Rady, kompleksową metodykę oceny 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.

([3]) Regulamin pracowniczy urzędników Unii Europejskiej i warunki zatrudnienia innych pracowników Unii Europejskiej, zwane dalej „regulaminem pracowniczym"

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2018/1725 z dnia 23 października 2018 r.w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych (Dz.U. L 295 z 21.11.2018, s. 39).

3. Role, zakresy odpowiedzialności i zadania określone w niniejszej decyzji pozostają bez uszczerbku dla odpowiedzialności każdego członka personelu podlegającego 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 mających zastosowanie przepisów, zasad, procedur i instrukcji dotyczących bezpieczeństwa.

4. Aby zapobiegać ryzyku związanemu z bezpieczeństwem i kontrolować je, upoważnieni pracownicy mogą dokonać kontroli przeszłości osób objętych zakresem niniejszej decyzji w celu ustalenia, czy przyznanie takim osobom dostępu do obiektów ESDZ lub jej informacji nie stanowi zagrożenia dla bezpieczeństwa. W tym celu i zgodnie z rozporządzeniem (UE) 2018/1725 odpowiedni upoważniony personel może: a) korzystać z wszelkich dostępnych ESDZ źródeł informacji, uwzględniając wiarygodność danego źródła informacji; b) uzyskać dostęp do akt personalnych lub danych ESDZ na temat osób, które ESDZ zatrudnia lub planuje zatrudnić, lub na temat pracowników zatrudnianych przez wykonawców, gdy jest to należycie uzasadnione.

5. ESDZ podejmuje wszelkie racjonalne środki w celu zapewnienia ochrony swoich interesów dotyczących bezpieczeństwa i zapobieżenia dającym się racjonalnie przewidzieć szkodom dla tych interesów.

6. Środki bezpieczeństwa w ESDZ dotyczące ochrony EUCI przez cały okres ich użyteczności są współmierne w szczególności do poziomu klauzuli tajności, postaci i ilości informacji lub materiału, lokalizacji i konstrukcji obiektów, w których przechowywane są EUCI, oraz zagrożenia, w tym oszacowanego na poziomie lokalnym zagrożenia działaniami podejmowanymi w złym zamiarze lub działalnością przestępczą, taką jak działalność szpiegowska, sabotażowa lub terrorystyczna.

Artykuł 12

Świadomość w kwestiach związanych z bezpieczeństwem i szkolenie

1. Organ ESDZ ds. bezpieczeństwa zapewnia, aby dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ opracowała odpowiednie programy podnoszenia świadomości w zakresie bezpieczeństwa oraz szkolenia w zakresie bezpieczeństwa. Personel siedziby otrzymuje niezbędne briefingi i szkolenia w zakresie świadomości bezpieczeństwa, które mają być prowadzone przez zespoły ds. świadomości bezpieczeństwa w dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ. Pracownicy delegatur Unii, a także, w stosownych przypadkach, kwalifikujące się osoby pozostające na ich utrzymaniu, otrzymają niezbędne briefingi w zakresie świadomości bezpieczeństwa oraz szkolenia współmierne do ryzyka w ich miejscu pracy lub zamieszkania, które mają być prowadzone przez zespoły zarządzania bezpieczeństwem w koordynacji z dyrekcją odpowiedzialną za centrum reagowania kryzysowego.

2. Przed uzyskaniem dostępu do EUCI oraz w regularnych odstępach czasu po jego uzyskaniu członkowie personelu informowani są o obowiązku ochrony informacji niejawnych UE zgodnie z przepisami na podstawie 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, by:

a) środki bezpieczeństwa koordynowano w razie potrzeby z właściwymi organami państw członkowskich, Sekretariatu Generalnego Rady i Komisji oraz, w stosownych przypadkach, państw trzecich lub organizacji międzynarodowych w odniesieniu do wszelkich kwestii związanych z bezpieczeństwem, które są istotne dla działań ESDZ, w tym charakteru ryzyka dla interesów ESDZ dotyczących bezpieczeństwa oraz sposobów ochrony przed tymi zagrożeniami;

b) we wszystkich działaniach ESDZ od samego początku w pełni uwzględniano aspekty bezpieczeństwa;

c) dostępu do informacji niejawnych udzielano wyłącznie osobom, które spełniają warunki określone w art. 5 załącznika A;

d) podejmowano odpowiednie działania w celu zarządzania statusem poświadczenia bezpieczeństwa wszystkich pracowników podlegających ESDZ i wykonawców pracujących dla ESDZ;

e) utworzono system rejestrów w celu zapewnienia, aby informacje opatrzone klauzulą CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą były przetwarzane w ESDZ zgodnie z niniejszą decyzją oraz wtedy, gdy są udostępniane 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;

f) przeprowadzano kontrole w zakresie bezpieczeństwa, o których mowa w art. 16;

g) w sprawie wszelkich przypadków lub podejrzeń naruszenia zasad bezpieczeństwa, oraz faktycznego lub podejrzewanego narażenia na szwank informacji niejawnych będących w posiadaniu lub pochodzących z ESDZ bądź ich utraty, przeprowadzano postępowanie wyjaśniające oraz by o pomoc w takich postępowaniach zwracano się do odpowiednich organów ds. bezpieczeństwa;

h) 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 dotyczące bezpieczeństwa;

i) podejmowano odpowiednie środki w razie nieprzestrzegania przez osoby przepisów niniejszej decyzji.

j) wprowadzono odpowiednie środki fizyczne i organizacyjne w celu ochrony interesów ESDZ dotyczących bezpieczeństwa.

W tym względzie organ ESDZ ds.bezpieczeństwa :

— ustala kategorię bezpieczeństwa delegatur Unii, w konsultacji z Komisją;

— tworzy mechanizm reagowania kryzysowego oraz określa jego zadania i obowiązki;

— podejmuje decyzję, po konsultacji, w stosownych przypadkach, z WP, kiedy personel delegatury Unii powinien zostać ewakuowany, jeżeli wymaga tego sytuacja w zakresie bezpieczeństwa,

— podejmuje decyzję w sprawie środków, które należy zastosować w celu ochrony kwalifikujących się osób pozostających na utrzymaniu, w stosownych przypadkach, z uwzględnieniem ustaleń z instytucjami UE, o których mowa w art. 3 ust. 3;

— zatwierdza politykę przekazywania informacji kryptograficznych, w szczególności program instalacji mechanizmu i produktów kryptograficznych.

2. Zgodnie z art. 10 ust. 3 decyzji Rady 2010/427/UE organ ESDZ ds. bezpieczeństwa jest wspierany w realizacji tych zadań wspólnie przez:

(i). dyrektora generalnego ds. zarządzania zasobami, wspomaganego przez dyrektora ds. bezpieczeństwa siedziby i bezpieczeństwa informacji ESDZ,

(ii). dyrektora centrum reagowania kryzysowego,

oraz, w stosownych przypadkach, przez zastępcę sekretarza generalnego ds. pokoju, bezpieczeństwa i obrony, w celu zapewnienia spójności ze środkami bezpieczeństwa, które mają zostać podjęte w odniesieniu do misji i operacji w dziedzinie WPBiO.

3. Sekretarz generalny jako organ ESDZ ds. bezpieczeństwa może, w stosownych przypadkach, podzlecać swoje zadania.

4. Każdy szef departamentu/działu jest odpowiedzialny za zapewnienie wdrożenia tych zasad, jak również wytycznych dotyczących bezpieczeństwa, o których mowa w art. 21 niniejszej decyzji, oraz wszelkich innych procedur lub środków mających na celu ochronę EUCI w ramach swojego departamentu/działu.

Oprócz wspomnianej wyżej odpowiedzialności, każdy kierownik departamentu/działu wyznacza personel do pełnienia funkcji koordynatora ds. bezpieczeństwa departamentu. Liczba pracowników pełniących takie funkcje musi być proporcjonalna do ilości EUCI przetwarzanych przez ten departament/dział.

Koordynatorzy ds. bezpieczeństwa w departamentach, w stosownych przypadkach, pomagają i wspierają kierownika departamentu/działu w wykonywaniu zadań związanych z bezpieczeństwem, takich jak:

a) opracowywanie wszelkich dodatkowych wymogów bezpieczeństwa odpowiednich do szczególnych potrzeb departamentu/działu w porozumieniu z dyrekcją odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ;

b) uzupełnienie okresowych briefingów dotyczących bezpieczeństwa dostarczanych członkom departamentu/działu przez dyrekcję odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ o informacje na temat dodatkowych wymogów bezpieczeństwa, o których mowa w lit. a);

c) zapewnienie przestrzegania zasady ograniczonego dostępu w ich departamencie/dziale;

d) w stosownych przypadkach aktualizowanie wykazu bezpiecznych szyfrów i kluczy;

e) zapewnianie, w stosownych przypadkach, aktualności i skuteczności procedur bezpieczeństwa i środków bezpieczeństwa;

f) zgłaszanie wszelkich przypadków naruszenia zasad bezpieczeństwa lub narażenia na szwank EUCI zarówno dyrektorowi, jak i dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ;

g) przeprowadzanie rozmów z pracownikami odchodzącymi z pracy w ESDZ;

h) regularne składanie sprawozdań na temat kwestii bezpieczeństwa departamentu/działu za pośrednictwem swoich przełożonych;

i) kontakty z dyrekcją odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ we wszelkich kwestiach związanych z bezpieczeństwem.

O wszelkich działaniach lub kwestiach, które mogą mieć wpływ na bezpieczeństwo, powiadamia się w odpowiednim czasie dyrekcję odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ.

Sekcja 2. Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ

1. Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ administracyjnie podlega Dyrekcji Generalnej ds. Zarządzania Zasobami. Do jej zadań należy:

(a) wywiązywanie się z obowiązku dochowania należytej staranności przez ESDZ w siedzibie ESDZ i odpowiedzialność za wszystkie kwestie związane z bezpieczeństwem w siedzibie ESDZ, w tym w odniesieniu do systemów teleinformatycznych i bezpieczeństwa informacji w delegaturach Unii;

(b) zarządzanie wszystkimi środkami bezpieczeństwa we wszystkich siedzibach ESDZ, koordynowanie, nadzorowanie lub wdrażanie wszystkich środków bezpieczeństwa;

(c) zapewnianie spójności i zgodności wszelkich działań, które mogą wpływać na ochronę interesów bezpieczeństwa ESDZ, z niniejszą decyzją i przepisami wykonawczymi;

(d) wspieranie działań organu ESDZ ds. akredytacji bezpieczeństwa poprzez przeprowadzanie ocen bezpieczeństwa fizycznego ogólnego i lokalnego środowiska bezpieczeństwa systemów teleinformatycznych, w których wykorzystuje się EUCI, oraz wszystkich lokali ESDZ, które mają zostać dopuszczone do przetwarzania i przechowywania EUCI.

Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ jest wspomagana przez właściwe służby państw członkowskich, zgodnie z art. 10 ust. 3 decyzji Rady 2010/427/UE.

2. Dyrektor ds. bezpieczeństwa siedziby i bezpieczeństwa informacji ESDZ jest odpowiedzialny za:

(a) zapewnianie całościowej ochrony interesów ESDZ w zakresie bezpieczeństwa w obszarze odpowiedzialności dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ;

(b) redagowanie, przegląd i aktualizowanie przepisów bezpieczeństwa, a także koordynowanie środków bezpieczeństwa z dyrektorem centrum reagowania kryzysowego, właściwymi organami państw członkowskich oraz, w stosownych przypadkach, właściwymi organami państw trzecich i organizacjami międzynarodowymi powiązanymi z UE na mocy umów lub ustaleń dotyczących bezpieczeństwa;

(c) pełnienie funkcji głównego doradcy WP, organu ESDZ ds. bezpieczeństwa oraz zastępcy sekretarza generalnego ds. pokoju, bezpieczeństwa i obrony we wszystkich kwestiach związanych z bezpieczeństwem w siedzibie oraz z bezpieczeństwem informacji ESDZ;

(d) zarządzanie statusem poświadczenia bezpieczeństwa wszystkich pracowników podlegających ESDZ i wykonawców pracujących dla ESDZ;

(e) przewodniczenie Komitetowi ESDZ ds. Bezpieczeństwa w składzie krajowych organów bezpieczeństwa, jak określono w art. 15 ust. 1 niniejszej decyzji, na polecenie organu ESDZ ds. bezpieczeństwa, oraz wspieranie jego prac;

(f) utrzymywanie kontaktów z wszelkimi partnerami lub organami innymi niż te, o których mowa w lit. b) powyżej, w kwestiach bezpieczeństwa w obszarze odpowiedzialności dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ;

(g) ustalanie priorytetów i przedstawianie wniosków dotyczących zarządzania budżetem przeznaczonym na bezpieczeństwo w siedzibie i w delegaturach Unii, przy czym te ostatnie w koordynacji z dyrektorem centrum reagowania kryzysowego;

(h) zapewnianie rejestrowania naruszeń bezpieczeństwa i narażania na szwank bezpieczeństwa, o których mowa w art. 9 niniejszej decyzji, oraz wszczynania i podejmowania dochodzeń w razie konieczności;

(i) zwoływanie regularnych i doraźnych spotkań w celu omówienia obszarów będących przedmiotem wspólnego zainteresowania z dyrektorem ds. bezpieczeństwa Sekretariatu Generalnego Rady i dyrektorem Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa Komisji.

3. Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ nawiązuje kontakty i utrzymuje ścisłą współpracę w swoim obszarze odpowiedzialności z:

— krajowymi organami bezpieczeństwa 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 informacjom niejawnym w miejscu, w którym zwykle prowadzi ona działalność;

— właściwymi organami bezpieczeństwa państw trzecich, z którymi UE zawarła umowę o bezpieczeństwie informacji lub na których terytorium Unia rozmieszcza misję lub operację w dziedzinie WPBiO; Dyrekcją Bezpieczeństwa i Ochrony 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;

— departamentem ds. bezpieczeństwa organizacji międzynarodowych, z którymi UE zawarła umowę o bezpieczeństwie informacji, oraz

— krajowymi organami bezpieczeństwa państw członkowskich w odniesieniu do wszelkich kwestii związanych z ochroną EUCI, w tym poświadczeń bezpieczeństwa osobowego.

Sekcja 3. Dyrekcja odpowiadająca za centrum reagowania kryzysowego

1. Dyrekcja centrum reagowania kryzysowego:

(a) wywiązuje się z obowiązku dochowania należytej staranności przez ESDZ w delegaturach Unii;

(b) zapewnia bezpieczeństwo personelu podlegającego ESDZ w delegaturach Unii na co dzień, proponuje środki, które należy przyjąć w przypadku kryzysu, aby zapewnić ciągłość działania w delegaturach Unii, oraz wdraża procedury ewakuacyjne w ścisłej koordynacji z działem koordynacji w Dyrekcji Generalnej ds. Zarządzania Zasobami;

(c) zarządza , koordynuje, nadzoruje lub wdraża wszystkie środki bezpieczeństwa w obiektach ESDZ w ramach delegatur Unii;

(d) zapewnia spójność i zgodność wszelkich działań ESDZ, które mogą wpływać na ochronę interesów bezpieczeństwa ESDZ w zakresie odpowiedzialności centrum reagowania kryzysowego z niniejszą decyzją i przepisami wykonawczymi;

(e) wspiera działania organu ESDZ ds. akredytacji bezpieczeństwa w zakresie przeprowadzania ocen bezpieczeństwa fizycznego pomieszczeń delegatur Unii, które mają być dopuszczone do przetwarzania i przechowywania EUCI;

2. Dyrektor centrum reagowania kryzysowego odpowiada za:

(a) zapewnianie ogólnej ochrony interesów ESDZ w zakresie bezpieczeństwa w obszarze odpowiedzialności dyrekcji odpowiadającej za centrum reagowania kryzysowego;

(b) koordynowanie środków i procedur bezpieczeństwa z właściwymi organami państw przyjmujących oraz, w stosownych przypadkach, z odpowiednimi organizacjami międzynarodowymi;

(c) zapewnienie uruchomienia mechanizmu reagowania kryzysowego ESDZ i zarządzania nim;

(d) projektowanie zdolności ESDZ w zakresie zdolności rozmieszczania (mobilny zespół wsparcia, w tym niezbędny sprzęt) i zarządzanie tą zdolnością oraz zapewnianie jej stałej gotowości;

(e) pełnienie funkcji głównego doradcy WP, organu ESDZ ds. bezpieczeństwa oraz zastępcy sekretarza generalnego ds. pokoju, bezpieczeństwa i obrony we wszystkich kwestiach związanych z bezpieczeństwem w delegaturach Unii oraz w zakresie reagowania na dotykające ich kryzysy;

(f) przewodniczenie Komitetowi ESDZ ds. Bezpieczeństwa w składzie ministrów spraw zagranicznych, jak określono w art. 15 ust. 1 niniejszej decyzji, na polecenie organu ESDZ ds. bezpieczeństwa, oraz wspieranie jego prac;

(g) utrzymywanie kontaktów z wszelkimi partnerami lub organami innymi niż te, o których mowa w lit. b) powyżej, w kwestiach bezpieczeństwa w obszarze odpowiedzialności dyrekcji odpowiadającej za centrum reagowania kryzysowego;

(h) przyczynianie się do ustalania priorytetów i przedstawiania wniosków dotyczących zarządzania budżetem przeznaczonym na bezpieczeństwo w delegaturach Unii, koordynowanego przez dyrektora ds. bezpieczeństwa siedziby i bezpieczeństwa informacji ESDZ;

(i) zapewnienie, aby Dyrekcja odpowiedzialna za centrum reagowania kryzysowego była powiadamiana o naruszeniach bezpieczeństwa i zagrożeniach w obszarze odpowiedzialności dyrekcji odpowiadającej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ w celu podjęcia odpowiednich działań następczych;

3. Dyrekcja odpowiedzialna za centrum reagowania kryzysowego nawiązuje kontakty i utrzymuje ścisłą współpracę w swoim obszarze odpowiedzialności z:

— właściwymi departamentami w Ministerstwach Spraw Zagranicznych państw członkowskich;

— w niezbędnym zakresie, z właściwymi organami bezpieczeństwa państw przyjmujących, na których terytorium utworzono delegatury UE, w odniesieniu do interesów ESDZ w zakresie bezpieczeństwa;

— Dyrekcją Bezpieczeństwa i Ochrony 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, w zakresie swoich kompetencji;

— departamentami bezpieczeństwa organizacji międzynarodowych, mając na względzie wszelką przydatną koordynację, w zakresie swoich kompetencji.

Sekcja 4. Delegatury Unii

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

Pod kierunkiem centrum reagowania kryzysowego i w razie potrzeby w porozumieniu z właściwymi organami państwa przyjmującego podejmuje on wszelkie możliwe do wykonania działania w celu zapewnienia wprowadzenia odpowiednich środków fizycznych i organizacyjnych, aby wypełnić spoczywający na nim obowiązek dochowania należytej staranności.

W stosownych przypadkach szef delegatury opracowuje procedury bezpieczeństwa w celu ochrony uprawnionych osób pozostających na utrzymaniu, jak określono w art. 2 lit. c), biorąc pod uwagę wszelkie ustalenia administracyjne, o których mowa w art. 3 ust. 3.

Szef delegatury składa dyrektorowi centrum reagowania kryzysowego oraz dyrektorowi dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ sprawozdania dotyczące wszystkich kwestii związanych z obowiązkiem dochowania należytej staranności w ramach swoich kompetencji w odniesieniu do innych kwestii związanych z bezpieczeństwem.

Jest on wspomagany przez dyrekcję odpowiedzialną za centrum reagowania kryzysowego, zespół ds. zarządzania bezpieczeństwem w delegaturze Unii, w skład którego wchodzą pracownicy wykonujący zadania i funkcje w zakresie bezpieczeństwa, oraz, w razie potrzeby, personel ochrony. Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ udziela pomocy w swoim obszarze odpowiedzialności.

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

2. Ponadto szef delegatury:

— opracowuje, w koordynacji z centrum reagowania kryzysowego szczegółowe plany bezpieczeństwa i plany awaryjne delegatur Unii na podstawie ogólnych standardowych procedur operacyjnych;

— zapewnia skuteczne całodobowe i codzienne działanie systemu zarządzania incydentami dotyczącymi 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 bezpieczeństwo było częścią szkolenia wprowadzającego w delegaturze Unii dla wszystkich członków personelu oddelegowanych w tej delegaturze po przybyciu do niej; oraz

— zapewnia realizację wszelkich zaleceń wydanych w następstwie ocen bezpieczeństwa oraz w regularnych odstępach czasu przedstawia pisemne sprawozdania z ich realizacji dyrektorowi centrum reagowania kryzysowego oraz dyrektorowi ds. bezpieczeństwa siedziby i bezpieczeństwa informacji ESDZ.

3. Pozostając jednocześnie odpowiedzialnymi i rozliczalnymi za zapewnianie zarządzania bezpieczeństwem oraz za zapewnienie odporności korporacyjnej, szef delegatury może delegować wykonywanie zadań w zakresie bezpieczeństwa koordynatorowi delegatury ds. bezpieczeństwa („DSC"), który jest zastępcą szefa delegatury lub, w przypadku braku mianowania, odpowiednim zastępcą.

W szczególności delegowane mogą zostać następujące obowiązki:

— koordynacja funkcji bezpieczeństwa w delegaturze Unii;

— utrzymywanie kontaktów w kwestiach bezpieczeństwa z właściwymi organami państwa przyjmującego i odpowiednimi odpowiednikami w ambasadach i misjach dyplomatycznych państw członkowskich;

— wdrożenie odpowiednich procedur zarządzania bezpieczeństwem związanych z interesami ESDZ w zakresie bezpieczeństwa, w tym ochrony EUCI;

— zapewnienie przestrzegania przepisów i instrukcji bezpieczeństwa;

— informowanie pracowników o przepisach bezpieczeństwa, które mają do nich zastosowanie, oraz o szczególnych zagrożeniach w państwie przyjmującym;

— składanie wniosków do dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ w celu uzyskania poświadczenia bezpieczeństwa osobowego oraz wniosków dotyczących stanowisk, które wymagają poświadczenia bezpieczeństwa osobowego; oraz

— stałe informowanie szefa delegatury, regionalnego urzędnika ds. bezpieczeństwa i dyrekcji odpowiedzialnej za centrum reagowania kryzysowego o incydentach lub wydarzeniach związanych z bezpieczeństwem na tym obszarze, które mają wpływ na ochronę interesów ESDZ dotyczących bezpieczeństwa.

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 urzędnik ds. bezpieczeństwa. Regionalni urzędnicy ds. bezpieczeństwa pełnią niżej określone role w delegaturach Unii w swoich odpowiednich geograficznych zakresach kompetencji.

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

Regionalny urzędnik ds. bezpieczeństwa może być zobowiązany do przeniesienia się poza obecny obszar odpowiedzialności, w tym do siedziby, lub nawet do objęcia stanowiska na miejscu zgodnie z sytuacją w zakresie bezpieczeństwa w dowolnym kraju oraz zgodnie z wymogami dyrekcji odpowiedzialnej za centrum reagowania kryzysowego.

6. Regionalni urzędnicy ds. bezpieczeństwa podlegają bezpośredniej kontroli operacyjnej służb w siedzibie ESDZ odpowiedzialnych za bezpieczeństwo w terenie, ale pozostają pod wspólną kontrolą administracyjną szefa delegatury w miejscu zatrudnienia i służb w siedzibie 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 urzędnicy ds. bezpieczeństwa służą szefowi i personelowi delegatury Unii radą i wsparciem. W stosownych przypadkach, w szczególności gdy regionalny urzędnik ds. bezpieczeństwa jest stałym mieszkańcem, powinien on [...] pomagać delegaturze Unii w zarządzaniu bezpieczeństwem i realizacji, w tym w przygotowywaniu umów dotyczących bezpieczeństwa, zarządzaniu akredytacjami i poświadczeniami.

Artykuł 14

Operacje w dziedzinie WPBiO i specjalni przedstawiciele UE

Dyrektor ds. bezpieczeństwa siedziby i bezpieczeństwa informacji ESDZ oraz dyrektor centrum reagowania kryzysowego doradzają, w obszarach odpowiedzialności ich dyrekcji oraz w razie potrzeby, dyrektorowi zarządzającemu ds. wspólnej polityki bezpieczeństwa i obrony (WPBiO), dyrektorowi generalnemu Sztabu Wojskowego UE (EUMS), również jako dyrektorowi Komórki Planowania i Prowadzenia Operacji Wojskowych (MPCC), oraz dyrektorowi zarządzającemu Komórki Planowania i Prowadzenia Operacji Cywilnych (CPCC), w zakresie aspektów bezpieczeństwa planowania i prowadzenia misji i operacji w dziedzinie WPBiO, a specjalnym przedstawicielom UE w odniesieniu do aspektów bezpieczeństwa ich mandatu, w uzupełnieniu do przepisów szczegółowych istniejących w tym zakresie 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. bezpieczeństwa lub wyznaczona przez niego osoba, a posiedzenia Komitetu odbywają się na polecenie przewodniczącego lub na wniosek jednego z członków. Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ oraz Dyrekcja odpowiedzialna za centrum reagowania kryzysowego wspierają przewodniczącego w obszarze ich odpowiedzialności i w razie potrzeby udzielają pomocy administracyjnej w pracach Komitetu.

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

— każdego z państw członkowskich;

— Dyrekcji Bezpieczeństwa i Ochrony Sekretariatu Generalnego Rady;

— Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej Komisji Europejskiej ds. Zasobów Ludzkich i Bezpieczeństwa;

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

— krajowego organu bezpieczeństwa lub wyznaczonego organu bezpieczeństwa;

— departamentów odpowiedzialnych za bezpieczeństwo w Ministerstwach 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 bezpieczeństwa tych podmiotów.

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 i delegatur Unii.

W szczególności, nie naruszając przepisów ust. 5 poniżej ESDZ

a) konsultuje się z Komitetem ds. Bezpieczeństwa ESDZ w sprawie:

   — polityk bezpieczeństwa, wytycznych, koncepcji lub innych dokumentów metodycznych dotyczących bezpieczeństwa, w szczególności w odniesieniu do ochrony informacji niejawnych i środków, które należy podjąć w przypadku nieprzestrzegania przepisów bezpieczeństwa przez personel ESDZ;

   — technicznych aspektów bezpieczeństwa, które mogą mieć wpływ na decyzję WP o przedstawieniu Radzie zalecenia dotyczącego rozpoczęcia negocjacji na temat umów o bezpieczeństwie informacji, o których mowa w art. 10 ust. 1 lit. a) załącznika A;

   — wszelkich zmian niniejszej decyzji.

b) może konsultować się z Komitetem ds. Bezpieczeństwa ESDZ lub informować go, w stosownych przypadkach, w odniesieniu do kwestii dotyczących bezpieczeństwa personelu i majątku w siedzibie ESDZ i w delegaturach Unii, nie naruszając art. 3 ust. 3;

c) może informować 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:

— rozpoczęciem negocjacji w sprawie 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.

Jeżeli wymagana jest jednogłośna pozytywna opinia, warunek ten zostanie spełniony, jeżeli delegacje państw członkowskich nie wyrażą sprzeciwu w trakcie prac 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 kontroli ESDZ oraz sprawozdania z kontroli po ich zakończeniu.

8. Organizacja posiedzeń:

— Komitet ds. Bezpieczeństwa ESDZ zbiera się co najmniej dwa razy w roku. Przewodniczący może organizować dodatkowe posiedzenia w pełnym składzie bądź z udziałem przedstawicieli krajowych organów bezpieczeństwa, wyznaczonych organów bezpieczeństwa lub ministrów spraw zagranicznych; o zorganizowanie takich posiedzeń mogą też zwracać się członkowie Komitetu.

— Komitet ds. Bezpieczeństwa ESDZ organizuje swoją działalność w taki sposób, aby móc przedstawiać zalecenia w konkretnych dziedzinach dotyczących bezpieczeństwa. Może on w razie potrzeby powoływać inne podgrupy eksperckie. Wyznacza on zakres zadań takich podgrup eksperckich i otrzymuje od nich sprawozdania z działalności.

— Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ oraz Dyrekcja odpowiedzialna za centrum reagowania kryzysowego są odpowiedzialne za przygotowanie punktów do dyskusji w ich obszarach odpowiedzialności. Przewodniczący sporządza wstępny porządek obrad każdego posiedzenia. Członkowie Komitetu mogą proponować dodatkowe punkty do dyskusji.

Artykuł 16

Kontrole bezpieczeństwa

1. Organ bezpieczeństwa ESDZ zapewnia regularne przeprowadzanie kontroli w zakresie bezpieczeństwa w siedzibie ESDZ i w delegaturach Unii w celu oceny adekwatności wdrożenia środków bezpieczeństwa oraz sprawdzenia ich zgodności z niniejszą decyzją. Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ, we współpracy z dyrekcją odpowiedzialną za centrum reagowania kryzysowego, może, w stosownych przypadkach, wyznaczyć ekspertów, którzy wezmą udział w kontrolach bezpieczeństwa w agencjach i organach UE utworzonych na mocy tytułu V rozdział 2 TUE.

2. Kontrole bezpieczeństwa są prowadzone przez ESDZ pod zwierzchnictwem dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i za bezpieczeństwo informacji ESDZ, w stosownych przypadkach przy wsparciu centrum reagowania kryzysowego ESDZ oraz, w ramach ustaleń, o których mowa w art. 3 ust. 3, przy wsparciu ekspertów ds. bezpieczeństwa reprezentujących inne instytucje UE lub państwa członkowskie.

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

W razie potrzeby do udziału w kontroli w zakresie bezpieczeństwa w delegaturze Unii mogą być zaproszeni odpowiedni eksperci z dziedziny bezpieczeństwa działający w misjach państw członkowskich w państwach trzecich lub przedstawiciele departamentów ds. bezpieczeństwa dyplomatycznego w państwach członkowskich.

4. Przepisy dotyczące wykonania niniejszego artykułu w zakresie ochrony EUCI znajdują się 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 mocy porozumienia administracyjnego wymienionego w art. 10 ust. 1 lit. b) załącznika A, przeprowadzane są wizyty oceniające.

Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ może wyznaczyć ekspertów, którzy wezmą udział w wizytach oceniających w państwach trzecich lub organizacjach międzynarodowych, z którymi UE zawarła umowę o bezpieczeństwie informacji, wspomnianą w art. 10 ust. 1 lit. a) załącznika A.

Artykuł 18

Planowanie ciągłości działania

Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ oraz Dyrekcja odpowiedzialna za centrum reagowania kryzysowego wspierają organ bezpieczeństwa ESDZ w zarządzaniu związanymi z bezpieczeństwem aspektami procesów ciągłości działania ESDZ w ramach ogólnego planowania ciągłości działania ESDZ.

Artykuł 19

Porady dla osób podróżujących służbowo poza UE

Dyrekcja odpowiedzialna za centrum reagowania kryzysowego zapewnia dostępność porad w odniesieniu do podróży służbowych personelu podlegającego ESDZ poza UE, korzystając z zasobów wszystkich właściwych służb ESDZ – w szczególności INTCEN, komórki kontrwywiadowczej Dyrekcji Generalnej ds. Zarządzania Zasobami, departamentów geograficznych i delegatur Unii.

Dyrekcja odpowiedzialna za centrum reagowania kryzysowego udziela, na wniosek i korzystając z wyżej wymienionych zasobów, konkretnych porad dotyczących podróży służbowych personelu podlegającego ESDZ do państw trzecich o wysokim lub podwyższonym poziomie ryzyka.

Artykuł 20

Bezpieczeństwo i higiena pracy

Przepisy bezpieczeństwa ESDZ stanowią uzupełnienie przyjętych przez Wysokiego Przedstawiciela przepisów ESDZ dotyczących bezpieczeństwa i higieny pracy.

Artykuł 21

Wdrożenie i przegląd

1. Organ bezpieczeństwa ESDZ, 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 bezpieczeństwa w państwach członkowskich oraz przy wsparciu odpowiednich służb instytucji UE.

2. Zgodnie z art. 4 ust. 5 decyzji Rady 2010/427/UE i w razie potrzeby ESDZ może zawierać umowy o gwarantowanym poziomie usług z odpowiednimi służbami Sekretariatu Generalnego Rady i Komisji.

3. WP zapewnia ogólną spójność stosowania niniejszej decyzji i prowadzi przeglądy tych 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. Sekretarz generalny, jako organ ds. bezpieczeństwa, dyrektor dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ oraz dyrektor centrum reagowania kryzysowego zapewniają wykonanie niniejszej decyzji.

Artykuł 22

Zastąpienie poprzednich decyzji

Niniejsza decyzja uchyla i zastępuje decyzję Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa ADMIN(2017)10 z dnia 19 września 2017 r. w sprawie przepisów bezpieczeństwa mających zastosowanie do Europejskiej Służby Działań Zewnętrznych ([5]).

Artykuł 23

Przepisy końcowe

Niniejsza decyzja wchodzi w życie z dniem przyjęcia.

Niniejsza decyzja zostaje opublikowana w *Dzienniku Urzędowym Unii Europejskiej*.

Organ bezpieczeństwa ESDZ należycie i terminowo informuje wszystkich pracowników objętych zakresem niniejszej decyzji i załączników do niej o jej treści, wejściu w życie i wszelkich późniejszych zmianach.

Sporządzono w Brukseli w dniu 19 czerwca 2023 r.

Josep BORRELL FONTELLES

Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa

([5]) Dz.U. C 126 z 10.4.2018, 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. Te podstawowe zasady i minimalne normy mają zastosowanie do ESDZ w rozumieniu art. 1 niniejszej decyzji oraz personelu podlegającego 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 nadaje się klauzulę tajności zgodnie z ust. 2. Można nadać im dodatkowe oznaczenie wskazujące na dziedzinę działalności, do której się odnoszą, na 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. Do obniżenia lub zniesienia klauzuli tajności nadanej EUCI oraz do zmiany lub usunięcia oznaczeń, o których mowa w art. 2 ust. 3, potrzebna jest uprzednia pisemna zgoda wytwórcy.

3. Organ ESDZ ds. bezpieczeństwa, po konsultacji z Komitetem ds. Bezpieczeństwa ESDZ zgodnie z art. 15 ust. 5 niniejszej decyzji, zatwierdza wytyczne w zakresie bezpieczeństwa dotyczące wytwarzania EUCI, które obejmują praktyczny przewodnik nadawania klauzul tajności.

Artykuł 4

Ochrona informacji niejawnych

1. EUCI są chronione zgodnie z niniejszą decyzją.

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

3. Jeżeli państwa członkowskie wprowadzają do struktur lub sieci ESDZ informacje niejawne, którym nadano krajową klauzulę tajności, ESDZ obejmuje te informacje ochroną zgodnie z wymogami, które mają zastosowanie do EUCI o równoważnej klauzuli tajności – zgodnie z tabelą równoważności klauzul tajności zamieszczoną w dodatku B.

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

— informacji niejawnych otrzymywanych przez ESDZ oraz

— materiałów źródłowych zawartych w informacjach niejawnych wytworzonych przez ESDZ.

Komitet ds. Bezpieczeństwa ESDZ jest informowany o tych procedurach.

4. Uzasadnione może być objęcie dużej ilości lub zbioru EUCI ochroną na poziomie właściwym dla wyższej klauzuli tajności niż klauzula nadana poszczególnym składnikom tego zbioru.

Artykuł 5

Bezpieczeństwo osobowe przy przetwarzaniu informacji niejawnych UE

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

— muszą mieć dostęp w ramach zasady ograniczonego dostępu;

— w przypadku dostępu do informacji niejawnych opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą – otrzymały poświadczenie bezpieczeństwa do odpowiedniego poziomu lub ze względu na pełnione przez nie funkcje przyznano im inne odpowiednie upoważnienie zgodnie z krajowymi przepisami ustawowymi i wykonawczymi; oraz

— zostały poinformowane o swoich obowiązkach.

2. Procedury prowadzenia postępowań sprawdzających mają na celu stwierdzenie, czy daną osobę, ze względu na jej lojalność, wiarygodność i rzetelność, można upoważnić 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 wykonania niniejszego artykułu znajdują się w załączniku A I.

Artykuł 6

Bezpieczeństwo fizyczne informacji niejawnych UE

1. Bezpieczeństwo fizyczne oznacza stosowanie fizycznych i technicznych środków ochrony, aby zapobiec nieuprawnionemu dostępowi 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, udaremnienie ich i wykrycie oraz umożliwienie podziału pracowników pod względem dostępu do EUCI zgodnie z zasadą ograniczonego dostępu. Środki te określane są w ramach procesu zarządzania ryzykiem.

3. Środkami bezpieczeństwa fizycznego obejmuje się wszystkie obiekty, budynki, biura, pomieszczenia i inne strefy, w których są wykorzystywane lub przechowywane EUCI, w tym strefy, w których znajdują się systemy teleinformatyczne określone w dodatku A do niniejszej decyzji.

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

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

6. Przepisy dotyczące wykonania 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 uzupełnieniu do środków przewidzianych w art. 5, 6 i 8, co ma pomóc w powstrzymywaniu zamierzonego lub przypadkowego narażenia na szwank tych informacji lub ich utraty i w wykrywaniu takich przypadków oraz w przywracaniu poprzedniego stanu po ich wystąpieniu. Środki takie dotyczą w szczególności wytwarzania, rejestracji, kopiowania, tłumaczenia, przemieszczania, przetwarzania, przechowywania i niszczenia EUCI.

2. Informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej są ze względów bezpieczeństwa rejestrowane przed dystrybucją i w momencie wpłynięcia. Właściwe organy ESDZ ustanawiają do tego celu system kancelarii tajnych. Informacje niejawne o klauzuli tajności TRES SECRET UE/EU TOP SECRET rejestruje się w wyznaczonych kancelariach tajnych.

3. Jednostki organizacyjne i obiekty, w których są wykorzystywane lub przechowywane EUCI, poddawane są regularnym inspekcjom przeprowadzanym przez organ bezpieczeństwa ESDZ.

4. Poza strefami chronionymi fizycznie EUCI są przekazywane między jednostkami organizacyjnymi i obiektami w sposób następujący:

a) zasadniczo EUCI są przekazywane drogą elektroniczną chronioną przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 7 ust. 5 niniejszej decyzji i zgodnie z wyraźnie określonymi procedurami bezpiecznej eksploatacji systemu (SecOp);

b) gdy sposób, o którym mowa w lit. a), nie jest wykorzystywany, EUCI są przemieszczane:

   i) za pomocą środków elektronicznych (jak np. nośniki pamięci USB, płyty kompaktowe, dyski twarde) chronionych przy użyciu produktów kryptograficznych zatwierdzonych zgodnie z art. 8 ust. 5 niniejszej decyzji; lub

   ii) we wszystkich pozostałych przypadkach, zgodnie z wytycznymi organu bezpieczeństwa ESDZ wydanymi zgodnie z odpowiednimi środkami ochrony określonymi w załączniku A III, sekcja V.

5. Przepisy dotyczące wykonania 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 zgodnie z przeznaczeniem, w razie potrzeby pod kontrolą uprawnionych użytkowników. Skuteczne zabezpieczanie informacji gwarantuje odpowiedni poziom poufności, integralności, dostępności, niezaprzeczalności i autentyczności. Zabezpieczanie informacji opiera się na procesie zarządzania ryzykiem.

2. W systemach teleinformatycznych przetwarza się EUCI zgodnie z koncepcją zabezpieczania informacji.

3. Wszystkie systemy teleinformatyczne, w których przetwarza się EUCI, przechodzą proces akredytacji. Celem akredytacji jest upewnienie się, że zastosowano wszystkie odpowiednie środki bezpieczeństwa i że osiągnięto wystarczający poziom ochrony EUCI oraz systemów teleinformatycznych zgodnie z niniejszą decyzją. W świadectwie akredytacji określa się najwyższą klauzulę tajności informacji, które mogą być przetwarzane w ramach danego systemu teleinformatycznego, oraz odpowiednie warunki.

4. Systemy teleinformatyczne przetwarzające informacje niejawne o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i wyższej są chronione w taki sposób, by informacje nie mogły zostać narażone na szwank z powodu niezamierzonych emisji elektromagnetycznych („środki bezpieczeństwa TEMPEST").

5. Jeżeli EUCI podlegają ochronie przy użyciu produktów kryptograficznych, produkty te są zatwierdzane zgodnie z art. 8 ust. 5 niniejszej decyzji.

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

7. Zgodnie z art. 8 ust. 6 niniejszej decyzji ustanawia się, w niezbędnym zakresie, 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.

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

a) organ ds. akredytacji bezpieczeństwa;

b) organ operacyjny ds. zabezpieczania informacji.

9. Przepisy dotyczące wykonania 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. Ogólnie umowy takie nie obejmują dostępu do informacji niejawnych o klauzuli tajności TRES SECRET UE/EU TOP SECRET.

2. ESDZ może na podstawie umowy powierzyć zadania obejmujące EUCI lub wiążące się z przetwarzaniem lub przechowywaniem tych informacji przez podmioty prowadzące działalność przemysłową lub inną, zarejestrowane w państwie członkowskim lub w państwie trzecim, które zawarło umowę lub porozumienie administracyjne zgodnie z art 10 ust. 1 załącznika A.

3. Jako instytucja zamawiająca ESDZ zapewnia, by w przypadku zawierania umów niejawnych z podmiotami prowadzącymi działalność przemysłową lub inną spełnione były minimalne normy bezpieczeństwa przemysłowego określone w niniejszej decyzji i te, o których mowa w danej umowie. ESDZ zapewnia zgodność ze wspomnianymi minimalnymi normami za pośrednictwem odpowiednich krajowych lub wyznaczonych organów bezpieczeństwa.

4. Wykonawcy lub podwykonawcy zarejestrowani w państwie członkowskim i uczestniczący w umowach niejawnych lub w niejawnych umowach o podwykonawstwo, którzy są zobowiązani do przetwarzania i przechowywania informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET w swoich obiektach, w ramach wykonywania takich umów lub na etapie poprzedzającym zawarcie umowy, posiadają świadectwo bezpieczeństwa przemysłowego (FSC) na odpowiednim poziomie klauzuli, przyznane przez krajowy organ bezpieczeństwa, wyznaczony organ bezpieczeństwa lub jakikolwiek inny właściwy organ bezpieczeństwa tego państwa członkowskiego.

5. Odpowiedni krajowy organ bezpieczeństwa, wyznaczony organ bezpieczeństwa lub jakikolwiek inny właściwy organ bezpieczeństwa wydaje pracownikom wykonawcy lub podwykonawcy, którym przy wykonywaniu umowy niejawnej niezbędny jest dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, poświadczenie bezpieczeństwa osobowego (PBO) zgodnie z krajowymi przepisami ustawowymi i wykonawczymi oraz minimalnymi normami bezpieczeństwa określonymi w załączniku A I.

6. Przepisy dotyczące wykonania 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) weszło w życie ustalenie administracyjne między WP a właściwymi organami bezpieczeństwa tego państwa trzeciego lub tej organizacji międzynarodowej dotyczące wymiany informacji opatrzonych co do zasady klauzulą tajności nie wyższą niż RESTREINT UE/EU RESTRICTED, zawarte zgodnie z procedurą określoną w art. 15 ust. 5 niniejszej decyzji; lub

c) zastosowanie ma umowa ramowa w sprawie udziału lub umowa ad hoc w sprawie udziału zawarta między UE a tym państwem trzecim w ramach operacji zarządzania kryzysowego w dziedzinie WPBiO zgodnie z art. 37 TUE i art. 218 TFUE;

i spełniono warunki określone w tym akcie.

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 mające służyć temu, 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 nie mogą być 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 w dziedzinie WPBiO, w których dane państwo trzecie uczestniczy na podstawie tych umów i zgodnie z ich postanowieniami.

3. Jeżeli uczestniczące w operacji państwo trzecie lub organizacja międzynarodowa zawrze następnie z Unią umowę o bezpieczeństwie informacji, zastępuje ona przepisy dotyczące wymiany informacji niejawnych zawarte we wszelkich umowach ramowych w sprawie udziału, umowach ad hoc w sprawie udziału i porozumieniach administracyjnych ad hoc związanych z wymianą EUCI i ich przetwarzaniem.

4. EUCI wytworzone do celów operacji w dziedzinie WPBiO mogą być ujawnione personelowi oddelegowanemu do tej operacji przez państwa trzecie lub organizacje międzynarodowe zgodnie z pkt 1–3 i załącznikiem A VI. Upoważniając taki personel do dostępu do EUCI w obiektach lub w ramach systemów teleinformatycznych operacji w dziedzinie WPBiO, stosuje się środki (w tym rejestrację ujawnianych EUCI) służące złagodzeniu ryzyka utraty lub narażenia na szwank 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. Decyzja o udostępnieniu państwu trzeciemu lub organizacji międzynarodowej EUCI posiadanych przez ESDZ podejmowana jest dla każdego przypadku z osobna, w zależności od charakteru i treści takich informacji, od tego, czy odbiorca spełnia wymóg zasady ograniczonego dostępu, i od tego, w jakim stopniu jest to korzystne dla UE.

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

Jeżeli wytwórcą informacji niejawnych, o których udostępnienie wystąpiono, nie jest ESDZ, ESDZ najpierw zwraca się o pisemną zgodę wytwórcy na ich udostępnienie.

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

7. Przepisy dotyczące wykonania niniejszego artykułu znajdują się w załączniku A VI.

Artykuł 11

Naruszenie zasad bezpieczeństwa i narażenie na szwank informacji niejawnych

1. O każdym naruszeniu lub podejrzeniu naruszenia zasad bezpieczeństwa, a także o wszelkich przypadkach narażenia na szwank lub podejrzeń narażenia na szwank informacji niejawnych powiadamia się niezwłocznie dyrekcję odpowiadającą za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ, która w odpowiednim przypadku informuje dane państwo członkowskie lub wszelki inny podmiot.

2. Jeżeli wiadomo lub istnieją uzasadnione podstawy, by podejrzewać, że informacje niejawne zostały narażone na szwank lub utracone, dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ informuje krajowy organ bezpieczeństwa danego państwa członkowskiego (krajowe organy bezpieczeństwa danych państw członkowskich) i podejmuje wszelkie właściwe środki zgodnie z odpowiednimi przepisami ustawowymi i wykonawczymi w celu:

a) zabezpieczenia dowodów;

b) zapewnienia zbadania tego przypadku przez personel niezwiązany bezpośrednio z tym naruszeniem lub narażeniem na szwank w celu ustalenia przebiegu wydarzeń;

c) bezzwłocznego powiadomienia wytwórcy informacji lub wszelkich innych podmiotów, których sprawa dotyczy;

d) podjęcia właściwych środków w celu zapobieżenia 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 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 informacji niejawnych lub za ich utratę podlega postępowaniu dyscyplinarnemu lub sądowemu zgodnie z mającymi zastosowanie przepisami ustawowymi, zasadami i przepisami wykonawczymi.

4. Podczas trwania dochodzenia w sprawie naruszenia lub narażenia na szwank, szef dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ może zawiesić dostęp danej osoby do EUCI i do obiektów ESDZ. O takiej decyzji informuje się niezwłocznie Dyrekcję ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji, Dyrekcję Bezpieczeństwa i Ochrony Sekretariatu Generalnego Rady lub krajowy organ bezpieczeństwa państwa członkowskiego lub państw członkowskich lub inne podmioty, których sprawa dotyczy.

ZAŁĄCZNIK A I

BEZPIECZEŃSTWO OSOBOWE

I. WPROWADZENIE

1. W niniejszym załączniku przedstawia się przepisy dotyczące wprowadzania w życie art. 5 załącznika A. Określa się w nim kryteria wykorzystywane 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" do celów dostępu do EUCI jest to oświadczenie przez właściwy organ państwa członkowskiego dokonane w następstwie zakończenia postępowania w sprawie bezpieczeństwa przeprowadzonego przez właściwe organy państwa członkowskiego; w dokumencie tym zaświadcza się, że dana osoba może, o ile ustalono jej potrzeby w ramach zasady ograniczonego dostępu, otrzymać dostęp do EUCI do ustalonego poziomu (klauzula CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższa) do określonego terminu; o takiej osobie mówi się, że została „sprawdzona pod względem bezpieczeństwa".

3. „Zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego" jest to zaświadczenie wydawane przez organ ESDZ ds. ESDZ, stwierdzające, że dana osoba została sprawdzona pod względem bezpieczeństwa i wskazujący poziom EUCI, do którego danej osobie można udzielić dostępu, datę ważności odnośnego zaświadczenia oraz datę ważności samego dokumentu.

4. „Uprawnienie do dostępu do EUCI" jest to zezwolenie przez organ bezpieczeństwa ESDZ, udzielane zgodnie z niniejszą decyzją po wydaniu poświadczenia bezpieczeństwa osobowego przez właściwe organy państwa członkowskiego, i zaświadczające, że dana osoba może, o ile ustalono jej potrzeby w ramach zasady ograniczonego dostępu, uzyskać dostęp do EUCI do ustalonego poziomu klauzuli niejawności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej) do określonego terminu. o takiej osobie mówi się, że została „sprawdzona pod względem bezpieczeństwa".

II. PRZYZNAWANIE UPRAWNIEŃ DO DOSTĘPU DO EUCI

5. Dostęp do informacji opatrzonych klauzulą niejawności RESTREINT UE/EU RESTRICTED nie wymaga poświadczenia bezpieczeństwa i jest udzielany po:

   a) ustaleniu związku ustawowego lub umownego danej osoby z ESDZ;

   b) stwierdzeniu, że dana osoba spełnia wymogi zasady ograniczonego dostępu;

   c) poinformowaniu tej osoby o zasadach i procedurach bezpieczeństwa służących ochronie EUCI i potwierdzeniu przez nią na piśmie, że zapoznała się ze swoimi obowiązkami 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) stwierdzeniu, że spełnia ona wymogi zasady ograniczonego dostępu;

   c) otrzymaniu przez tę osobę PBO do odpowiedniego poziomu lub innego odpowiedniego upoważnienia ze względu na pełnione przez nią funkcje, zgodnie z krajowymi przepisami ustawowymi i wykonawczymi; oraz

   d) została ona poinformowana o zasadach i procedurach bezpieczeństwa służących ochronie EUCI i potwierdziła, że zapoznała się ze swoimi obowiązkami w zakresie ochrony takich informacji.

7. ESDZ określa stanowiska w swoich strukturach, które wymagają dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej i w związku z tym wymagają PBO na odpowiednim poziomie, o którym mowa w 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 bezpieczeństwa ESDZ przekazuje wypełnioną ankietę bezpieczeństwa osobowego krajowemu organowi bezpieczeństwa państwa członkowskiego, 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 krajowego organu bezpieczeństwa w tym państwie, którego obywatelstwem legitymowała się dana osoba przy przyjmowaniu jej do pracy.

11. Jeżeli ESDZ znajdzie się w posiadaniu informacji dotyczącej osoby, która złożyła wniosek o PBO, istotnej w odniesieniu do postępowania sprawdzającego, powiadamia o tym odpowiedni krajowy organ bezpieczeństwa, działając zgodnie z odpowiednimi zasadami i przepisami wykonawczymi.

12. Po zakończeniu postępowania sprawdzającego właściwy krajowy organ bezpieczeństwa powiadamia dyrekcję ESDZ odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ o wynikach takiego postępowania.

    a) Jeżeli w wyniku postępowania sprawdzającego uzyskuje się pewność, że nie istnieją żadne niekorzystne okoliczności, które mogłyby podważać lojalność, wiarygodność i rzetelność danej osoby, organ bezpieczeństwa ESDZ może wydać tej osobie upoważnienie do dostępu do EUCI o odpowiedniej klauzuli tajności i do określonej daty.

    b) ESDZ podejmuje wszystkie właściwe środki dla zapewnienia należytego uwzględnienia warunków lub ograniczeń nałożonych przez krajowy organ bezpieczeństwa. Krajowy organ bezpieczeństwa informuje się o wyniku.

    c) Jeżeli w wyniku dochodzenia w sprawie bezpieczeństwa nie uzyskuje się takiej pewności, organ bezpieczeństwa ESDZ powiadamia o tym fakcie daną osobę, a ona może się do niego zwrócić z prośbą o wysłuchanie. Organ bezpieczeństwa ESDZ może zwrócić się do właściwego krajowego organu bezpieczeństwa o przedstawienie wszelkich dalszych wyjaśnień, których organ ten może udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli wynik zostanie potwierdzony, nie wydaje się upoważnienia 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 organu bezpieczeństwa 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 bezpieczeństwa ESDZ mogą być przedmiotem odwołania na warunkach przewidzianych w art. 90 i 91 regulaminu pracowniczego.

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 agencję Unii Europejskiej, o ile jest ono nadal ważne. Uprawnienia te dotyczą każdego zadania powierzonego danej osobie w obrębie ESDZ. Instytucja, organ lub agencja Unii, w której dana osoba zostaje zatrudniona, poinformuje odpowiedni krajowy organ bezpieczeństwa o tej zmianie pracodawcy.

16. Jeżeli okres wykonywania przez daną osobę obowiązków służbowych nie rozpocznie się w terminie 12 miesięcy od powiadomienia organu bezpieczeństwa ESDZ 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 odpowiedniemu krajowemu organowi bezpieczeństwa 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 odpowiedni krajowy organ bezpieczeństwa i może zawiesić dostęp do EUCI lub wycofać uprawnienie do dostępu do EUCI. Jeżeli krajowy organ bezpieczeństwa powiadomi ESDZ o utracie pewności uzyskanej zgodnie z pkt 12 lit. a) w odniesieniu do osoby posiadającej ważne uprawnienie do dostępu do EUCI, organ bezpieczeństwa ESDZ może zwrócić się o przedstawienie wszelkich dalszych wyjaśnień, których krajowy organ bezpieczeństwa może udzielić zgodnie z krajowymi przepisami ustawowymi i wykonawczymi. Jeżeli niekorzystne informacje zostaną potwierdzone, wspomniane upoważnienie 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 bezpieczeństwa ESDZ z prośbą o wysłuchanie. Informacje przedstawione przez krajowy organ bezpieczeństwa podlegają odpowiednim przepisom ustawowym i wykonawczym obowiązującym w danym państwie członkowskim, w tym także przepisom dotyczącym środków odwoławczych. Decyzje organu bezpieczeństwa ESDZ mogą być przedmiotem odwołania na warunkach przewidzianych w art. 90 i 91 regulaminu pracowniczego.

19. Eksperci krajowi oddelegowani do ESDZ na stanowisko wymagające dostępu do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej przedstawiają organowi bezpieczeństwa ESDZ – przed rozpoczęciem wykonywania swoich zadań – ważne PBO uprawniające do dostępu do EUCI. Wyżej opisanym procesem zarządza wysyłające państwo członkowskie.

Rejestr PBO

20. Dyrekcja ESDZ odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji 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 ESDZ oraz personelu wykonawców ESDZ pod względem poświadczenia bezpieczeństwa.

22. Organ bezpieczeństwa ESDZ 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 siedziby i bezpieczeństwo informacji ESDZ 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. Rejestr takiego pisemnego potwierdzenia jest przechowywany przez dyrekcję odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ.

25. Wszystkie osoby, które są upoważnione do dostępu do EUCI lub muszą wykorzystywać te informacje, na początku powiadamiane są o zagrożeniach bezpieczeństwa, a następnie regularnie informowane o tych zagrożeniach; osoby te muszą bezzwłocznie zgłaszać wszelkie zdarzenia lub wszelką działalność, które uznają za podejrzane lub nietypowe, odpowiednim koordynatorom ds. bezpieczeństwa w danym departamencie lub delegaturze oraz dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ.

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 ustalenie prawa dostępu danej osoby oraz 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 solidnej 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 państwa członkowskie uruchamiają 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, powiadamiane są o obowiązku stałej ochrony EUCI; w odpowiednich przypadkach świadomość tego obowiązku potwierdzają one na piśmie.

IV. SZCZEGÓLNE OKOLICZNOŚCI

28. W nagłych przypadkach, jeżeli jest to należycie uzasadnione interesami ESDZ, oraz w oczekiwaniu na zakończenie pełnego postępowania sprawdzającego organ bezpieczeństwa ESDZ może, po konsultacji z krajowym organem bezpieczeństwa 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 upoważnienie do dostępu do EUCI, by mogli wykonać określone zadania. Pełne postępowanie sprawdzające należy przeprowadzić w najbliższym możliwym terminie. Takie tymczasowe upoważnienia zachowają 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 upoważnienie, potwierdzają na piśmie, że zrozumiały spoczywające na nich obowiązki w zakresie ochrony EUCI i konsekwencje narażenia na szwank EUCI. Takie pisemne potwierdzenie jest przechowywane przez dyrekcję odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ.

29. Jeżeli dana osoba ma objąć stanowisko, które wymaga PBO na poziomie o jeden poziom wyższym niż aktualnie przez nią posiadany, może ona tymczasowo pełnić obowiązki związane z tym stanowiskiem, pod warunkiem że:

a) bezwzględna potrzeba dostępu do EUCI na wyższym szczeblu jest uzasadniona na piśmie przez właściwego bezpośredniego przełożonego danej osoby na szczeblu dyrektora/dyrektora zarządzającego/szefa delegatury, stosownie do przypadku;

b) dostęp jest ograniczony do konkretnych EUCI, które są potrzebne do pracy na tym stanowisku;

c) c) osoba ta posiada ważne PBO;

d) podjęto czynności w celu uzyskania upoważnienia do dostępu do informacji na poziomie wymaganym na tym stanowisku;

e) właściwy organ dokonał sprawdzenia, które potwierdziło, że dana osoba nie naruszała poważnie ani wielokrotnie przepisów dotyczących bezpieczeństwa;

f) objęcie tego stanowiska przez daną osobę zatwierdził właściwy organ ESDZ;

g) zasięgnięto opinii odpowiedniego krajowego lub wyznaczonego organu bezpieczeństwa, który wydał PBO danej osoby, i organ ten nie wyraził 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 ma ona dostęp po dokonaniu odpowiedniego sprawdzenia. 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 bezpieczeństwa ESDZ lub dyrektor generalny ds. zarządzania zasobami 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. Dyrekcja odpowiedzialna za bezpieczeństwo i bezpieczeństwo informacji ESDZ rejestruje takie zezwolenie, opisując informacje, do których dostęp został zatwierdzony.

32. Taki dostęp w sytuacjach nadzwyczajnych 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. Komitet ds. Bezpieczeństwa ESDZ informowany jest o przypadkach skorzystania z procedury przedstawionej w pkt 31 i 32.

34. Komitet ds. Bezpieczeństwa ESDZ otrzymuje roczne sprawozdanie na temat korzystania z procedur określonych w niniejszej sekcji.

V. UDZIAŁ W POSIEDZENIACH W SIEDZIBIE ESDZ I W DELEGATURACH UNII

35. Osoby wyznaczone do udziału w posiedzeniach w siedzibie 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 odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ 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 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 dyrekcję odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji 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, zostają odpowiednio sprawdzone 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 systemy teleinformatyczne.

2. Środki bezpieczeństwa fizycznego mają na celu zapobieżenie nieuprawnionemu dostępowi do EUCI przez:

   a) zapewnienie właściwego wykorzystywania i przechowywania EUCI;

   b) umożliwienie podziału pracowników pod względem dostępu do EUCI zgodnie z zasadą ograniczonego dostępu i, w stosownych przypadkach, posiadanym przez nich poświadczeniem bezpieczeństwa;

   c) powstrzymywanie nieuprawnionych działań, ich udaremnianie i wykrywanie; 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 obiektach 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 zbiór mogą wymagać zastosowania bardziej rygorystycznych środków ochrony;

   c) otoczenie i strukturę budynków lub stref, w których znajdują się EUCI; oraz

   d) ocenę zagrożenia w państwach trzecich opracowaną przez INTCEN, komórkę kontrwywiadowczą dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ, w szczególności na podstawie sprawozdań delegatury 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 bezpieczeństwa ESDZ 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 wykrywania intruzów i włamań (SWIiW): SWiIW można stosować w celu podwyższenia poziomu bezpieczeństwa, który daje ogrodzenie, a 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 lub też strefy lub pomieszczenia wewnątrz budynku. Kontrolę można prowadzić za pomocą środków elektronicznych, środków elektromechanicznych, za pośrednictwem pracowników ochrony lub pracowników recepcji lub za pomocą wszelkich innych środków fizycznych;

   d) pracownicy ochrony: przeszkoleni, nadzorowani, a w razie konieczności odpowiednio sprawdzeni pracownicy ochrony mogą być zatrudniani, między innymi 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 SWIiW 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 powstrzymywaniu lub wykrywaniu przypadków nieuprawnionego dostępu lub zapobieganiu utracie EUCI lub narażeniu na szwank ich bezpieczeństwa.

5. Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ może być uprawniona do przeprowadzania przeszukania osób wchodzących i wychodzących, co ma stanowić środek odstraszający przed nieuprawnionym wnoszeniem materiałów lub nieuprawnionym wynoszeniem EUCI z obiektów 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 określane 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, niszczarki, zamki do drzwi, telewizja przemysłowa, elektroniczne systemy kontroli dostępu, SWIiW, systemy alarmowe) organ bezpieczeństwa ESDZ zapewnia, by sprzęt ten spełniał zatwierdzone normy techniczne i minimalne wymogi.

9. Specyfikacje techniczne sprzętu, który ma być wykorzystywany do fizycznej ochrony EUCI, określane 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. Komitet ds. bezpieczeństwa ESDZ 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 pozwalającą na kontrolę osób i, jeżeli to możliwe, pojazdów;

    b) dostęp bez eskorty jest przyznawany wyłącznie osobom należycie upoważnionym – w siedzibie przez Dyrekcję odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ, a w delegaturach Unii przez szefa delegatury; oraz

    c) wszystkim innym osobom przez cały czas towarzyszy eskorta lub poddaje się je równoważnej 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 równoważnej 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 do tej strefy, przez cały czas towarzyszyć im musi eskorta i muszą być odpowiednio sprawdzone, chyba że podjęte zostały kroki służące zapewnieniu, aby nie był możliwy dostęp do EUCI;

    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 SWIiW, 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) takie strefy są regularnie poddawane kontroli fizycznej lub technicznej zgodnie z wymogami dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ. 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 komunikacyjne, 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, takie urządzenia i taki sprzęt zostają najpierw sprawdzone przez zespół ds. technicznych środków przeciwdziałania zagrożeniom działający w dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo i bezpieczeństwo informacji ESDZ w celu zapewnienia, aby żadne zrozumiałe informacje nie zostały nieumyślnie ani nielegalnie przesłane przez taki sprzęt poza granicę strefy bezpieczeństwa.

19. Strefy bezpieczeństwa, w których nie pracują w systemie całodobowym pracownicy pełniący dyżur, są w odpowiednich przypadkach poddawane inspekcji na koniec normalnych godzin pracy i w wyrywkowo poza tymi godzinami, chyba że znajdują się tam SWIiW.

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 bezpieczeństwa 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 zgodnie z zasadą ograniczonego dostępu i z uwagi na 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 ramach stref bezpieczeństwa budowane są, w razie potrzeby, wzmocnione pomieszczenia. Ściany, podłogi, sufity, okna i wyposażone w zamek drzwi zatwierdzane są przez organ bezpieczeństwa ESDZ i zapewniają ochronę równoważną zabezpieczonym szafom zatwierdzonym do celów przechowywania EUCI o tym samym poziomie klauzuli tajności.

V. FIZYCZNE ŚRODKI OCHRONY NA POTRZEBY PRZETWARZANIA I PRZECHOWYWANIA EUCI

23. Przetwarzanie EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED może się odbywać:

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 przemieszcza EUCI zgodnie z załącznikiem III pkt 30–42 i zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa wydanych przez organ bezpieczeństwa ESDZ, 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 ich posiadacz zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa, wydanych przez organ bezpieczeństwa ESDZ.

25. Przetwarzanie EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET może się odbywać:

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 ich posiadacz:

i) przemieszcza EUCI zgodnie z załącznikiem A III pkt 30–42;

ii) zobowiązał się do zastosowania środków równoważnych określonych w instrukcjach bezpieczeństwa, które wydał organ bezpieczeństwa ESDZ, 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 we wzmocnionym pomieszczeniu.

27. Przetwarzanie EUCI o klauzuli tajności TRÈS 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, 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 odpowiednio sprawdzonych 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 SWIiW w połączeniu z obecnością pracowników odpowiedzialnych za bezpieczeństwo.

29. Przepisy regulujące przemieszczanie EUCI poza strefami chronionymi fizycznie znajdują się w załączniku A III.

VI. KONTROLA KLUCZY I KODÓW WYKORZYSTYWANYCH DO OCHRONY EUCI

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

31. Kody są zapamiętywane przez jak najmniejszą liczbę osób, którym ich znajomość jest niezbędna. Kody do zabezpieczonych szaf i wzmocnionych pomieszczeń, w których przechowywane są EUCI, są zmieniane:

    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) nie rzadziej niż co 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. Wytwórca EUCI jest odpowiedzialny za określenie poziomu klauzuli tajności, stosowanie odpowiedniego oznaczenia klauzuli tajności, określanie sposobu rozpowszechniania informacji wśród zamierzonych odbiorców, stosowanie odpowiedniego oznaczenia możliwości udostępnienia, zgodnie z odpowiednimi wytycznymi ESDZ dotyczącymi tworzenia i przetwarzania EUCI.

4. Poziom klauzuli tajności EUCI określa się zgodnie z art. 2 ust. 2 załącznika A i przez odniesienie do wytycznych bezpieczeństwa, [...] zatwierdzonymi 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 równoważną klauzulą tajności. Tabela równoważnych 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 jakąkolwiek 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, także wtedy, gdy są przechowywane w formie elektronicznej.

8. W stopniu, w jakim jest to możliwe, dokumenty, których częściom nadaje się różne klauzule tajności, są sporządzane w taki sposób, aby części oznaczone różnymi klauzulami można było łatwo zidentyfikować i w razie konieczności rozdzielić.

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 tym 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, szczególny sposób dystrybucji dokumentu zgodnie z zasadą ograniczonego dostępu lub ograniczenia w zakresie wykorzystania;

    c) oznaczenia możliwości udostępnienia;

12. W następstwie decyzji o udostępnieniu EUCI państwu trzeciemu lub organizacji międzynarodowej dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ przekazuje daną informację niejawną, która jest opatrzona oznaczeniem dotyczącym udostępnienia, wskazującym państwo trzecie lub organizację międzynarodową, którym ta informacja ma zostać udostępniona.

13. Organ bezpieczeństwa ESDZ 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) strony numeruje się;

    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 rozdystrybuowane 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, [...] ustalonymi zgodnie z niniejszą decyzją.

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 z daną datą lub w następstwie konkretnego wydarzenia klauzula tajności EUCI może zostać obniżona lub zniesiona.

19. ESDZ przeprowadza regularne przeglądy EUCI znajdujących się w jego 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 tworzy się główną kancelarię tajną. Dla każdej jednostki organizacyjnej w ESDZ, w której przetwarza się EUCI, tworzy 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 tworzy własną kancelarię tajną na potrzeby EUCI.

Organ bezpieczeństwa ESDZ 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 rozpowszechniania 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, również delegatury Unii, lub wysłania z tej jednostki. Informacje niejawne o klauzuli 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 bezpieczeństwa ESDZ 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 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 konieczności można wyznaczyć podległe kancelarie tajne do wykorzystywania 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 z jej strony.

IV. KOPIOWANIE I TŁUMACZENIE DOKUMENTÓW NIEJAWNYCH UE

27. Dokumenty o klauzuli tajności TRÈS 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 polecenie posiadacza.

29. Środki bezpieczeństwa, które stosuje się do oryginału dokumentu, mają zastosowanie do jego kopii i tłumaczeń. Kopie dokumentów o klauzuli CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej są tworzone wyłącznie przez odpowiednią (pod) kancelarię przy użyciu zabezpieczonej kopiarki. Kopie muszą być rejestrowane.

V. PRZEMIESZCZANIE EUCI

30. Przemieszczanie EUCI podlega środkom ochrony określonym w pkt 32–42. Gdy EUCI są przemieszczane z użyciem środków 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 narażenia na szwank informacji.

31. Organ ESDZ ds. bezpieczeństwa wydaje instrukcje dotyczące przemieszczania EUCI zgodnie z niniejszą decyzją.

W obrębie budynku lub grupy budynków stanowiącej zamkniętą całość

32. EUCI przemieszczane w ramach budynku lub grupy budynków stanowiącej zamkniętą całość są zakrywane, aby nie można było zobaczyć ich treści.

33. W ramach budynku lub grupy budynków stanowiącej zamkniętą całość informacje niejawne o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET są przemieszczane przez osoby odpowiednio sprawdzone pod względem bezpieczeństwa, w zabezpieczonej kopercie, na której znajduje się jedynie nazwisko adresata.

Na terytorium UE

34. EUCI przemieszczane między budynkami lub obiektami na terytorium UE są pakowane w taki sposób, by chronić je przed nieuprawnionym ujawnieniem.

35. Przemieszczanie informacji niejawnych o klauzuli tajności SECRET UE/EU SECRET na terytorium UE odbywa się za pomocą jednego z następujących środków:

a) za pośrednictwem, w odpowiednich przypadkach, kurierów wojskowych, rządowych lub dyplomatycznych;

b) osobiście, pod warunkiem że:

(i) EUCI przez cały czas znajdują się w posiadaniu osoby przewożącej je, 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 przewożące są sprawdzone pod względem bezpieczeństwa na odpowiednim poziomie i są poinformowane o swoich obowiązkach w zakresie bezpieczeństwa;

(iv) w odpowiednich przypadkach właściwym osobom wydaje się list kurierski;

c) za pośrednictwem usług pocztowych lub prywatnych służb kurierskich, pod warunkiem że:

(i) są one zatwierdzone przez odpowiedni krajowy organ bezpieczeństwa 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 na mocy art. 21 ust. 1 niniejszej decyzji.

W przypadku przemieszczania 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 przemieszczany środkami, o których mowa w pkt 34, jest transportowany jako ładunek przez prywatne firmy przewozowe zgodnie z załącznikiem A V.

37. Przemieszczanie informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET między budynkami lub obiektami na terytorium UE odbywa się za pośrednictwem, w odpowiednich przypadkach, kurierów wojskowych, rządowych lub dyplomatycznych.

Z terytorium UE na terytorium państwa trzeciego lub pomiędzy podmiotami UE w państwach trzecich

38. EUCI przemieszczane z terytorium UE na terytorium państwa trzeciego, lub między podmiotami UE w państwach trzecich, są pakowane w taki sposób, by chronić je przed nieuprawnionym ujawnieniem.

39. Przemieszczanie informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET z terytorium Unii na terytorium państwa trzeciego i przemieszczanie jakichkolwiek EUCI o klauzuli tajności do SECRET UE/EU SECRET włącznie między podmiotami 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) właściwa osoba posiada list kurierski zawierający informacje o przesyłce i upoważniający ją do przewożenia tej przesyłki;

(iii) EUCI przez cały czas znajdują się w posiadaniu osoby przewożącej je, 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 przewożące są sprawdzone pod względem bezpieczeństwa na odpowiednim poziomie i są poinformowane o swoich obowiązkach w zakresie bezpieczeństwa.

40. Przemieszczanie informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL i SECRET UE/EU SECRET udostępnionych przez UE państwu trzeciemu lub organizacji międzynarodowej spełnia odpowiednie przepisy 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 przemieszczane z terytorium UE na terytorium państwa trzeciego także za pośrednictwem usług pocztowych lub prywatnych służb kurierskich.

42. Przemieszczanie informacji niejawnych o klauzuli tajności TRÈS SECRET UE/EU TOP SECRET z terytorium UE na terytorium państwa trzeciego, lub między podmiotami 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 odniesieniu do dokumentów niejawnych o klauzuli tajności SECRET UE/EU SECRET lub TRÈS SECRET UE/EU TOP SECRET niszczenie przebiega w obecności świadka, który został odpowiednio sprawdzony pod względem 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 TRÈS SECRET UE/EU TOP SECRET przechowuje się 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 ani częściowo odtworzone.

48. Niszczenie komputerowych nośników EUCI odbywa się zgodnie z procedurami zatwierdzonymi przez organ ESDZ ds. bezpieczeństwa.

VII. KONTROLE W ZAKRESIE BEZPIECZEŃSTWA

Kontrole ESDZ w zakresie bezpieczeństwa

49. Zgodnie z art. 16 niniejszej decyzji kontrole ESDZ w zakresie bezpieczeństwa obejmują:

a) ogólne kontrole w zakresie bezpieczeństwa, mające na celu ocenę ogólnego poziomu bezpieczeństwa siedziby głównej ESDZ, delegatur Unii i wszelkich obiektów zależnych lub powiązanych, w szczególności w celu oceny skuteczności środków bezpieczeństwa wdrożonych dla ochrony interesów ESDZ w zakresie bezpieczeństwa;

b) kontrole 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 takie kontrole przeprowadza się m.in., aby:

(i) zapewnić przestrzeganie określonych w niniejszej decyzji wymaganych norm minimalnych w zakresie ochrony EUCI;

(ii) podkreślić znaczenie bezpieczeństwa i skutecznego zarządzania ryzykiem wewnątrz podmiotów poddawanych kontroli;

(iii) zalecić środki zaradcze mające złagodzić konkretne skutki, jakie może powodować utrata poufności, integralności lub dostępności informacji niejawnych; oraz

(iv) ulepszyć istniejące programy, opracowane przez organy bezpieczeństwa, dotyczące szkoleń i upowszechniania wiedzy w dziedzinie bezpieczeństwa.

Przeprowadzanie kontroli ESDZ w zakresie bezpieczeństwa i związana z tym sprawozdawczość

50. Kontrole ESDZ w zakresie bezpieczeństwa są przeprowadzane przez zespół kontrolny dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ oraz, w razie potrzeby, przy wsparciu ekspertów ds. 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 systemy teleinformatyczne.

51. Kontrole ESDZ w zakresie bezpieczeństwa w delegaturach Unii prowadzone są w koordynacji z dyrekcją odpowiedzialną za centrum reagowania kryzysowego oraz, w razie potrzeby, przy wsparciu urzędników ds. bezpieczeństwa z ambasad państw członkowskich znajdujących się w państwach trzecich.

52. Przed końcem każdego roku kalendarzowego organ ESDZ ds. bezpieczeństwa przyjmuje program kontroli w zakresie bezpieczeństwa dla ESDZ na kolejny rok.

53. W razie potrzeby organ ESDZ ds. bezpieczeństwa może organizować kontrole w zakresie bezpieczeństwa, które nie zostały przewidziane w wyżej wspomnianym programie.

54. Pod koniec kontroli w zakresie bezpieczeństwa kontrolowanemu podmiotowi przedstawiane są główne wnioski i zalecenia. Następnie zespół kontrolny sporządza sprawozdanie z kontroli. W przypadku gdy zostały zaproponowane działania naprawcze i zalecenia, w raporcie zamieszcza się odpowiednio szczegółowe dane uzasadniające dojście do takich wniosków. Sprawozdanie jest przekazywane organowi ESDZ ds. bezpieczeństwa, dyrektorowi centrum reagowania kryzysowego, w odniesieniu do kontroli w zakresie bezpieczeństwa w delegaturach Unii, oraz szefowi kontrolowanego podmiotu.

Pod nadzorem dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ sporządza się regularne sprawozdania w celu uwypuklenia wniosków wyciągniętych z kontroli przeprowadzonych w określonym czasie i zbadanych przez Komitet ds. Bezpieczeństwa ESDZ.

Przeprowadzanie kontroli w zakresie bezpieczeństwa w agencjach i organach UE ustanowionych na mocy tytułu V rozdział 2 TUE i związana z tym sprawozdawczość.

55. Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ może, w stosownych przypadkach, wyznaczyć dodatkowych ekspertów do udziału we wspólnych zespołach kontrolnych UE przeprowadzających kontrole w agencjach i organach UE ustanowionych na mocy tytułu V rozdział 2 TUE.

Lista kontrolna dotycząca kontroli ESDZ w zakresie bezpieczeństwa

56. Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i organ bezpieczeństwa ESDZ sporządzają i uaktualniają listę kontrolną wykorzystywaną podczas kontroli bezpieczeństwa i zawierającą kwestie, które należy sprawdzić w trakcie kontroli ESDZ w zakresie bezpieczeństwa. Lista kontrolna przekazywana jest Komitetowi ds. Bezpieczeństwa ESDZ.

57. Informacji służących uzupełnieniu listy kontrolnej udziela, w szczególności podczas kontroli, personel zajmujący się kontrolą bezpieczeństwa w podmiocie, w którym przeprowadzana jest kontrola. Po uzupełnieniu listy kontrolnej przez podanie szczegółowych odpowiedzi nadaje się jej klauzulę tajności w porozumieniu z podmiotem poddawanym kontroli. Lista ta nie jest częścią raportu z kontroli.

ZAŁĄCZNIK IV

OCHRONA EUCI PRZETWARZANYCH W SYSTEMACH TELEINFORMATYCZNYCH

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wykonania art. 8 załącznika A.

2. Następujące cechy i koncepcje zabezpieczania informacji są niezbędne dla bezpieczeństwa i prawidłowego funkcjonowania operacji dokonywanych w ramach systemów teleinformatycznych:

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 ochronie 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 teleinformatycznych, w ramach których przetwarzane są EUCI. Szczegółowe wymogi dotyczące wdrażania tych przepisów są zdefiniowane w wytycznych dotyczących bezpieczeństwa w zakresie zabezpieczania informacji.

Zarządzanie ryzykiem dla bezpieczeństwa

4. Zarządzanie ryzykiem dla bezpieczeństwa stanowi integralną część definiowania, rozwijania, obsługiwania i konserwacji systemów teleinformatycznych. 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 systemów teleinformatycznych oraz ich zasobów jest jasno definiowany na początku procesu zarządzania ryzykiem.

5. Właściwe organy ESDZ dokonują przeglądu potencjalnych zagrożeń dla systemów teleinformatycznych i posiadają aktualne i dokładne oceny zagrożeń, odzwierciedlające aktualne środowisko operacyjne. Stale uaktualniają swoją wiedzę na temat podatności na zagrożenia i dokonują okresowych przeglądów oceny podatności, aby dostosować się do zmieniających się technologii informatycznych (IT).

6. Celem zarządzania ryzykiem naruszenia zasad bezpieczeństwa jest zastosowanie zestawu środków bezpieczeństwa prowadzących do osiągnięcia zadowalającej równowagi między wymaganiami użytkownika a szczątkowym ryzykiem naruszenia zasad bezpieczeństwa.

7. Szczególne wymogi, skala i stopień szczegółowości określone przez odpowiedni organ ds. akredytacji bezpieczeństwa (SAA) do celów przyznania akredytacji systemu teleinformatycznego są proporcjonalne do szacowanego ryzyka z uwzględnieniem wszystkich odpowiednich czynników, w tym poziomu klauzuli tajności EUCI przetwarzanych w danym systemie teleinformatycznym. Akredytacja obejmuje oficjalne oświadczenie o ryzyku szczątkowym oraz akceptację ryzyka szczątkowego przez odpowiedzialny organ.

Bezpieczeństwo w całym cyklu życia systemów teleinformatycznych

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

9. Dla każdego etapu cyklu życia systemu teleinformatycznego określana jest rola i interakcja każdego z podmiotów związanych z systemem teleinformatycznym w odniesieniu do jego bezpieczeństwa.

10. Wszystkie systemy teleinformatyczne wraz z technicznymi i innymi środkami bezpieczeństwa są podczas procedury akredytacji poddawane testom bezpieczeństwa, aby zapewnić osiągnięcie odpowiedniego stopnia pewności co do wdrożonych środków bezpieczeństwa oraz sprawdzić, czy są one prawidłowo wdrożone, zintegrowane i skonfigurowane.

11. Oceny bezpieczeństwa, kontrole i przeglądy przeprowadzane są okresowo w fazie operacyjnej oraz podczas konserwacji systemu teleinformatycznego, jak również przy pojawieniu się nadzwyczajnych okoliczności.

12. Dokumentacja bezpieczeństwa systemu teleinformatycznego ewoluuje podczas wszystkich etapów jego cyklu życia na zasadzie integralnej części procesu zmian i zarządzania konfiguracjami.

Optymalne rozwiązania

13. ESDZ współpracuje z SGR, Komisją i państwami członkowskimi, aby opracować optymalne rozwiązania dotyczące ochrony EUCI, które przetwarza się w ramach systemu teleinformatycznego. Wytyczne w zakresie optymalnych rozwiązań zawierają techniczne fizyczne, organizacyjne i proceduralne środki bezpieczeństwa dotyczące systemu teleinformatycznego o sprawdzonej skuteczności w zapobieganiu danym zagrożeniom i podatności.

14. Ochrona EUCI przetwarzanych w ramach systemu teleinformatycznego opiera się na doświadczeniach podmiotów zaangażowanych w zabezpieczanie informacji, zarówno w UE, jak i poza nią.

15. Rozpowszechnianie, a następnie wdrażanie optymalnych rozwiązań pomaga w osiągnięciu równoważnego poziomu pewności różnych systemów teleinformatycznych eksploatowanych przez ESDZ, które przetwarzają EUCI.

Ochrona w głąb

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

    (a) *powstrzymywanie*: środki bezpieczeństwa ukierunkowane na zniechęcenie osób planujących atak na system teleinformatyczny;

    b) *zapobieganie*: środki bezpieczeństwa ukierunkowane na udaremnienie lub powstrzymanie ataku na system teleinformatyczny;

    c) *wykrywanie*: środki bezpieczeństwa ukierunkowane na ujawnienie ataku na system teleinformatyczny;

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

    e) *usuwanie skutków*: środki bezpieczeństwa ukierunkowane na odzyskanie bezpiecznego statusu systemu teleinformatycznego.

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

17. Właściwe organy ESDZ dbają o to, by były 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 niezbędne do spełnienia wymogów operacyjnych.

19. Aby ograniczyć szkody wynikające z wypadków, błędów lub nieuprawnionego korzystania z zasobów systemu teleinformatycznego, użytkownicy systemu teleinformatycznego 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 systemu teleinformatycznego sprawdzane są jako element procedury akredytacji.

Świadomość zabezpieczania informacji

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

a) że niedopatrzenia w zakresie bezpieczeństwa mogą znacznie zaszkodzić systemowi teleinformatycznemu i całej organizacji;

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

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

22. Aby zapewnić zrozumienie obowiązków związanych z bezpieczeństwem, wszyscy członkowie personelu związani z systemem teleinformatycznym, w tym wyższe kierownictwo i użytkownicy systemu teleinformatycznego, 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 pewności, 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 pewności 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. Urządzenia kryptograficzne służące ochronie informacji niejawnych UE są oceniane i zatwierdzane przez krajowy organ ds. zatwierdzania produktów kryptograficznych (CAA) danego państwa członkowskiego.

26. Przed zaleceniem organowi ESDZ ds. zatwierdzania produktów kryptograficznych w zatwierdzenia produktów kryptograficznych, zgodnie z art. 8 ust. 5 niniejszej decyzji, produkty te muszą uzyskać pozytywny wynik podczas zewnętrznej oceny dokonywanej przez odpowiednio wykwalifikowany organ (AQUA) państwa członkowskiego, które nie jest zaangażowane w projektowanie ani wytwarzanie tego sprzętu. Wymagany stopień szczegółowości oceny zewnętrznej zależy od przewidywanego najwyższego poziomu klauzuli tajności EUCI, które mają być chronione za pomocą tych produktów.

27. Jeżeli uzasadniają to określone względy operacyjne, organ ESDZ ds. zatwierdzania produktów kryptograficznych może, na zalecenie Komitetu ds. Bezpieczeństwa przy Radzie, znieść wymogi wynikające z pkt 25 lub 26 i udzielić tymczasowej akceptacji na dany okres zgodnie z procedurą art. 8 ust. 5 niniejszej decyzji.

28. AQUA jest organem ds. zatwierdzania produktów kryptograficznych 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 strefie bezpieczeństwa

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

Bezpieczne połączenia międzysystemowe systemu teleinformatycznego

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. Systemu teleinformatyczny traktuje każdy system informatyczny przyłączony połączeniem międzysystemowym jako niezaufany i stosuje środki ochrony, aby kontrolować wymianę informacji niejawnych.

33. Wszystkie połączenia międzysystemowe systemu teleinformatycznego 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 SAA; oraz

    c) na granicach wszystkich systemów teleinformatycznych stosowane są usługi ochrony na granicy systemów (BPS).

34. Pomiędzy systemem teleinformatycznym posiadającym akredytację a siecią niezabezpieczoną lub publiczną brak jest połączeń międzysystemowych z wyjątkiem sytuacji, w których w ramach systemu teleinformatycznego zainstalowano w tym celu zatwierdzone BPS między systemem teleinformatycznym a siecią niezabezpieczoną lub publiczną. Środki bezpieczeństwa dotyczące takich połączeń międzysystemowych są poddawane przeglądowi przez właściwy organ ds. zabezpieczania informacji i zatwierdzane przez właściwy organ ds. akredytacji bezpieczeństwa.

    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 systemu teleinformatycznego posiadającego akredytację do przetwarzania informacji o klauzuli tajności TRÈS 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. Komputerowe nośniki informacji są ponownie używane, ich klauzula tajności może zostać obniżona lub zniesiona zgodnie z wytycznymi ESDZ dotyczącymi obniżania lub znoszenia klauzuli tajności EUCI, ustanowionymi 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 stosować przez pewien ograniczony czas specjalne procedury opisane poniżej.

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

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

    b) materiały niejawne nie mogą być dostarczone na czas w inny sposób.

40. Informacje niejawne transmitowane w okolicznościach przedstawionych w pkt 39 nie są opatrzone żadnymi oznaczeniami ani wskazaniami odróżniającymi je od informacji jawnych lub informacji, które mogą być chronione przy pomocy dostępnego urządzenia szyfrującego. Odbiorcy są za pomocą innych środków bezzwłocznie powiadamiani o poziomie klauzuli tajności.

41. W przypadku stosowania przepisów pkt 39 należy następnie sporządzić sprawozdanie dla dyrekcji odpowiedzialnej za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ; dyrekcja ta powinna również sporządzić sprawozdanie dla Komitetu ds. Bezpieczeństwa ESDZ. W sprawozdaniu określa się przynajmniej nadawcę, odbiorcę oraz wytwórcę każdej EUCI.

III. FUNKCJE I ORGANY ZABEZPIECZANIA INFORMACJI

42. ESDZ otrzymuje wymienione poniżej zadania dotyczące zabezpieczania informacji. Zadania te nie muszą być skupione w tych samych jednostkach organizacyjnych. Są one objęte oddzielnymi mandatami. Zadania te, oraz związana z nimi odpowiedzialność, mogą być jednak połączone lub zintegrowane w tej samej jednostce organizacyjnej lub też podzielone na różne jednostki organizacyjne, nie dopuszczając do wewnętrznych konfliktów interesów lub zadań.

Organ ds. zabezpieczania informacji (IAA)

43. Organ ds. zabezpieczania informacji (IAA) odpowiada za:

a) opracowywanie wytycznych dotyczących bezpieczeństwa w zakresie zabezpieczania informacji oraz za monitorowanie ich skuteczności i adekwatności;

b) zabezpieczanie informacji technicznych związanych z produktami kryptograficznymi i zarządzanie tymi informacjami;

c) zapewnianie, by środki zabezpieczania informacji wybrane do ochrony EUCI były zgodne z odpowiednimi wytycznymi dotyczącymi kryteriów ich przydatności i wyboru;

d) zapewnianie, by wybór produktów kryptograficznych następował zgodnie z wytycznymi dotyczącymi kryteriów ich przydatności i wyboru;

e) koordynowanie szkoleń i upowszechnianie wiedzy na temat zabezpieczania informacji;

f) konsultowanie się z dostawcą systemu, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w związku z wytycznymi dotyczącymi bezpieczeństwa w zakresie zabezpieczania informacji; oraz

g) 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 systemu teleinformatycznego z politykami i wytycznymi TEMPEST. Zatwierdza on środki zaradcze TEMPEST dla instalacji i produktów służące temu, by w środowisku operacyjnym chronić EUCI do określonego poziomu klauzuli tajności.

Organ ds. zatwierdzania produktów kryptograficznych (CAA)

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

Organ ds. dystrybucji produktów kryptograficznych (CDA)

46. CDA odpowiada za:

a) zarządzanie materiałami kryptograficznymi UE i przyjęcie za nie odpowiedzialności;

b) zapewnianie stosowania odpowiednich procedur i stworzenia kanałów umożliwiających przyjmowanie odpowiedzialności za wszystkie materiały kryptograficzne UE, ich bezpieczne wykorzystywanie, przechowywanie i rozpowszechnianie; oraz

c) 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:

a) zapewnianie zgodności systemu teleinformatycznego z odpowiednimi wytycznymi dotyczącymi bezpieczeństwa, dostarczając poświadczenie zatwierdzenia systemu teleinformatycznego do celów przetwarzania EUCI do określonego poziomu klauzuli tajności w jego środowisku operacyjnym; w poświadczeniu określa się warunki akredytacji oraz kryteria, które muszą być spełnione, by konieczne było ponowne zatwierdzenie;

b) stworzenie procesu akredytacji bezpieczeństwa, zgodnie z odpowiednimi wytycznymi, z wyraźnie określonymi warunkami zatwierdzenia systemu teleinformatycznego pod nadzorem tego organu;

c) określanie strategii akredytacji bezpieczeństwa przez ustalenie stopnia szczegółowości procedury akredytacji proporcjonalnego do wymaganego poziomu pewności;

d) analizowanie i zatwierdzanie dokumentacji związanej z bezpieczeństwem, w tym oświadczeń o zarządzaniu ryzykiem i o ryzyku szczątkowym, oświadczeń o szczególnych wymaganiach bezpieczeństwa systemu (zwanych dalej „SSRS"), dokumentacji związanej z weryfikacją zapewnienia bezpieczeństwa oraz procedur bezpiecznej eksploatacji systemu (zwanych dalej „SecOP"), jak również zapewnianie zgodności

e) sprawdzanie wdrażania środków bezpieczeństwa w odniesieniu do systemu teleinformatycznego przez dokonywanie ocen, kontroli lub przeglądów bezpieczeństwa czy też wspieranie takich działań;

f) określanie wymogów bezpieczeństwa (np. poziomów poświadczenia bezpieczeństwa pracowników) w przypadku stanowisk o szczególnie wrażliwym charakterze w odniesieniu do systemu teleinformatycznego;

g) zatwierdzanie wyboru produktów kryptograficznych i produktów klasy TEMPEST wykorzystywanych do zapewnienia bezpieczeństwa systemu teleinformatycznego;

(h) zatwierdzanie lub w odpowiednich przypadkach uczestniczenie we wspólnym zatwierdzaniu międzysystemowego połączenia systemu teleinformatycznego z innymi systemami teleinformatycznymi; 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. Organ ds. akredytacji bezpieczeństwa w ESDZ jest odpowiedzialny za przyznawanie akredytacji wszystkim systemom teleinformatycznym działającym pod nadzorem ESDZ.

Rada ds. akredytacji bezpieczeństwa (SAB)

49. Wspólna SAB jest odpowiedzialna za przyznawanie akredytacji systemu teleinformatycznego działającym pod nadzorem zarówno organu ds. akredytacji bezpieczeństwa w 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 z SGR i Komisji. Inne podmioty posiadające połączenia z danym systemem teleinformatycznym są zapraszane do uczestnictwa w obradach, gdy omawiany jest ten system.

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

Operacyjny organ ds. zabezpieczania informacji

50. Operacyjny organ ds. zabezpieczania informacji odpowiada w każdym systemie za:

a) opracowanie dokumentacji bezpieczeństwa zgodnie z wytycznymi dotyczącymi bezpieczeństwa, zwłaszcza oświadczeń o szczególnych wymaganiach bezpieczeństwa systemu (**SSRS)**, w tym oświadczenia o ryzyku szczątkowym, procedur bezpiecznej eksploatacji systemu (**SecOPs)** i planu kryptograficznego w ramach procesu akredytacji systemu teleinformatycznego;

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 zlecanie właścicielowi systemu operacyjnych obowiązków w zakresie bezpieczeństwa;

e) zarządzanie produktami kryptograficznymi i ich wykorzystywanie, 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 systemów teleinformatycznych;

(h) wdrażanie środków bezpieczeństwa w odniesieniu do poszczególnych systemów teleinformatycznych i stosowanie tych środków.

ZAŁĄCZNIK A V

BEZPIECZEŃSTWO PRZEMYSŁOWE

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wykonania art. 9 załącznika A. Ustanawia on ogólne przepisy w zakresie bezpieczeństwa mające zastosowanie do podmiotów prowadzących działalność gospodarczą lub inną 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, w szczególności szczegółowe wymogi w odniesieniu do świadectwa bezpieczeństwa przemysłowego (SBP), dokumentów określających aspekty bezpieczeństwa (DOAB), wizyt, transmisji i przemieszczania EUCI.

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 przekazał wytwórca i których wykorzystanie do celów umowy zatwierdził;

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

   c) w odpowiednich przypadkach ESDZ działa w porozumieniu z krajowymi organami bezpieczeństwa/wyznaczonymi organami bezpieczeństwa 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 odpowiednich 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 EUCI, ich wykorzystywanie lub przechowywanie, organ wyznaczony do zarządzania danym programem lub projektem może sporządzić specjalne instrukcje bezpieczeństwa programu/projektu (IBP). IBP wymagają zatwierdzenia przez krajowy organ bezpieczeństwa/wyznaczony organ bezpieczeństwa państw członkowskich lub jakikolwiek inny właściwy organ bezpieczeństwa uczestniczący w programie/projekcie i mogą zawierać dodatkowe wymogi bezpieczeństwa.

III. ŚWIADECTWO BEZPIECZEŃSTWA PRZEMYSŁOWEGO (SBP)

8. Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ zwraca się do krajowego organu bezpieczeństwa/wyznaczonego organu bezpieczeństwa, lub jakiegokolwiek innego właściwego organu bezpieczeństwa państwa danego członkowskiego o wydanie SBP w celu zaświadczenia zgodnie z krajowymi przepisami ustawowymi i wykonawczymi, że dany podmiot prowadzący działalność gospodarczą lub inną jest w stanie zapewnić w swoich obiektach ochronę EUCI odpowiadającą określonemu poziomowi klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET). Do czasu przekazania ESDZ potwierdzenia wydania SBP żadnemu faktycznemu ani potencjalnemu wykonawcy ani podwykonawcy nie udziela się ani nie umożliwia się dostępu do EUCI.

9. W stosownych przypadkach ESDZ, jako instytucja zamawiająca, powiadamia odpowiedni krajowy organ bezpieczeństwa/wyznaczony organ bezpieczeństwa 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 niejawnej z wybranym oferentem, zanim nie otrzyma od krajowego organu bezpieczeństwa/wyznaczonego organu bezpieczeństwa lub jakiegokolwiek innego właściwego organu bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest ten wykonawca lub podwykonawca, potwierdzenia, że wydane zostało, jeśli istnieje taki wymóg, odpowiednie SBP.

11. ESDZ jako instytucja zamawiająca zwraca się do krajowego organu bezpieczeństwa/wyznaczonego organu bezpieczeństwa lub do innego właściwego organu bezpieczeństwa, który wydał SBP, o przekazywanie ESDZ wszelkich niekorzystnych informacji dotyczących tego SBP. W przypadku umowy o podwykonawstwo krajowy organ bezpieczeństwa/wyznaczony organ bezpieczeństwa lub jakikolwiek inny właściwy organ bezpieczeństwa są o tym informowane.

12. Cofnięcie SBP przez odpowiedni krajowy organ bezpieczeństwa/wyznaczony organ bezpieczeństwa lub jakikolwiek inny właściwy organ bezpieczeństwa stanowią dla ESDZ, jako instytucji zamawiającej, wystarczającą podstawę do rozwiązania umowy niejawnej lub wykluczenia oferenta z postępowania.

IV. Poświadczenia bezpieczeństwa osobowego (PBO) dla pracowników wykonawcy

13. Cały personel pracujący dla wykonawców wymagających dostępu do EUCI o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej musi zostać odpowiednio sprawdzony pod względem bezpieczeństwa, a dostęp do informacji jest mu udzielany na zasadzie ograniczonego dostępu. Chociaż do uzyskania dostępu do EUCI na poziomie RESTREINT UE/EU RESTRICTED nie jest wymagane PBO, stosowana jest zasada ograniczonego dostępu.

14. Wnioski o PBO dla pracowników wykonawcy składa się do krajowego organu bezpieczeństwa/wyznaczonego organu bezpieczeństwa odpowiedzialnego 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 krajowy organ bezpieczeństwa/wyznaczony organ bezpieczeństwa państwa członkowskiego, w którym znajduje się siedziba podmiotu zatrudniającego i w którym ten podmiot jest zarejestrowany; do obowiązków tego krajowego organu bezpieczeństwa/wyznaczonego organu bezpieczeństwa 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 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 niejawnej lub niejawnej umowy o podwykonawstwo ESDZ, jako instytucja zamawiająca, powiadamia krajowy organ bezpieczeństwa/wyznaczony organ bezpieczeństwa 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 odpowiednim przypadku, krajowy organ bezpieczeństwa/wyznaczony organ bezpieczeństwa lub jakikolwiek inny właściwy organ bezpieczeństwa w przypadku umowy o podwykonawstwo) niezwłocznie powiadamia o tym fakcie krajowy organ bezpieczeństwa/wyznaczony organ bezpieczeństwa lub jakikolwiek inny właściwy organ bezpieczeństwa państwa członkowskiego, w którym zarejestrowany jest wykonawca lub podwykonawca.

19. Z reguły od wykonawcy lub podwykonawcy wymaga się zwrotu do instytucji zamawiającej wszelkich posiadanych przez niego EUCI po rozwiązaniu lub lub wygaśnięciu umowy niejawnej lub niejawnej umowy o podwykonawstwo.

20. W DOAB określa się szczególne przepisy dotyczące niszczenia EUCI podczas wykonywania umowy lub po jej rozwiązaniu bądź wygaśnięciu.

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 niejawnej wykonawca uzyskuje zgodę ESDZ jako instytucji zamawiającej. Nie można zawrzeć umowy o podwykonawstwo z podmiotami prowadzącymi działalność gospodarczą lub inną zarejestrowanymi w państwie niebędącym członkiem UE, które 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 wykorzystywanych przez wykonawcę lub podwykonawcę prawa przysługujące wytwórcy są wykonywane przez instytucję zamawiającą.

VI. WIZYTY ZWIĄZANE Z UMOWAMI NIEJAWNYMI

26. Jeżeli ESDZ lub wykonawcy bądź podwykonawcy niezbędny jest w związku z wykonaniem umowy niejawnej dostęp do informacji niejawnych o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET w swoich obiektach, organizowane są wizyty wraz z krajowym organem bezpieczeństwa/wyznaczonym organem bezpieczeństwa lub jakimkolwiek innym właściwym organem bezpieczeństwa. Pozostaje to bez uszczerbku dla prerogatyw krajowego organu bezpieczeństwa/wyznaczonego organu bezpieczeństwa, w ramach konkretnych projektów, do uzgodnienia procedury pozwalającej na bezpośrednie organizowanie takich wizyt.

27. Wszyscy goście posiadają odpowiednie PBO i podlegają zasadzie ograniczonego dostępu, co uprawnia je do dostępu do EUCI związanych z umową zawartą przez ESDZ.

28. Gościom umożliwia się dostęp wyłącznie do EUCI związanych z celem wizyty.

VII. TRANSMISJA I PRZEMIESZCZANIE EUCI

29. Do transmisji EUCI drogą elektroniczną zastosowanie mają odpowiednie przepisy art. 8 załącznika A oraz załącznika A IV.

30. Do przemieszczania EUCI zastosowanie mają odpowiednie przepisy załącznika A III zgodnie z krajowymi przepisami ustawowymi i wykonawczymi.

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

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

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

c) firmy dokonujące przewozu muszą uzyskać SBP na odpowiednim poziomie, jeśli przewóz wymaga również przechowywania informacji niejawnych w obiektach wykonawcy. W takich przypadkach pracownicy zajmujący się przesyłką są odpowiednio sprawdzani pod względem bezpieczeństwa zgodnie z załącznikiem A I;

d) przed jakimkolwiek transgranicznym przewożeniem materiałów o klauzuli tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub SECRET UE/EU SECRET, nadawca sporządza plan przewozu, który jest zatwierdzany przez ESDZ, w odpowiednich przypadkach w porozumieniu z odpowiednim krajowym organem bezpieczeństwa/wyznaczonym organem bezpieczeństwa lub jakimkolwiek innym właściwym organem bezpieczeństwa;

e) przejazdy odbywają się w miarę możliwości bezpośrednio między dwoma punktami i kończą się tak szybko, jak pozwolą na to 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 o bezpieczeństwie zgodnie ze środkami bezpieczeństwa uzgodnionymi przez ESDZ, jako instytucję zamawiającą, z krajowym organem bezpieczeństwa/wyznaczonym organem bezpieczeństwa państwa trzeciego, w którym zarejestrowany jest wykonawca.

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

33. W porozumieniu, odpowiednio, z krajowym organem bezpieczeństwa/wyznaczonym organem bezpieczeństwa państwa członkowskiego, ESDZ, jako instytucja zamawiająca, jest upoważniony na podstawie przepisów umownych do przeprowadzania wizyt w obiektach wykonawców/podwykonawców, aby sprawdzić, czy wprowadzone zostały odpowiednie środki bezpieczeństwa mające zapewnić ochronę EUCI o klauzuli tajności RESTREINT UE/EU RESTRICTED zgodnie z wymogami umowy.

34. W zakresie, jaki jest wymagany na mocy krajowych przepisów ustawowych i wykonawczych, krajowy organ bezpieczeństwa/wyznaczony organ bezpieczeństwa lub jakikolwiek inny właściwy organ bezpieczeństwa są powiadamiane przez ESDZ, jako instytucję zamawiającą, o umowach niejawnych lub niejawnych 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 ogłoszenia o przetargu w przypadku umów, które wymagają dostępu do informacji niejawnych o klauzuli tajności RESTREINT UE/EU RESTRICTED, niezależnie od jakichkolwiek wymogów związanych z SBP lub PBO, które mogą być określone przez krajowe przepisy ustawowe i wykonawcze.

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 systemu teleinformatycznego, który eksploatuje wykonawca, ESDZ, jako instytucja zamawiająca, zapewnia, aby umowa lub jakakolwiek umowa o podwykonawstwo określała niezbędne wymogi techniczne i administracyjne dotyczące akredytacji systemu teleinformatycznego, które są proporcjonalne do szacowanego ryzyka z uwzględnieniem wszystkich odpowiednich czynników. Zakres akredytacji dla takiego systemu teleinformatycznego jest uzgadniany między instytucją zamawiającą a odpowiednim krajowym organem bezpieczeństwa/wyznaczonym organem bezpieczeństwa.

ZAŁĄCZNIK A VI

WYMIANA INFORMACJI NIEJAWNYCH Z PAŃSTWAMI TRZECIMI I ORGANIZACJAMI MIĘDZYNARODOWYMI

I. WPROWADZENIE

1. Niniejszy załącznik zawiera przepisy dotyczące wykonania 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 WP w wykonywaniu jego obowiązków określonych w art. 218 TFUE:

a) właściwy dział geograficzny lub tematyczny ESDZ, w porozumieniu z dyrekcją odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ, określa, w stosownych przypadkach, potrzebę długoterminowej wymiany EUCI z danym państwem trzecim lub daną organizacją międzynarodową;

b) dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ, w porozumieniu z właściwym działem geograficznym ESDZ, w stosownych przypadkach przedkłada WP projekty tekstów, które mają zostać przedłożone Radzie na mocy art. 218 ust. 3, 5 i 6 TFUE;

c) dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ wspiera WP w prowadzeniu negocjacji;

d) w odniesieniu do umów lub ustaleń z państwami trzecimi dotyczących ich udziału w operacjach zarządzania kryzysowego w dziedzinie WPBiO, o których mowa w art. 10 ust. 1 lit. c) załącznika A, ESDZ wspiera WP w pracach nad wnioskami, które mają zostać przedłożone Radzie zgodnie z art. 218 ust. 3, 5 i 6 TFUE, oraz wspiera WP w prowadzeniu negocjacji.

3. W przypadku gdy umowy o bezpieczeństwie informacji przewidują techniczne ustalenia wykonawcze, które mają zostać uzgodnione między dyrekcją odpowiedzialną za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ a właściwym organem bezpieczeństwa danego państwa trzeciego lub danej organizacji międzynarodowej, takie uzgodnienia uwzględniają poziom ochrony przewidziany w przepisach, strukturach i procedurach bezpieczeństwa obowiązujących w danym państwie trzecim lub danej organizacji międzynarodowej. Dyrekcja odpowiedzialna za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ koordynuje działania w odniesieniu do takich ustaleń z Dyrekcją ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa w Komisji oraz z Dyrekcją Bezpieczeństwa i Ochrony Sekretariatu Generalnego Rady.

4. Jeżeli istnieje długoterminowa potrzeba wymiany przez ESDZ z państwem trzecim lub organizacją międzynarodową informacji niejawnych o klauzuli tajności z reguły nie wyższej niż RESTREINT UE/EU RESTRICTED i jeżeli ustalono, że dana strona nie dysponuje wystarczająco rozwiniętym systemem bezpieczeństwa, tak aby było możliwe zawarcie umowy o bezpieczeństwie informacji, WP, po uzyskaniu jednomyślnej pozytywnej opinii Komitetu ds.. Bezpieczeństwa ESDZ, zgodnie z art. 15 ust. 5 niniejszej decyzji, może zawrzeć porozumienie administracyjne z właściwymi organami danego państwa trzeciego lub danej organizacji międzynarodowej.

5. EUCI nie mogą być wymieniane drogą elektroniczną z państwem trzecim lub organizacją międzynarodową, chyba że wyraźnie przewidziano to w umowie o bezpieczeństwie informacji lub w porozumieniu administracyjnym.

6. Na mocy porozumienia administracyjnego o wymianie informacji niejawnych ESDZ i państwo trzecie lub organizacja międzynarodowa wyznaczają kancelarię tajną jako główny punkt wejścia i wyjścia dla wymienianych informacji niejawnych. 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 daną organizacją międzynarodową i służą one ocenie:

   a) ram prawnych mających zastosowanie do ochrony informacji niejawnych;

   b) wszelkich cech charakterystycznych przepisów ustawowych i wykonawczych, polityk i procedur danego państwa trzeciego lub danej organizacji międzynarodowej w zakresie bezpieczeństwa, które mogą mieć wpływ na to, jaką najwyższą klauzulę tajności mogą mieć wymieniane informacje niejawne;

   c) stosowanych w danym czasie środków i procedur bezpieczeństwa służących ochronie informacji niejawnych; oraz

   d) procedur prowadzenia postępowań sprawdzających 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.

   Jeżeli w oczekiwaniu na taką wizytę oceniającą WP zostanie powiadomiony o jakichkolwiek wyjątkowych lub pilnych powodach wymiany informacji niejawnych, organ ESDZ ds. bezpieczeństwa:

   a) najpierw zwraca się do wytwórcy o pisemną zgodę na ustalenie, że nie ma zastrzeżeń do udostępnienia;

   b) może podjąć decyzję o udostępnieniu, pod warunkiem uzyskania jednomyślnej pozytywnej opinii państw członkowskich reprezentowanych w Komitecie ds. Bezpieczeństwa ESDZ.

   Jeśli ESDZ nie jest w stanie ustalić wytwórcy informacji, organ ESDZ ds. bezpieczeństwa przyjmuje na siebie odpowiedzialność wytwórcy po uzyskaniu jednomyślnej przychylnej 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.

11. Jeżeli ESDZ nie jest wytwórcą informacji niejawnych, które mają zostać udostępnione, ani wytwórcą materiału źródłowego, który mogą one zawierać, to organ ESDZ ds. bezpieczeństwa 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, organ ESDZ ds. bezpieczeństwa przyjmuje na siebie odpowiedzialność wytwórcy po uzyskaniu jednogłośnej przychylnej 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.

   Organ ESDZ ds. bezpieczeństwa, po zapewnieniu spełnienia warunków określonych w pkt 11 powyżej:

   a) w miarę możliwości sprawdza z organami bezpieczeństwa danego państwa trzeciego 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 ESDZ, by na podstawie dostępnych informacji wydał opinię dotyczącą pewności, jaką można mieć w stosunku do przepisów, struktur i procedur dotyczących bezpieczeństwa w państwie trzecim lub organizacji międzynarodowej, którym mają zostać udostępnione EUCI;

c) może podjąć decyzję o udostępnieniu, pod warunkiem uzyskania jednomyślnej pozytywnej 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:

(a) „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 wdrożony został zatwierdzony zestaw technicznych, fizycznych, organizacyjnych i proceduralnych środków bezpieczeństwa;

(b) „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;

(c) „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 ustalono jej potrzebę zgodnie z zasadą ograniczonego dostępu – może uzyskać dostęp do EUCI opatrzonych klauzulą tajności do określonego poziomu (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższego) do określonego terminu zgodnie z art. 2 załącznika A I;

(d) „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;

(e) „cykl życia systemu teleinformatycznego" oznacza cały okres istnienia systemu teleinformatycznego, który obejmuje powstanie pomysłu, opracowanie koncepcji, zaplanowanie, analizę wymogów, zaprojektowanie, utworzenie, testowanie, wdrożenie, działanie, konserwację i wycofanie z działania;

(f) „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;

(g) „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;

(h) „system teleinformatyczny" oznacza system umożliwiający przetwarzanie informacji w formie elektronicznej. System teleinformatyczny obejmuje wszystkie zasoby niezbędne do jego funkcjonowania, w tym infrastrukturę, organizację, personel oraz zasoby informatyczne;

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

(j) „wykonawca" oznacza osobę fizyczną lub prawną posiadającą zdolność prawną do zawierania umów;

(k) „produkty kryptograficzne" oznaczają algorytmy kryptograficzne, sprzęt i oprogramowanie kryptograficzne, a także produkty zawierające szczegóły stosowania i związaną z nim dokumentację oraz klucze;

(l) „operacja WPBiO" oznacza wojskową lub cywilną operację zarządzania kryzysowego prowadzoną na mocy tytułu V rozdział 2 TUE;

(m) „zniesienie klauzuli tajności" oznacza zniesienie jakiejkolwiek klauzuli tajności;

(n) „ochrona w głąb" oznacza stosowanie szeregu środków bezpieczeństwa w formie wielu warstw zabezpieczeń;

(o) „wyznaczony organ bezpieczeństwa" oznacza organ podporządkowany krajowemu organowi bezpieczeństwa państwa członkowskiego, odpowiedzialny za informowanie podmiotów prowadzących działalność gospodarczą lub inną o krajowej polityce w zakresie wszelkich kwestii związanych z bezpieczeństwem przemysłowym oraz za udzielanie wskazówek i pomocy w ich wdrażaniu. Zadania wyznaczonego organu bezpieczeństwa może wykonywać krajowy organ bezpieczeństwa lub dowolny inny właściwy organ;

(p) „dokument" oznacza każdą zapisaną informację, niezależnie od jej postaci fizycznej lub cech;

(q) „obniżenie klauzuli tajności" oznacza obniżenie poziomu klauzuli tajności;

(r) „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));

(s) „świadectwo bezpieczeństwa przemysłowego" oznacza stwierdzenie przez krajowy organ bezpieczeństwa lub wyznaczony organ bezpieczeństwa w wyniku procedur administracyjnych, że z punktu widzenia bezpieczeństwa dany obiekt jest w stanie zapewnić odpowiednią ochronę EUCI opatrzonych określoną klauzulą tajności, a personel tego obiektu, któremu niezbędny jest dostęp do EUCI, został odpowiednio sprawdzony pod względem bezpieczeństwa i odebrał instruktaż dotyczący odpowiednich wymogów bezpieczeństwa niezbędnych do uzyskania dostępu do EUCI i do ochrony EUCI;

(t) „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 systemu teleinformatycznego pojęcie to obejmuje również gromadzenie, wyświetlanie, przesyłanie i przechowywanie EUCI;

(u) „posiadacz" oznacza osobę posiadającą odpowiednie uprawnienia i spełniającą wymogi zasady ograniczonego dostępu, znajdującą się w posiadaniu EUCI i w związku z tym odpowiedzialną za ich ochronę;

(v) „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;

(w) „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;

(x) „zabezpieczanie informacji" w ramach systemów teleinformatycznych oznacza pewność, że systemy te będą chronić informacje, które są w nich przetwarzane, i będą działać zgodnie z przeznaczeniem, w razie potrzeby pod kontrolą uprawnionych użytkowników. Skuteczne zabezpieczanie informacji gwarantuje odpowiedni poziom poufności, integralności, dostępności, niezaprzeczalności i autentyczności. Zabezpieczanie informacji opiera się na procesie zarządzania ryzykiem – zob. art. 8 ust. 1 załącznika A;

(y) „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);

(z) „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 powstrzymywaniu od zamierzonego lub przypadkowego narażenia na szwank bezpieczeństwa tych informacji lub ich utraty i w wykrywaniu takich przypadków oraz w przywracaniu poprzedniego stanu po ich wystąpieniu. Środki takie dotyczą w szczególności wytwarzania, rejestracji, kopiowania, tłumaczenia, przenoszenia, przetwarzania, przechowywania i niszczenia EUCI – zob. art. 7 ust. 1 załącznika A;

(aa) „materiały" oznaczają jakikolwiek dokument lub dowolny mechanizm lub sprzęt, już wytworzone lub będące w trakcie wytwarzania;

(bb) „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;

(cc) „bezpieczeństwo osobowe" oznacza stosowanie środków zapewniających, aby dostęp do EUCI był przyznawany tylko tym osobom, które:

— muszą mieć dostęp w ramach zasady ograniczonego dostępu;

— w przypadku dostępu do informacji opatrzonych klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą – zostały sprawdzone pod względem bezpieczeństwa do odpowiedniego poziomu lub ze względu na pełnione przez nie funkcje przyznano im inne odpowiednie upoważnienie zgodnie z krajowymi przepisami ustawowymi i wykonawczymi; oraz

— zostały poinformowane o swoich obowiązkach –

zgodnie z art. 5 ust. 1 załącznika A;

(dd) „poświadczenie bezpieczeństwa osobowego" (PBO) do celów dostępu do EUCI oznacza oświadczenie wydane przez właściwy organ państwa członkowskiego w następstwie zakończenia postępowania w sprawie bezpieczeństwa przeprowadzonego przez właściwe organy państwa członkowskiego; w dokumencie tym zaświadcza się, że dana osoba może, o ile ustalono jej potrzeby w ramach zasady ograniczonego dostępu, otrzymać dostęp do EUCI do ustalonego poziomu (klauzula CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższa) do określonego terminu; o takiej osobie mówi się, że została „sprawdzona pod względem bezpieczeństwa";

(ee) „zaświadczenie potwierdzające posiadanie poświadczenia bezpieczeństwa osobowego" (ZPBO) jest to zaświadczenie wydawane przez właściwy organ, stwierdzające, że dana osoba została sprawdzona pod względem bezpieczeństwa i posiada odpowiednie poświadczenie bezpieczeństwa osobowego lub upoważnienie od dyrektora odpowiedzialnego za bezpieczeństwo siedziby i bezpieczeństwo informacji ESDZ; poświadczenie to wskazuje poziom EUCI, do którego danej osobie można udzielić dostępu (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższy), datę ważności odnośnego PBO oraz datę ważności samego zaświadczenia;

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

(gg) „instrukcje bezpieczeństwa programu/projektu" (IBP) oznaczają wykaz procedur bezpieczeństwa stosowanych do określonego programu/projektu w celu ujednolicenia procedur bezpieczeństwa. Instrukcje te mogą być zmieniane podczas trwania programu/projektu;

(hh) „rejestracja" oznacza stosowanie procedur rejestrowania etapów cyklu życia informacji, w tym jej rozpowszechniania i zniszczenia – zob. pkt 21 załącznika A III;

(ii) „ryzyko szczątkowe" oznacza ryzyko, które pozostaje po wdrożeniu środków bezpieczeństwa, przy założeniu, że nie przeciwdziała się wszystkim zagrożeniom i że nie każdą podatność można wyeliminować;

(jj) „ryzyko" oznacza prawdopodobieństwo, że dane zagrożenie wykorzysta wewnętrzną i zewnętrzną podatność danej organizacji lub jakiegokolwiek systemu, z którego korzysta, i tym samym spowoduje szkody dla tej organizacji i jej materialnych lub niematerialnych zasobów; Ryzyko mierzone jest jako połączenie prawdopodobieństwa wystąpienia zagrożeń oraz ich skutków;

(kk) „akceptacja ryzyka" jest decyzją o zaakceptowaniu dalszego występowania określonego ryzyka szczątkowego po zmniejszeniu ryzyka;

(ll) „ocena ryzyka" polega na określaniu zagrożeń i podatności oraz przeprowadzeniu odpowiedniej analizy ryzyka, tj. analizy prawdopodobieństwa i skutków;

(mm) „powiadamianie o ryzyku" polega na upowszechnianiu wiedzy o ryzyku wśród społeczności korzystających z systemów teleinformatycznych, na informowaniu o takim ryzyku organów zatwierdzających i na składaniu sprawozdań z nich organom operacyjnym;

(nn) „proces zarządzania ryzykiem" oznacza cały proces określania, kontrolowania i minimalizacji niepewnych zdarzeń, które mogą wpłynąć na bezpieczeństwo danej organizacji lub jakiegokolwiek systemu, z którego korzysta; Pojęcie to obejmuje wszelkie działania związane z ryzykiem, w tym ocenę, zmniejszanie, akceptację i powiadamianie;

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

(pp) „dokument określający aspekty bezpieczeństwa" (DOAB) oznacza zbiór specjalnych warunków umownych, wydany przez instytucję zamawiającą, stanowiący integralną część każdej umowy niejawnej 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;

(qq) „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 DOAB – zob. sekcja II załącznika A V;

(rr) „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 lub unijnego PBO umożliwiającego dostęp do EUCI do określonego poziomu klauzuli tajności (CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższej);

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

(tt) „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 ([1]) w związku z odpowiednim orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej lub dane osobowe objęte zakresem rozporządzenia (UE) nr 2018/1725;

(uu) „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 systemów teleinformatycznych;

(vv) „TEMPEST" oznacza sprawdzenie, analizę i kontrolę emisji elektromagnetycznych umożliwiających przechwycenie danych oraz środki służące tłumieniu takich emisji;

(ww) „zagrożenie" oznacza potencjalną przyczynę niepożądanego incydentu, który może skutkować szkodą dla organizacji lub jakiegokolwiek systemu, z którego korzysta. Zagrożenia takie mogą być przypadkowe lub zamierzone (rozmyślne) i obejmują elementy zagrażające, potencjalne cele i metody ataku;

(xx) „podatność" oznacza każdego rodzaju słaby punkt, który może zostać wykorzystany przez jedno zagrożenie lub większą ich liczbę. Podatność może wynikać z zaniechania 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

Równoważność klauzul tajności

UE	TRES SECRET UE/EU TOP SECRET	TRÈS SECRET UE/UE TOP SECRET	SECRET UE/EU SECRET CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA 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)	Uwaga ([1]) poniżej
Bułgaria	Строго секретно	Секретно	Поверително	За служебно ползване
Republika Czeska	Přísně 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 Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Hiszpania	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Francja	TRÈS SECRET TRÈS SECRET DÉFENSE ([3])	SECRET SECRET DÉFENSE ([3])	CONFIDENTIEL DÉFENSE ([3]) ([4])	Nota ([5]) below
Chorwacja	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Włochy	Segretissimo	Segreto	Riservatissimo	Riservato
Cypr	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (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-Għola Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted ([6])
Niderlandy	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austria	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polska	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalia	Muito Secreto	Secreto	Confidencial	Reservado
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	Kvaliciferat hemlig	Hemlig	Konfidentiell	Begränsat hemlig

([1]) Diffusion Restreinte/Beperkte Verspreiding nie jest w Belgii uznawane za klauzulę tajności. W Belgii pracuje się z wykorzystaniem informacji oznaczonych „RESTREINT UE/EU RESTRICTED" i chroni je w sposób nie mniej rygorystyczny, niż przewidują to normy i procedury opisane w przepisach bezpieczeństwa Rady Unii Europejskiej.

([2]) Niemcy: VS = Verschlusssache.

([3]) Informacje wytworzone przez Francję przed dniem 1 lipca 2021 r. i opatrzone klauzulą „TRÈS SECRET DÉFENSE", „SECRET DÉFENSE" oraz „CONFIDENTIEL DÉFENSE" są nadal przetwarzane i chronione na równoważnym poziomie odpowiednio „TRÈS SECRET UE/EU TOP SECRET", „SECRET UE/EU SECRET" oraz „CONFIDENTIEL UE/EU CONFIDENTIAL".

([4]) We Francji pracuje się z wykorzystaniem informacji niejawnych oznaczonych „CONFIDENTIEL UE/EU CONFIDENTIAL" i chroni je zgodnie z obowiązującymi we Francji środkami bezpieczeństwa służącymi ochronie informacji oznaczonych klauzulą „SECRET".

([5]) Francja nie stosuje klauzuli „RESTREINT" w swoim systemie krajowym. We Francji pracuje się z wykorzystaniem informacji oznaczonych „RESTREINT UE/EU RESTRICTED" i chroni je w sposób nie mniej rygorystyczny, niż przewidują to normy i procedury opisane.

([6]) W przypadku Malty oznaczenia maltańskie i angielskie można stosować wymiennie.