DECYZJA KOMISJI (UE) 2022/640

z dnia 7 kwietnia 2022 r.

w sprawie przepisów wykonawczych dotyczących ról i obowiązków głównych podmiotów w obszarze bezpieczeństwa

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 249,

uwzględniając decyzję Komisji (UE, Euratom) 2015/443 z dnia 13 marca 2015 r. w sprawie bezpieczeństwa w Komisji ([1]),

uwzględniając decyzję Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE ([2]),

a także mając na uwadze, co następuje:

(1) Decyzję (UE, Euratom) 2015/443 i decyzję (UE, Euratom) 2015/444 stosuje się do wszystkich departamentów Komisji i do wszystkich jej obiektów.

(2) W razie potrzeby przyjmuje się, w myśl art. 60 decyzji (UE, Euratom) 2015/444, przepisy wykonawcze w celu uzupełnienia lub wsparcia tejże decyzji.

(3) Środki bezpieczeństwa służące ochronie informacji niejawnych UE na wszystkich etapach ich cyklu życia powinny być proporcjonalne w szczególności do ich klauzuli tajności.

(4) Środki bezpieczeństwa w zakresie ochrony systemów teleinformatycznych w Komisji określono w decyzji Komisji (UE, Euratom) 2017/46 ([3]), w szczególności w art. 3 dotyczącym zasad bezpieczeństwa IT w Komisji i w art. 9 dotyczącym właścicieli systemów.

(5) Celem przepisów wykonawczych dotyczących ról i obowiązków głównych podmiotów w obszarze bezpieczeństwa jest zapewnienie wytycznych dotyczących warunków wstępnych i obowiązków określonych w odniesieniu do tych ról w decyzji (UE, Euratom) 2015/443 i w decyzji (UE, Euratom) 2015/444.

(6) W art. 36 ust. 7 decyzji (UE, Euratom) 2015/444 określono szereg dodatkowych funkcji związanych z bezpieczeństwem, które sprawuje organ ds. bezpieczeństwa Komisji. W niniejszej decyzji określono zadania związane z tymi funkcjami.

(7) Zgodnie z decyzją (UE, Euratom) 2015/444 szczególne zadania związane z ochroną informacji niejawnych UE w poszczególnych departamentach powierzono lokalnym pełnomocnikom ochrony i urzędnikom kontroli kancelarii.

(8) 4 maja 2016 r. Komisja przyjęła decyzję ([4]) upoważniającą członka Komisji odpowiedzialnego za kwestie bezpieczeństwa do przyjęcia w imieniu Komisji i na jej odpowiedzialność przepisów wykonawczych przewidzianych w art. 60 decyzji (UE, Euratom) 2015/444. Następnie 13 kwietnia 2021 r. członek Komisji odpowiedzialny za kwestie bezpieczeństwa przyjął w imieniu Komisji i na jej odpowiedzialność decyzję ([5]) subdelegującą przyjęcie tych przepisów wykonawczych dyrektorowi generalnemu Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa,

([1]) Dz.U. L 72 z 17.3.2015, s. 41.
([2]) Dz.U. L 72 z 17.3.2015, s. 53.
([3]) Decyzja Komisji (UE, Euratom) 2017/46 z dnia 10 stycznia 2017 r. w sprawie bezpieczeństwa systemów teleinformatycznych w Komisji Europejskiej (Dz.U. L 6 z 11.1.2017, s. 40).
([4]) Decyzja C(2016) 2797 final z dnia 4 maja 2016 r. w sprawie upoważnienia związanego z bezpieczeństwem.
([5]) Decyzja C(2021) 2684 final z dnia 13 kwietnia 2021 r. subdelegująca uprawnienia przyznane w decyzji Komisji C(2016) 2797 w sprawie upoważnienia związanego z bezpieczeństwem.

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Rozdział 1

Przepisy ogólne

Artykuł 1

Przedmiot i zakres stosowania

1. W niniejszej decyzji określono role i obowiązki głównych podmiotów w obszarze bezpieczeństwa odpowiedzialnych za ochronę informacji niejawnych UE (EUCI) w Komisji na podstawie decyzji (UE, Euratom) 2015/443 i decyzji (UE, Euratom) 2015/444.

2. Niniejszą decyzję stosuje się do wszystkich departamentów Komisji i do wszystkich obiektów Komisji.

Rozdział 2

Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa

Artykuł 2

Organ ds. bezpieczeństwa Komisji

1. Dyrektor Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa jest organem ds. bezpieczeństwa Komisji, o którym mowa w art. 7 decyzji (UE, Euratom) 2015/444.

2. Organ ds. bezpieczeństwa Komisji obejmuje powierzone mu funkcje w następujących obszarach określonych w decyzji (UE, Euratom) 2015/444, zgodnie z art. 3–7 niniejszej decyzji:

a) bezpieczeństwo osobowe,

b) bezpieczeństwo fizyczne,

c) zarządzanie EUCI,

d) akredytacja każdego systemu teleinformatycznego (CIS), w którym przetwarza się EUCI,

e) bezpieczeństwo przemysłowe i

f) wymiana informacji niejawnych.

3. Organ ds. bezpieczeństwa Komisji zapewnia lokalnym pełnomocnikom ochrony i ich zastępcom oraz urzędnikom kontroli kancelarii i ich zastępcom obowiązkowe szkolenia w zakresie ich zadań i obowiązków.

Artykuł 3

Organ ds. zabezpieczania informacji

Organ ds. zabezpieczania informacji odpowiada za następujące działania związane z ochroną EUCI:

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

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

c) zapewnienie zgodności środków w zakresie zabezpieczania informacji, odpowiednio, z polityką bezpieczeństwa i zamówień publicznych Komisji;

d) zapewnienie, by wybór produktów kryptograficznych następował zgodnie z polityką dotyczącą kryteriów ich kwalifikowalności i wyboru;

e) konsultowanie się z właścicielami systemów, dostawcami systemów, podmiotami odpowiedzialnymi za bezpieczeństwo i przedstawicielami użytkowników w kwestii polityki bezpieczeństwa w zakresie zabezpieczania informacji i wytycznych dotyczących bezpieczeństwa.

Artykuł 4

Organ ds. akredytacji bezpieczeństwa

1. Organ ds. bezpieczeństwa Komisji odpowiada za akredytację stref bezpieczeństwa spełniających wymogi określone w art. 18 decyzji 2015/444 i CIS, w których przetwarza się EUCI.

2. Departamenty Komisji konsultują się z organem ds. akredytacji bezpieczeństwa w porozumieniu ze swoim lokalnym pełnomocnikiem ochrony i w stosownych przypadkach lokalnym pełnomocnikiem ds. bezpieczeństwa teleinformatycznego zawsze wówczas, gdy dany departament planuje:

a) stworzyć strefę bezpieczeństwa;

b) wdrożyć CIS, w którym przetwarza się EUCI;

c) zainstalować wszelkie inne urządzenia służące do korzystania z informacji niejawnych, w tym połączenia z zewnętrznym CIS.

Organ ds. akredytacji bezpieczeństwa zapewnia doradztwo w zakresie tych działań zarówno w procesie planowania, jak i w procesie budowy lub rozwoju.

3. EUCI nie wolno przetwarzać w strefie bezpieczeństwa ani w CIS przed wydaniem przez organ ds. akredytacji bezpieczeństwa akredytacji na odpowiednim poziomie klauzuli tajności EUCI.

4. Wymogi w zakresie akredytacji strefy bezpieczeństwa obejmują:

a) zatwierdzenie planów danej strefy bezpieczeństwa;

b) zatwierdzenie wszelkich umów na roboty realizowane przez wykonawców zewnętrznych z uwzględnieniem przepisów dotyczących bezpieczeństwa przemysłowego, w tym wszelkich wymogów w zakresie poświadczenia bezpieczeństwa wydawanego wykonawcom i ich pracownikom;

c) udostępnienie wszystkich wymaganych deklaracji i certyfikatów zgodności;

d) fizyczną kontrolę danej strefy bezpieczeństwa w celu weryfikacji, czy materiały i metody budowlane, kontrole dostępu, sprzęt służący do ochrony i wszelkie inne elementy są zgodne z wymogami określonymi przez organ ds. bezpieczeństwa Komisji;

e) zatwierdzenie środków przeciwdziałania promieniowaniu elektromagnetycznemu w przypadku każdej strefy technicznie zabezpieczonej;

f) zatwierdzenie procedur bezpiecznej eksploatacji systemu (SecOP) w odniesieniu do danej strefy bezpieczeństwa.

5. Wymogi w zakresie akredytacji CIS, w którym przetwarza się EUCI, obejmują:

a) utworzenie strategii akredytacji systemu;

b) zatwierdzenie planu bezpieczeństwa CIS na podstawie podejścia zakładającego zarządzanie ryzykiem;

c) zatwierdzenie procedur bezpiecznej eksploatacji systemu w odniesieniu do danego CIS;

d) zatwierdzenie całej pozostałej dokumentacji dotyczącej bezpieczeństwa, wskazanej przez organ ds. akredytacji bezpieczeństwa;

e) zatwierdzenie każdego zastosowania technologii szyfrujących;

f) zatwierdzenie środków przeciwdziałania promieniowaniu elektromagnetycznemu w przypadku CIS, w którym przetwarza się informacje z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą;

g) inspekcję CIS w celu weryfikacji prawidłowego wdrożenia udokumentowanych środków bezpieczeństwa.

6. Po skutecznym spełnieniu wymogów w zakresie akredytacji organ ds. akredytacji bezpieczeństwa wydaje formalne upoważnienie do przetwarzania EUCI w strefie bezpieczeństwa lub CIS w odniesieniu do wskazanego maksymalnego poziomu klauzuli tajności EUCI i na okres nie dłuższy niż 5 lat, w zależności od poziomu klauzuli tajności wykorzystywanych EUCI i występujących rodzajów ryzyka.

7. Po uzyskaniu powiadomienia o wystąpieniu naruszenia bezpieczeństwa lub wprowadzeniu istotnej zmiany w projekcie lub środkach bezpieczeństwa strefy bezpieczeństwa lub CIS organ ds. akredytacji bezpieczeństwa przeprowadza przegląd i w razie potrzeby może cofnąć upoważnienie do przetwarzania EUCI do czasu rozwiązania wszelkich zidentyfikowanych kwestii.

Artykuł 5

Organ ds. TEMPEST

1. Wdrażane są środki bezpieczeństwa TEMPEST w celu ochrony CIS, w których przetwarza się informacje z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą; środki te można wdrażać w przypadku informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED.

2. Organ ds. TEMPEST odpowiada za zatwierdzanie środków podejmowanych w celu ochrony przeciwko narażeniu EUCI na szwank za sprawą niezamierzonych emisji elektromagnetycznych.

3. Na wniosek właściciela CIS, w którym przetwarza się EUCI, organ ds. TEMPEST wydaje specyfikację środków bezpieczeństwa TEMPEST odpowiednich do danego poziomu klauzuli tajności informacji.

4. Organ ds. TEMPEST przeprowadza badanie techniczne w ramach akredytacji stref bezpieczeństwa i CIS, w których przetwarza się EUCI z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą, i po uzyskaniu pozytywnych wyników tych badań wydaje certyfikat TEMPEST.

5. Certyfikat TEMPEST zawiera co najmniej:

a) datę przeprowadzenia badania;

b) opis środków bezpieczeństwa TEMPEST wraz z planami obiektów;

c) termin ważności certyfikatu;

d) wskazanie wszelkich zmian, które będą skutkować unieważnieniem certyfikatu;

e) podpis w imieniu organu ds. TEMPEST.

6. Lokalny pełnomocnik ochrony lub organizator posiedzeń odpowiedzialny za zorganizowanie niejawnego posiedzenia we współpracy z lokalnym pełnomocnikiem ochrony może zwrócić się z wnioskiem do organu ds. TEMPEST o zbadanie pomieszczeń, w których posiedzenie ma się odbyć, w celu zapewnienia, aby takie pomieszczenia były technicznie zabezpieczone.

Artykuł 6

Organ ds. zatwierdzania produktów kryptograficznych

1. Organ ds. zatwierdzania produktów kryptograficznych odpowiada za korzystanie z technologii szyfrujących.

2. Organ ds. zatwierdzania produktów kryptograficznych wydaje wytyczne dotyczące stosowania i zatwierdzania technologii szyfrujących.

3. Organ ds. zatwierdzania produktów kryptograficznych zatwierdza korzystanie z rozwiązań w zakresie szyfrowania na podstawie wniosku właściciela systemu. Zatwierdzenia tego dokonuje się na podstawie pozytywnej weryfikacji co najmniej następujących elementów:

a) potrzeb w zakresie bezpieczeństwa informacji, które należy objąć ochroną;

b) przeglądu CIS wykorzystywanych w ramach danego rozwiązania;

c) oceny ryzyka nieodłącznego i szczątkowego;

d) opisu proponowanego rozwiązania;

e) procedur bezpiecznej eksploatacji systemu w odniesieniu do danego rozwiązania w zakresie szyfrowania.

4. Organ ds. zatwierdzania produktów kryptograficznych prowadzi rejestr zatwierdzonych rozwiązań w zakresie szyfrowania.

Artykuł 7

Organ ds. dystrybucji produktów kryptograficznych

1. Organ ds. dystrybucji produktów kryptograficznych odpowiada za dystrybucję materiałów kryptograficznych wykorzystywanych do ochrony EUCI (głównie sprzętu kryptograficznego, kluczy kryptograficznych, certyfikatów i powiązanych elementów uwierzytelniających) wśród:

a) użytkowników lub departamentów w Komisji w przypadku CIS zarządzanych przez podmioty zewnętrzne;

b) użytkowników lub organizacji spoza Komisji w przypadku CIS zarządzanych przez Komisję.

2. Organ ds. dystrybucji produktów kryptograficznych może przekazać zadanie dystrybucji materiałów kryptograficznych dla stron trzecich innym departamentom zgodnie z art. 17 ust. 3 decyzji 2015/443.

3. Organ ds. dystrybucji produktów kryptograficznych zapewnia, aby wszystkie materiały kryptograficzne przesyłano bezpiecznymi kanałami chroniącymi przed ingerencją i sygnalizującymi widoczne ślady ingerencji, zgodnie z przepisami bezpieczeństwa mającymi zastosowanie do poziomu klauzuli tajności EUCI, które będą chronione tymi materiałami.

4. Organ ds. dystrybucji produktów kryptograficznych zapewnia wytyczne dla lokalnego pełnomocnika ochrony i, w stosownych przypadkach, dla lokalnego pełnomocnika ds. bezpieczeństwa teleinformatycznego w każdym departamencie Komisji, którzy uczestniczą w opracowywaniu, dystrybucji lub stosowaniu materiałów kryptograficznych.

5. Organ ds. dystrybucji produktów kryptograficznych zapewnia ustanowienie odpowiednich procedur bezpiecznej eksploatacji systemu na potrzeby procesu dystrybucji.

Rozdział 3

Departamenty Komisji

Artykuł 8

Kierownicy departamentów

1. Każdy kierownik departamentu wyznacza:

a) lokalnego pełnomocnika ochrony i co najmniej jednego jego zastępcę, odpowiednio, w przypadku departamentu lub gabinetu;

b) urzędnika kontroli kancelarii i co najmniej jednego jego zastępcę, odpowiednio, w odniesieniu do każdego departamentu prowadzącego kancelarię tajną UE;

c) właściciela poszczególnych CIS, w których przetwarza się EUCI.

2. Przed wyznaczeniem lokalnych pełnomocników ochrony i ich zastępców oraz urzędników kontroli kancelarii i ich zastępców kierownik departamentu zwraca się o zatwierdzenie do Dyrektora Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa.

3. Kierownik departamentu, w porozumieniu z lokalnym pełnomocnikiem ochrony, identyfikuje wszystkie stanowiska wymagające poświadczenia bezpieczeństwa w celu uzyskania dostępu do EUCI. W procesie rekrutacji na takie stanowiska kandydatów informuje się o wymogu uzyskania poświadczenia bezpieczeństwa.

4. W razie potrzeby kierownik każdego departamentu posiadającego EUCI odpowiada za uruchomienie planów ewakuacji i niszczenia EUCI w sytuacjach nadzwyczajnych. W takich planach należy przewidzieć alternatywny tryb postępowania w sytuacji, w której niemożliwe jest nawiązanie kontaktu z kierownikiem departamentu.

Artykuł 9

Właściciele CIS, w których przetwarza się EUCI

1. Realizując projekt służący wdrożeniu CIS, w którym przetwarza się EUCI, właściciel systemu jak najszybciej kontaktuje się z organem ds. akredytacji bezpieczeństwa, aby ustalić odpowiednie standardy i wymogi bezpieczeństwa oraz rozpocząć proces akredytacji bezpieczeństwa.

2. Właściciel systemu zapewnia, aby środki bezpieczeństwa spełniały wymogi określone przez organ ds. akredytacji bezpieczeństwa oraz aby w danym CIS nie przetwarzano EUCI, zanim system ten nie otrzyma akredytacji.

3. Właściciel systemu zwraca się do organu ds. zatwierdzania produktów kryptograficznych o zgodę na stosowanie wszelkich technologii szyfrujących. Właściciele systemów nie mogą stosować technologii szyfrujących w systemach produkcji bez uzyskania wcześniejszej zgody.

4. Właściciel systemu konsultuje się z lokalnym pełnomocnikiem ds. bezpieczeństwa teleinformatycznego w danym departamencie w sprawach związanych z bezpieczeństwem CIS.

5. Właściciel systemu co najmniej raz w roku dokonuje przeglądu środków bezpieczeństwa stosowanych w przypadku danego systemu, w tym dotyczącego go planu bezpieczeństwa.

6. Gdy w CIS dochodzi do incydentu związanego z bezpieczeństwem, w wyniku którego wskazuje się, że taki CIS nie może już zapewnić odpowiedniej ochrony EUCI, właściciel systemu informuje o tym lokalnego pełnomocnika ochrony i niezwłocznie zwraca się do organu ds. akredytacji bezpieczeństwa w celu uzyskania porady odnośnie do dalszego postępowania. W takim przypadku akredytacja może zostać zawieszona, a system wycofany z eksploatacji do czasu podjęcia odpowiednich działań naprawczych.

7. Właściciel systemu zawsze udziela organowi ds. akredytacji bezpieczeństwa pełnego wsparcia w zakresie realizacji obowiązków tego organu związanych z akredytacją danego CIS.

Artykuł 10

Operacyjny organ ds. zabezpieczania informacji

Operacyjny organ ds. zabezpieczania informacji w odniesieniu do każdego CIS:

a) opracowuje dokumentację bezpieczeństwa zgodnie z polityką bezpieczeństwa i wytycznymi dotyczącymi bezpieczeństwa, zwłaszcza plan bezpieczeństwa, SecOP związane z systemem i dokumentację kryptograficzną w ramach procesu akredytacji CIS;

b) uczestniczy w wyborze i testowaniu technicznych środków bezpieczeństwa, urządzeń i oprogramowania dla poszczególnych systemów, nadzoruje ich wdrażanie i zapewnienie ich bezpiecznego zainstalowania, skonfigurowania oraz konserwacji, zgodnie z odpowiednią dokumentacją bezpieczeństwa;

c) uczestniczy w wyborze środków bezpieczeństwa i urządzeń klasy TEMPEST, jeżeli jest to wymagane w planie bezpieczeństwa i zapewnia ich bezpieczną instalację i konserwację we współpracy z organem ds. TEMPEST;

d) monitoruje wdrażanie i stosowanie SecOP związanych z funkcjonowaniem danego systemu;

e) zarządza produktami kryptograficznymi i z nich korzysta, we współpracy z organem ds. dystrybucji produktów kryptograficznych, w celu zapewnienia nadzoru nad materiałami kryptograficznymi i kontrolowanymi obiektami oraz, jeżeli jest to wymagane, zapewnia wytwarzanie zmiennych kryptograficznych;

f) przeprowadza przeglądy, testy i analizy bezpieczeństwa, w szczególności w celu sporządzenia odpowiednich sprawozdań o ryzyku, zgodnie z wymogami organu ds. akredytacji bezpieczeństwa;

g) zapewnia szkolenia w zakresie zabezpieczania informacji w odniesieniu do poszczególnych CIS;

h) wdraża i stosuje środki bezpieczeństwa w odniesieniu do poszczególnych CIS.

Rozdział 4

Lokalny pełnomocnik ochrony

Artykuł 11

Wyznaczanie lokalnego pełnomocnika ochrony

1. Lokalny pełnomocnik ochrony i jego zastępcy są urzędnikami lub pracownikami zatrudnionymi na czas określony.

2. Wszyscy lokalni pełnomocnicy ochrony i ich zastępcy muszą posiadać ważne upoważnienie w zakresie bezpieczeństwa, aby uzyskać dostęp do EUCI z klauzulą tajności nie wyższą niż SECRET UE/EU SECRET i w razie potrzeby z klauzulą tajności nie wyższą niż TRES SECRET UE/EU TOP SECRET. Lokalny pełnomocnik ochrony lub jego zastępca musi otrzymać upoważnienie w zakresie bezpieczeństwa, zanim zostanie mianowany na to stanowisko.

3. Przedstawicielstwa Komisji mogą zwrócić się z wnioskiem do organu ds. bezpieczeństwa Komisji o wyłączenie z obowiązku spełnienia wymogów określonych w ust. 1 i 2.

Artykuł 12

Procedury bezpiecznej eksploatacji systemu w odniesieniu do stref bezpieczeństwa

1. Lokalny pełnomocnik ochrony w danym departamencie Komisji opracowuje procedury SecOP dla każdej strefy bezpieczeństwa, za którą ponosi odpowiedzialność.

2. Lokalny pełnomocnik ochrony zapewnia, aby SecOP obejmowały następujące wymogi:

a) na dostęp bez eskorty do strefy bezpieczeństwa w godzinach pracy można zezwolić jedynie pracownikom posiadającym ważne upoważnienie w zakresie bezpieczeństwa i potwierdzoną potrzebę uzyskania dostępu do dokumentów z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą;

b) na dostęp bez eskorty do strefy bezpieczeństwa poza godzinami pracy można zezwolić jedynie lokalnemu pełnomocnikowi ochrony danego departamentu, urzędnikom kontroli kancelarii danej strefy bezpieczeństwa, ich zastępcom oraz upoważnionym pracownikom Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa;

c) do strefy bezpieczeństwa nie można wnosić – bez uzyskania wcześniejszej zgody organu ds. bezpieczeństwa Komisji – urządzeń do nagrywania i komunikacji, takich jak telefony komórkowe, komputery, kamery lub inne inteligentne urządzenia; o przyznanie wszelkich odstępstw należy zwracać się z wyprzedzeniem do organu ds. bezpieczeństwa Komisji; lokalny pełnomocnik ochrony pełni rolę punktu kontaktowego;

d) wszyscy wewnętrzni lub zewnętrzni pracownicy, którym potrzebny jest dostęp do strefy bezpieczeństwa, ale którzy nie spełniają już kryteriów określonych w lit. a) powyżej, uzyskują taki dostęp pod ciągłą eskortą i ciągłym nadzorem ze strony odpowiednio upoważnionego pracownika; wszystkie takie przypadki uzyskania dostępu do strefy bezpieczeństwa należy rejestrować w dzienniku znajdującym się przy wejściu do strefy bezpieczeństwa;

e) lokalny pełnomocnik ochrony zapewnia, aby systemy wykrywania włamań monitorujące strefę bezpieczeństwa były zawsze włączone i zawsze działały prawidłowo; zarządza on ponadto wszystkimi powiązanymi hasłami, kluczami, PIN-ami lub innymi mechanizmami dostępu i uwierzytelniania;

f) alarmy w strefie bezpieczeństwa są zgłaszane Dyrekcji ds. Bezpieczeństwa w Dyrekcji Generalnej ds. Zasobów Ludzkich i Bezpieczeństwa, która natychmiast powiadamia lokalnego pełnomocnika ochrony;

g) lokalny pełnomocnik ochrony w departamencie, w którym zlokalizowana jest dana strefa bezpieczeństwa, rejestruje każdą interwencję podejmowaną po uruchomieniu alarmu lub wystąpieniu incydentu związanego z bezpieczeństwem;

h) ustanawia się procedury na wypadek uruchomienia alarmu lub wystąpienia innej sytuacji nadzwyczajnej w strefie bezpieczeństwa, w tym procedury ewakuacji personelu i zapewnienia szybkiego działania zespołu reagującego na sytuacje nadzwyczajne, podlegającego organowi ds. bezpieczeństwa Komisji, i – w razie potrzeby – zewnętrznych służb ratunkowych;

i) lokalny pełnomocnik ochrony niezwłocznie zgłasza organowi ds. bezpieczeństwa Komisji każde naruszenie bezpieczeństwa występujące wewnątrz strefy bezpieczeństwa lub w związku ze strefą bezpieczeństwa w celu ustalenia odpowiednich dalszych działań;

j) poszczególne biura, pomieszczenia i sejfy w strefie bezpieczeństwa muszą pozostawać zamknięte zawsze, gdy są pozostawione bez dozoru;

k) pracownicy muszą unikać omawiania informacji niejawnych na korytarzach lub w innych wspólnych przestrzeniach strefy bezpieczeństwa, gdy w pobliżu znajdują się nieupoważnione osoby.

Artykuł 13

Klucze i kody bezpieczeństwa

1. Lokalny pełnomocnik ochrony ponosi ogólną odpowiedzialność za zapewnienie prawidłowego wykorzystania i przechowywania kluczy i kodów stosowanych w strefach bezpieczeństwa lub na potrzeby uzyskania dostępu do stref bezpieczeństwa. Klucze i kody przechowuje się w zabezpieczonej szafie i podlegają one ochronie co najmniej na poziomie ochrony materiału, do którego zapewniają dostęp.

2. Lokalny pełnomocnik ochrony prowadzi rejestr zabezpieczonych szaf i wzmocnionych pomieszczeń wraz z aktualnym wykazem wszystkich pracowników upoważnionych do dostępu do nich bez eskorty.

3. Lokalny pełnomocnik ochrony prowadzi rejestr kluczy do zabezpieczonych szaf i wzmocnionych pomieszczeń wraz z wykazem pracowników, którym klucze te przydzielono. W przypadku każdego wydanego klucza przechowuje się potwierdzenie obejmujące dane identyfikacyjne klucza, odbiorcę, datę i godzinę.

4. Klucze i kody wydaje się wyłącznie na zasadzie ograniczonego dostępu pracownikom, którzy posiadają odpowiednie upoważnienia do dostępu do EUCI. Lokalny pełnomocnik ochrony odzyskuje każdy klucz, gdy warunki te przestają być spełnione.

5. Lokalny pełnomocnik ochrony przechowuje zapasowe klucze i pisemny rejestr kodów w osobnych, zamkniętych, nieprzezroczystych, podpisanych i opatrzonych datą kopertach zapewnionych przez pracownika odpowiedzialnego za klucze. Koperty te przechowuje się w zabezpieczonej szafie o stopniu ochrony określanym dla najwyższego poziomu klauzuli tajności materiałów przechowywanych w odpowiedniej szafie lub odpowiednim wzmocnionym pomieszczeniu.

6. Jeżeli w momencie zmiany kodu lub rotacji kluczy, na kopercie widoczne są ślady ingerencji lub uszkodzenia, lokalny pełnomocnik ochrony uznaje ten fakt za incydent związany z bezpieczeństwem i niezwłocznie powiadania organ ds. bezpieczeństwa Komisji.

7. Zmiany kodów do zabezpieczonych szaf w strefie bezpieczeństwa przeprowadza się pod nadzorem lokalnego pełnomocnika ochrony. Reset kodów następuje co 12 miesięcy oraz zawsze wówczas, gdy:

a) zostaje dostarczona nowa szafa lub zamontowany nowy zamek (zmiany wymagają zwłaszcza kody domyślne);

b) mogło dojść lub faktycznie doszło do narażenia bezpieczeństwa na szwank;

c) osoba posiadająca kod nie potrzebuje już dostępu.

8. Lokalny pełnomocnik ochrony rejestruje daty zmian kodów, o których mowa w ust. 7.

Artykuł 14

Plany ewakuacji i niszczenia EUCI w sytuacjach nadzwyczajnych

1. Lokalny pełnomocnik ochrony pomaga kierownikowi departamentu w ustanowieniu planów ewakuacji i niszczenia EUCI w sytuacjach nadzwyczajnych na podstawie wytycznych zapewnionych przez HR.DS.

2. Lokalny pełnomocnik ochrony zapewnia, aby każdy sprzęt potrzebny do realizacji planów przewidzianych w ust. 1 był łatwo dostępny i utrzymywany w dobrym stanie technicznym.

3. Lokalny pełnomocnik ochrony dokonuje, wraz z urzędnikami wskazanymi w planach przewidzianych w ust. 1, przeglądu stanu gotowości tych planów co najmniej co 12 miesięcy i podejmuje wszelkie działania konieczne do ich aktualizacji.

Artykuł 15

Upoważnienia w zakresie bezpieczeństwa

1. Lokalny pełnomocnik ochrony prowadzi rejestr wszystkich stanowisk w danym departamencie, które wymagają upoważnienia Komisji w zakresie bezpieczeństwa, oraz pracowników zajmujących te stanowiska. Wymóg posiadania upoważnienia w zakresie bezpieczeństwa należy określić w ogłoszeniu o naborze w trakcie procesu rekrutacji i należy o nim poinformować kandydatów podczas rozmowy kwalifikacyjnej.

2. Lokalny pełnomocnik ochrony nadzoruje wszystkie wnioski o upoważnienie w zakresie bezpieczeństwa do dostępu do EUCI. Lokalny pełnomocnik ochrony pełni rolę punktu kontaktowego w danym departamencie i kontaktuje się z organem ds. bezpieczeństwa Komisji w sprawie upoważnień w zakresie bezpieczeństwa.

3. Lokalny pełnomocnik ochrony wszczyna procedurę wydawania upoważnień w zakresie bezpieczeństwa danemu pracownikowi i dopilnowuje, aby taki pracownik szybko przekazał kwestionariusz krajowego poświadczenia bezpieczeństwa organowi ds. bezpieczeństwa Komisji.

4. Lokalny pełnomocnik ochrony zapewnia, aby odpowiednio sprawdzeni pracownicy w danym departamencie postępowali zgodnie z obowiązkowymi instrukcjami w zakresie EUCI w celu uzyskania upoważnienia w zakresie bezpieczeństwa.

5. Lokalny pełnomocnik ochrony regularnie kontaktuje się z Wydziałem ds. Zasobów Kadrowych w danym departamencie w celu uzyskania informacji na temat wszystkich zmian na stanowiskach wymagających upoważnienia w zakresie bezpieczeństwa i niezwłocznie informuje o takich zmianach organ ds. bezpieczeństwa Komisji.

6. Lokalny pełnomocnik ochrony informuje organ ds. bezpieczeństwa Komisji o przybyciu nowego pracownika posiadającego ważne poświadczenie bezpieczeństwa, który to pracownik ma objąć stanowisko wymagające posiadania upoważnienia w zakresie bezpieczeństwa.

7. Lokalny pełnomocnik ochrony zapewnia, aby pracownicy danego departamentu przeszli procedurę przedłużenia ważności poświadczenia bezpieczeństwa w wymaganym terminie. Każdy pracownik, który odmawia udziału w tej procedurze, jest zobowiązany do przejścia na stanowisko niewymagające posiadania upoważnienia w zakresie bezpieczeństwa.

Artykuł 16

Kancelaria tajna UE

1. Jeżeli dany departament prowadzi kancelarię tajną UE, lokalny pełnomocnik ochrony nadzoruje działania urzędników kontroli kancelarii w zakresie korzystania z EUCI i zgodności z przepisami bezpieczeństwa dotyczącymi ochrony EUCI.

2. Co najmniej raz na 12 miesięcy oraz w chwili zmiany urzędnika kontroli kancelarii lub jego zastępcy lokalny pełnomocnik ochrony przeprowadza następujące kontrole:

a) kontrolę próby dokumentów przechowywanych w kancelarii tajnej UE w celu potwierdzenia ich statusu oraz prawidłowości rejestru dokumentów niejawnych;

b) kontrolę próby wszystkich potwierdzeń i specyfikacji przekazania w przypadku dystrybucji EUCI do kancelarii tajnej UE lub z kancelarii tajnej UE;

c) kontrolę próby wszystkich protokołów zniszczenia.

3. Co najmniej raz w miesiącu lokalny pełnomocnik ochrony przeprowadza na miejscu kontrole rejestru dokumentów niejawnych i nowo otrzymanych dokumentów niejawnych w celu zapewnienia prawidłowej rejestracji dokumentów.

4. Wszystkie kontrole dokumentuje się w logu w rejestrze dokumentów niejawnych.

Artykuł 17

Pozostałe obowiązki związane z bezpieczeństwem

Pozostałe obowiązki związane z bezpieczeństwem lokalnego pełnomocnika ochrony są określane w instrukcji bezpieczeństwa obejmującej w szczególności fizyczne bezpieczeństwo osób, obiektów i innych aktywów oraz informacji.

Rozdział 5

Urzędnik kontroli kancelarii

Artykuł 18

Wyznaczanie urzędnika kontroli kancelarii

1. Urzędnik kontroli kancelarii i jego zastępcy są urzędnikami lub pracownikami zatrudnionymi na czas określony.

2. Wszyscy urzędnicy kontroli kancelarii i ich zastępcy muszą posiadać ważne upoważnienie w zakresie bezpieczeństwa, aby uzyskać dostęp do EUCI z klauzulą tajności nie wyższą niż SECRET UE/EU SECRET i w razie potrzeby z klauzulą tajności nie wyższą niż TRES SECRET UE/EU TOP SECRET. Urzędnik kontroli kancelarii lub jego zastępca musi otrzymać upoważnienie w zakresie bezpieczeństwa, zanim zostanie mianowany na to stanowisko.

3. Przedstawicielstwa Komisji mogą zwrócić się z wnioskiem do organu ds. bezpieczeństwa Komisji o wyłączenie z obowiązku spełnienia wymogów określonych w ust. 1 i 2.

Artykuł 19

Obowiązki

1. Urzędnik kontroli kancelarii rejestruje informacje z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą do celów bezpieczeństwa:

a) w momencie ich wpłynięcia do departamentu Komisji lub wysłania z departamentu Komisji, lub

b) w momencie ich wpłynięcia do CIS lub wysłania z CIS.

2. Urzędnik kontroli kancelarii rejestruje wszystkie zdarzenia w cyklu życia wszystkich informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą. Urzędnik kontroli kancelarii zapewnia ponadto rejestrowanie wszystkich wymienianych z krajami trzecimi i organizacjami międzynarodowymi informacji z klauzulą tajności RESTREINT UE/EU RESTRICTED lub równoważną. Dokonuje się tego we współpracy z kancelarią tajną UE zarządzaną przez Sekretariat Generalny.

3. Urzędnik kontroli kancelarii rejestruje dokumenty z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą w rejestrze dokumentów niejawnych i zapewnia bezpieczne przechowywanie tych dokumentów w kancelarii tajnej UE.

4. Urzędnik kontroli kancelarii pomaga pracownikom Komisji w tworzeniu i przesyłaniu informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą.

5. W przypadku otrzymania dokumentów z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą od innych departamentów lub stron zewnętrznych urzędnik kontroli kancelarii zapewnia, aby wytwórca otrzymał należyte potwierdzenie odbioru.

6. Przed udzieleniem członkowi personelu dostępu do dokumentu niejawnego przechowywanego w kancelarii tajnej UE urzędnik kontroli kancelarii zwraca się do lokalnego pełnomocnika ochrony w celu weryfikacji, czy dany pracownik posiada poświadczenie bezpieczeństwa wydane przez organ ds. bezpieczeństwa Komisji.

7. Urzędnik kontroli kancelarii każdorazowo rejestruje wszystkie przypadki wejścia do kancelarii tajnej UE i wyjścia z niej pracowników nieupoważnionych do dostępu bez eskorty i towarzyszy im w trakcie wizyty.

8. Gdy członek personelu wynosi dokument do konsultacji poza kancelarię tajną UE, urzędnik kontroli kancelarii zapewnia, aby taka osoba była świadoma stosownych kompensacyjnych środków bezpieczeństwa i zwróciła dany dokument, gdy tylko nie będzie jej już potrzebny. Urzędnik kontroli kancelarii przypomina pracownikom o jak najszybszym zwracaniu takich dokumentów.

9. Kancelaria tajna UE wydaje list kurierski, jeżeli dokumenty niejawne zostają wyniesione poza państwo, w którym kancelaria ta się znajduje.

10. Szczegółowe instrukcje dla urzędnika kontroli kancelarii w zakresie rejestracji dokumentów niejawnych określa się w instrukcji bezpieczeństwa.

Artykuł 20

Obniżanie i znoszenie klauzul tajności

Urzędnik kontroli kancelarii pomaga departamentom będącym wytwórcami w procesie przeglądu zarejestrowanych EUCI w celu potwierdzenia, czy pierwotny poziom klauzuli tajności jest nadal odpowiedni, czy też w przypadku danego dokumentu można obniżyć lub znieść daną klauzulę tajności.

Artykuł 21

Niszczenie

1. Urzędnik kontroli kancelarii odpowiada za zniszczenie informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą w zatwierdzony sposób, w stosownych przypadkach w obecności odpowiednio sprawdzonych świadków.

2. Urzędnik kontroli kancelarii rejestruje każde zniszczenie informacji z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą w niejawnym rejestrze dokumentów i przechowuje odpowiedni protokół zniszczenia w kancelarii tajnej UE.

Artykuł 22

Dodatkowe zadania

1. Urzędnik kontroli kancelarii zapewnia wszelką niezbędną pomoc lokalnemu pełnomocnikowi ochrony, gdy ten przeprowadza działania nadzorcze w kancelarii tajnej UE.

2. Urzędnik kontroli kancelarii zgłasza wszelkie podejrzewane lub faktyczne incydenty związane z bezpieczeństwem lokalnemu pełnomocnikowi ochrony, który z kolei zgłasza te incydenty organowi ds. bezpieczeństwa Komisji.

3. Urzędnik kontroli danej kancelarii tajnej UE w departamencie Komisji organizującym niejawne posiedzenie z klauzulą tajności CONFIDENTIEL UE/EU CONFIDENTIAL lub wyższą przygotowuje EUCI, które będą wykorzystywane w trakcie tego posiedzenia, oraz współpracuje z organizatorem posiedzenia w celu zapewnienia, aby wszystkie dokumenty i potwierdzenia były przetwarzane zgodnie z odpowiednimi przepisami.

Rozdział 6

Przepisy końcowe

Artykuł 23

Przejrzystość

Niniejsza decyzja zostaje podana do wiadomości służb Komisji i wszystkich osób, których dotyczy, oraz zostaje opublikowana w *Dzienniku Urzędowym Unii Europejskiej*.

Artykuł 24

Niniejsza decyzja wchodzi w życie następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w Brukseli dnia 7 kwietnia 2022 r.

W imieniu Komisji,
za Przewodniczącą,
Gertrud INGESTAD
Dyrektor Generalna
Dyrekcja Generalna ds. Zasobów Ludzkich i Bezpieczeństwa