ROZHODNUTIE KOMISIE (EÚ) 2022/640

zo 7. apríla 2022

o vykonávacích predpisoch týkajúcich sa úloh a zodpovedností hlavných aktérov v oblasti bezpečnosti

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 249,

so zreteľom na rozhodnutie Komisie (EÚ, Euratom) 2015/443 z 13. marca 2015 o bezpečnosti v Komisii ([1]),

so zreteľom na rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ ([2]),

keďže:

(1) Rozhodnutia (EÚ, Euratom) 2015/443 a (EÚ, Euratom) 2015/444 sa uplatňujú na všetky oddelenia a objekty Komisie.

(2) V prípade potreby sa v súlade s článkom 60 rozhodnutia (EÚ, Euratom) 2015/444 prijmú vykonávacie predpisy, ktorými sa uvedené rozhodnutie doplní alebo podporí.

(3) Bezpečnostné opatrenia na ochranu utajovaných skutočností EÚ v priebehu celého ich životného cyklu majú byť primerané najmä stupňu ich utajenia.

(4) Bezpečnostné opatrenia na ochranu komunikačných a informačných systémov v Komisii sú stanovené v rozhodnutí Komisie (EÚ, Euratom) 2017/46 ([3]), najmä v článku 3 o zásadách pre bezpečnosť informačných technológií v Komisii a v článku 9 o vlastníkoch systémov.

(5) Cieľom vykonávacích predpisov o úlohách a povinnostiach hlavných aktérov v oblasti bezpečnosti je poskytnúť usmernenia týkajúce sa predpokladov a povinností, ktoré sú pre tieto úlohy stanovené v rozhodnutiach (EÚ, Euratom) 2015/443 a (EÚ, Euratom) 2015/444.

(6) V článku 36 ods. 7 rozhodnutia (EÚ, Euratom) 2015/444 sa stanovuje niekoľko ďalších funkcií súvisiacich s bezpečnosťou, ktoré má prevziať bezpečnostný orgán Komisie. Úlohy súvisiace s týmito funkciami sú stanovené v tomto rozhodnutí.

(7) Miestni bezpečnostní úradníci a kontrolní úradníci registra majú podľa rozhodnutia (EÚ, Euratom) 2015/444 osobitné povinnosti v oblasti ochrany utajovaných skutočností EÚ vo svojich oddeleniach.

(8) Komisia 4. mája 2016 prijala rozhodnutie ([4]), ktorým poverila člena Komisie zodpovedného za bezpečnostné záležitosti, aby v mene Komisie a na jej zodpovednosť prijal vykonávacie predpisy podľa článku 60 rozhodnutia (EÚ, Euratom) 2015/444; následne 13. apríla 2021 člen Komisie zodpovedný za bezpečnostné záležitosti prijal v mene Komisie a na jej zodpovednosť rozhodnutie ([5]) o ďalšom delegovaní týchto vykonávacích predpisov na generálneho riaditeľa Generálneho riaditeľstva pre ľudské zdroje a bezpečnosť,

([1]) Ú. v. EÚ L 72, 17.3.2015, s. 41.
([2]) Ú. v. EÚ L 72, 17.3.2015, s. 53.
([3]) Rozhodnutie Komisie (EÚ, Euratom) 2017/46 z 10. januára 2017 o bezpečnosti komunikačných a informačných systémov v Európskej komisii (Ú. v. EÚ L 6, 11.1.2017, s. 40).
([4]) Rozhodnutie C(2016) 2797 final zo 4. mája 2016 o poverení v súvislosti s bezpečnosťou.
([5]) Rozhodnutie C(2021) 2684 final z 13. apríla 2021 o ďalšom delegovaní právomocí udelených v rozhodnutí Komisie C(2016) 2797 o poverení v súvislosti s bezpečnosťou.

PRIJALA TOTO ROZHODNUTIE:

KAPITOLA 1

Všeobecné ustanovenia

Článok 1

Predmet úpravy a rozsah pôsobnosti

1. V tomto rozhodnutí sa stanovujú úlohy a povinnosti hlavných aktérov v oblasti bezpečnosti, ktorí sú v Komisii zodpovední za ochranu utajovaných skutočností EÚ (ďalej len „EUCI“) podľa rozhodnutí (EÚ, Euratom) 2015/443 a (EÚ, Euratom) 2015/444.

2. Toto rozhodnutie sa uplatňuje na všetky oddelenia Komisie a vo všetkých objektoch Komisie.

KAPITOLA 2

Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť

Článok 2

Bezpečnostný orgán Komisie

1. Riaditeľ riaditeľstva pre bezpečnosť na Generálnom riaditeľstve pre ľudské zdroje a bezpečnosť je bezpečnostným orgánom Komisie uvedeným v článku 7 rozhodnutia (EÚ, Euratom) 2015/444.

2. V zmysle rozhodnutia (EÚ, Euratom) 2015/444 a v súlade s článkami 3 až 7 tohto rozhodnutia vykonáva bezpečnostný orgán Komisie svoje funkcie v týchto oblastiach:

a) personálna bezpečnosť;

b) fyzická bezpečnosť;

c) správa EUCI;

d) akreditácia komunikačných a informačných systémov (ďalej len „CIS“), ktorými sa manipuluje s EUCI;

e) priemyselná bezpečnosť a

f) výmena utajovaných skutočností.

3. Bezpečnostný orgán Komisie zabezpečí povinné školenie miestnych bezpečnostných úradníkov, ich zástupcov, kontrolných úradníkov registra a ich zástupcov o ich povinnostiach a úlohách.

Článok 3

Orgán pre informačnú bezpečnosť

Orgán pre informačnú bezpečnosť je v súvislosti s ochranou EUCI zodpovedný za:

a) vypracovanie bezpečnostných politík a bezpečnostných usmernení v oblasti informačnej bezpečnosti a monitorovanie ich účinnosti a relevantnosti;

b) ochranu a správu technických informácií týkajúcich sa kryptografických produktov;

c) zaistenie toho, aby opatrenia informačnej bezpečnosti boli náležite v súlade s bezpečnostnou politikou a politikou obstarávania Komisie;

d) zabezpečenie toho, aby sa kryptografické produkty vyberali v súlade s politikami, ktorými sa upravuje ich vhodnosť a výber;

e) konzultácie s vlastníkmi systémov, poskytovateľmi systémov, aktérmi v oblasti bezpečnosti a so zástupcami používateľov týkajúce sa bezpečnostných politík a bezpečnostných usmernení v oblasti informačnej bezpečnosti.

Článok 4

Bezpečnostný akreditačný orgán

1. Bezpečnostný orgán Komisie je zodpovedný za akreditáciu zabezpečených priestorov, ktoré spĺňajú požiadavky článku 18 rozhodnutia 2015/444, a komunikačných a informačných systémov na manipuláciu s EUCI.

2. Oddelenia Komisie sa v koordinácii s miestnym bezpečnostným úradníkom a prípadne s miestnym úradníkom informačnej bezpečnosti poradia s bezpečnostným akreditačným orgánom vždy, keď oddelenie zamýšľa:

a) vybudovať zabezpečený priestor;

b) zaviesť CIS na manipuláciu s EUCI;

c) inštalovať akékoľvek iné zariadenie na manipuláciu s utajovanými skutočnosťami vrátane pripojení k CIS tretej strany.

Bezpečnostný akreditačný orgán poskytuje poradenstvo v súvislosti s týmito činnosťami počas procesu plánovania aj výstavby alebo rozvoja.

3. S EUCI sa nesmie manipulovať v zabezpečenom priestore alebo CIS skôr, ako bezpečnostný akreditačný orgán vydá akreditáciu na príslušnej úrovni EUCI.

4. Požiadavky na akreditáciu zabezpečeného priestoru zahŕňajú:

a) schválenie plánov pre zabezpečený priestor;

b) schválenie zákaziek na práce vykonávané externými dodávateľmi, pričom sa zohľadnia ustanovenia o priemyselnej bezpečnosti, ako sú požiadavky na bezpečnostné previerky dodávateľov a ich zamestnancov;

c) dostupnosť všetkých požadovaných vyhlásení o zhode a certifikátov zhody;

d) fyzickú kontrolu zabezpečeného priestoru s cieľom overiť, či stavebné materiály a metódy, kontroly prístupu, bezpečnostné zariadenia a všetky ostatné položky spĺňajú požiadavky stanovené bezpečnostným orgánom Komisie;

e) schválenie protiopatrení proti elektromagnetickému žiareniu pre každý technicky zabezpečený priestor;

f) schválenie operačných bezpečnostných postupov pre zabezpečený priestor.

5. Požiadavky na akreditáciu CIS, ktorým sa manipuluje s EUCI, zahŕňajú:

a) vytvorenie stratégie pre akreditáciu systému;

b) schválenie bezpečnostného plánu CIS, ktorý je založený na prístupe riadenia rizík;

c) schválenie operačných bezpečnostných postupov pre CIS;

d) schválenie všetkej ďalšej požadovanej bezpečnostnej dokumentácie určenej bezpečnostným akreditačným orgánom;

e) schválenie akéhokoľvek použitia šifrovacích technológií;

f) schválenie protiopatrení proti elektromagnetickému žiareniu pre CIS, ktorými sa manipuluje s utajovanými skutočnosťami so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším;

g) kontrolu CIS s cieľom overiť, či sa zdokumentované bezpečnostné opatrenia vykonávajú správne.

6. Po úspešnom splnení požiadaviek na akreditáciu vydá bezpečnostný akreditačný orgán formálne povolenie na manipuláciu s EUCI v zabezpečenom priestore alebo CIS pre stanovený maximálny stupeň utajenia EUCI a na obdobie najviac päť rokov v závislosti od úrovní utajenia EUCI, s ktorými sa manipuluje, a súvisiacich rizík.

7. Po oznámení narušenia bezpečnosti alebo pri významnej zmene konštrukcie alebo bezpečnostných opatrení zabezpečeného priestoru alebo CIS bezpečnostný akreditačný orgán preskúma a v prípade potreby zruší povolenie na manipuláciu s EUCI, až kým sa zistené problémy nevyriešia.

Článok 5

Orgán pre TEMPEST

1. Bezpečnostné opatrenia TEMPEST sa zavádzajú na ochranu CIS, ktorými sa manipuluje s utajovanými skutočnosťami so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, a môžu sa zaviesť aj pre utajované skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED.

2. Orgán pre TEMPEST je zodpovedný za schválenie opatrení prijatých na ochranu proti vyzradeniu EUCI prostredníctvom neúmyselného elektronického vyžarovania.

3. Na žiadosť vlastníka systému CIS, ktorým sa manipuluje s EUCI, vydá orgán pre TEMPEST špecifikácie bezpečnostných opatrení TEMPEST podľa stupňa utajenia utajovaných skutočností.

4. Počas akreditácie zabezpečených priestorov a CIS na manipuláciu s EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším vykoná orgán pre TEMPEST technické testovanie a po úspešnom testovaní vydá osvedčenie TEMPEST.

5. V osvedčení TEMPEST sa uvedie minimálne:

a) dátum testovania;

b) opis bezpečnostných opatrení TEMPEST s plánmi priestorov;

c) dátum skončenia platnosti osvedčenia;

d) všetky zmeny, ktoré spôsobia neplatnosť certifikácie;

e) podpis orgánu pre TEMPEST.

6. Miestny bezpečnostný úradník alebo organizátor zasadnutia zodpovedný za organizáciu utajovaného zasadnutia v koordinácii s miestnym bezpečnostným úradníkom môže požiadať orgán pre TEMPEST o otestovanie zasadacích miestností s cieľom zaistiť, aby boli technicky zabezpečené.

Článok 6

Kryptografický schvaľovací orgán

1. Kryptografický schvaľovací orgán je zodpovedný za schvaľovanie používania šifrovacích technológií.

2. Kryptografický schvaľovací orgán vydáva usmernenia týkajúce sa požiadaviek na používanie a schvaľovanie šifrovacích technológií.

3. Kryptografický schvaľovací orgán schvaľuje používanie šifrovacích riešení na základe žiadosti vlastníka systému. Schválenie sa zakladá na uspokojivom vyhodnotení prinajmenšom:

a) potrieb týkajúcich sa bezpečnosti informácií, ktoré sa majú chrániť;

b) prehľadu CIS zahrnutých v riešení;

c) posúdenia inherentných a zvyškových rizík;

d) opisu navrhovaného riešenia;

e) operačných bezpečnostných postupov pre šifrovacie riešenie.

4. Kryptografický schvaľovací orgán vedie register schválených šifrovacích riešení.

Článok 7

Kryptografický distribučný orgán

1. Kryptografický distribučný orgán je zodpovedný za distribúciu kryptografických materiálov používaných na ochranu EUCI (najmä šifrovacích zariadení, kryptografických kľúčov, certifikátov a súvisiacich autentifikátorov):

a) používateľom alebo oddeleniam v rámci Komisie v prípade CIS, ktoré spravujú externé strany;

b) používateľom alebo organizáciám mimo Komisie v prípade CIS, ktoré spravuje Komisia.

2. Kryptografický distribučný orgán môže distribúciu kryptografických materiálov tretím stranám delegovať na iné oddelenia v súlade s článkom 17 ods. 3 rozhodnutia 2015/443.

3. Kryptografický distribučný orgán zabezpečí, aby sa všetky kryptografické materiály posielali bezpečnými kanálmi, ktoré chránia pred neoprávnenou manipuláciou a upozorňujú na ňu, v súlade s bezpečnostnými pravidlami platnými pre stupeň utajenia EUCI, ktoré budú uvedenými materiálmi chránené.

4. Kryptografický distribučný orgán poskytuje usmernenia miestnemu bezpečnostnému úradníkovi a prípadne miestnemu úradníkovi informačnej bezpečnosti každého oddelenia Komisie, ktoré sa podieľa na výrobe, distribúcii alebo používaní kryptografických materiálov.

5. Kryptografický distribučný orgán zabezpečí, aby boli pre proces distribúcie vytvorené vhodné operačné bezpečnostné postupy.

KAPITOLA 3

Oddelenia Komisie

Článok 8

Vedúci oddelenia

1. Každý vedúci oddelenia vymenuje:

a) miestneho bezpečnostného úradníka a v prípade potreby jedného alebo viacerých zástupcov pre oddelenie alebo kabinet;

b) kontrolného úradníka registra a v prípade potreby jedného alebo viacerých zástupcov pre každé oddelenie, ktoré prevádzkuje register EUCI;

c) vlastníka systému pre každý CIS, ktorým sa manipuluje s EUCI.

2. Vedúci oddelenia pred vymenovaním miestneho bezpečnostného úradníka, jeho zástupcov, kontrolného úradníka registra a jeho zástupcov požiada o súhlas riaditeľa riaditeľstva pre bezpečnosť na Generálnom riaditeľstve pre ľudské zdroje a bezpečnosť.

3. Vedúci oddelenia po porade s miestnym bezpečnostným úradníkom určí všetky pozície, na ktorých sa vyžaduje previerka na prístup k EUCI. Uchádzači o takéto pozície sú o požiadavke na previerku informovaní počas výberového konania.

4. Vedúci každého oddelenia, ktoré drží EUCI, je zodpovedný za aktiváciu plánov núdzovej evakuácie a likvidácie v prípade potreby. Plány zahŕňajú alternatívu pre prípad, keď nie je možné kontaktovať vedúceho oddelenia.

Článok 9

Vlastníci systémov CIS, ktorými sa manipuluje s EUCI

1. Vlastník systému kontaktuje bezpečnostný akreditačný orgán v čo najskoršej fáze projektu zavádzania CIS, ktorým sa manipuluje s EUCI, aby bolo možné určiť príslušné bezpečnostné normy a požiadavky a začať proces bezpečnostnej akreditácie.

2. Vlastník systému zabezpečí, aby bezpečnostné opatrenia spĺňali požiadavky bezpečnostného akreditačného orgánu a aby sa prostredníctvom CIS nemanipulovalo s EUCI skôr, ako získa akreditáciu.

3. Vlastník systému sa obráti na kryptografický schvaľovací orgán, aby získal súhlas na používanie šifrovacích technológií. Vlastníci systémov nesmú šifrovacie technológie prevádzkovať v produkčných systémoch bez predchádzajúceho schválenia.

4. Vlastník systému konzultuje záležitosti týkajúce sa bezpečnosti CIS s miestnym úradníkom informačnej bezpečnosti oddelenia.

5. Vlastník systému aspoň raz ročne preskúma bezpečnostné opatrenia, ktoré sa uplatňujú na systém, vrátane bezpečnostného plánu.

6. Ak sa v CIS vyskytne bezpečnostný incident, pri ktorom sa ukáže, že CIS už nemôže primerane chrániť EUCI, vlastník systému informuje miestneho bezpečnostného úradníka a bezodkladne kontaktuje bezpečnostný akreditačný orgán, aby mu poradil, ako postupovať. V takom prípade sa môže akreditácia pozastaviť a systém vyradiť z prevádzky, až kým sa neprijmú vhodné nápravné opatrenia.

7. Vlastník systému vždy poskytuje bezpečnostnému akreditačnému orgánu plnú podporu pri plnení jeho povinností súvisiacich s akreditáciou CIS.

Článok 10

Operačný orgán pre informačnú bezpečnosť

Operačný orgán pre informačnú bezpečnosť pre každý CIS:

a) vypracúva v rámci procesu akreditácie CIS bezpečnostnú dokumentáciu v súlade s bezpečnostnými politikami a usmerneniami, najmä bezpečnostný plán, operačné bezpečnostné postupy súvisiace so systémom a kryptografickú dokumentáciu;

b) zúčastňuje sa na výbere a testovaní technických bezpečnostných opatrení, zariadení a softvéru špecifických pre daný systém, zaisťuje dohľad nad ich zavádzaním a zabezpečuje ich bezpečnú inštaláciu, konfiguráciu a údržbu v súlade s príslušnou bezpečnostnou dokumentáciou;

c) podieľa sa na výbere bezpečnostných opatrení a zariadení TEMPEST, ak sa to v bezpečnostnom pláne vyžaduje, a v spolupráci s orgánom pre TEMPEST zaisťuje ich bezpečnú inštaláciu a údržbu;

d) monitoruje vykonávanie a uplatňovanie operačných bezpečnostných postupov súvisiacich s prevádzkou systému;

e) v spolupráci s kryptografickým distribučným orgánom spravuje kryptografické produkty a manipuluje s nimi s cieľom zabezpečiť riadnu úschovu kryptografických materiálov a kontrolovaných položiek a v prípade potreby zabezpečuje generovanie kryptografických premenných parametrov;

f) vykonáva bezpečnostné analytické previerky a testy najmä s cieľom vypracovať príslušné správy o rizikách v zmysle požiadaviek bezpečnostného akreditačného orgánu;

g) poskytuje odbornú prípravu o informačnej bezpečnosti špecifickú pre CIS;

h) zavádza a prevádzkuje bezpečnostné opatrenia špecifické pre CIS.

KAPITOLA 4

Miestny bezpečnostný úradník

Článok 11

Vymenovanie miestneho bezpečnostného úradníka

1. Miestny bezpečnostný úradník a jeho zástupcovia sú úradníkmi alebo dočasnými zamestnancami.

2. Všetci miestni bezpečnostní úradníci a ich zástupcovia majú platné bezpečnostné oprávnenie na prístup k EUCI po stupeň utajenia SECRET UE/EU SECRET a v prípade potreby až po stupeň utajenia TRÈS SECRET UE/EU TOP SECRET. Miestny bezpečnostný úradník alebo jeho zástupca získa bezpečnostné oprávnenie pred svojím vymenovaním.

3. Zastúpenia Komisie môžu požiadať bezpečnostný orgán Komisie o udelenie výnimky z požiadaviek uvedených v odsekoch 1 a 2.

Článok 12

Bezpečnostné prevádzkové postupy pre zabezpečené priestory

1. Miestny bezpečnostný úradník príslušného oddelenia Komisie vypracuje operačné bezpečnostné postupy pre každý zabezpečený priestor, za ktorý zodpovedá.

2. Miestny bezpečnostný úradník zaistí, aby operačné bezpečnostné postupy zahŕňali tieto požiadavky:

a) prístup do zabezpečeného priestoru bez sprievodu počas úradných hodín majú povolený len zamestnanci s platným bezpečnostným oprávnením a preukázanou potrebou prístupu k dokumentom so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším;

b) prístup do zabezpečeného priestoru bez sprievodu mimo úradných hodín je povolený len miestnemu bezpečnostnému úradníkovi oddelenia, kontrolným úradníkom registra zabezpečeného priestoru, ich zástupcom a oprávneným zamestnancom z riaditeľstva pre bezpečnosť na Generálnom riaditeľstve pre ľudské zdroje a bezpečnosť;

c) nahrávacie a komunikačné zariadenia, ako sú mobilné telefóny, počítače, fotoaparáty alebo iné inteligentné zariadenia, nie sú bez predchádzajúceho povolenia bezpečnostného orgánu Komisie vnútri zabezpečených priestorov povolené; o akúkoľvek výnimku je potrebné vopred požiadať bezpečnostný orgán Komisie; miestny bezpečnostný úradník vystupuje ako kontaktná osoba;

d) všetci interní alebo externí zamestnanci, ktorí potrebujú prístup do zabezpečeného priestoru, ale nespĺňajú kritériá uvedené v písmene a), musia mať nepretržitý sprievod a sú pod neustálym dohľadom riadne oprávneného zamestnanca; každý takýto prístup do zabezpečeného priestoru sa zaznamenáva do denníka, ktorý sa nachádza pri vstupe do zabezpečeného priestoru;

e) miestny bezpečnostný úradník zabezpečí, aby boli systémy detekcie narušenia monitorujúce zabezpečený priestor vždy aktívne a riadne funkčné, a spravuje všetky súvisiace heslá, kľúče, PIN kódy alebo iné prístupové a overovacie mechanizmy.

f) poplachy v zabezpečenom priestore sa hlásia riaditeľstvu pre bezpečnosť na Generálnom riaditeľstve pre ľudské zdroje a bezpečnosť, ktoré o tom bezodkladne informuje miestneho bezpečnostného úradníka;

g) miestny bezpečnostný úradník oddelenia, v ktorom sa nachádza zabezpečený priestor, vedie záznamy o každom zásahu po poplachu alebo bezpečnostnom incidente;

h) musia byť zavedené postupy v prípade poplachu alebo inej núdzovej situácie v zabezpečenom priestore vrátane evakuácie zamestnancov a zabezpečenia rýchlej reakcie pohotovostného tímu pod vedením bezpečnostného orgánu Komisie a v prípade potreby aj externých pohotovostných služieb;

i) miestny bezpečnostný úradník bezodkladne oznámi bezpečnostnému orgánu Komisie každé narušenie bezpečnosti, ku ktorému dôjde vnútri zabezpečeného priestoru alebo ktoré sa ho týka, s cieľom určiť vhodnú reakciu;

j) jednotlivé kancelárie, miestnosti a trezory v rámci zabezpečeného priestoru musia byť uzamknuté vždy, keď sú ponechané bez dozoru;

k) zamestnanci sa vyhýbajú diskusiám o utajovaných skutočnostiach na chodbách alebo v iných spoločných priestoroch zabezpečeného priestoru, ak sa v ich blízkosti nachádzajú neoprávnené osoby.

Článok 13

Bezpečnostné kľúče a kombinácie

1. Miestny bezpečnostný úradník nesie celkovú zodpovednosť za zabezpečenie správnej manipulácie s kľúčmi a kombináciami používanými v zabezpečených priestoroch alebo na prístup do nich, ako aj za ich úschovu. Kľúče a kombinácie sú uložené v bezpečnostnej schránke a chránené minimálne na rovnakej úrovni ako materiál, ku ktorému umožňujú prístup.

2. Miestny bezpečnostný úradník vedie register bezpečnostných schránok a komorových trezorov spolu s aktuálnym zoznamom všetkých zamestnancov, ktorí do nich majú prístup bez sprievodu.

3. Miestny bezpečnostný úradník vedie register kľúčov od bezpečnostných schránok a komorových trezorov vrátane zoznamu zamestnancov, ktorým sú pridelené. Pre každý vydaný kľúč sa uchováva potvrdenie o jeho prevzatí, ktoré obsahuje identifikáciu kľúča, príjemcu, dátum a čas.

4. Kľúče a kombinácie sa vydávajú len zamestnancom, ktorí sa s utajovanými informáciami potrebujú oboznámiť a ktorým bolo udelené náležité povolenie na prístup k EUCI. Ak uvedené podmienky už nie sú splnené, miestny bezpečnostný úradník daný kľúč odoberie.

5. Miestny bezpečnostný úradník uchováva náhradné kľúče a písomný záznam o všetkých nastavených kombináciách v samostatných zapečatených, nepriehľadných a podpísaných obálkach s označením dátumu, ktoré mu poskytne zamestnanec zodpovedný za kľúče. Uvedené obálky sú uložené v bezpečnostnej schránke, ktorej ochrana zodpovedá najvyššiemu stupňu utajenia materiálu uloženého v príslušnej schránke alebo komorovom trezore.

6. Ak pri zmene kombinácie alebo rotácii kľúčov obálka vykazuje známky neoprávnenej manipulácie alebo poškodenia, miestny bezpečnostný úradník to považuje za bezpečnostný incident a okamžite informuje bezpečnostný orgán Komisie.

7. Zmeny nastavených kombinácií bezpečnostných schránok v zabezpečených priestoroch sa vykonávajú pod dohľadom miestneho bezpečnostného úradníka. Kombinácie sa menia najmenej každých 12 mesiacov a vždy, keď:

a) je prijatá nová schránka alebo sa nainštaluje nový zámok (okamžite sa zmenia najmä predvolené kombinácie);

b) existuje podozrenie na vyzradenie alebo k nemu došlo;

c) osoba, ktorá pozná kombináciu, už nepotrebuje prístup.

8. Miestny bezpečnostný úradník vedie záznamy o dátumoch zmien kombinácií uvedených v odseku 7.

Článok 14

Plány núdzovej evakuácie a ničenia EUCI

1. Miestny bezpečnostný úradník pomáha vedúcemu oddelenia pri vypracúvaní plánov núdzovej evakuácie a ničenia EUCI na základe usmernení riaditeľstva pre bezpečnosť.

2. Miestny bezpečnostný úradník zabezpečí, aby bolo všetko vybavenie potrebné na fungovanie plánov uvedených v odseku 1 ľahko dostupné a udržiavané v dobrom stave.

3. Miestny bezpečnostný úradník spolu s úradníkmi vymenovanými v plánoch ustanovených v odseku 1 aspoň raz za 12 mesiacov preskúma stav pripravenosti plánov a prijme všetky opatrenia potrebné na ich aktualizáciu.

Článok 15

Bezpečnostné oprávnenia

1. Miestny bezpečnostný úradník vedie záznamy o všetkých pozíciách v rámci oddelenia, na ktorých sa vyžaduje bezpečnostné oprávnenie Komisie, a zamestnancoch, ktorí tieto pozície zastávajú. Požiadavka bezpečnostného oprávnenia musí byť uvedená v oznámení o voľnom pracovnom mieste počas výberového konania a oznámená uchádzačovi počas pohovoru.

2. Miestny bezpečnostný úradník dohliada na všetky žiadosti o bezpečnostné oprávnenia na prístup k EUCI. Miestny bezpečnostný úradník je kontaktnou osobou v rámci oddelenia a na bezpečnostných oprávneniach spolupracuje s bezpečnostným orgánom Komisie.

3. Miestny bezpečnostný úradník iniciuje žiadosť o začatie postupu bezpečnostného oprávnenia v súvislosti s príslušným zamestnancom a zabezpečí, aby zamestnanec bezodkladne odovzdal bezpečnostnému orgánu Komisie dotazník o národnej bezpečnostnej previerke.

4. Miestny bezpečnostný úradník zabezpečí, aby zamestnanci s bezpečnostnou previerkou v oddelení absolvovali povinné poučenie o EUCI s cieľom získať bezpečnostné oprávnenie.

5. Miestny bezpečnostný úradník pravidelne spolupracuje s útvarom ľudských zdrojov oddelenia, aby bol informovaný o všetkých zmenách na pozíciách, na ktorých sa vyžaduje bezpečnostné oprávnenie, a o každej takejto zmene bezodkladne informuje bezpečnostný orgán Komisie.

6. Miestny bezpečnostný úradník informuje bezpečnostný orgán Komisie o príchode nového zamestnanca s existujúcou bezpečnostnou previerkou, ktorý má nastúpiť na pozíciu vyžadujúcu bezpečnostné oprávnenie.

7. Miestny bezpečnostný úradník zabezpečí, aby zamestnanci oddelenia dokončili postup obnovenia bezpečnostnej previerky v požadovanom termíne. Každý zamestnanec, ktorý odmietne tento postup podstúpiť, je povinný prestúpiť na pozíciu, na ktorej sa nevyžaduje bezpečnostné oprávnenie zamestnanca.

Článok 16

Register EUCI

1. Ak oddelenie prevádzkuje register EUCI, miestny bezpečnostný úradník dohliada na činnosti kontrolných úradníkov registra týkajúce sa manipulácie s EUCI a dodržiavania bezpečnostných pravidiel ochrany EUCI.

2. Miestny bezpečnostný úradník vykonáva aspoň raz za 12 mesiacov a pri zmene kontrolného úradníka registra alebo jeho zástupcu tieto kontroly:

a) kontrolu vzorky dokumentov v registri EUCI s cieľom potvrdiť ich status a presnosť registra utajovaných dokumentov;

b) kontrolu vzorky potvrdení o prijatí a prenose EUCI do registra EUCI a z neho;

c) kontrola vzorky osvedčení o zničení.

3. Miestny bezpečnostný úradník aspoň raz mesačne vykonáva kontroly registra utajovaných dokumentov a nedávno prijatých utajovaných dokumentov na mieste s cieľom zabezpečiť správnu evidenciu dokumentov.

4. Všetky kontroly sa zaznamenávajú do denníka registra utajovaných dokumentov.

Článok 17

Ďalšie zodpovednosti v oblasti bezpečnosti

Ďalšie zodpovednosti miestneho bezpečnostného úradníka v oblasti bezpečnosti sú uvedené v bezpečnostnom oznámení a týkajú sa najmä fyzickej bezpečnosti osôb, priestorov a iného majetku, ako aj informácií.

KAPITOLA 5

Kontrolný úradník registra

Článok 18

Vymenovanie kontrolného úradníka registra

1. Kontrolný úradník registra a jeho zástupcovia sú úradníkmi alebo dočasnými zamestnancami.

2. Všetci kontrolní úradníci registra a ich zástupcovia majú platné bezpečnostné oprávnenie na prístup k EUCI po stupeň utajenia SECRET UE/EU SECRET a v prípade potreby až po stupeň utajenia TRÈS SECRET UE/EU TOP SECRET. Kontrolný úradník registra alebo jeho zástupca získa bezpečnostné oprávnenie pred svojím vymenovaním.

3. Zastúpenia Komisie môžu požiadať bezpečnostný orgán Komisie o udelenie výnimky z požiadaviek uvedených v odsekoch 1 a 2.

Článok 19

Povinnosti

1. Kontrolní úradníci registra zaevidujú utajované skutočnosti so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším na bezpečnostné účely:

a) keď sa doručia do oddelenia Komisie alebo keď ho opúšťajú, alebo

b) keď sa doručia do CIS alebo keď ho opúšťajú.

2. Kontrolní úradníci registra evidujú všetky udalosti v životnom cykle všetkých utajovaných skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším. Kontrolní úradníci registra takisto zabezpečia, aby sa viedli záznamy o všetkých utajovaných skutočnostiach so stupňom utajenia RESTREINT UE/EU RESTRICTED alebo jeho ekvivalentom, ktoré sa vymieňajú s tretími krajinami a medzinárodnými organizáciami. Toto sa vykonáva v koordinácii s registrom EUCI, ktorý spravuje generálny sekretariát.

3. Kontrolný úradník registra eviduje dokumenty so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším v registri utajovaných dokumentov a zabezpečuje ich bezpečné uchovávanie v rámci registra EUCI.

4. Kontrolný úradník registra pomáha zamestnancom Komisie pri vytváraní a odosielaní utajovaných skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším.

5. Ak sú dokumenty so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším prijaté z iných oddelení alebo od externých strán, kontrolný úradník registra zabezpečí riadne odovzdanie potvrdenia o doručení pôvodcovi.

6. Skôr ako kontrolný úradník registra umožní zamestnancovi prístup k utajovanému dokumentu, ktorý sa nachádza v registri EUCI, overí u miestneho bezpečnostného úradníka, či má zamestnanec bezpečnostné oprávnenie od bezpečnostného orgánu Komisie.

7. Kontrolný úradník registra eviduje vstup všetkých zamestnancov, ktorí nemajú oprávnenie na prístup bez sprievodu, do registra EUCI a odchod z neho a sprevádza ich počas celej návštevy.

8. Ak si zamestnanec vezme dokument na nahliadnutie mimo registra EUCI, kontrolný úradník registra zabezpečí, aby bol oboznámený s príslušnými náhradnými bezpečnostnými opatreniami a aby zamestnanec dokument vrátil hneď, keď ho už nebude potrebovať. Kontrolný úradník registra pripomenie zamestnancom, aby každý takýto dokument vrátili čo najskôr.

9. Ak sa utajované dokumenty fyzicky vynášajú z krajiny, v ktorej sa nachádza register, register EUCI vydá kuriérske osvedčenie.

10. Podrobné pokyny pre kontrolných úradníkov registra týkajúce sa evidencie utajovaných dokumentov sa uvedú v bezpečnostnom oznámení.

Článok 20

Zníženie stupňa utajenia a zrušenie utajenia

Kontrolný úradník registra pomáha oddeleniam, ktoré sú pôvodcami, pri preskúmaní evidovaných EUCI s cieľom zistiť, či je pôvodný stupeň utajenia stále vhodný alebo či je možné stupeň utajenia dokumentu znížiť, prípadne utajenie zrušiť.

Článok 21

Ničenie

1. Kontrolní úradníci registra sú zodpovední za zničenie utajovaných skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a vyšším, a to schválenými prostriedkami, prípadne za prítomnosti svedkov s bezpečnostnou previerkou.

2. Kontrolní úradníci registra evidujú každé zničenie utajovaných skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL v registri utajovaných dokumentov a uchovávajú príslušné protokoly o zničení v registri EUCI.

Článok 22

Ďalšie úlohy

1. Kontrolný úradník registra poskytuje miestnemu bezpečnostnému úradníkovi všetku potrebnú pomoc pri vykonávaní činností dohľadu v registri EUCI.

2. Kontrolný úradník registra hlási všetky podozrenia alebo skutočné bezpečnostné incidenty miestnemu bezpečnostnému úradníkovi, ktorý ich následne hlási bezpečnostnému orgánu Komisie.

3. Kontrolný úradník registra EUCI oddelenia Komisie, ktoré organizuje utajované zasadnutie na úrovni CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyššej, pripraví EUCI, s ktorými sa bude počas zasadnutia manipulovať, a koordinuje svoju činnosť s organizátorom zasadnutia s cieľom zabezpečiť, aby sa so všetkými dokumentmi a potvrdeniami manipulovalo v súlade s príslušnými pravidlami.

KAPITOLA 6

Záverečné ustanovenia

Článok 23

Transparentnosť

Toto rozhodnutie sa dá na vedomie zamestnancom Komisie a všetkým osobám, ktorých sa týka, a uverejní sa v *Úradnom vestníku Európskej únie*.

Článok 24

Toto rozhodnutie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

V Bruseli 7. apríla 2022

Za Komisiu
v mene predsedníčky
Gertrud INGESTAD
generálna riaditeľka
Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť