ROZHODNUTÍ KOMISE (EU) 2022/640

ze dne 7. dubna 2022

o prováděcích pravidlech pro úkoly a povinnosti hlavních bezpečnostních činitelů

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 249 této smlouvy,

s ohledem na rozhodnutí Komise (EU, Euratom) 2015/443 ze dne 13. března 2015 o bezpečnosti v Komisi ([1]),

s ohledem na rozhodnutí Komise (EU, Euratom) 2015/444 ze dne 13. března 2015 o bezpečnostních pravidlech na ochranu utajovaných informací EU ([2]),

vzhledem k těmto důvodům:

(1) Rozhodnutí (EU, Euratom) 2015/443 a (EU, Euratom) 2015/444 se použijí na všechny útvary Komise a ve všech prostorách Komise.

(2) Je-li to nezbytné, přijmou se v souladu s článkem 60 rozhodnutí (EU, Euratom) 2015/444 prováděcí pravidla, která toto rozhodnutí doplní či podpoří.

(3) Bezpečnostní opatření na ochranu utajovaných informací EU během celého jejich životního cyklu by měla být přiměřená zejména jejich stupni utajení.

(4) Bezpečnostní opatření pro ochranu komunikačních a informačních systémů v Komisi jsou vymezena v rozhodnutí Komise (EU, Euratom) 2017/46 ([3]), zejména v článku 3, pokud jde o zásady bezpečnosti IT v Komisi, a v článku 9, pokud jde o vlastníky systému.

(5) Cílem prováděcích pravidel pro úkoly a povinnosti hlavních bezpečnostních činitelů je poskytnout pokyny k předpokladům a povinnostem, které jsou vymezeny pro tyto úkoly v rozhodnutích (EU, Euratom) 2015/443 a (EU, Euratom) 2015/444.

(6) Ustanovení čl. 36 odst. 7 rozhodnutí (EU, Euratom) 2015/444 stanoví, že bezpečnostní orgán Komise působí jako orgán pro řadu dalších funkcí souvisejících s bezpečností. Úkoly související s těmito funkcemi jsou stanoveny v tomto rozhodnutí.

(7) Místní bezpečnostní úředníci a vedoucí registru mají zvláštní odpovědnost za ochranu utajovaných informací EU ve svých útvarech na základě rozhodnutí (EU, Euratom) 2015/444.

(8) Dne 4. května 2016 Komise přijala rozhodnutí ([4]), které zmocňuje člena Komise odpovědného za bezpečnostní otázky přijímat jménem Komise a na její odpovědnost prováděcí pravidla stanovená v článku 60 rozhodnutí (EU, Euratom) 2015/444; následně dne 13. dubna 2021 přijal člen Komise odpovědný za bezpečnostní otázky jménem Komise a na její odpovědnost rozhodnutí ([5]), kterým se tato prováděcí pravidla dále přenášejí do pravomoci generálního ředitele Generálního ředitelství pro lidské zdroje a bezpečnost,

([1]) Úř. věst. L 72, 17.3.2015, s. 41.
([2]) Úř. věst. L 72, 17.3.2015, s. 53.
([3]) Rozhodnutí Komise (EU, Euratom) 2017/46 ze dne 10. ledna 2017 o bezpečnosti komunikačních a informačních systémů v Evropské komisi (Úř. věst. L 6, 11.1.2017, s. 40).
([4]) Rozhodnutí C(2016) 2797 final ze dne 4. května 2016 o zmocnění týkajícím se bezpečnosti.
([5]) Rozhodnutí C(2021) 2684 final ze dne 13. dubna 2021 o dalším přenesení pravomocí udělených rozhodnutím Komise C(2016) 2797 o zmocnění týkajícím se bezpečnosti.

PŘIJALA TOTO ROZHODNUTÍ:

KAPITOLA 1

Obecná ustanovení

Článek 1

Předmět a oblast působnosti

1. Toto rozhodnutí stanoví úkoly a povinnosti hlavních bezpečnostních činitelů odpovědných za ochranu utajovaných informací EU v Komisi dle rozhodnutí (EU, Euratom) 2015/443 a (EU, Euratom) 2015/444.

2. Toto rozhodnutí se použije na všechny útvary Komise a ve všech prostorách Komise.

KAPITOLA 2

Generální ředitelství pro lidské zdroje a bezpečnost

Článek 2

Bezpečnostní orgán Komise

1. Ředitel ředitelství pro bezpečnost Generálního ředitelství pro lidské zdroje a bezpečnost je bezpečnostním orgánem Komise ve smyslu článku 7 rozhodnutí (EU, Euratom) 2015/444.

2. Bezpečnostní orgán Komise vykonává své funkce dle rozhodnutí (EU, Euratom) 2015/444 a v souladu s články 3 a 7 tohoto rozhodnutí v těchto oblastech:

a) personální bezpečnost;

b) fyzická bezpečnost;

c) správa utajovaných informací EU;

d) akreditace jakýchkoli komunikačních a informačních systémů nakládajících s utajovanými informacemi EU;

e) průmyslová bezpečnost a

f) výměna utajovaných informací.

3. Bezpečnostní orgán Komise poskytne místním bezpečnostním úředníkům, zástupcům místních bezpečnostních úředníků, vedoucím registru a zástupcům vedoucích registru povinné školení týkající se jejich povinností a úkolů.

Článek 3

Orgán pro zabezpečení informací

Orgán pro zabezpečení informací je odpovědný za tyto činnosti ve vztahu k ochraně utajovaných informací EU:

a) vypracování bezpečnostních politik a pokynů pro zabezpečení informací a sledování jejich účinnosti a relevantnosti;

b) zajištění a správa technických informací týkajících se kryptografických prostředků;

c) zajištění, aby opatření pro zabezpečení informací byla v souladu s bezpečnostními politikami Komise a politikami Komise pro zadávání veřejných zakázek;

d) zajištění, aby volba kryptografických prostředků byla v souladu s politikami, jimiž se řídí jejich způsobilost a výběr;

e) konzultování vlastníků systémů, poskytovatelů systémů, bezpečnostních činitelů a zástupců uživatelů, pokud jde o bezpečnostní politiky a pokyny pro zabezpečení informací.

Článek 4

Orgán pro bezpečnostní akreditaci

1. Bezpečnostní orgán Komise odpovídá za akreditaci zabezpečených oblastí, které splňují požadavky dle článku 18 rozhodnutí 2015/444 a požadavky na komunikační a informační systémy nakládající s utajovanými informacemi EU.

2. Útvary Komise konzultují podle potřeby orgán pro bezpečnostní akreditaci v koordinaci s jejich místními bezpečnostními úředníky a jejich úředníky pro bezpečnost informatiky na místní úrovni, kdykoli má útvar v úmyslu:

a) vybudovat zabezpečenou oblast;

b) zavést komunikační a informační systém nakládající s utajovanými informacemi EU;

c) instalovat jakékoli jiné vybavení pro nakládání s utajovanými informacemi, včetně připojení ke komunikačním a informačním systémům třetí strany.

Orgán pro bezpečnostní akreditaci poskytuje poradenství ohledně těchto činností, a to během plánování a stavebních nebo vývojových procesů.

3. S utajovanými informacemi EU se v zabezpečené oblasti nebo komunikačním a informačním systému nenakládá dříve, než orgán pro bezpečnostní akreditaci vydá akreditaci na příslušné úrovni utajovaných informací EU.

4. Požadavky na akreditaci zabezpečené oblasti zahrnují:

a) schválení plánů pro zabezpečenou oblast;

b) schválení zakázek na práce prováděné externími zhotoviteli, s přihlédnutím k ustanovením o průmyslové bezpečnosti, jako jsou požadavky na bezpečnostní prověrky zhotovitelů a jejich zaměstnanců;

c) dostupnost všech požadovaných prohlášení a osvědčení o shodě;

d) fyzickou prohlídku zabezpečené oblasti s cílem ověřit, zda stavební materiály a metody, kontroly přístupu, bezpečnostní vybavení a jakékoli jiné položky splňují požadavky vydané příslušným bezpečnostním orgánem Komise;

e) ověření protiopatření proti elektromagnetickému záření pro každou technicky zabezpečenou oblast;

f) schválení bezpečnostních provozních postupů pro zabezpečenou oblast.

5. Požadavky na akreditaci komunikačního a informačního systému nakládajícího s utajovanými informacemi EU zahrnují:

a) vytvoření strategie pro akreditaci systému;

b) schválení bezpečnostního plánu komunikačního a informačního systému na základě přístupu k řízení rizik;

c) schválení bezpečnostních provozních postupů pro komunikační a informační systém;

d) schválení všech ostatních požadovaných bezpečnostních dokumentací stanovených orgánem pro bezpečnostní akreditaci;

e) schválení jakéhokoli používání šifrovacích technologií;

f) ověření protiopatření proti elektromagnetickému záření pro komunikační a informační systém, který nakládá s informacemi se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším;

g) kontrolu komunikačního a informačního systému s cílem ověřit, zda jsou doložená bezpečnostní opatření správně provedena.

6. Po úspěšném splnění požadavků na akreditaci vydá orgán pro bezpečnostní akreditaci formální oprávnění k nakládání s utajovanými informacemi EU v zabezpečené oblasti nebo komunikačním a informačním systému, pro stanovený maximální stupeň utajení utajovaných informací EU a na dobu až pěti let v závislosti na úrovni utajení informací EU, s nimiž se nakládá, a na souvisejících rizicích.

7. Po oznámení narušení bezpečnosti nebo při významné změně koncepce nebo bezpečnostních opatření zabezpečené oblasti nebo komunikačního a informačního systému orgán pro bezpečnostní akreditaci přezkoumá oprávnění k nakládání s utajovanými informacemi EU a v případě potřeby je může zrušit, a to dokud nebudou napraveny jakékoli zjištěné nedostatky.

Článek 5

Orgán TEMPEST

1. Na ochranu komunikačních a informačních systémů, které nakládají s informacemi se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším, se zavedou bezpečnostní opatření TEMPEST; tato opatření mohou být zavedena i u informací se stupněm utajení RESTREINT UE/EU RESTRICTED.

2. Orgán TEMPEST odpovídá za schvalování opatření přijatých na ochranu před ohrožením utajovaných informací EU kompromitujícím elektronickým vyzařováním.

3. Na žádost vlastníka komunikačního a informačního systému nakládajícího s utajovanými informacemi EU vydá orgán TEMPEST specifikace pro bezpečnostní opatření TEMPEST, pokud je to vhodné pro stupeň utajení těchto informací.

4. Orgán TEMPEST provádí technické testování během akreditace zabezpečených oblastí a komunikačních a informačních systémů pro nakládání s utajovanými informacemi EU se stupněm utajení CONFIDENTIAL UE/EU CONFIDENTIAL nebo vyšším a po úspěšném testování vydá certifikát TEMPEST.

5. Certifikát TEMPEST musí obsahovat alespoň:

a) datum zkoušky;

b) popis bezpečnostních opatření TEMPEST s plány prostor;

c) datum ukončení platnosti certifikátu;

d) jakékoli změny, které zneplatní certifikaci;

e) podpis oprávněné osoby orgánu TEMPEST.

6. Místní bezpečnostní úředník nebo organizátor jednání odpovědný za organizaci neveřejného jednání ve spolupráci s místním bezpečnostním úředníkem může požádat orgán TEMPEST, aby otestoval zasedací místnosti s cílem zajistit, aby byly technicky zabezpečené.

Článek 6

Schvalovací orgán pro kryptografickou ochranu

1. Schvalovací orgán pro kryptografickou ochranu odpovídá za schvalování používání šifrovacích technologií.

2. Schvalovací orgán pro kryptografickou ochranu vydá pokyny týkající se požadavků na používání a schvalování šifrovacích technologií.

3. Schvalovací orgán pro kryptografickou ochranu schvaluje používání šifrovacích řešení na základě žádosti vlastníka systému. Schválení musí být založeno na uspokojivém vyhodnocení alespoň:

a) bezpečnostních potřeb u informací, které mají být chráněny;

b) přehledu komunikačních a informačních systémů zapojených do řešení;

c) posouzení inherentních a zbytkových rizik;

d) popisu navrhovaného řešení;

e) bezpečnostních provozních postupů pro šifrovací řešení.

4. Schvalovací orgán pro kryptografickou ochranu vede registr schválených šifrovacích řešení.

Článek 7

Orgán pro distribuci kryptografických materiálů

1. Orgán pro distribuci kryptografických materiálů odpovídá za distribuci kryptografických materiálů používaných k ochraně utajovaných informací EU (především šifrovacího zařízení, kryptografických klíčů, certifikátů a souvisejících ověřovacích prostředků) těmto subjektům:

a) uživatelům nebo útvarům v rámci Komise, pokud jde o komunikační a informační systémy, které jsou spravovány externími stranami;

b) uživatelům nebo organizacím mimo Komisi, pokud jde o komunikační a informační systémy, které jsou spravovány Komisí.

2. Orgán pro distribuci kryptografických materiálů může v souladu s čl. 17 odst. 3 rozhodnutí 2015/443 přenést odpovědnost za distribuci kryptografických materiálů třetím osobám na jiné útvary.

3. Orgán pro distribuci kryptografických materiálů zajistí, aby všechny kryptografické materiály byly zasílány zabezpečenými kanály, které chrání proti jakýmkoli manipulacím a jsou schopné takové manipulace prokázat, v souladu s bezpečnostními pravidly platnými pro stupeň utajení utajovaných informací EU, které budou těmito materiály chráněny.

4. Orgán pro distribuci kryptografických materiálů poskytne pokyny místnímu bezpečnostnímu úředníkovi a případně úředníkovi pro bezpečnost informatiky na místní úrovni každého útvaru Komise, který se podílí na výrobě, distribuci nebo používání kryptografických materiálů.

5. Orgán pro distribuci kryptografických materiálů zajistí, aby byly pro distribuční proces zavedeny vhodné bezpečnostní provozní postupy.

KAPITOLA 3

Útvary Komise

Článek 8

Vedoucí útvaru

1. Každý vedoucí útvaru jmenuje:

a) místního bezpečnostního úředníka a případně jednoho nebo více zástupců pro útvar nebo kabinet;

b) vedoucího registru a případně jednoho nebo více zástupců pro každý útvar, který vede registr utajovaných informací EU;

c) vlastníka každého komunikačního a informačního systému nakládajícího s utajovanými informacemi EU.

2. Vedoucí útvaru požádá před jmenováním místních bezpečnostních úředníků, zástupců místních bezpečnostních úředníků, vedoucích registru a zástupců vedoucích registru o schválení ředitele ředitelství pro bezpečnost Generálního ředitelství pro lidské zdroje a bezpečnost.

3. Vedoucí útvaru určí po konzultaci s místním bezpečnostním úředníkem všechny pracovní pozice vyžadující prověrku pro přístup k utajovaným informacím EU. Uchazeči o takové pracovní pozice musí být během přijímacího řízení informováni o požadavku na prověrku.

4. Vedoucí každého útvaru, který drží utajované informace EU, odpovídá za aktivaci plánů na zničení a vyklizení v případech nouze, je-li to nezbytné. Plány musí obsahovat alternativu pro situace, kdy nelze kontaktovat vedoucího útvaru.

Článek 9

Vlastníci komunikačních a informačních systémů nakládajících s utajovanými informacemi EU

1. Vlastník systému kontaktuje orgán pro bezpečnostní akreditaci co nejdříve v rámci projektu zavedení komunikačního a informačního systému nakládajícího s utajovanými informacemi EU, aby bylo možné určit příslušné bezpečnostní standardy a požadavky a zahájit proces bezpečnostní akreditace.

2. Vlastník systému zajistí, aby bezpečnostní opatření splňovala požadavky orgánu pro bezpečnostní akreditaci a aby komunikační a informační systém nenakládal s utajovanými informacemi EU před tím, než bude akreditován.

3. Vlastník systému se musí před použitím jakékoli šifrovací technologie obrátit na schvalovací orgán pro kryptografickou ochranu s žádostí o schválení. Vlastníci systémů nesmí provozovat šifrovací technologie ve výrobních systémech bez předchozího schválení.

4. Vlastník systému konzultuje s úředníkem pro bezpečnost informatiky na místní úrovni daného útvaru záležitosti týkající se bezpečnosti komunikačních a informačních systémů.

5. Vlastník systému nejméně jednou ročně přezkoumá bezpečnostní opatření, která se týkají systému, včetně jeho bezpečnostního plánu.

6. Dojde-li v komunikačním a informačním systému k bezpečnostnímu incidentu, kdy je uvedeno, že daný komunikační a informační systém již nemůže náležitě chránit utajované informace EU, informuje o tom vlastník systému místního bezpečnostního úředníka a neprodleně se obrátí na orgán pro bezpečnostní akreditaci s žádostí o radu ohledně dalšího postupu. V takovém případě může být akreditace pozastavena a systém může být vyřazen z provozu, dokud nebudou přijata vhodná nápravná opatření.

7. Vlastník systému poskytuje orgánu pro bezpečnostní akreditaci vždy plnou podporu při plnění povinností orgánu souvisejících s akreditací komunikačního a informačního systému.

Článek 10

Provozní orgán pro zabezpečení informací

Provozní orgán pro zabezpečení informací pro každý komunikační a informační systém:

a) vytváří bezpečnostní dokumentaci v souladu s bezpečnostními politikami a pokyny, zejména bezpečnostním plánem, bezpečnostními provozními postupy souvisejícími se systémem a kryptografickou dokumentací v rámci akreditačního procesu komunikačního a informačního systému;

b) účastní se výběru a testování technických bezpečnostních opatření, zařízení a softwaru pro konkrétní systémy, dohlíží na jejich používání a zajišťuje jejich bezpečnou instalaci, konfiguraci a údržbu v souladu s příslušnou bezpečnostní dokumentací;

c) účastní se výběru bezpečnostních opatření a zařízení TEMPEST, pokud je to vyžadováno bezpečnostním plánem, a ve spolupráci s orgánem TEMPEST zajišťuje jejich bezpečnou instalaci a údržbu;

d) sleduje provádění a uplatňování bezpečnostních provozních postupů souvisejících s provozem systému;

e) ve spolupráci s orgánem pro distribuci kryptografických materiálů spravuje kryptografické prostředky a nakládá s nimi s cílem zajistit řádné uchování kryptografických materiálů a kontrolovaných položek a v případě potřeby zajišťuje vytváření kryptografických proměnných;

f) provádí bezpečnostní analýzy, přezkumy a testy, zejména za účelem vypracování příslušných zpráv o rizicích, jak požaduje orgán pro bezpečnostní akreditaci;

g) poskytuje školení v oblasti zabezpečení informací v komunikačních a informačních systémech;

h) zavádí bezpečnostní opatření u konkrétních komunikačních a informačních systémů a řídí jejich uplatňování.

KAPITOLA 4

Místní bezpečnostní úředník

Článek 11

Jmenování místního bezpečnostního úředníka

1. Místní bezpečnostní úředník a zástupci místních bezpečnostních úředníků jsou úředníci nebo dočasní zaměstnanci.

2. Všichni místní bezpečnostní úředníci a zástupci místních bezpečnostních úředníků jsou držiteli platného bezpečnostního oprávnění pro přístup k utajovaným informacím EU do stupně utajení SECRET UE/EU SECRET a v případě potřeby do stupně utajení TRES SECRET UE/EU TOP SECRET. Místní bezpečnostní úředník nebo zástupce místního bezpečnostního úředníka získá bezpečnostní oprávnění před svým jmenováním.

3. Zastoupení Komise mohou požádat bezpečnostní orgán Komise o udělení výjimky z požadavků stanovených v odstavcích 1 a 2.

Článek 12

Bezpečnostní provozní postupy pro zabezpečené oblasti

1. Místní bezpečnostní úředník příslušného útvaru Komise vypracuje bezpečnostní provozní postupy pro každou zabezpečenou oblast, za kterou odpovídá.

2. Místní bezpečnostní úředník zajistí, aby bezpečnostní provozní postupy obsahovaly tyto náležitosti:

a) přístup bez doprovodu do zabezpečené oblasti během úředních hodin je povolen pouze zaměstnancům s platným bezpečnostním oprávněním a prokázanou potřebou přístupu k dokumentům se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším;

b) přístup bez doprovodu do zabezpečené oblasti mimo úřední hodiny se umožní pouze místním bezpečnostním úředníkům útvaru, vedoucím registru zabezpečené oblasti, jejich zástupcům a pověřeným zaměstnancům ředitelství pro bezpečnost Generálního ředitelství pro lidské zdroje a bezpečnost;

c) záznamové a komunikační přístroje, jako jsou mobilní telefony, počítače, kamery nebo jiná inteligentní zařízení, nejsou uvnitř zabezpečených oblastí povoleny bez předchozího povolení bezpečnostního orgánu Komise; o jakoukoli odchylku je třeba požádat bezpečnostní orgán Komise předem; místní bezpečnostní úředník působí jako kontaktní osoba;

d) všichni interní nebo externí zaměstnanci, kteří potřebují přístup do zabezpečené oblasti, avšak nesplňují kritéria stanovená výše v písmenu a), musí být neustále doprovázeni řádně oprávněným zaměstnancem, který zároveň vykonává dohled; jakýkoli takový přístup do zabezpečené oblasti se zaznamená do deníku vedeného u vstupu do zabezpečené oblasti;

e) místní bezpečnostní úředník zajistí, aby systémy detekce narušení monitorující zabezpečenou oblast byly vždy aktivní a řádně fungovaly, a spravuje všechna související hesla, klíče, kódy PIN nebo jiné přístupové a ověřovací mechanismy;

f) poplachy v zabezpečené oblasti se nahlašují bezpečnostnímu ředitelství Generálního ředitelství pro lidské zdroje a bezpečnost, které neprodleně informuje místního bezpečnostního úředníka;

g) místní bezpečnostní úředník útvaru, v němž se zabezpečená oblast nachází, vede záznamy o každém zásahu po poplachu nebo bezpečnostním incidentu;

h) musí být zavedeny postupy pro případ poplachu nebo jiné nouzové situace uvnitř zabezpečené oblasti, včetně evakuace personálu a zajištění rychlé reakce nouzového týmu pod dohledem bezpečnostního orgánu Komise a podle potřeby externích záchranných služeb;

i) místní bezpečnostní úředník neprodleně oznámí bezpečnostnímu orgánu Komise jakékoli narušení bezpečnosti, k němuž dojde uvnitř zabezpečené oblasti nebo které se této oblasti týká, aby mohla být stanovena vhodná reakce;

j) jednotlivé kanceláře, místnosti a trezory v zabezpečené oblasti musí být uzamčeny vždy, když jsou ponechány bez dozoru;

k) zaměstnanci se vyvarují hovoru o utajovaných informacích na chodbách nebo v jiných společných prostorech zabezpečené oblasti, jsou-li v blízkosti neoprávněné osoby.

Článek 13

Bezpečnostní klíče a kódy

1. Místní bezpečnostní úředník nese celkovou odpovědnost za zajištění řádného nakládání s klíči a kódy používanými v zabezpečených oblastech a za jejich uchovávání. Klíče a kódy musí být uloženy v bezpečnostním úschovném objektu a musí být chráněny alespoň na stejné úrovni jako materiál, k němuž umožňují přístup.

2. Místní bezpečnostní úředník vede registr bezpečnostních úschovných objektů a trezorových místností a aktualizovaný seznam všech zaměstnanců, kteří k nim mají přístup bez doprovodu.

3. Místní bezpečnostní úředník vede registr klíčů k bezpečnostním úschovným objektům a trezorovým místnostem, včetně registru zaměstnanců, kterým jsou přiděleny. U každého vydaného klíče se uchovává potvrzení, včetně identifikace klíče, příjemce, data a času.

4. Klíče a kódy se vydávají pouze zaměstnancům, kterým bylo uděleno příslušné oprávnění k přístupu k utajovaným informacím EU a kteří se s těmito informacemi potřebují seznámit. Pokud tyto podmínky již nejsou splněny, místní bezpečnostní úředník všechny klíče odebere zpět.

5. Místní bezpečnostní úředník uchovává náhradní klíče a písemný záznam o každém nastavení kódu v samostatných zapečetěných, neprůhledných, podepsaných a datovaných obálkách, které poskytne zaměstnanec odpovědný za klíče. Tyto obálky se uchovávají v bezpečnostním úschovném objektu, který je určen pro nejvyšší stupeň utajení materiálu, který je skladován v příslušném úschovném objektu nebo v trezorové místnosti.

6. Pokud je při změně kódu nebo střídání majitelů klíčů zjevné, že došlo k manipulaci s obálkou nebo jejímu poškození, místní bezpečnostní úředník takovou situaci posoudí jako bezpečnostní incident a neprodleně o tom informuje bezpečnostní orgán Komise.

7. Změny nastavení kódu bezpečnostních úschovných objektů v zabezpečených oblastech se provádějí pod dohledem místního bezpečnostního úředníka. Kódy se resetují nejméně každých 12 měsíců a vždy, když:

a) je přijat nový úschovný objekt nebo je instalován nový zámek (zejména výchozí kombinace se změní okamžitě);

b) existuje podezření na ohrožení nebo k němu došlo;

c) přístup osoby, která disponuje kódem, již není vyžadován.

8. Místní bezpečnostní úředník vede záznamy o datech změn kódu dle odstavce 7.

Článek 14

Plány na zničení a vyklizení v případech nouze pro utajované informace EU

1. Místní bezpečnostní úředník napomáhá vedoucímu útvaru při vypracování plánů pro utajované informace EU na zničení a vyklizení v případech nouze na základě pokynů poskytnutých ředitelstvím pro bezpečnost Generálního ředitelství pro lidské zdroje a bezpečnost.

2. Místní bezpečnostní úředník zajistí, aby veškerá vybavení nezbytná pro provádění plánů uvedených v odstavci 1 byla snadno dostupná a udržovaná v dobrém provozním stavu.

3. Místní bezpečnostní úředník spolu s úředníky jmenovanými v plánech uvedených v odstavci 1 alespoň jednou za dvanáct měsíců přezkoumá stav připravenosti plánů a přijme veškerá opatření nezbytná k jejich aktualizaci.

Článek 15

Bezpečnostní oprávnění

1. Místní bezpečnostní úředník vede záznamy o všech pracovních pozicích v rámci útvaru, které vyžadují bezpečnostní oprávnění Komise, a o personálu, který tyto pozice zaujímá. Požadavek na bezpečnostní oprávnění musí být uveden v oznámení o volném pracovním místě během výběrového řízení a musí být během pohovoru oznámen uchazeči.

2. Místní bezpečnostní úředník dohlíží na všechny žádosti o bezpečnostní oprávnění pro přístup k utajovaným informacím EU. Místní bezpečnostní úředník je kontaktní osobou v rámci útvaru a spolupracuje s bezpečnostním orgánem Komise, pokud jde o bezpečnostní oprávnění.

3. Místní bezpečnostní úředník zahájí žádost o zahájení řízení o bezpečnostním oprávnění pro dotčeného zaměstnance a zajistí, aby zaměstnanec neprodleně vrátil dotazník o vnitrostátní bezpečnostní prověrce bezpečnostnímu orgánu Komise.

4. Místní bezpečnostní úředník zajistí, aby se zaměstnanci útvaru, kteří prošli bezpečnostní prověrkou, zúčastnili povinné informativní schůze o utajovaných informacích EU za účelem získání bezpečnostního oprávnění.

5. Místní bezpečnostní úředník pravidelně spolupracuje se službou pro lidské zdroje útvaru pro informace ve věci všech změn na pracovních pozicích vyžadujících bezpečnostní oprávnění a neprodleně o každé takové změně informuje bezpečnostní orgán Komise.

6. Místní bezpečnostní úředník informuje bezpečnostní orgán Komise o příchodu nového zaměstnance, který má stávající bezpečnostní prověrku, aby mohl nastoupit na pracovní pozici, pro kterou se vyžaduje zaměstnanec s bezpečnostním oprávněním.

7. Místní bezpečnostní úředník zajistí, aby zaměstnanci útvaru prošli procesem obnovení bezpečnostní prověrky v požadované lhůtě. Zaměstnanec, který odmítne proces podstoupit, je povinen změnit pracovní pozici na pozici, pro kterou se nevyžaduje zaměstnanec s bezpečnostním oprávněním.

Článek 16

Registr utajovaných informací EU

1. Pokud útvar provozuje registr utajovaných informací EU, místní bezpečnostní úředník dohlíží na činnosti vedoucích registru, pokud jde o nakládání s utajovanými informacemi EU a dodržování bezpečnostních pravidel na ochranu utajovaných informací EU.

2. Místní bezpečnostní úředník provádí alespoň každých 12 měsíců a po změně vedoucího registru nebo zástupce vedoucího registru tyto kontroly:

a) kontrolu vzorku dokumentů v registru utajovaných informací EU s cílem potvrdit jejich status a přesnost registru utajovaných dokumentů;

b) kontrolu vzorku příjmů a potvrzení o přenosu informací u případů přenosu utajovaných informací EU do registru utajovaných informací EU a z něj;

c) kontrolu vzorku zápisů o zničení.

3. Nejméně jednou za měsíc provádí místní bezpečnostní úředník namátkové kontroly registru utajovaných dokumentů a nedávno obdržených utajovaných dokumentů, aby se ujistil, že dokumenty jsou řádně registrovány.

4. Všechny kontroly se zaznamenávají do deníku registru utajovaných dokumentů.

Článek 17

Další povinnosti v oblasti bezpečnosti

Další povinnosti místního bezpečnostního úředníka v oblasti bezpečnosti jsou stanoveny v bezpečnostním upozornění, které se týká zejména fyzické bezpečnosti osob, prostor a jiného majetku a informací.

KAPITOLA 5

Vedoucí registru

Článek 18

Jmenování vedoucího registru

1. Vedoucí registru a zástupci vedoucích registru jsou úředníci nebo dočasní zaměstnanci.

2. Všichni vedoucí registru a zástupci vedoucích registru jsou držiteli platného bezpečnostního oprávnění pro přístup k utajovaným informacím EU do stupně utajení SECRET UE/EU SECRET a v případě potřeby do stupně utajení TRES SECRET UE/EU TOP SECRET. Vedoucí registru nebo zástupce vedoucího registru získá bezpečnostní oprávnění před svým jmenováním.

3. Zastoupení Komise mohou požádat bezpečnostní orgán Komise o udělení výjimky z požadavků stanovených v odstavcích 1 a 2.

Článek 19

Povinnosti

1. Vedoucí registru registrují informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším pro bezpečnostní účely:

a) v okamžiku, kdy jsou doručeny do útvaru Komise nebo když jej opouští, nebo

b) v okamžiku, kdy jsou doručeny do komunikačního a informačního systému nebo když ho opouští.

2. Vedoucí registru registrují veškeré události v životním cyklu všech informací se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším. Vedoucí registru rovněž zajistí, aby byly uchovávány záznamy o všech informacích se stupněm utajení RESTREINT UE/EU RESTRICTED nebo s rovnocenným stupněm, které jsou vyměňovány se třetími státy a mezinárodními organizacemi. To se provádí v koordinaci s registrem utajovaných informací EU spravovaným generálním sekretariátem.

3. Vedoucí registru registruje dokumenty se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším v registru utajovaných dokumentů a zajišťují, aby byly bezpečně uloženy v registru utajovaných informací EU.

4. Vedoucí registru je nápomocen zaměstnancům Komise při vytváření a zasílání informací se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším.

5. Jsou-li dokumenty se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším obdrženy od jiných útvarů nebo externích subjektů, vedoucí registru zajistí, aby dodací list byl řádně vrácen původci.

6. Před tím, než vedoucí registru zaměstnanci umožní přístup k utajovanému dokumentu drženému v registru utajovaných informací EU, ověří u místního bezpečnostního úředníka, že zaměstnanec je bezpečnostním orgánem Komise bezpečnostně oprávněn.

7. Vedoucí registru vede záznam všech pracovníků, kteří vstupují do registru utajovaných informací EU a opouštějí jej a kteří nejsou oprávněni k přístupu bez doprovodu, a po dobu jejich návštěvy je doprovází.

8. Pokud zaměstnanec odnáší dokument k nahlédnutí mimo registr utajovaných informací EU, vedoucí registru se ujistí, že zaměstnanec ví o příslušných náhradních bezpečnostních opatřeních a že dokument vrátí, jakmile jej již nebude potřeba. Vedoucí registru připomene zaměstnancům, aby takový dokument co nejdříve vrátili.

9. Registr utajovaných informací EU vydá osvědčení kurýra, pokud jsou utajované dokumenty přenášeny mimo stát, v němž se registr nachází.

10. Podrobné pokyny pro vedoucí registru ohledně registrace utajovaných dokumentů jsou uvedeny v bezpečnostním upozornění.

Článek 20

Snížení stupně utajení a odtajnění

Vedoucí registru je nápomocen útvarům, které jsou původci, při přezkumu evidovaných utajovaných informací EU prováděného za účelem zjištění, zda je původní stupeň utajení stále vhodný nebo zda lze stupeň utajení dokumentu snížit nebo dokument odtajnit.

Článek 21

Zničení

1. Vedoucí registru odpovídají za zničení informací se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a vyšším schválenými prostředky, případně za přítomnosti bezpečnostně prověřených svědků.

2. Vedoucí registru zaznamenávají veškeré zničení informací se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a vyšším do registru utajovaných dokumentů a uchovávají odpovídající zápisy o zničení v registru utajovaných informací EU.

Článek 22

Další úkoly

1. Vedoucí registru poskytuje místnímu bezpečnostnímu úředníkovi vykonávajícímu dohled v registru utajovaných informací EU veškerou nezbytnou součinnost.

2. Vedoucí registru oznámí veškeré skutečné bezpečnostní incidenty nebo podezření na ně místnímu bezpečnostnímu úředníkovi, který je následně oznámí bezpečnostnímu orgánu Komise.

3. Vedoucí registru utajovaných informací EU útvaru Komise, který pořádá utajované jednání se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším, připraví utajované informace EU, s nimiž se bude nakládat během jednání, a koordinuje svou činnost s organizátorem jednání, aby bylo zajištěno, že se všemi dokumenty a potvrzeními bude nakládáno v souladu s příslušnými pravidly.

KAPITOLA 6

Závěrečná ustanovení

Článek 23

Transparentnost

Toto rozhodnutí se dá na vědomí zaměstnancům Komise a všem osobám, na které se vztahuje, a zveřejní se v *Úředním věstníku Evropské unie*.

Článek 24

Toto rozhodnutí vstupuje v platnost prvním dnem po vyhlášení v *Úředním věstníku Evropské unie*.

V Bruselu dne 7. dubna 2022.

Za Komisi,
jménem předsedkyně,
Gertrud INGESTAD
generální ředitelka
Generální ředitelství pro lidské zdroje a bezpečnost