ROZHODNUTIE KOMISIE (EÚ, Euratom) 2015/444

z 13. marca 2015

o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ

EURÓPSKA KOMISIA,

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

so zreteľom na Zmluvu o založení Európskeho spoločenstva pre atómovú energiu, a najmä na jej článok 106,

so zreteľom na Protokol č. 7 o výsadách a imunitách Európskej únie pripojený k zmluvám, a najmä na jeho článok 18,

keďže:

(1) Ustanovenia Komisie o bezpečnosti týkajúce sa ochrany utajovaných skutočností Európskej únie (European Union Classified Information – EUCI) sa musia prehodnotiť a aktualizovať, aby sa zohľadnil inštitucionálny, organizačný, prevádzkový a technologický vývoj.

(2) Európska komisia uzavrela dohody o otázkach bezpečnosti týkajúce sa jej najväčších pracovísk s vládami Belgicka, Luxemburska a Talianska ([1]).

(3) Komisia, Rada a Európska služba pre vonkajšiu činnosť sa zaviazali, že budú uplatňovať rovnaké bezpečnostné normy na ochranu EUCI.

(4) Je dôležité, aby sa v prípade potreby Európsky parlament a ostatné inštitúcie, agentúry, orgány alebo úrady EÚ zapojili do uplatňovania zásad, noriem a predpisov týkajúcich sa ochrany utajovaných skutočností, ktoré sú potrebné na ochranu záujmov Únie a jej členských štátov.

(5) Riadenie rizík týkajúcich sa EUCI sa uskutočňuje ako proces. Tento proces sa zameriava na určenie známych bezpečnostných rizík, stanovenie bezpečnostných opatrení na zníženie týchto rizík na prijateľnú úroveň v súlade so základnými zásadami a minimálnymi normami stanovenými v tomto rozhodnutí a na uplatňovanie týchto opatrení v súlade s koncepciou hĺbkovej ochrany. Účinnosť týchto opatrení sa priebežne vyhodnocuje.

(6) V Komisii sa pod fyzickou bezpečnosťou zameranou na ochranu utajených skutočností rozumie uplatňovanie fyzických a technických ochranných opatrení na zamedzenie neoprávneného prístupu k EUCI.

(7) Správa EUCI znamená uplatňovanie administratívnych opatrení na kontrolu EUCI počas ich životného cyklu s cieľom doplniť opatrenia stanovené v kapitolách 2, 3 a 5 tohto rozhodnutia, a tým pomôcť pri odradení od úmyselného alebo náhodného vyzradenia alebo straty takýchto utajovaných skutočností, pri zistení tohto vyzradenia alebo straty a pri obnove bezpečnosti. Takéto opatrenia sa týkajú najmä vytvárania, uchovávania, evidencie, rozmnožovania, prekladu, zníženia stupňa utajenia, zrušenia utajenia, prepravy a ničenia EUCI a dopĺňajú všeobecné predpisy o správe dokumentov Komisie (rozhodnutie 2002/47/ES, ESUO, Euratom ([2]) a rozhodnutie 2004/563/ES, Euratom ([3])).

([1]) Pozri „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité“ z 31. decembra 2004, „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois“ z 20. januára 2007 a „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale“ z 22. júla 1959.

([2]) Rozhodnutie Komisie 2002/47/ES, ESUO, Euratom z 23. januára 2002, ktorým sa mení a dopĺňa jej rokovací poriadok (Ú. v. ES L 21, 24.1.2002, s. 23).

([3]) Rozhodnutie Komisie 2004/563/ES, Euratom zo 7. júla 2004, ktorým sa mení a dopĺňa jej rokovací poriadok (Ú. v. EÚ L 251, 27.7.2004, s. 9).

(8) Týmto rozhodnutím nie je dotknuté:

a) nariadenie (Euratom) č. 3 ([1]);

b) nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 ([2]);

c) nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 ([3]);

d) nariadenie Rady (EHS, Euratom) č. 354/83 ([4]),

PRIJALA TOTO ROZHODNUTIE:

KAPITOLA 1

ZÁKLADNÉ ZÁSADY A MINIMÁLNE NORMY

Článok 1

Vymedzenie pojmov

Na účely tohto rozhodnutia sa uplatňuje toto vymedzenie pojmov:

1. „oddelenie Komisie“ je akékoľvek generálne riaditeľstvo či útvar Komisie alebo kabinet člena Komisie;

2. „kryptografický materiál“ sú kryptografické algoritmy, kryptografické hardvérové a softvérové moduly a produkty, ktoré obsahujú podrobnosti implementácie, ako aj príslušnú dokumentáciu a kryptografické kľúče;

3. „zrušenie utajenia“ je odňatie bezpečnostného utajenia;

4. „hĺbková ochrana“ je uplatňovanie škály bezpečnostných opatrení usporiadaných do viacerých ochranných úrovní;

5. „dokument“ je každá zaznamenaná informácia bez ohľadu na jej fyzickú podobu alebo vlastnosti;

6. „zníženie stupňa utajenia“ je zaradenie do nižšieho stupňa;

7. „manipulácia“ s EUCI je akýkoľvek úkon v súvislosti s EUCI, ktorý sa môže vykonať počas ich životného cyklu. Patrí sem vytváranie, evidencia, spracúvanie, preprava, zníženie stupňa utajenia, zrušenie utajenia a zničenie. V súvislosti s komunikačnými a informačnými systémami zahŕňa aj zber, zobrazenie, prenos a uchovávanie EUCI;

8. „držiteľ“ je riadne oprávnená osoba, u ktorej sa zistila potreba poznať EUCI a ktorá má v držbe položku EUCI, a preto zodpovedá za jej ochranu;

9. „vykonávacie predpisy“ je akýkoľvek súbor predpisov alebo bezpečnostných oznámení prijatý v súlade s kapitolou 5 rozhodnutia Komisie (EÚ, Euratom) 2015/443 ([5]);

10. „vec“ je akékoľvek médium, nosič dát alebo prístroj či zariadenie vyrobené alebo v procese výroby;

11. „pôvodca“ je inštitúcia, agentúra alebo orgán Únie, členský štát, tretí štát alebo medzinárodná organizácia, v ktorej právomoci sa utajované skutočnosti vytvorili a/alebo zaviedli do štruktúr Únie;

12. „objekt“ je všetok nehnuteľný alebo pridružený majetok a imanie Komisie;

([1]) Nariadenie (Euratom) č. 3 z 31. júla 1958, ktorým sa vykonáva článok 24 Zmluvy o založení Európskeho spoločenstva pre atómovú energiu (Ú. v. ES 17, 6.10.1958, s. 406).

([2]) Nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie (Ú. v. ES L 145, 31.5.2001, s. 43).

([3]) Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, 12.1.2001, s. 1).

([4]) Nariadenie Rady (EHS, Euratom) č. 354/83 z 1. februára 1983 o otvorení historických archívov Európskeho hospodárskeho spoločenstva a Európskeho spoločenstva pre atómovú energiu pre verejnosť (Ú. v. ES L 43, 15.2.1983, s. 1).

([5]) Rozhodnutie Komisie (EÚ, Euratom) 2015/443 zo 13. marca 2015 o bezpečnosti v Komisii (pozri stranu 41 tohto úradného vestníka).

13. „proces riadenia bezpečnostných rizík“ je celkový proces zameraný na určenie, kontrolu a minimalizáciu neistých udalostí, ktoré môžu mať vplyv na bezpečnosť organizácie alebo akýkoľvek systém, ktorý používa. Zahŕňa všetky činnosti vzťahujúce sa na riziká vrátane ich vyhodnocovania, zabezpečenia sa proti nim, akceptácie a oznamovania;

14. „služobný poriadok“ je Služobný poriadok úradníkov Európskej únie a Podmienky zamestnávania ostatných zamestnancov Únie stanovený nariadením Rady (EHS, Euratom, ESUO) č. 259/68 ([1]);

15. „hrozba“ je potenciálna príčina neželaného incidentu, ktorého výsledkom môže byť poškodenie organizácie alebo akéhokoľvek systému, ktorý používa; takéto hrozby môžu byť náhodné alebo úmyselné (so zlým úmyslom) a sú charakterizované prvkami hrozby, potenciálnymi cieľmi a metódami útoku;

16. „zraniteľnosť“ je slabá stránka akejkoľvek povahy, ktorú možno zneužiť v rámci jednej alebo viacerých hrozieb. Zraniteľnosť môže predstavovať opomenutie alebo sa môže týkať nedostatočnosti kontroly z hľadiska jej intenzity, úplnosti alebo súdržnosti a môže mať technickú, procesnú, fyzickú, organizačnú alebo prevádzkové povahu.

Článok 2

Predmet úpravy a rozsah pôsobnosti

1. Týmto rozhodnutím sa stanovujú základné zásady a minimálne normy bezpečnosti na ochranu EUCI.

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

3. Bez ohľadu na akékoľvek osobitné ustanovenia týkajúce sa konkrétnych skupín zamestnancov, sa toto rozhodnutie uplatňuje na členov Komisie, zamestnancov Komisie zamestnaných podľa služobného poriadku a Podmienok zamestnávania ostatných zamestnancov Európskych spoločenstiev, národných expertov vyslaných do Komisie, poskytovateľov služieb a ich zamestnancov, stážistov a všetky osoby s prístupom do budov Komisie alebo k ostatnému majetku, alebo na skutočnosti, s ktorými manipuluje Komisia.

4. Týmto rozhodnutím nie je dotknuté rozhodnutie 2002/47/ES, ESUO, Euratom a rozhodnutie 2004/563/ES, Euratom.

Článok 3

Vymedzenie utajovanej skutočnosti EÚ, stupne utajenia a označenia

1. „Utajovaná skutočnosť Európskej únie“ (European Union classified information – EUCI) je akákoľvek informácia alebo vec označená stupňom utajenia EÚ, ktorej neoprávnené zverejnenie by mohlo v rôznej miere poškodiť záujmy Európskej únie alebo jedného či viacerých jej členských štátov.

2. Utajované skutočnosti EÚ sa utajujú na jednom z týchto stupňov:

a) TRÈS SECRET UE/EU TOP SECRET: informácia alebo vec, ktorej neoprávnené zverejnenie by mohlo mimoriadne vážne poškodiť základné záujmy Európskej únie alebo jedného či viacerých jej členských štátov;

b) SECRET UE/EU SECRET: informácia alebo vec, ktorej neoprávnené zverejnenie by mohlo vážne poškodiť základné záujmy Európskej únie alebo jedného či viacerých jej členských štátov;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informácia alebo vec, ktorej neoprávnené zverejnenie by mohlo poškodiť základné záujmy Európskej únie alebo jedného či viacerých jej členských štátov;

d) RESTREINT UE/EU RESTRICTED: informácia alebo vec, ktorej neoprávnené zverejnenie by mohlo byť nevýhodné pre záujmy Európskej únie alebo jedného či viacerých jej členských štátov.

3. EUCI sa označujú stupňami utajenia uvedenými v odseku 2. Okrem toho môžu mať aj doplňujúce označenia, ktoré neoznačujú stupeň utajenia, ale určujú príslušnú oblasť činnosti, identifikujú pôvodcu, obmedzujú distribúciu, ohraničujú použitie alebo uvádzajú rozsah možného postúpenia.

([1]) Nariadenie Rady (EHS, Euratom, ESUO) č. 259/68 z 29. februára 1968, ktorým sa ustanovuje Služobný poriadok úradníkov Európskych spoločenstiev a Podmienky zamestnávania ostatných zamestnancov Európskych spoločenstiev a prijímajú osobitné opatrenia dočasne uplatniteľné na úradníkov Komisie (Podmienky zamestnávania ostatných zamestnancov) (Ú. v. ES L 56, 4.3.1968, s. 1).

Článok 4

Riadenie utajovania

1. Každý člen Komisie alebo oddelenia Komisie zabezpečuje, že EUCI, ktorú vytvorí, je náležite utajovaná, jasne označená ako EUCI a že podlieha príslušnému stupňu utajenia, len pokiaľ je to nevyhnutné.

2. Bez ohľadu na článok 26 sa stupeň utajenia EUCI neznižuje, nezrušuje ani sa nijaké označenia stupňa utajenia podľa článku 3 ods. 2 neupravujú ani neodstraňujú bez predchádzajúceho písomného súhlasu pôvodcu.

3. V prípade potreby sa prijmú vykonávacie predpisy týkajúce sa manipulácie s EUCI vrátane praktického sprievodcu stupňami utajenia v súlade s článkom 60.

Článok 5

Ochrana utajovaných skutočností

1. EUCI sa chránia v súlade s týmto rozhodnutím a s jeho vykonávacími predpismi.

2. Držiteľ každej položky EUCI je zodpovedný za jej ochranu v súlade s týmto rozhodnutím a jeho vykonávacími predpismi podľa predpisov uvedených v kapitole 4.

3. Keď členské štáty poskytnú štruktúram alebo sieťam Komisie utajované skutočnosti, ktoré sú označené vnútroštátnym stupňom utajenia, Komisia ich chráni v súlade s požiadavkami uplatňovanými na EUCI s rovnocenným stupňom utajenia podľa ekvivalenčnej tabuľky stupňov utajenia uvedenej v prílohe I.

4. Súbor EUCI si môže vyžadovať ochranu na úrovni, ktorá zodpovedá vyššiemu stupňu utajenia, než je stupeň utajenia jeho jednotlivých častí.

Článok 6

Riadenie bezpečnostných rizík

1. Bezpečnostné opatrenia na ochranu EUCI počas celého ich životného cyklu zodpovedajú najmä stupňu utajenia, podobe a objemu informácií alebo vecí, polohe a konštrukcii zariadení, v ktorých sa EUCI uchovávajú, a na mieste vyhodnotenej hrozbe zákerných a/alebo trestných činností vrátane špionáže, sabotáže a terorizmu.

2. V pohotovostných plánoch sa prihliada na potrebu chrániť EUCI počas núdzových situácií s cieľom predísť neoprávnenému prístupu k nim, neoprávnenej manipulácii s nimi alebo strate ich integrity alebo dostupnosti.

3. Preventívne a nápravné opatrenia zamerané na minimalizáciu dôsledkov významného zlyhania alebo významných incidentov pri manipulácii s EUCI a ich uchovávaní sú uvedené vo všetkých služobných plánoch na zabezpečenie kontinuity činností.

Článok 7

Vykonávanie tohto rozhodnutia

1. V prípade potreby sa v súlade s článkom 60 prijmú vykonávacie predpisy, ktorými sa toto rozhodnutie doplní alebo podporí.

2. Oddelenia Komisie prijmú všetky potrebné opatrenia, ktoré patria do ich zodpovednosti na zabezpečenie toho, aby sa pri manipulácii s EUCI alebo inými utajovanými skutočnosťami alebo ich uchovávaní uplatňovalo toto rozhodnutie a príslušné vykonávacie predpisy.

3. Bezpečnostné opatrenia na vykonávanie tohto rozhodnutia musia byť v súlade so zásadami bezpečnosti v Komisii stanovenými v článku 3 rozhodnutia (EÚ, Euratom) 2015/443

4. Generálny riaditeľ pre ľudské zdroje a bezpečnosť zriadi v rámci Generálneho riaditeľstva pre ľudské zdroje a bezpečnosť bezpečnostný orgán Komisie. Bezpečnostný orgán Komisie má povinnosti, ktoré mu boli pridelené na základe tohto rozhodnutia a jeho vykonávacích pravidiel.

5. V každom oddelení Komisie miestny bezpečnostný úradník, ako sa uvádza v článku 20 rozhodnutia (EÚ, Euratom) 2015/443, má tieto celkové povinnosti chrániť EUCI podľa tohto rozhodnutia v úzkej spolupráci s Generálnym riaditeľstvom pre ľudské zdroje a bezpečnosť:

a) vybavovať žiadosti o bezpečnostné oprávnenia pre zamestnancov;

b) prispievať k bezpečnostným školeniam a informačným stretnutiam;

c) dohliadať nad oddelením kontrolného úradníka registra;

d) podávať správy o narušení bezpečnosti a vyzradení EUCI;

e) uchovávať náhradné kľúče a písomný záznam o všetkých nastavených kombináciách;

f) plniť ďalšie úlohy súvisiace s ochranou EUCI alebo vymedzené vo vykonávacích predpisoch.

Článok 8

Narušenie bezpečnosti a vyzradenie EUCI

1. Narušenie bezpečnosti nastáva v dôsledku konania alebo opomenutia zo strany osoby, ktoré je v rozpore s bezpečnostnými predpismi stanovenými v tomto rozhodnutí a jeho vykonávacích predpisoch.

2. Vyzradenie EUCI nastáva, keď k nim v dôsledku narušenia bezpečnosti úplne alebo čiastočne získala prístup neoprávnená osoba.

3. Každé narušenie alebo podozrenie z narušenia sa ihneď oznamuje bezpečnostnému orgánu Komisie.

4. Ak je známe alebo ak existuje dostatočný dôvod domnievať sa, že došlo k vyzradeniu alebo strate EUCI, vykoná sa bezpečnostné vyšetrovanie v súlade s článkom 13 rozhodnutia (EÚ, Euratom) č. 2015/443

5. Prijmú sa všetky vhodné opatrenia s cieľom:

a) informovať pôvodcu;

b) zabezpečiť, že na účely zistenia skutočností prípad vyšetria zamestnanci, ktorých sa narušenie bezpečnosti bezprostredne netýka;

c) vyhodnotiť možné poškodenie záujmov Únie alebo členských štátov;

d) prijať vhodné opatrenia na predchádzanie opätovnému výskytu a

e) informovať príslušné orgány o prijatých opatreniach.

6. Každá osoba, ktorá je zodpovedná za porušenie bezpečnostných predpisov stanovených v tomto rozhodnutí, môže byť disciplinárne stíhaná v súlade so služobným poriadkom. Každá osoba, ktorá je zodpovedná za vyzradenie alebo stratu EUCI, podlieha disciplinárnemu a/alebo súdnemu konaniu podľa príslušných zákonov, pravidiel a iných právnych predpisov.

KAPITOLA 2

PERSONÁLNA BEZPEČNOSŤ

Článok 9

Vymedzenie pojmov

Na účely tejto kapitoly sa uplatňuje toto vymedzenie pojmov:

1. „Oprávnenie na prístup k EUCI“ je rozhodnutie bezpečnostného orgánu Komisie prijaté na základe ubezpečenia udeleného príslušným orgánom členského štátu o tom, že sa úradníkovi, inému zamestnancovi alebo vyslanému národnému expertovi Komisie môže v prípade, ak sa zistila jeho potreba poznať EUCI a bol náležitým spôsobom poučený o svojich povinnostiach, udeliť prístup k EUCI do určeného stupňa utajenia (CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyššieho) a do určeného dátumu. Takáto osoba sa označuje ako „bezpečnostne oprávnená“.

2. „Personálne bezpečnostné oprávnenie“ je uplatňovanie opatrení s cieľom zabezpečiť, že prístup k EUCI sa udeľuje len osobám, ktoré:

   a) majú potrebu poznať utajované skutočnosti;

   b) prípadne boli bezpečnostne oprávnené pre príslušný stupeň utajenia a

   c) boli poučené o svojich povinnostiach.

3. „Personálna bezpečnostná previerka“ (Personnel Security Clearance – PSC) je vyhlásenie príslušného orgánu členského štátu, ktoré sa vydáva na základe ukončeného bezpečnostného vyšetrovania vykonaného príslušnými orgánmi členského štátu a ktorým sa potvrdzuje, že osobe sa môže za predpokladu, že sa zistila jej potreba poznať EUCI a bola náležitý spôsobom poučená o svojich povinnostiach, udeliť prístup k EUCI do určeného stupňa utajenia (CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyššieho) a do určeného dátumu.

4. „Certifikát o personálnej bezpečnostnej previerke“ (PSCC) je certifikát vydaný príslušným orgánom, ktorým sa potvrdzuje, že osoba je držiteľom platnej bezpečnostnej previerky alebo bezpečnostného oprávnenia vydaného bezpečnostným orgánom Komisie, a v ktorom sa uvádza, do akého stupňa utajenia EUCI sa môže tejto osobe udeliť prístup (CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšší), obdobie platnosti príslušnej bezpečnostnej previerky alebo oprávnenia a dátum skončenia platnosti samotného certifikátu.

5. „Bezpečnostné vyšetrovanie“ sú vyšetrovacie postupy vykonávané príslušným vnútroštátnym orgánom členského štátu v súlade s jeho zákonmi a inými právnymi predpismi s cieľom získať ubezpečenie, že nie je známe nič, čo by bránilo udeliť osobe bezpečnostnú previerku do určeného stupňa utajenia (CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyššieho).

Článok 10

Základné zásady

1. Osobe sa udelí prístup k EUCI len po tom, ako:

1. sa zistila jej potreba poznať utajované skutočnosti;

2. bola poučená o bezpečnostných predpisoch na ochranu EUCI a príslušných bezpečnostných normách a usmerneniach a akceptovala svoje povinnosti v súvislosti s ochranou takýchto utajovaných skutočností;

3. dostala na prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším bezpečnostné oprávnenie pre príslušný stupeň alebo iné náležité oprávnenie vyplývajúce z povahy jej funkcie v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi.

2. Všetky osoby, ktoré môžu na plnenie svojich úloh potrebovať prístup k EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, musia dostať pred udelením prístupu k takýmto EUCI bezpečnostné oprávnenie pre príslušný stupeň. Dotknutá osoba musí dať písomný súhlas na vykonanie personálnej bezpečnostnej previerky. Ak tak neurobí, znamená to, že jej nemôže byť zverené pracovné miesto, funkcia ani úloha, ktoré zahŕňajú prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším.

3. Personálna bezpečnostná previerka je koncipovaná tak, aby určila, či osoba pri zohľadnení jej lojality, dôveryhodnosti a spoľahlivosti môže byť oprávnená na prístup k EUCI.

4. Skutočnosť, či je osoba lojálna, dôveryhodná a spoľahlivá na účely bezpečnostného preverenia na prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, sa stanovuje prostredníctvom bezpečnostného vyšetrovania, ktoré vykonávajú príslušné orgány členského štátu v súlade s jeho vnútroštátnymi zákonmi a inými právnymi predpismi.

5. Bezpečnostný orgán Komisie nesie výlučnú zodpovednosť za styk s národnými bezpečnostnými orgánmi (National Security Authority – NSA) alebo inými príslušnými vnútroštátnymi orgánmi v súvislosti so všetkými otázkami týkajúcimi sa bezpečnostnej previerky. Všetky kontakty medzi útvarmi Komisie a ich zamestnancami, NSA a ostatnými príslušnými orgánmi sa uskutočňujú prostredníctvom bezpečnostného orgánu Komisie.

Článok 11

Postup bezpečnostného oprávnenia

1. Každý generálny riaditeľ alebo vedúci útvaru v Komisii určí v rámci svojho oddelenia pozície, ktorých držitelia potrebujú mať prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším na plnenie svojich povinností, a preto potrebujú bezpečnostné oprávnenie.

2. Hneď ako je známe, že osobe bude zverená pozícia, ktorá si vyžaduje prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, miestny bezpečnostný úradník dotknutého oddelenia Komisie informuje bezpečnostný orgán Komisie, ktorý danej osobe zašle dotazník bezpečnostnej previerky vydaný NSA členského štátu, ktorého štátnu príslušnosť má osoba prijatá do pracovného pomeru v inštitúciách EÚ. Osoba musí dať písomný súhlas na vykonanie postupu bezpečnostnej previerky a vrátiť vyplnený dotazník čo najskôr bezpečnostnému orgánu Komisie.

3. Bezpečnostný orgán Komisie potom zašle vyplnený dotazník NSA členského štátu, ktorého štátnu príslušnosť má osoba prijatá do pracovného pomeru v inštitúciách EÚ, a požiada o vykonanie bezpečnostného vyšetrovania pre stupeň utajenia EUCI, ku ktorým bude táto osoba potrebovať prístup.

4. Ak bezpečnostný orgán Komisie zistí o osobe, ktorá požiadala o bezpečnostnú previerku, informácie relevantné z hľadiska bezpečnostného vyšetrovania, oznámi túto skutočnosť v súlade s príslušnými pravidlami a právnymi predpismi príslušnému NSA.

5. Bezpečnostný orgán Komisie po ukončení bezpečnostného vyšetrovania a čo najskôr po tom, ako mu príslušný NSA oznámil celkové hodnotenie zistení bezpečnostného vyšetrovania:

a) môže udeliť povolenie na prístup k EUCI dotknutej osobe a povoliť prístup k EUCI do príslušného stupňa utajenia do dátumu, ktorý určil, avšak najviac na 5 rokov, keď výsledkom bezpečnostného vyšetrovania je ubezpečenie, že nie je známe nič, čo by spochybňovalo lojalitu, dôveryhodnosť a spoľahlivosť danej osoby;

b) v prípade, že výsledkom bezpečnostného vyšetrovania nie je takéto ubezpečenie, oznámi túto skutočnosť v súlade s príslušnými pravidlami a právnymi predpismi dotknutej osobe, ktorá môže požiadať bezpečnostný orgán Komisie o vypočutie. Ten zasa môže požiadať príslušný NSA o ďalšie objasnenie, ktoré tento NSA na základe vnútroštátnych zákonov a iných právnych predpisov môže poskytnúť. Ak sa výsledok bezpečnostného vyšetrovania potvrdí, oprávnenie na prístup k EUCI sa neudelí.

6. Na bezpečnostné vyšetrovanie a získané výsledky sa vzťahujú príslušné zákony a iné právne predpisy, ktoré sú platné v dotknutom členskom štáte, vrátane tých, ktoré sa týkajú odvolania. Proti rozhodnutiam bezpečnostného orgánu Komisie možno podať odvolanie v súlade so služobným poriadkom.

7. Komisia akceptuje oprávnenie na prístup k EUCI udelené ktoroukoľvek inou inštitúciou, orgánom alebo agentúrou Únie za predpokladu, že je naďalej platné. Oprávnenie platí pre každú úlohu, ktorú dotknutá osoba v Komisii vykonáva. Inštitúcia, orgán alebo agentúra Únie, v ktorej sa osoba zamestná, oznámi príslušnému NSA zmenu zamestnávateľa.

8. Ak sa obdobie služby osoby nezačne do 12 mesiacov od oznámenia výsledku bezpečnostného vyšetrovania bezpečnostnému orgánu Komisie alebo ak sa služba osoby preruší na obdobie 12 mesiacov, počas ktorých táto osoba nie je zamestnaná v Komisii ani v ktorejkoľvek inej inštitúcii, orgáne alebo agentúre Únie, ani na pozícii vo verejnej správe členského štátu, bezpečnostný orgán Komisie postúpi záležitosť príslušnému NSA na potvrdenie platnosti a správnosti bezpečnostnej previerky.

9. Ak bezpečnostný orgán Komisie zistí informácie týkajúce sa bezpečnostného rizika, ktoré predstavuje osoba, ktorá je držiteľom platnej bezpečnostnej previerky, bezpečnostný orgán v súlade s príslušnými pravidlami a právnymi predpismi oznámi túto skutočnosť príslušnému NSA.

10. Ak NSA informuje bezpečnostný orgán Komisie o odňatí záruky udelenej v súlade s odsekom 5 písm. a) osobe, ktorá je držiteľom platného oprávnenia na prístup k EUCI, bezpečnostný orgán Komisie môže požiadať o akékoľvek objasnenie, ktoré NSA môže poskytnúť na základe vnútroštátnych zákonov a iných právnych predpisov. Ak príslušný NSA potvrdí nepriaznivé informácie, bezpečnostné oprávnenie sa odníme a možnosť prístupu k EUCI sa zruší a dotknutej osobe sa neumožní zastávať pozíciu, kde takáto možnosť prístupu existuje alebo kde by táto osoba mohla predstavovať bezpečnostné riziko.

11. Každé rozhodnutie o odňatí alebo pozastavení oprávnenia na prístup k EUCI každej osobe, ktorá patrí do rozsahu pôsobnosti tohto rozhodnutia, a prípadne dôvody takéhoto odňatia alebo pozastavenia sa oznámia dotknutej osobe, ktorá môže požiadať bezpečnostný orgán Komisie o vypočutie. Na informácie, ktoré poskytuje NSA, sa vzťahujú príslušné zákony a iné právne predpisy platné v dotknutom členskom štáte. Proti rozhodnutiam bezpečnostného orgánu Komisie uskutočneným v tomto kontexte možno podať odvolanie v súlade so služobným poriadkom.

12. Oddelenia Komisie zabezpečia, že národní experti vyslaní pracovať na pozícii, ktorá si vyžaduje bezpečnostné oprávnenie na prístup k EUCI, pred začatím vykonávania funkcie podľa vnútroštátnych zákonov a iných právnych predpisov predložia platnú personálnu bezpečnostnú previerku alebo certifikát o personálnej bezpečnostnej previerke (PSCC) bezpečnostnému orgánu Komisie, ktorý na tomto základe udelí bezpečnostné oprávnenie na prístup k EUCI pre stupeň rovnajúci sa stupňu uvedenému v národnej bezpečnostnej previerke s maximálnou platnosťou počas ich vyslania.

Prístup k EUCI pre osoby riadne oprávnené na základe ich funkcie

13. Členovia Komisie, ktorí majú prístup k EUCI vyplývajúci z povahy ich funkcie na základe zmluvy, sú poučení o svojich bezpečnostných povinnostiach v súvislosti s ochranou EUCI.

Záznamy o bezpečnostnej previerke a bezpečnostnom oprávnení

14. Záznamy o bezpečnostných previerkach a oprávneniach udelených na prístup k EUCI uchováva bezpečnostný orgán Komisie v súlade s týmto rozhodnutím. Tieto záznamy obsahujú minimálne stupeň utajenia EUCI, pre ktorý sa osobe môže udeliť prístup, dátum vydania bezpečnostnej previerky a obdobie jej platnosti.

15. Príslušný bezpečnostný orgán Komisie môže vydať PSCC, v ktorom sa uvádza, do akého stupňa utajenia EUCI sa môže osobe udeliť prístup (CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšší), dátum platnosti príslušného oprávnenia na prístup k EUCI a dátum ukončenia platnosti samotného certifikátu.

Predĺženie platnosti bezpečnostného oprávnenia

16. Po prvom udelení bezpečnostného oprávnenia a za predpokladu, že osoba je nepretržite zamestnaná v Európskej komisii alebo inej inštitúcii, orgáne alebo agentúre Únie a naďalej potrebuje prístup k EUCI, bezpečnostné oprávnenie na prístup k EUCI sa na účely obnovenia prehodnotí, spravidla každých päť rokov odo dňa oznámenia výsledku posledného bezpečnostného vyšetrovania, na ktorom bolo založené.

17. Bezpečnostný orgán Komisie môže predĺžiť platnosť existujúceho bezpečnostného oprávnenia na obdobie najviac 12 mesiacov, ak neboli doručené žiadne nepriaznivé informácie od príslušného NSA alebo iného príslušného vnútroštátneho orgánu v lehote dvoch mesiacov od dátumu predloženia žiadosti o predĺženie a zodpovedajúceho dotazníka bezpečnostnej previerky. Ak do konca tohto 12-mesačného obdobia príslušný NSA alebo iný príslušný vnútroštátny orgán neoznámi bezpečnostnému orgánu Komisii svoje stanovisko, osobe sa pridelia úlohy, ktoré si nevyžadujú bezpečnostné oprávnenie.

Článok 12

Poučenia o bezpečnostnom oprávnení

1. Každá osoba, ktorá dostala bezpečnostné oprávnenie po tom, ako sa zúčastnila na poučení o bezpečnostnom oprávnení organizovanom bezpečnostným orgánom Komisie, písomne potvrdí, že porozumela svojim povinnostiam týkajúcim sa ochrany EUCI a následkom v prípade ich vyzradenia. Záznam o takomto písomnom potvrdení uchováva bezpečnostný orgán Komisie.

2. Každá osoba, ktorá je oprávnená na prístup k EUCI alebo od ktorej sa vyžaduje, aby s nimi manipulovala, je na začiatku poučená a ďalej pravidelne poučovaná o bezpečnostných hrozbách a je povinná bezodkladne oznámiť príslušnému bezpečnostnému orgánu Komisie všetky kontakty alebo aktivity, ktoré považuje za podozrivé alebo neobvyklé.

3. Každá osoba, ktorá ukončila zamestnanie vyžadujúce si prístup k EUCI, je poučená o svojich povinnostiach naďalej chrániť EUCI, čo v prípade potreby potvrdí aj písomne.

Článok 13

Dočasné bezpečnostné oprávnenia

1. Vo výnimočných prípadoch, ktoré sú náležite odôvodnené služobnými záujmami, a do ukončenia úplného bezpečnostného vyšetrovania môže bezpečnostný orgán Komisie po porade s NSA členského štátu, ktorého je osoba štátnym príslušníkom, a na základe predbežných preverení slúžiacich na overenie, či nie sú známe nepriaznivé informácie, udeliť osobám dočasné oprávnenie na prístup k EUCI pre konkrétnu úlohu bez toho, aby boli dotknuté ustanovenia týkajúce sa predĺženia bezpečnostných previerok. Takéto dočasné oprávnenie na prístup k EUCI je platné počas jednorazového obdobia, ktoré nepresahuje šesť mesiacov, a nemôže sa ním povoliť prístup k utajovaným skutočnostiam so stupňom utajenia TRÈS SECRET UE/EU TOP SECRET.

2. Po poučení v súlade s článkom 12 ods. 1 každá osoba, ktorej sa udelilo dočasné oprávnenie, písomne potvrdí, že porozumela svojim povinnostiam týkajúcim sa ochrany EUCI a následkom v prípade ich vyzradenia. Záznam o takomto písomnom potvrdení uchováva bezpečnostný orgán Komisie.

Článok 14

Účasť na utajovaných zasadnutiach organizovaných Komisiou

1. Oddelenia Komisie zodpovedné za organizovanie zasadnutí, na ktorých sa prerokúvajú utajované skutočnosti so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, informujú prostredníctvom svojho miestneho bezpečnostného úradníka alebo prostredníctvom organizátora zasadnutia bezpečnostný orgán Komisie v dostatočnom predstihu o dátumoch, čase, mieste a účastníkoch týchto zasadnutí.

2. S výhradou ustanovení článku 11 ods. 13 osoby poverené, aby sa zúčastnili na zasadnutiach organizovaných Komisiou, na ktorých sa prerokúvajú utajované skutočnosti so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, sa môžu na týchto zasadnutiach zúčastňovať len na základe potvrdenia ich statusu bezpečnostnej previerky alebo bezpečnostného oprávnenia. Prístup k takýmto utajovaným zasadnutiam sa zamietne osobám, v prípade ktorých bezpečnostný orgán Komisie nevidel PSCC alebo iný doklad o bezpečnostnej previerke, alebo účastníkom Komisie, ktorí nemajú bezpečnostné oprávnenie.

3. Pred zorganizovaním zasadnutia o utajovaných skutočnostiach zodpovedný organizátor zasadnutia alebo miestny bezpečnostný úradník oddelenia Komisie, ktoré zasadnutie organizuje, požiada externých účastníkov, aby bezpečnostnému orgánu Komisie poskytli PSCC alebo iný doklad o bezpečnostnej previerke. Bezpečnostný orgán Komisie informuje miestneho bezpečnostného úradníka alebo organizátora zasadnutia o PSCC alebo iných doručených dokladoch o PSC. V prípade potreby sa môže použiť súhrnný zoznam mien, v ktorom sú uvedené príslušné informácie o bezpečnostnej previerke.

4. Ak príslušné orgány informovali bezpečnostný orgán Komisie, že personálna bezpečnostná previerka bola odobratá osobe, ktorej povinnosti si vyžadujú účasť na zasadnutiach organizovaných Komisiou, bezpečnostný orgán Komisie to oznámi miestnemu bezpečnostnému úradníkovi oddelenia Komisie zodpovednému za organizovanie zasadnutia.

Článok 15

Prípadný prístup k EUCI

Kuriéri, príslušníci bezpečnostnej služby a sprievodu sú bezpečnostne oprávnení pre vhodný stupeň utajenia alebo vyšetrení iným vhodným spôsobom v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi, poučení o bezpečnostných postupoch na ochranu utajovaných skutočností EÚ a informovaní o svojich povinnostiach v súvislosti s ochranou EUCI, ktoré sú im zverené.

KAPITOLA 3

FYZICKÁ BEZPEČNOSŤ ZAMERANÁ NA OCHRANU UTAJOVANÝCH SKUTOČNOSTÍ

Článok 16

Základné zásady

1. Opatrenia fyzickej bezpečnosti sú určené na zabránenie tajnému alebo násilnému vniknutiu narušiteľa, odradenie od neoprávnených činností, ich zamedzenie a odhalenie a na umožnenie rozdelenia pracovníkov na účely prístupu k EUCI na základe potreby poznať. Tieto opatrenia sa stanovujú na základe procesu riadenia rizík a v súlade s týmto rozhodnutím a jeho vykonávacími predpismi.

2. Opatrenia fyzickej bezpečnosti majú predovšetkým zabrániť neoprávnenému prístupu k EUCI tým, že:

a) zaisťujú, aby sa s EUCI manipulovalo vhodným spôsobom a aby boli uchovávané vhodným spôsobom;

b) umožňujú rozdelenie personálu, pokiaľ ide o prístup k EUCI, na základe ich potreby poznať a prípadne na základe ich bezpečnostného oprávnenia;

c) odrádzajú od neoprávnených činností, takéto činnosti zamedzujú a odhaľujú a

d) znemožňujú alebo spomaľujú tajný alebo násilný vstup narušiteľov.

3. Opatrenia fyzickej bezpečnosti treba zaviesť vo všetkých objektoch, budovách, kanceláriách, miestnostiach a iných priestoroch, v ktorých sa manipuluje s EUCI alebo sa takéto utajované skutočnosti uchovávajú, vrátane priestorov, v ktorých sú umiestnené komunikačné a informačné systémy uvedené v kapitole 5.

4. Priestory, v ktorých sa uchovávajú utajované skutočnosti EÚ so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, treba zriadiť ako zabezpečené priestory podľa tejto kapitoly a musí ich schváliť bezpečnostný akreditačný orgán Komisie.

5. Na ochranu EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším sa používa iba vybavenie alebo prostriedky schválené bezpečnostným orgánom Komisie.

Článok 17

Požiadavky a opatrenia fyzickej bezpečnosti

1. Opatrenia fyzickej bezpečnosti sa vyberú na základe posúdenia hrozby, ktoré vykoná bezpečnostný orgán Komisie v prípade potreby po porade s inými oddeleniami Komisie, inými inštitúciami, agentúrami alebo orgánmi Únie a/alebo príslušnými orgánmi v členských štátoch. Na zabezpečenie úrovne fyzickej ochrany zodpovedajúcej vyhodnotenému riziku uplatňuje Komisia vo svojich objektoch proces riadenia rizík na ochranu EUCI. V procese riadenia rizík sa zohľadnia všetky relevantné faktory, a to najmä:

a) stupeň utajenia EUCI;

b) podoba a objem EUCI s prihliadnutím na skutočnosť, že veľké množstvo alebo kompilácia EUCI si môže vyžiadať uplatňovanie prísnejších ochranných opatrení;

c) okolité prostredie a štruktúra budov alebo priestorov, v ktorých sa utajované skutočnosti EÚ nachádzajú, a

d) vyhodnotená hrozba zo strany spravodajských služieb zameraných na Úniu, jej inštitúcie, orgány alebo agentúry alebo členské štáty, a hrozba sabotáže a teroristických, podvratných alebo iných trestných činností.

2. Bezpečnostný orgán Komisie určuje na základe koncepcie hĺbkovej ochrany vhodnú kombináciu opatrení fyzickej bezpečnosti, ktoré sa musia uplatňovať. Na tento účel bezpečnostný orgán Komisie vypracuje minimálne normy, štandardy a kritériá stanovené vo vykonávacích predpisoch.

3. Bezpečnostný orgán Komisie má právo vykonávať pri vstupe a odchode prehliadky, ktorých cieľom je odradiť od nepovoleného prinesenia vecí alebo nepovoleného odnesenia EUCI z objektov alebo budov.

4. Ak pri EUCI existuje riziko, aj keď len náhodné, že budú prehliadnuté, dotknuté oddelenia Komisie prijmú vhodné opatrenia vymedzené bezpečnostným orgánom Komisie na zabránenie tomuto riziku.

5. V prípade nových zariadení sa požiadavky fyzickej bezpečnosti a jej funkčnej špecifikácie vymedzujú so súhlasom bezpečnostného orgánu Komisie vo fáze plánovania a projektovania zariadení. V prípade existujúcich zariadení sa požiadavky fyzickej bezpečnosti uplatňujú v súlade s minimálnymi normami, štandardmi a kritériami stanovenými vo vykonávacích predpisoch.

Článok 18

Vybavenie na fyzickú ochranu EUCI

1. Na účely fyzickej ochrany EUCI sa zriadia dva typy fyzicky chránených priestorov:

a) administratívne priestory a

b) zabezpečené priestory (vrátane technicky zabezpečených priestorov).

2. Bezpečnostný akreditačný orgán Komisie stanoví, že priestor spĺňa požiadavky na označenie ako administratívny priestor, zabezpečený priestor alebo technicky zabezpečený priestor.

3. Pokiaľ ide o administratívne priestory:

a) zriadi sa viditeľne vymedzený obvod, ktorý umožňuje kontrolu osôb a v prípade možnosti aj vozidiel;

b) prístup bez sprievodu sa udeľuje len tým osobám, ktorým bezpečnostný orgán Komisie alebo akýkoľvek iný príslušný orgán udelil náležité oprávnenie, a

c) všetky ostatné osoby majú nepretržitý sprievod alebo podliehajú rovnocenným kontrolám.

4. Pokiaľ ide o zabezpečené priestory:

a) zriadi sa viditeľne vymedzený a chránený obvod, pričom každý vstup do tohto obvodu a odchod z neho sa kontroluje pomocou preukazu alebo personálneho identifikačného systému;

b) prístup bez sprievodu sa udeľuje len bezpečnostne previereným osobám, ktorým sa udelilo osobitné oprávnenie na vstup do priestoru vzhľadom na ich potrebu poznať;

c) všetky ostatné osoby majú nepretržitý sprievod alebo podliehajú rovnocenným kontrolám.

5. Ak vstup do zabezpečeného priestoru predstavuje zo všetkých praktických hľadísk priamy prístup k utajovaným skutočnostiam, ktoré obsahuje, uplatňujú sa tieto dodatočné požiadavky:

a) jasne sa označuje najvyšší stupeň utajenia utajovaných skutočností, ktoré sa bežne v tomto priestore nachádzajú;

b) všetci návštevníci musia mať na vstup do tohto priestoru osobitné oprávnenie, musia mať nepretržitý sprievod a byť náležite bezpečnostne preverení, pokiaľ sa nezabezpečí, že prístup k EUCI je nemožný.

6. Zabezpečené priestory chránené pred odpočúvaním sú označené ako technicky zabezpečené priestory. Uplatňujú sa tieto dodatočné požiadavky:

a) takéto priestory sú vybavené systémom detekcie narušenia, sú uzamknuté, keď sa v nich nikto nenachádza, a strážené, keď je v nich niekto prítomný; Všetky kľúče sa kontrolujú v súlade s článkom 20;

b) kontrolujú sa všetky osoby vstupujúce do týchto priestorov a všetky prinášané veci;

c) bezpečnostný orgán Komisie pravidelne vykonáva v týchto priestoroch fyzickú a/alebo technickú kontrolu. Takéto kontroly sa musia vykonávať aj po každom neoprávnenom vstupe alebo podozrení na takýto vstup a

d) v týchto priestoroch sa nesmú nachádzať žiadne nepovolené komunikačné linky, nepovolené telefóny či iné nepovolené komunikačné zariadenia a elektrické alebo elektronické vybavenie.

7. Bez ohľadu na odsek 6 písm. d) bezpečnostný orgán Komisie skontroluje v prípade, že sa ohrozenie EUCI vyhodnotí ako vysoké, všetky komunikačné zariadenia a elektrické alebo elektronické vybavenie skôr, ako sa použijú v priestoroch, kde sa konajú zasadnutia alebo kde sa pracuje s utajovanými skutočnosťami so stupňom utajenia SECRET UE/EU SECRET a vyšším, aby sa zaistilo, že sa týmto vybavením neúmyselne alebo neoprávnene neprenesú za obvod príslušného zabezpečeného priestoru žiadne zrozumiteľné informácie.

8. V zabezpečených priestoroch, v ktorých nevykonáva personál službu 24 hodín denne, sa podľa potreby vykonávajú kontroly na konci bežného pracovného času a v náhodných intervaloch mimo bežných pracovných hodín, pokiaľ nie je nainštalovaný systém detekcie narušenia.

9. Zabezpečené priestory a technicky zabezpečené priestory sa môžu dočasne zriadiť v rámci administratívneho priestoru na utajované zasadnutie alebo iné podobné účely.

10. Miestny bezpečnostný úradník príslušného oddelenia Komisie vypracuje bezpečnostné prevádzkové postupy (SecOPs) pre každý zabezpečený priestor v jeho zodpovednosti a zároveň v súlade s ustanoveniami tohto rozhodnutia a jeho vykonávacích pravidiel stanoví:

a) stupeň utajenia EUCI, s ktorými sa môže manipulovať alebo ktoré sa môžu uchovávať v tomto priestore;

b) opatrenia dohľadu a ochrany, ktoré sa musia uplatňovať;

c) osoby oprávnené na vstup do tohto priestoru bez sprievodu so zreteľom na ich potrebu poznať a bezpečnostné oprávnenie;

d) v prípade potreby postupy týkajúce sa sprievodu alebo ochrany EUCI pri udelení oprávnenia vstupu do tohto priestoru akýmkoľvek iným osobám;

e) akékoľvek ďalšie príslušné opatrenia a postupy.

11. V zabezpečených priestoroch sa vybudujú komorové trezory. Steny, podlahy, stropy, okná a uzamykateľné dvere musia byť schválené bezpečnostným orgánom Komisie a musia poskytovať ochranu, ktorá je rovnocenná ochrane poskytovanej bezpečnostnými schránkami schválenými na uchovávanie EUCI s rovnakým stupňom utajenia.

Článok 19

Fyzické ochranné opatrenia pre manipuláciu s EUCI a ich uchovávanie

1. S EUCI so stupňom utajenia RESTREINT UE/EU RESTRICTED sa môže manipulovať:

a) v zabezpečenom priestore;

b) v administratívnom priestore za predpokladu, že EUCI sú chránené pred prístupom zo strany neoprávnených osôb, alebo

c) mimo zabezpečeného priestoru alebo administratívneho priestoru za predpokladu, že držiteľ prenáša tieto EUCI v súlade s článkom 31 a zaviazal sa dodržiavať kompenzačné opatrenia stanovené vo vykonávacích predpisoch, aby sa zabezpečilo, že EUCI sú chránené pred prístupom neoprávnených osôb.

2. EUCI so stupňom utajenia RESTREINT UE/EU RESTRICTED sa uchovávajú vo vhodnom uzamknutom kancelárskom nábytku v administratívnom alebo zabezpečenom priestore. Dočasne sa môžu uchovávať mimo administratívneho alebo zabezpečeného priestoru za predpokladu, že sa držiteľ zaviazal dodržiavať kompenzačné opatrenia stanovené vo vykonávacích predpisoch.

3. S EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET sa môže manipulovať:

a) v zabezpečenom priestore;

b) v administratívnom priestore za predpokladu, že EUCI sú chránené pred prístupom neoprávnených osôb, alebo

c) mimo zabezpečeného alebo administratívneho priestoru za predpokladu, že držiteľ:

   i) sa zaviazal dodržiavať kompenzačné opatrenia stanovené vo vykonávacích predpisoch, aby sa zabezpečilo, že EUCI sú chránené pred prístupom neoprávnených osôb;

   ii) má EUCI vždy pod osobnou kontrolou a

   iii) v prípade dokumentov v papierovej podobe túto skutočnosť oznámil príslušnému registru.

4. EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET sa v zabezpečenom priestore uchovávajú v bezpečnostnej schránke alebo komorovom trezore.

5. S EUCI so stupňom utajenia TRÈS SECRET UE/EU TOP SECRET sa manipuluje v zabezpečenom priestore, ktorý zriadi a spravuje bezpečnostný orgán Komisie a ktorý na túto úroveň akreditoval bezpečnostný akreditačný orgán Komisie.

6. EUCI so stupňom utajenia TRÈS SECRET UE/EU TOP SECRET sa uchovávajú v zabezpečenom priestore, ktorý na túto úroveň akreditoval bezpečnostný akreditačný orgán Komisie, pričom musí byť splnená jedna z týchto podmienok:

a) uchovávajú sa v bezpečnostnej schránke v súlade s ustanoveniami článku 18 uplatňujúc jeden alebo viaceré z týchto dodatočných kontrolných mechanizmov:

   1. nepretržitá ochrana alebo kontroly vykonávané preverenými bezpečnostnými pracovníkmi alebo službukonajúcim personálom;

   2. schválený systém detekcie narušenia v kombinácii so zásahovým bezpečnostným personálom

   alebo

b) v komorovom trezore vybavenom systémom detekcie narušenia v kombinácii so zásahovým bezpečnostným personálom.

Článok 20

Správa kľúčov a kombinácií používaných na ochranu EUCI

1. Postupy pre správu kľúčov a nastavení kombinácií na prístup do kancelárií, miestností, komorových trezorov a bezpečnostných schránok sa stanovia vo vykonávacích predpisoch podľa článku 60. Účelom týchto postupov je zabrániť neoprávnenému prístupu.

2. Nastavenia kombinácií do pamäte ukladá čo najmenší možný počet osôb, ktoré ich potrebujú poznať. Nastavenia kombinácií do bezpečnostných schránok a komorových trezorov, v ktorých sa uchovávajú EUCI, sa menia:

a) pri prijatí novej schránky;

b) vždy keď nastane zmena personálu, ktorý pozná kombináciu;

c) vždy keď došlo k vyzradeniu alebo existuje podozrenie vyzradenia;

d) po vykonaní údržby alebo opravy zámku a

e) minimálne každých 12 mesiacov.

KAPITOLA 4

SPRÁVA UTAJOVANÝCH SKUTOČNOSTÍ EÚ

Článok 21

Základné zásady

1. Všetky dokumenty EUCI by sa mali spravovať v súlade s politikou Komisie o spravovaní dokumentov, a preto by mali byť evidované, zatriedené, uchovávané a napokon zničené, zaradené do vzorky alebo presunuté do historických archívov v súlade so spoločným zoznamom pre uchovávanie spisov Európskej komisie.

2. Pred poskytnutím utajovaných skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším a po ich prijatí sa utajované skutočnosti evidujú na bezpečnostné účely. Utajované skutočnosti so stupňom utajenia TRÈS SECRET UE/EU TOP SECRET sa evidujú v osobitných registroch.

3. V Komisii musí byť systém registrov EUCI zostavený v súlade s ustanoveniami článku 27.

4. Oddelenia a objekty Komisie, v ktorých sa s EUCI manipuluje alebo sa tam uchovávajú, podliehajú pravidelným inšpekciám, ktoré vykonáva bezpečnostný orgán Komisie.

5. EUCI sa prenášajú medzi útvarmi a objektmi mimo fyzicky chránených priestorov takto:

a) vo všeobecnosti sa EUCI prenášajú elektronickými prostriedkami, ktoré sú chránené kryptografickými produktmi schválenými v súlade s kapitolou 5;

b) keď sa prostriedky uvedené v písmene a) nepoužívajú, EUCI sa prepravujú buď:

   i) na elektronických nosičoch dát (napr. USB kľúčoch, CD, pevných diskoch), ktoré sú chránené kryptografickými produktmi schválenými v súlade s kapitolou 5, alebo

   ii) vo všetkých ostatných prípadoch, ako je stanovené vo vykonávacích predpisoch.

Článok 22

Stupne utajenia a ich označenie

1. Skutočnosti sa utajujú, ak je to potrebné na ochranu ich dôvernosti v súlade s článkom 3 ods. 1.

2. Zodpovednosť za určenie stupňa utajenia v súlade s príslušnými vykonávacím predpismi, normami a usmerneniami pre utajovanie a za prvú distribúciu EUCI nesie jej pôvodca.

3. Stupeň utajenia EUCI sa stanovuje v súlade s článkom 3 ods. 2, ako aj s príslušnými vykonávacími predpismi.

4. Stupeň utajenia sa uvádza jasne a správne bez ohľadu na to, či má EUCI písomnú, ústnu, elektronickú, alebo inú podobu.

5. Jednotlivé časti daného dokumentu (napr. stránky, odseky, oddiely, doplnky, dodatky, pripojenia a prílohy) si môžu vyžiadať rôzny stupeň utajenia a podľa toho sa označujú, a to aj vtedy, keď sa uchovávajú v elektronickej podobe.

6. Celkový stupeň utajenia dokumentu alebo spisu musí byť aspoň taký vysoký ako v prípade jeho časti s najvyšším stupňom utajenia. Keď sa spájajú utajované skutočnosti z rôznych zdrojov, konečný produkt sa preskúma s cieľom určiť celkový stupeň utajenia, keďže si môže vyžadovať vyšší stupeň utajenia ako jeho jednotlivé časti.

7. Dokumenty, ktoré obsahujú časti podliehajúce rozdielnym stupňom utajenia, sa v maximálnej možnej miere usporadúvajú tak, aby sa časti s iným stupňom utajenia dali ľahko identifikovať a v prípade potreby oddeliť.

8. Stupeň utajenia listu alebo sprievodného listu obsahujúceho prílohy zodpovedá najvyššiemu stupňu utajenia príloh. Pôvodca jednoznačne uvedie stupeň utajenia listu bez príloh, a to príslušným označením, napríklad:

CONFIDENTIEL UE/EU CONFIDENTIAL

Bez prílohy (príloh) RESTREINT UE/EU RESTRICTED

Článok 23

Označenia

Okrem niektorého z označení stupňa utajenia podľa článku 3 ods. 2 môžu mať EUCI aj doplňujúce označenie, napríklad:

a) identifikačný znak, ktorým sa označuje pôvodca;

b) upozornenia, kódové slová alebo akronymy, ktorými sa označuje oblasť činnosti, ktorej sa dokument týka, osobitná distribúcia na základe potreby poznať alebo obmedzenie použitia;

c) označenia rozsahu možného postúpenia;

d) prípadne dátum alebo konkrétnu udalosť, po ktorej možno znížiť stupeň utajenia alebo utajenie zrušiť.

Článok 24

Skrátené označenia stupňov utajenia

1. Na označenie stupňa utajenia jednotlivých odsekov textu sa môžu používať štandardné skrátené označenia stupňov utajenia. Skratky nenahrádzajú plné označenia stupňov utajenia.

2. Na označenie stupňa utajenia oddielov alebo častí textu, ktoré sú kratšie ako jedna strana, možno v utajených dokumentoch EÚ používať tieto štandardné skratky:

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

Článok 25

Vytvorenie EUCI

1. Pri vytvorení utajovaného dokumentu EÚ:

a) každá strana sa zreteľne označí stupňom utajenia;

b) každá strana sa očísluje;

c) dokumentu sa priradí evidenčné číslo a predmet, ktorý samotný nie je utajovanou skutočnosťou, pokiaľ nie je ako utajovaná skutočnosť označený;

d) dokumentu sa priradí dátum;

e) na každej strane dokumentov so stupňom utajenia SECRET UE/EU SECRET alebo vyšším sa uvedie číslo vyhotovenia, pokiaľ sa dokumenty distribuujú vo viacerých vyhotoveniach.

2. Ak na EUCI nemožno uplatniť odsek 1, prijmú sa iné primerané opatrenia v súlade s vykonávacími predpismi.

Článok 26

Zníženie stupňa utajenia a zrušenie utajenia EUCI

1. Ak je to možné, pôvodca v čase vytvorenia EUCI uvedie, či je možné znížiť jej stupeň utajenia alebo utajenie zrušiť k určitému dátumu alebo po istej udalosti.

2. Každé oddelenie Komisie vykonáva pravidelné preskúmanie EUCI, ktorých je pôvodcom, aby sa uistilo, či je naďalej potrebný daný stupeň utajenia. Podľa vykonávacích predpisov sa zriadi systém, ktorým sa aspoň raz za päť rokov posúdi stupeň utajenia evidovaných EUCI, ktoré majú pôvod v Komisii. Takéto posúdenie nie je potrebné, keď pôvodca hneď na začiatku uviedol, že stupeň utajenia danej utajovanej skutočnosti sa automaticky zníži alebo sa utajenie zruší, a utajovaná skutočnosť bola príslušne označená.

3. Skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED, ktoré majú pôvod v Komisii, sa po uplynutí tridsiatich rokov automaticky odtajnia v súlade s nariadením (EHS, Euratom) č. 354/83 zmeneným a doplneným nariadením Rady (ES, Euratom) č. 1700/2003 ([1]).

Článok 27

Systém registrov utajovaných skutočností EÚ v Komisii

1. Bez toho, aby bol dotknutý článok 52 ods. 5, v každom oddelení Komisie, v ktorom sa manipuluje s EUCI alebo uchovávajú utajované skutočnosti na stupni CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET, sa stanoví zodpovedný miestny register EUCI tak, aby sa zabezpečila manipulácia s EUCI v súlade s týmto rozhodnutím.

2. Register EUCI, ktorý spravuje generálny sekretariát, je centrálnym registrom EUCI Komisie. Funguje ako:

— miestny register EUCI pre generálny sekretariát Komisie,

— register EUCI pre súkromné kancelárie členov Komisie, pokiaľ nemajú určený miestny register EUCI,

— register EUCI pre generálne riaditeľstvá alebo útvary, ktoré nemajú miestny register EUCI,

— hlavný vstupný a výstupný bod pre všetky utajované skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED až po stupeň utajenia SECRET UE/EU SECRET, ktoré si Komisia a jej útvary vymieňajú s tretími štátmi a medzinárodnými organizáciami, a ak sa tak stanovuje v osobitných dojednaniach, pre ostatné inštitúcie, agentúry a orgány Únie.

3. Bezpečnostný orgán Komisie zriadi v Komisii register, ktorý funguje ako centrálny orgán na prijímanie a odosielanie utajovaných skutočností so stupňom utajenia TRÈS SECRET UE/EU TOP SECRET. V prípade potreby sa môžu zriadiť podriadené registre, aby sa s týmito utajovanými skutočnosťami manipulovalo na účely evidencie.

4. Podriadené registre nesmú priamo odosielať dokumenty so stupňom utajenia TRÈS SECRET UE/EU TOP SECRET iným podriadeným registrom toho istého centrálneho registra TRÈS SECRET UE/EU TOP SECRET alebo externe, pokiaľ to uvedený centrálny register výslovne písomne nepovolí.

5. Registre EUCI sa zriadia ako zabezpečené priestory, ako sú definované v kapitole 3, a akredituje ich bezpečnostný akreditačný orgán Komisie.

Článok 28

Kontrolný úradník registra

1. Každý register EUCI spravuje kontrolný úradník registra (Registry Control Officer – RCO).

2. RCO sa náležite bezpečnostne preverí.

3. RCO podlieha dohľadu miestneho bezpečnostného úradníka v rámci oddelenia Komisie, pokiaľ ide o uplatňovanie ustanovení týkajúcich sa manipulácie s dokumentmi EUCI a súlad s príslušnými bezpečnostnými predpismi, normami a usmerneniami.

4. V rámci svojej zodpovednosti za správu registra EUCI, ku ktorému bol pridelený, RCO v súlade s týmto rozhodnutím a príslušnými vykonávacími predpismi, normami a usmerneniami vykonáva tieto celkové úlohy:

— riadi operácie týkajúce sa evidencie, zachovania, reprodukcie, prekladu, prenosu, odoslania a zničenia alebo presunu do útvaru historických archívov EUCI,

— pravidelne preveruje potrebu zachovávať utajenie informácií,

— plní všetky ďalšie úlohy súvisiace s ochranou EUCI vymedzené vo vykonávacích predpisoch.

Článok 29

Evidencia EUCI na bezpečnostné účely

1. Na účely tohto rozhodnutia znamená evidencia na bezpečnostné účely (ďalej len „evidencia“) uplatňovanie postupov, ktorými sa zaznamenáva životný cyklus EUCI vrátane ich distribúcie.

([1]) Nariadenie Rady (ES, Euratom) č. 1700/2003 z 22. septembra 2003, ktorým sa mení a dopĺňa nariadenie (EHS, Euratom) č. 354/83 o otvorení historických archívov Európskeho hospodárskeho spoločenstva a Európskeho spoločenstva pre atómovú energiu pre verejnosť (Ú. v. EÚ L 243, 27.9.2003, s. 1).

2. Všetky informácie alebo veci so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a vyšším sa evidujú v určených registroch, keď sú doručené do organizačnej jednotky alebo sú z nej odosielané.

3. Pri manipulácii s EUCI a ich uchovávaní s použitím komunikačného a informačného systému (Communication and Information System – CIS) sa môžu evidenčné postupy vykonávať prostredníctvom procesov v rámci samotného CIS.

4. Podrobnejšie ustanovenia týkajúce sa evidencie EUCI na bezpečnostné účely sa stanovia vo vykonávacích predpisoch.

Článok 30

Rozmnožovanie a preklad utajovaných dokumentov EÚ

1. Dokumenty so stupňom utajenia TRÈS SECRET UE/EU TOP SECRET sa nesmú rozmnožovať ani prekladať bez predchádzajúceho písomného súhlasu pôvodcu.

2. Keď pôvodca dokumentov so stupňom utajenia SECRET UE/EU SECRET alebo nižším neuvedie nijakú výhradu týkajúcu sa rozmnožovania alebo prekladu, takéto dokumenty sa môžu rozmnožovať alebo prekladať na základe pokynu držiteľa.

3. Bezpečnostné opatrenia uplatniteľné na pôvodný dokument sa uplatňujú aj na jeho kópie a preklady.

Článok 31

Preprava EUCI

1. EUCI sa prepravujú tak, aby sa ochránili pred neoprávneným zverejnením počas ich prepravy.

2. Na prepravu EUCI sa vzťahujú ochranné opatrenia, ktoré musia byť:

— primerané stupňu utajenia prenášaných EUCI a

— prispôsobené osobitným podmienkam ich prepravy, najmä v závislosti od toho, či sa EUCI prepravujú:

  — v rámci budovy alebo samostatnej skupiny budov Komisie,

  — medzi budovami Komisie, ktoré sa nachádzajú v tom istom členskom štáte,

  — v rámci Únie,

  — z Únie na územie tretieho štátu a

  — prispôsobené povahe a podobe EUCI.

3. Tieto ochranné opatrenia sú podrobne stanovené vo vykonávacích predpisoch, alebo v prípade projektov a programov uvedených v článku 42 sú neoddeliteľnou súčasťou príslušných bezpečnostných pokynov pre program alebo projekt (Programme or Project Security Instructions – PSI).

4. Vykonávacie predpisy alebo PSI obsahujú ustanovenia primerané úrovni EUCI, pokiaľ ide o:

— typ prepravy, ako napríklad ručne, preprava diplomatickými alebo vojenskými kuriérmi, preprava poštovou službou alebo komerčnou kuriérskou službou,

— balenie EUCI,

— technické protiopatrenia pre EUCI prepravované na elektronických dátových nosičoch,

— akékoľvek ďalšie procesné, fyzické alebo elektronické opatrenia,

— postupy evidencie,

— využitie zamestnancov s bezpečnostným oprávnením.

5. Bez ohľadu na článok 21 ods. 5 pri preprave EUCI na elektronických dátových nosičoch možno ochranné opatrenia uvedené vo vykonávacích predpisoch doplniť o primerané technické protiopatrenia schválené bezpečnostným orgánom Komisie s cieľom minimalizovať riziko straty alebo vyzradenia.

Článok 32

Ničenie EUCI

1. Utajované dokumenty EÚ, ktoré už nie sú potrebné, sa môžu zničiť, berúc do úvahy predpisy o archívoch, ako aj pravidlá a predpisy Komisie týkajúce sa správy dokumentov a archivácie, a najmä v súlade so spoločným zoznamom pre uchovávanie spisov Komisie.

2. EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a vyšším musí zničiť RCO príslušného registra EUCI na základe pokynu držiteľa alebo príslušného orgánu. RCO náležite aktualizuje denníky a ostatné evidenčné záznamy.

3. Pokiaľ ide o utajované dokumenty so stupňom utajenia SECRET UE/EU SECRET alebo TRÈS SECRET UE/EU TOP SECRET, toto ničenie vykonáva RCO za prítomnosti svedka, ktorý je preverený minimálne pre stupeň utajenia ničeného dokumentu.

4. Pracovník registra a svedok, ak sa vyžaduje jeho prítomnosť, podpíšu protokol o zničení, ktorý sa archivuje v registri. RCO príslušného registra EUCI uchováva protokoly o zničení dokumentov so stupňom utajenia TRÈS SECRET UE/EU TOP SECRET najmenej desať rokov a protokoly o zničení dokumentov so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET najmenej päť rokov.

5. Utajované dokumenty vrátane dokumentov so stupňom utajenia RESTREINT UE/EU RESTRICTED sa ničia spôsobmi, ktoré sa stanovia vo vykonávacích predpisoch a ktoré spĺňajú príslušné normy EÚ alebo rovnocenné normy.

6. Počítačové zálohové médiá použité na uchovávanie EUCI sa ničia v súlade s postupmi stanovenými vo vykonávacích predpisoch.

Článok 33

Ničenie EUCI v núdzových situáciách

1. Oddelenia Komisie, ktoré držia EUCI, pripravia plány, vychádzajúce z miestnych podmienok, na ochranu utajovanej veci EÚ v krízovej situácii aj na prípadnú likvidáciu, ako aj evakuačné plány. Oznámia pokyny, ktoré sa považujú za potrebné na to, aby sa EUCI nedostali do rúk neoprávnených osôb.

2. Dojednania na ochranu a/alebo zničenie veci so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET v čase krízy nemajú za žiadnych okolností nepriaznivo ovplyvňovať ochranu alebo zničenie veci so stupňom utajenia TRÈS SECRET UE/EU TOP SECRET vrátane kódovacieho zariadenia, ktorého ochrana má prednosť pred všetkými ostatnými úlohami.

3. V prípade núdzovej situácie, ak hrozí bezprostredné riziko neoprávneného zverejnenia, držiteľ zničí EUCI takým spôsobom, aby ich nebolo možné obnoviť ani v celku, ani čiastočne. Pôvodca a register pôvodu sa informujú o núdzovom zničení evidovaných EUCI.

4. Podrobnejšie ustanovenia týkajúce ničenia EUCI sa stanovia vo vykonávacích predpisoch.

KAPITOLA 5

OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ EÚ V KOMUNIKAČNÝCH A INFORMAČNÝCH SYSTÉMOCH (CIS)

Článok 34

Základné zásady informačnej bezpečnosti

1. Informačná bezpečnosť (Information Assurance – IA) v oblasti komunikačných a informačných systémov je záruka, že takéto systémy ochránia informácie, s ktorými manipulujú, a budú fungovať vtedy, keď je to potrebné a tak, ako majú, pod dohľadom oprávnených používateľov.

2. Účinná informačná bezpečnosť zaisťuje náležitú mieru:

pravosti: záruka, že informácie sú pravé a pochádzajú z dôveryhodných zdrojov;

dostupnosti: vlastnosť charakterizovaná prístupnosťou informácií a ich použiteľnosťou na požiadanie oprávneného subjektu;

dôvernosti: vlastnosť, ktorá znamená, že informácie sa nesprístupnia neoprávneným osobám, subjektom či procesom;

integrity: vlastnosť charakterizovaná zabezpečením presnosti a úplnosti informácií a majetku;

nespochybniteľnosti: schopnosť preukázať, že sa činnosť alebo udalosť uskutočnila, takže túto činnosť alebo udalosť nie je možné následne poprieť.

3. IA sa zakladá na procese riadenia rizík.

Článok 35

Vymedzenie pojmov

Na účely tejto kapitoly sa uplatňuje toto vymedzenie pojmov:

a) „akreditácia“ je formálne povolenie a schválenie, ktoré bezpečnostný akreditačný orgán (Security Accreditation Authority – SAA) vydá pre komunikačný a informačný systém na spracovanie EUCI v ich operačnom prostredí v nadväznosti na formálne schválenie bezpečnostného plánu a jeho správnu implementáciu;

b) „akreditačný proces“ sú potrebné kroky a úlohy požadované pred akreditáciou bezpečnostným akreditačným orgánom. Tieto kroky a úlohy sa bližšie určia v norme pre akreditačný proces;

c) „komunikačný a informačný systém“ (Communication and Information System – CIS) je každý systém, ktorý umožňuje manipuláciu s informáciami v elektronickej podobe. Komunikačný a informačný systém zahŕňa všetky zložky potrebné na jeho fungovanie vrátane infraštruktúry, organizácie, zamestnancov a informačných zdrojov;

d) „zvyškové riziko“ je riziko, ktoré zostáva po zavedení bezpečnostných opatrení, vzhľadom na to, že nie je možné čeliť všetkým hrozbám a nie je možné odstrániť všetky zraniteľné miesta;

e) „riziko“ je možnosť, že daná hrozba využije vnútornú alebo vonkajšiu zraniteľnosť organizácie alebo niektorého z používaných systémov a poškodí tak organizáciu a jej hmotný alebo nehmotný majetok. Meria sa ako kombinácia pravdepodobnosti výskytu hrozieb a ich následkov;

f) „akceptácia rizika“ je rozhodnutie znášať ďalšiu existenciu zvyškového rizika po zabezpečení sa proti rizikám;

g) „vyhodnotenie rizika“ je určenie hrozieb a zraniteľnosti a vykonanie príslušnej analýzy rizík, t. j. analýzy ich pravdepodobnosti a následkov;

h) „oznamovanie rizika“ je rozvíjanie informovanosti o rizikách medzi používateľskými komunitami CIS, informovanie schvaľovacích orgánov o týchto rizikách a podávanie správ o nich operačným orgánom;

i) „zabezpečenie sa proti riziku“ je zmiernenie, odstránenie alebo zmenšenie rizika (prostredníctvom vhodnej kombinácie technických, fyzických, organizačných a procesných opatrení), prenosu rizika alebo jeho monitorovania.

Článok 36

CIS, ktorými sa manipuluje s EUCI

1. Prostredníctvom CIS sa manipuluje s EUCI v súlade s koncepciou informačnej bezpečnosti.

2. Pokiaľ ide o CIS, ktorými sa manipuluje s EUCI, dodržiavanie politiky Komisie týkajúcej sa bezpečnosti informačných systémov, ako sa uvádza v rozhodnutí Komisie K(2006) 3602 ([1]), znamená, že:

a) sa používa prístup „plánuj, urob, skontroluj, vykonaj“ (Plan-Do-Check-Act) na vykonávanie politiky bezpečnosti informačných systémov počas celého životného cyklu informačného systému;

b) sa musia identifikovať bezpečnostné potreby prostredníctvom hodnotenia obchodného dosahu;

c) informačný systém a v ňom uložené údaje musia podliehať formálnej klasifikácii aktív;

([1]) K(2006) 3602 zo 16. augusta 2006 o bezpečnosti informačných systémov používaných Európskou komisiou.

d) sa musia vykonávať všetky povinné bezpečnostné opatrenia, ako sa stanovuje v politike týkajúcej sa bezpečnosti informačných systémov;

e) sa musí uplatňovať proces riadenia rizík, ktorý pozostáva z týchto krokov: identifikácia hrozieb a zraniteľnosti, hodnotenie rizika, zabezpečenie sa proti riziku, akceptácia rizika a oznamovanie rizika;

f) sa vymedzí, vykonáva, kontroluje a prehodnocuje bezpečnostný plán vrátane bezpečnostnej politiky a bezpečnostných prevádzkových postupov.

3. Všetci zamestnanci zapojení do navrhovania, vývoja, testovania, prevádzky, riadenia alebo používania CIS, ktorými sa manipuluje s EUCI, oznámia bezpečnostnému akreditačnému orgánu všetky potenciálne bezpečnostné nedostatky, incidenty, narušenia bezpečnosti alebo vyzradenia, ktoré môžu mať vplyv na ochranu CIS a/alebo v nich uložených EUCI.

4. Ak ochranu EUCI zabezpečujú kryptografické produkty, tieto produkty sa schvaľujú takto:

a) uprednostnia sa produkty, ktoré boli schválené Radou alebo generálnym tajomníkom Rady v jeho funkcii kryptografického schvaľovacieho orgánu Rady na základe odporúčania skupiny bezpečnostných expertov Komisie;

b) ak si to vyžadujú osobitné operačné okolnosti, kryptografický schvaľovací orgán Komisie (Crypto Approval Authority – CAA) na základe odporúčania skupiny bezpečnostných expertov Komisie upustí od požiadaviek uvedených v písmene a) a udelí dočasné schválenie na určité obdobie.

5. Počas prenosu, spracovávania a uchovávania EUCI elektronickými prostriedkami sa použijú schválené kryptografické produkty. Bez ohľadu na túto požiadavku možno v núdzových situáciách alebo pri špecifických technických konfiguráciách použiť špecifické postupy schválené CAA.

6. CIS, ktorými sa manipuluje utajovanými skutočnosťami so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, sú bezpečnostnými opatreniami chránené proti vyzradeniu takýchto skutočností prostredníctvom neúmyselného elektromagnetického vyžarovania („bezpečnostné opatrenia TEMPEST“). Takéto bezpečnostné opatrenia sú primerané rizikám zneužitia a stupňu utajenia daných utajovaných skutočností.

7. Bezpečnostný orgán Komisie pôsobí ako:

— orgán pre informačnú bezpečnosť (IAA),

— bezpečnostný akreditačný orgán (SAA),

— orgán pre TEMPEST (TA),

— kryptografický schvaľovací orgán (CAA),

— kryptografický distribučný orgán (CDA).

8. Bezpečnostný orgán Komisie vymenuje pre každý systém operačný orgán pre informačnú bezpečnosť.

9. Povinnosti súvisiace s funkciami opísanými v odsekoch 7 a 8 sa stanovia vo vykonávacích predpisoch.

Článok 37

Akreditácia CIS, ktorými sa manipuluje s EUCI

1. Všetky CIS, ktorými sa manipuluje s EUCI, podliehajú akreditačnému procesu na základe zásad informačnej bezpečnosti, ktorých úroveň podrobnosti musí byť úmerná požadovanej úrovni ochrany.

2. Akreditačný proces musí obsahovať formálne potvrdenie bezpečnostného akreditačného orgánu Komisie týkajúce sa bezpečnostného plánu pre dotknutý CIS s cieľom uistiť sa, že:

a) proces riadenia rizík, ako sa uvádza v článku 36 ods. 2, bol riadne vykonaný;

b) vlastník systému vedome akceptoval zvyškové riziko a

c) sa dosiahla dostatočná úroveň ochrany CIS a EUCI, s ktorými sa v ňom manipuluje, v súlade s týmto rozhodnutím.

3. Bezpečnostný akreditačný orgán Komisie vydá potvrdenie o akreditácii, v ktorom sa stanoví najvyšší stupeň utajenia EUCI, s ktorými sa môže manipulovať v CIS, ako aj príslušné operačné podmienky a požiadavky. Netýka sa to úloh zverených rade pre bezpečnostnú akreditáciu vymedzenej v článku 11 nariadenia Európskeho parlamentu a Rady (EÚ) č. 512/2014 ([1]).

4. Spoločná rada pre bezpečnostnú akreditáciu (SAB) zodpovedá za akreditáciu CIS Komisie, na ktorej sa zúčastňujú viaceré strany. Skladá sa zo zástupcu SAA každej zúčastnenej strany a predsedá jej zástupca SAA Komisie.

5. Akreditačný proces pozostáva zo série úloh, ktoré musia zúčastnené strany vykonať. Zodpovednosť za prípravu akreditačných spisov a dokumentácie nesie v plnej miere vlastník systému CIS.

6. Za akreditáciu je zodpovedný bezpečnostný akreditačný orgán Komisie, ktorý kedykoľvek v priebehu životného cyklu CIS má právo:

a) vyžadovať vykonanie akreditačného procesu;

b) vykonať audit alebo inšpekciu CIS;

c) ak podmienky na prevádzku už nie sú splnené, vyžadovať vymedzenie a účinné vykonávanie plánu na zlepšovanie bezpečnosti v rámci presne stanoveného časového rozvrhu, prípadne odobratie povolenia na prevádzku CIS, kým podmienky na prevádzku nebudú opäť splnené.

7. Akreditačný proces musí byť stanovený v norme týkajúcej sa akreditačného procesu pre CIS, ktorými sa manipuluje s EUCI, ktorá sa prijme v súlade s článkom 10 ods. 3 rozhodnutia Komisie K(2006) 3602.

Článok 38

Núdzové situácie

1. Bez ohľadu na ustanovenia tejto kapitoly sa môžu v núdzových situáciách, ako napríklad pri bezprostredne hroziacej kríze alebo počas krízy, pri konflikte, vo vojnovom stave alebo pri výnimočných operačných okolnostiach, uplatňovať osobitné postupy uvedené nižšie.

2. EUCI sa môžu so súhlasom príslušného orgánu prenášať kryptografickými produktmi, ktoré boli schválené pre nižší stupeň utajenia, alebo v nešifrovanej podobe, pokiaľ by akékoľvek zdržanie spôsobilo škody, ktoré jednoznačne prevyšujú škodu spôsobenú akýmkoľvek neoprávneným zverejnením utajovanej veci, a ak:

a) odosielateľ a príjemca nemajú požadované šifrovacie zariadenie a

b) utajovanú vec nemožno včas doručiť inými prostriedkami.

3. Utajované skutočnosti prenášané za okolností uvedených v odseku 1 nesmú mať nijaké označenia alebo odkazy, ktorými by sa odlišovali od neutajovanej skutočnosti alebo skutočnosti, ktorá sa môže chrániť dostupným kryptografickým produktom. Príjemcovia sa o stupni utajenia skutočnosti bezodkladne informujú iným spôsobom.

4. Následná správa sa zašle príslušnému orgánu a skupine bezpečnostných expertov Komisie.

KAPITOLA 6

PRIEMYSELNÁ BEZPEČNOSŤ

Článok 39

Základné zásady

1. Priemyselná bezpečnosť je uplatňovanie opatrení na zabezpečenie ochrany EUCI

a) v rámci utajovaných zmlúv zo strany:

   i) záujemcov alebo uchádzačov počas výberového alebo zadávacieho konania;

   ii) dodávateľov alebo subdodávateľov počas celého životného cyklu utajovanej zmluvy;

([1]) Nariadenie Európskeho parlamentu a Rady (EÚ) č. 512/2014 zo 16. apríla 2014, ktorým sa mení nariadenie (EÚ) č. 912/2010 o zriadení Agentúry pre európsky GNSS (Ú. v. EÚ L 150, 20.5.2014, s. 72).

b) v rámci utajovaných dohôd o grante zo strany:

i) žiadateľov počas postupov udeľovania grantu;

ii) príjemcov počas celého životného cyklu utajovanej dohody o grante.

2. Takéto zmluvy alebo dohody o grante nezahŕňajú prístup k utajovaným skutočnostiam so stupňom utajenia TRÈS SECRET UE/EU TOP SECRET.

3. Pokiaľ sa neuvádza inak, ustanovenia tejto kapitoly týkajúce sa utajovaných zmlúv alebo dodávateľov sa uplatňujú aj na utajované subdodávateľské zmluvy alebo subdodávateľov.

Článok 40

Vymedzenie pojmov

Na účely tejto kapitoly sa uplatňuje toto vymedzenie pojmov:

a) „utajovaná zmluva“ je rámcová zmluva alebo zmluva, ako sa uvádza v nariadení Rady (ES, Euratom) č. 1605/2002 ([1]), ktorú Komisia alebo jedno z jej oddelení uzavrelo s dodávateľom na dodávku hnuteľného alebo nehnuteľného majetku, vykonanie prác alebo poskytnutie služieb, ktorej plnenie si vyžaduje alebo zahŕňa vytvorenie, uchovávanie EUCI alebo manipuláciu s nimi;

b) „utajovaná subdodávateľská zmluva“ je zmluva, ktorú dodávateľ Komisie alebo jedného z jej oddelení uzavrel s iným dodávateľom (t. j. subdodávateľom) na dodávku hnuteľného alebo nehnuteľného majetku, vykonanie prác alebo poskytnutie služieb, ktorej plnenie si vyžaduje alebo zahŕňa vytvorenie, uchovávanie EUCI alebo manipuláciu s nimi;

c) „utajovaná dohoda o grante“ je dohoda, ktorou Komisia udelí grant, ako sa uvádza v hlave VI časti I nariadenia (ES, Euratom) č. 1605/2002, ktorej plnenie si vyžaduje alebo zahŕňa vytvorenie, uchovávanie EUCI alebo manipuláciu s nimi;

d) „určený bezpečnostný orgán“ (Designated Security Authority – DSA) je orgán podliehajúci národnému bezpečnostnému orgánu (NSA) členského štátu, ktorý je zodpovedný za informovanie priemyselných alebo iných subjektov o vnútroštátnej politike vo všetkých záležitostiach priemyselnej bezpečnosti a za usmerňovanie a podporu pri jej vykonávaní. Funkciu DSA môže vykonávať NSA alebo ktorýkoľvek iný príslušný orgán.

Článok 41

Postup v prípade utajovaných zmlúv alebo dohôd o grante

1. Každé oddelenie Komisie ako verejný obstarávateľ zabezpečí, že pri uzatváraní utajovaných zmlúv alebo dohôd o grante sú uvedené alebo do zmluvy zahrnuté a splnené minimálne normy priemyselnej bezpečnosti stanovené v tejto kapitole.

2. Na účely odseku 1 sa príslušné útvary Komisie obrátia na Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť, a najmä na riaditeľstvo pre bezpečnosť, a zabezpečia, aby vzorové zmluvy, subdodávateľské zmluvy a vzorové dohody o grante obsahovali ustanovenia, ktoré odrážajú základné zásady a minimálne normy na ochranu EUCI, ktoré musia dodržiavať dodávatelia a subdodávatelia, resp. príjemcovia prostriedkov na základe dohôd o grante.

3. Komisia úzko spolupracuje s NSA, DSA alebo akýmkoľvek iným príslušným orgánom dotknutého členského štátu.

4. Ak verejný obstarávateľ plánuje začať postup zameraný na uzavretie utajovanej zmluvy alebo dohody o grante, musí požiadať bezpečnostný orgán Komisie o radu k otázkam týkajúcim sa tajnej povahy a prvkov postupu vo všetkých jeho etapách.

5. Po konzultácii so skupinou bezpečnostných expertov Komisie sa vo vykonávacích predpisoch o priemyselnej bezpečnosti stanovia vzory a modely pre utajované zmluvy a subdodávateľské zmluvy, utajované dohody o grante, oznámenia o vyhlásení verejného obstarávania, usmernenia týkajúce sa okolností, keď sa vyžadujú priemyselné bezpečnostné previerky, bezpečnostné pokyny pre program alebo projekt, bezpečnostné doložky, návštevy, prenos a preprava EUCI v rámci utajovaných zmlúv alebo utajovaných dohôd o grante.

([1]) Nariadenie Rady (ES, Euratom) č. 1605/2002 z 25. júna 2002 o rozpočtových pravidlách, ktoré sa vzťahujú na všeobecný rozpočet Európskych spoločenstiev (Ú. v. ES L 248, 16.9.2002, s. 1).

6. Komisia môže uzavrieť utajovanú zmluvu alebo dohodu o grante, ktorou sa zverujú úlohy zahŕňajúce alebo vyžadujúce prístup k EUCI, manipuláciu s nimi alebo ich uchovávanie hospodárskymi subjektmi so sídlom v členskom štáte alebo v treťom štáte, ktorý uzavrel dohodu alebo administratívne dojednanie v súlade s kapitolou 7 tohto rozhodnutia.

Článok 42

Bezpečnostné prvky v utajovanej zmluve alebo dohode o grante

1. Utajované zmluvy alebo dohody o grante musia obsahovať tieto bezpečnostné prvky:

Bezpečnostné pokyny pre program alebo projekt

a) „Bezpečnostné pokyny pre program alebo projekt“ (Programme or Project Security Instruction – PSI) je zoznam bezpečnostných postupov, ktoré sa uplatňujú v rámci konkrétneho programu/projektu s cieľom štandardizovať bezpečnostné postupy. Počas trvania programu alebo projektu sa môžu revidovať.

b) Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť vypracuje všeobecné PSI. Oddelenia Komisie zodpovedné za programy alebo projekty zahŕňajúce manipuláciu s EUCI alebo ich uchovávanie môžu tam, kde je to vhodné, vypracovať špecifické PSI založené na všeobecných PSI.

c) Špecifické PSI sa vypracujú najmä pre programy a projekty, ktoré sa vyznačujú značným rozsahom, škálou alebo zložitosťou, alebo množstvom a/alebo rozmanitosťou dodávateľov, príjemcov a iných partnerov a zúčastnených strán, napríklad pokiaľ ide o ich právne postavenie. Špecifické PSI vypracuje oddelenie (oddelenia) Komisie, ktoré program alebo projekt riadi, v úzkej spolupráci s generálnym riaditeľstvom pre ľudské zdroje a bezpečnosť.

d) Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť predloží všeobecné a špecifické PSI skupine bezpečnostných expertov Komisie na posúdenie.

Bezpečnostná doložka

a) „Bezpečnostná doložka“ (Security Aspects Letter – SAL) je súbor osobitných zmluvných podmienok vydaných verejným obstarávateľom, v ktorom sa stanovujú bezpečnostné požiadavky alebo prvky zmluvy vyžadujúce si bezpečnostnú ochranu a ktorý tvorí neoddeliteľnú súčasť každej utajovanej zmluvy, ktorá si vyžaduje prístup k EUCI alebo v rámci ktorej sa takéto utajované skutočnosti tvoria.

b) Osobitné zmluvné podmienky sú opísané v bezpečnostnej doložke, ktorá v prípade potreby obsahuje sprievodcu stupňami utajenia (Security Classification Guide – SCG) a ktorá tvorí neoddeliteľnú súčasť utajovanej zmluvy alebo subdodávateľskej zmluvy, resp. dohody o grante.

c) SAL obsahuje ustanovenia, podľa ktorých musí dodávateľ alebo príjemca dodržiavať minimálne normy stanovené v tomto rozhodnutí. Verejný obstarávateľ zabezpečí, aby sa v SAL uvádzalo, že nedodržiavanie týchto minimálnych noriem sa môže považovať za dostatočné dôvody na vypovedanie zmluvy alebo dohody o grante.

2. PSI, ako aj SAL musia obsahovať ako povinný bezpečnostný prvok SCG:

a) „Sprievodca stupňami utajenia“ (SCG) je dokument, ktorý opisuje prvky programu, projektu, zmluvy alebo dohody o grante, ktoré sú utajené, pričom uvádza uplatniteľné stupne utajenia. SCG sa môže v priebehu programu, projektu, zmluvy alebo dohody o grante rozšíriť a stupeň utajenia prvkov informácií sa môže zmeniť alebo znížiť. Ak SCG existuje, musí byť súčasťou SAL.

b) Pred začatím výberového konania alebo uzavretím utajovanej zmluvy oddelenie Komisie ako verejný obstarávateľ určí stupeň utajenia všetkých utajovaných skutočností, ktoré sa majú poskytnúť záujemcom a uchádzačom alebo dodávateľom, ako aj stupeň utajenia všetkých utajovaných skutočností, ktoré dodávateľ vytvorí. Na tento účel oddelenie Komisie pripraví SCG, ktorý sa bude uplatňovať pri plnení zmluvy, v súlade s týmto rozhodnutím a jeho vykonávacími predpismi po porade s bezpečnostným orgánom Komisie.

c) Pri určovaní stupňa utajenia rôznych prvkov utajovanej zmluvy sa uplatňujú tieto zásady:

i) pri príprave SCG oddelenie Komisie ako verejný obstarávateľ zohľadňuje všetky príslušné bezpečnostné hľadiská vrátane stupňa utajenia, ktorý utajovanej skutočnosti poskytnutej a schválenej na použitie v súvislosti so zmluvou určil jej pôvodca;

ii) celkový stupeň utajenia zmluvy nesmie byť nižší ako najvyšší stupeň utajenia ktoréhokoľvek z jej prvkov;

iii) a ak je to relevantné, v prípade akejkoľvek zmeny týkajúcej sa stupňa utajenia skutočností, ktoré dodávatelia vytvorili alebo ktoré im boli poskytnuté počas plnenia zmluvy, alebo v prípade následných zmien v SCG, sa verejný obstarávateľ prostredníctvom bezpečnostného orgánu Komisie spojí s NSA, DSA členského štátu alebo s ktorýmkoľvek iným dotknutým príslušným bezpečnostným orgánom.

Článok 43

Prístup k EUCI pre zamestnancov dodávateľov a príjemcov

Verejný obstarávateľ alebo orgán poskytujúci grant zabezpečí, aby utajovaná zmluva alebo utajovaná dohoda o grante obsahovala ustanovenia, v ktorých sa uvádza, že zamestnancom dodávateľa, subdodávateľa alebo príjemcu, ktorí si na účely plnenia utajovanej zmluvy, subdodávateľskej zmluvy alebo dohody o grante vyžadujú prístup k EUCI, sa poskytuje takýto prístup, len ak:

a) dostali bezpečnostné oprávnenie na príslušný stupeň alebo boli inak riadne oprávnení z dôvodu ich potreby poznať;

b) boli poučení o uplatniteľných bezpečnostných predpisoch a postupoch ochrany EUCI a vzali na vedomie svoje povinnosti v súvislosti s ochranou takýchto utajovaných skutočností;

c) boli bezpečnostne preverení pre zodpovedajúci stupeň utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET príslušným NSA, DSA alebo akýmkoľvek iným príslušným orgánom.

Článok 44

Priemyselná bezpečnostná previerka

1. „Priemyselná bezpečnostná previerka“ (Facility Security Clearance – FSC) je správne rozhodnutie NSA, DSA alebo akéhokoľvek iného príslušného bezpečnostného orgánu, že zariadenie môže z hľadiska bezpečnosti zaistiť primeranú ochranu EUCI pre určený stupeň utajenia.

2. FSC udelená NSA, DSA alebo akýmkoľvek iným príslušným bezpečnostným orgánom členského štátu s cieľom uviesť v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi, že hospodársky subjekt je schopný chrániť EUCI na príslušnom stupni utajenia (CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET) vo svojich zariadeniach, sa predloží bezpečnostnému orgánu Komisie, ktorý ju postúpi oddeleniu Komisie konajúcemu ako verejný obstarávateľ alebo orgán poskytujúci grant pred tým, než sa záujemcovi, uchádzačovi alebo dodávateľovi, resp. žiadateľovi o grant alebo príjemcovi grantu poskytne alebo udelí prístup k EUCI.

3. V prípade potreby verejný obstarávateľ oznámi prostredníctvom bezpečnostného orgánu Komisie príslušnému NSA, DSA alebo akémukoľvek inému príslušnému bezpečnostnému orgánu, že FSC je potrebná na účely plnenia zmluvy. FSC alebo PSC sa vyžaduje, ak sa počas postupu verejného obstarávania alebo udelenia grantu musia poskytnúť EUCI so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET.

4. Verejný obstarávateľ alebo orgán poskytujúci grant neuzavrie utajovanú zmluvu alebo dohodu o grante s uprednostňovaným uchádzačom alebo účastníkom, kým mu NSA, DSA alebo akýkoľvek iný príslušný bezpečnostný orgán členského štátu, v ktorom má dotknutý dodávateľ alebo subdodávateľ sídlo, nepotvrdí, že príslušná FSC bola v potrebných prípadoch vydaná.

5. Keď bol bezpečnostný orgán Komisie informovaný NSA, DSA alebo akýmkoľvek iným príslušným bezpečnostným orgánom, ktorý vydal FSC, o zmenách, ktoré majú vplyv na FSC, informuje o tom oddelenie Komisie konajúce ako verejný obstarávateľ alebo orgán poskytujúci grant. V prípade subdodávateľskej zmluvy sa náležite informuje NSA, DSA alebo akýkoľvek iný príslušný bezpečnostný orgán.

6. Odňatie FSC príslušným NSA, DSA alebo akýmkoľvek iným príslušným bezpečnostným orgánom predstavuje pre verejného obstarávateľa alebo orgán poskytujúci grant dostatočný dôvod na vypovedanie utajovanej zmluvy alebo na vylúčenie záujemcu, uchádzača alebo žiadateľa zo súťaže. Ustanovenie v tomto zmysle sa uvedie vo vzorových zmluvách a dohodách o grante, ktoré sa majú vypracovať.

Článok 45

Ustanovenia týkajúce sa utajovaných zmlúv alebo dohôd o grante

1. Ak sa EUCI poskytujú záujemcovi, uchádzačovi alebo žiadateľovi počas postupu verejného obstarávania, výzva na predkladanie ponúk obsahuje ustanovenie, že záujemca, uchádzač alebo žiadateľ, ktorý nepredloží ponuku alebo ktorý nie je vybratý, musí v stanovenej lehote vrátiť všetky utajované dokumenty.

2. Verejný obstarávateľ alebo orgán poskytujúci grant oznámi prostredníctvom bezpečnostného orgánu Komisie príslušnému NSA, DSA alebo akémukoľvek inému príslušnému bezpečnostnému orgánu skutočnosť, že utajovaná zmluva alebo dohoda o grante bola udelená, ako aj relevantné údaje, ako sú meno dodávateľov alebo príjemcov, trvanie zmluvy a maximálny stupeň utajenia.

3. Keď sa takéto zmluvy alebo dohody o grante vypovedajú, verejný obstarávateľ alebo orgán poskytujúci grant to bezodkladne oznámi prostredníctvom bezpečnostného orgánu Komisie NSA, DSA alebo akémukoľvek inému príslušnému bezpečnostnému orgánu členského štátu, v ktorom má dodávateľ alebo príjemca grantu sídlo.

4. Od dodávateľa alebo príjemcu grantu sa spravidla požaduje, aby po vypovedaní utajovanej zmluvy alebo dohody o grante vrátil verejnému obstarávateľovi alebo orgánu poskytujúcemu grant všetky EUCI, ktorých je držiteľom.

5. V SAL sa stanovia osobitné ustanovenia týkajúce sa manipulácie s EUCI počas plnenia utajovanej zmluvy alebo utajovanej dohody o grante alebo po jej vypovedaní.

6. Ak sa dodávateľovi alebo príjemcovi dohody povolí, aby si ponechal utajované EUCI po vypovedaní utajovanej zmluvy alebo dohody o grante, musí naďalej spĺňať minimálne normy uvedené v tomto rozhodnutí a chrániť dôvernosť EUCI.

Článok 46

Osobitné ustanovenia týkajúce sa utajovaných zmlúv

1. Podmienky týkajúce sa ochrany EUCI, za ktorých môže dodávateľ uzatvárať subdodávateľské zmluvy, sa musia vymedziť vo výzve na predkladanie ponúk a v utajovanej zmluve.

2. Dodávateľ musí získať povolenie od verejného obstarávateľa pred tým, ako zadá niektorú z častí utajovanej zmluvy subdodávateľom. Žiadna zákazka, ktorá si vyžaduje prístup k EUCI, nesmie byť zadaná subdodávateľom so sídlom v tretej krajine, pokiaľ neexistuje regulačný rámec pre bezpečnosť informácií, ako sa uvádza v kapitole 7.

3. Dodávateľ je zodpovedný za zabezpečenie toho, aby boli všetky subdodávateľské činnosti realizované v súlade s minimálnymi normami stanovenými v tomto rozhodnutí, a nesmie poskytnúť EUCI subdodávateľovi bez predchádzajúceho písomného súhlasu verejného obstarávateľa.

4. Pokiaľ ide o EUCI, ktoré vytvoril alebo s ktorými manipuluje dodávateľ, Komisia sa považuje za pôvodcu, a práva prináležiace pôvodcovi vykonáva verejný obstarávateľ.

Článok 47

Návštevy vykonávané v súvislosti s utajovanými zmluvami

1. Ak zamestnanci Komisie alebo dodávateľa či príjemcu grantu potrebujú na účely plnenia utajovanej zmluvy alebo dohody o grante prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET v objektoch druhej strany, spoločne organizujú návštevy svojich objektov v spolupráci s NSA, DSA alebo akýmkoľvek iným dotknutým príslušným bezpečnostným orgánom. O týchto návštevách je informovaný bezpečnostný orgán Komisie. V súvislosti so špecifickými programami alebo projektmi však NSA, DSA alebo akýkoľvek iný príslušný bezpečnostný orgán môžu súhlasiť aj s postupom, pri ktorom sa takéto návštevy môžu organizovať priamo.

2. Všetci návštevníci musia byť držiteľmi príslušných personálnych bezpečnostných previerok a na účely prístupu k EUCI, ktoré sa týkajú utajovanej zmluvy, musia mať potrebu poznať.

3. Návštevníkom sa udelí prístup len k EUCI, ktoré sa týkajú účelu návštevy.

4. Podrobnejšie ustanovenia sa stanovia vo vykonávacích predpisoch.

5. Dodržiavanie ustanovení týkajúcich sa návštev v súvislosti s utajovanými zmluvami, ktoré sú stanovené v tomto rozhodnutí a vo vykonávacích pravidlách uvedených v odseku 4, je povinné.

Článok 48

Prenos a preprava EUCI v súvislosti s utajovanými zmluvami alebo utajovanými dohodami o grante

1. Pokiaľ ide o prenos EUCI elektronickými prostriedkami, uplatňujú sa príslušné ustanovenia kapitoly 5 tohto rozhodnutia.

2. Pokiaľ ide o prepravu EUCI, uplatňujú sa príslušné ustanovenia kapitoly 4 tohto rozhodnutia a jeho vykonávacích predpisov v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi.

3. Pri určovaní bezpečnostných opatrení na prepravu utajovaných vecí ako nákladu sa uplatňujú tieto zásady:

a) bezpečnosť sa zaisťuje počas všetkých etáp prepravy z miesta pôvodu na miesto konečného určenia;

b) úroveň ochrany zásielky sa určuje podľa stupňa utajenia veci s najvyšším stupňom utajenia, ktorá sa v nej nachádza;

c) pred každou cezhraničnou prepravou veci so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET odosielateľ vypracuje plán prepravy, ktorý schváli NSA, DSA alebo akýkoľvek iný dotknutý príslušný bezpečnostný orgán;

d) cesty sa v čo najväčšom možnom rozsahu vykonávajú priamo z miesta pôvodu na miesto určenia a uskutočňujú sa v čo najkratšom čase, aký umožňujú okolnosti;

e) ak je to možné, trasy ciest by mali prechádzať len cez územia členských štátov. Cesty cez štáty, ktoré nie sú členskými štátmi, by sa mali realizovať len v prípade, ak ich povolí NSA, DSA alebo akýkoľvek iný príslušný bezpečnostný orgán štátu odosielateľa aj príjemcu.

Článok 49

Postúpenie EUCI dodávateľom alebo príjemcom grantu, ktorí sa nachádzajú v tretích štátoch

Postúpenie EUCI dodávateľom alebo príjemcom grantu, ktorí sa nachádzajú v tretích štátoch, sa uskutočňuje v súlade s bezpečnostnými opatreniami dohodnutými medzi bezpečnostným orgánom Komisie, oddelením Komisie ako verejným obstarávateľom, resp. orgánom poskytujúcim grant a NSA, DSA alebo iným príslušným bezpečnostným orgánom dotknutého tretieho štátu, v ktorom má dodávateľ alebo príjemca grantu sídlo.

Článok 50

Manipulácia s utajovanými skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED v súvislosti s utajovanými zmluvami alebo utajovanými dohodami o grante

1. Ochrana utajovaných skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED, s ktorými sa manipuluje alebo ktoré sa uchovávajú v rámci utajovaných zmlúv alebo dohôd o grante, sa zakladá na zásadách proporcionality a nákladovej efektívnosti.

2. V súvislosti s utajovanými zmluvami alebo utajovanými dohodami o grante, ktoré zahŕňajú manipuláciu s utajovanými skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED, sa nevyžaduje žiadna FSC ani PSC.

3. Ak sa v rámci zmluvy alebo dohody o grante manipuluje s utajovanými skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED v CIS, ktorý prevádzkuje dodávateľ alebo príjemca grantu, verejný obstarávateľ, resp. orgán poskytujúci grant zabezpečí po konzultácii s bezpečnostným orgánom Komisie, aby sa v zmluve alebo dohode o grante uvádzali potrebné technické a administratívne požiadavky týkajúce sa akreditácie alebo schválenia CIS zodpovedajúce vyhodnotenému riziku, pričom sa zohľadnia všetky relevantné faktory. Rozsah akreditácie alebo schválenia takého CIS dohodnú bezpečnostný orgán Komisie a príslušný NSA alebo DSA.

KAPITOLA 7

VÝMENA UTAJOVANÝCH SKUTOČNOSTÍ S OSTATNÝMI INŠTITÚCIAMI, AGENTÚRAMI, ORGÁNMI A ÚRADMI ÚNIE, ČLENSKÝMI ŠTÁTMI A TRETÍMI ŠTÁTMI A MEDZINÁRODNÝMI ORGANIZÁCIAMI

Článok 51

Základné zásady

1. Ak Komisia alebo jedno z jej oddelení rozhodne, že je potrebná výmena EUCI s inou inštitúciou, agentúrou, orgánom alebo úradom Únie alebo s tretím štátom alebo medzinárodnou organizáciou, podniknú sa nevyhnutné kroky na vytvorenie vhodného právneho alebo administratívneho rámca na tento účel, čo môže zahŕňať dohody o bezpečnosti utajovaných skutočností alebo administratívne dojednania uzavreté v súlade s príslušnými právnymi predpismi.

2. Bez toho, aby bol dotknutý článok 57, EUCI sa vymieňajú s inou inštitúciou, agentúrou, orgánom alebo úradom Únie, alebo s tretím štátom alebo medzinárodnou organizáciou len vtedy, ak existuje takýto právny alebo administratívny rámec a ak existujú dostatočné záruky, že inštitúcia, agentúra, orgán alebo úrad Únie, alebo tretí štát alebo medzinárodná organizácia uplatňuje rovnaké základné zásady a minimálne normy na ochranu utajovaných skutočností.

Článok 52

Výmena EUCI s ostatnými inštitúciami, agentúrami, orgánmi a úradmi Únie

1. Pred uzavretím administratívneho dojednania o výmene EUCI s inou inštitúciou, agentúrou, orgánom alebo úradom Únie, si Komisia vyžiada záruku, že dotknutá inštitúcia, agentúra, orgán alebo úrad Únie:

a) má regulačný rámec na ochranu EUCI, v ktorom sa stanovujú základné zásady a minimálne normy rovnocenné s tými, ktoré sú stanovené v tomto rozhodnutí a jeho vykonávacích predpisoch;

b) uplatňuje bezpečnostné normy a usmernenia týkajúce sa personálnej bezpečnosti, fyzickej bezpečnosti, správy EUCI a bezpečnosti komunikačných a informačných systémov (CIS), ktoré zaručujú úroveň ochrany EUCI rovnocennú s úrovňou, ktorá sa uplatňuje v Komisii;

c) označuje utajované skutočností, ktoré vytvára, ako EUCI.

2. Generálne riaditeľstvo pre ľudské zdroje a bezpečnosť v úzkej spolupráci s ostatnými príslušnými oddeleniami Komisie je vedúcim útvarom v Komisii na uzavretie administratívnych dojednaní o výmene EUCI s ostatným inštitúciami, agentúrami, orgánmi alebo úradmi EÚ.

3. Administratívne dojednania majú spravidla formu výmeny listov, ktoré v mene Komisie podpisuje generálny riaditeľ pre ľudské zdroje a bezpečnosť.

4. Pred uzavretím administratívneho dojednania o výmene EUCI vykoná bezpečnostný orgán Komisie hodnotiacu návštevu zameranú na posúdenie regulačného rámca na ochranu EUCI a zistenie účinnosti opatrení zavedených na ochranu EUCI. Administratívne dojednanie nadobúda účinnosť a EUCI sa vymieňajú iba vtedy, ak výsledky tejto hodnotiacej návštevy boli uspokojivé a odporúčania v nadväznosti na návštevu boli splnené. Pravidelné následné hodnotiace návštevy sa vykonávajú na overenie, či sa dodržiavajú administratívne dojednania a či platné bezpečnostné opatrenia naďalej spĺňajú základné zásady a minimálne normy, ktoré boli dohodnuté.

5. V Komisii je register EUCI, ktorý spravuje Generálny sekretariát, spravidla hlavným vstupným a výstupným bodom utajovaných skutočností s ostatnými inštitúciami, agentúrami, orgánmi a úradmi Únie. Ak je to však z bezpečnostných, organizačných alebo prevádzkových dôvodov na ochranu EUCI vhodnejšie, miestne registre EUCI v oddeleniach Komisie v súlade s týmto rozhodnutím a jeho vykonávacími predpismi pôsobia ako vstupný a výstupný bod utajovaných skutočností, pokiaľ ide o záležitosti v rámci právomoci príslušných oddelení Komisie.

6. O procese uzatvárania administratívnych dojednaní podľa odseku 2 je informovaná skupina bezpečnostných expertov Komisie.

Článok 53

Výmena EUCI s členskými štátmi

1. EUCI sa môžu vymieňať a poskytovať členským štátom za predpokladu, že tieto ochraňujú EUCI v súlade s požiadavkami uplatňovanými na utajované skutočnosti, ktoré sú označené vnútroštátnym stupňom utajenia na rovnakej úrovni, ako sa uvádza v ekvivalenčnej tabuľke stupňov utajenia uvedenej v prílohe I.

2. Keď členské štáty poskytnú štruktúram alebo sieťam Európskej únie utajované skutočnosti, ktoré sú označené národným označením stupňa utajenia, Komisia ich chráni v súlade s požiadavkami uplatňovanými na EUCI s rovnocenným stupňom utajenia stanoveným podľa ekvivalenčnej tabuľky stupňov utajenia, ktorá sa uvádza v prílohe I.

Článok 54

Výmena EUCI s tretími štátmi a medzinárodnými organizáciami

1. Ak Komisia stanoví, že existuje dlhodobá potreba výmeny utajovaných skutočností s tretími štátmi alebo medzinárodnými organizáciami, podniknú sa nevyhnutné kroky na vytvorenie vhodného právneho alebo administratívneho rámca na tento účel, čo môže zahŕňať dohody o bezpečnosti utajovaných skutočností alebo administratívne dojednania uzavreté v súlade s príslušnými právnymi predpismi.

2. Tieto dohody o bezpečnosti utajovaných skutočností alebo administratívne dojednania uvedené v odseku 1 obsahujú ustanovenia, ktorými sa zabezpečuje, že tretie štáty alebo medzinárodné organizácie, ktoré prijmú EUCI, chránia takéto skutočnosti na úrovni, ktorá zodpovedá ich stupňu utajenia, a v súlade s minimálnymi normami, ktoré sú rovnocenné s normami stanovenými v tomto rozhodnutí.

3. Komisia môže v súlade s článkom 56 uzavrieť administratívne dojednania, pokiaľ stupeň utajenia EUCI spravidla nie je vyšší ako RESTREINT UE/EU RESTRICTED.

4. Tieto administratívne dojednania o výmene utajovaných skutočností uvedené v odseku 3 obsahujú ustanovenia, ktorými sa zabezpečuje, že tretie štáty alebo medzinárodné organizácie, ktoré prijmú EUCI, chránia takéto skutočnosti na úrovni, ktorá zodpovedá ich stupňu utajenia, a v súlade s minimálnymi normami, ktoré sú rovnocenné s normami stanovenými v tomto rozhodnutí. O uzavretí dohôd o bezpečnosti utajovaných skutočností alebo administratívnych dojednaní sa treba poradiť so skupinou bezpečnostných expertov Komisie.

5. Rozhodnutie o poskytnutí EUCI, ktorých pôvodcom je Komisia, tretiemu štátu alebo medzinárodnej organizácii prijíma v každom jednotlivom prípade oddelenie Komisie ako pôvodca EUCI v Komisii na základe povahy a obsahu týchto utajovaných skutočností, príjemcovej potreby poznať a miery výhod, ktoré z toho pre Úniu vyplývajú. Ak Komisia nie je pôvodcom utajovaných skutočností, ktoré sa majú poskytnúť, alebo zdrojového materiálu, ktorý môžu obsahovať, oddelenie Komisie, ktoré je držiteľom takých utajovaných informácií, najprv získa od ich pôvodcu písomný súhlas s poskytnutím. Ak nie je možné stanoviť pôvodcu, oddelenie Komisie, ktoré je držiteľom týchto utajovaných informácií, prevezme zodpovednosť pôvodcu po konzultácii so skupinou bezpečnostných expertov Komisie.

Článok 55

Dohody o bezpečnosti utajovaných skutočností

1. Dohody o bezpečnosti utajovaných skutočností s tretími štátmi alebo medzinárodnými organizáciami sa uzatvárajú v súlade s článkom 218 ZFEÚ.

2. Dohodami o bezpečnosti utajovaných skutočností:

a) sa stanovujú základné zásady a minimálne normy, ktorými sa riadi výmena utajovaných skutočností medzi Úniou a tretím štátom alebo medzinárodnou organizáciou;

b) sa stanovujú technické vykonávacie dojednania, ktoré sa dohodnú medzi príslušnými bezpečnostnými orgánmi dotknutých inštitúcií a orgánov Únie a príslušným bezpečnostným orgánom dotknutého tretieho štátu alebo medzinárodnej organizácie. V týchto dojednaniach sa prihliada na úroveň ochrany zabezpečenú uplatňovanými bezpečnostnými predpismi a zavedenými bezpečnostnými štruktúrami a postupmi v dotknutom treťom štáte alebo medzinárodnej organizácii;

c) sa stanovuje, že predtým, ako sa uskutoční výmena utajovaných skutočností na základe danej dohody, treba sa presvedčiť, či prijímajúca strana je schopná poskytnuté utajované skutočnosti primerane chrániť a zabezpečovať.

3. Ak sa podľa článku 51 ods. 1 stanoví potreba výmeny utajovaných skutočností, Komisia bude v náležitých prípadoch konzultovať s Európskou službou pre vonkajšiu činnosť, Generálnym sekretariátom Rady a ostatnými inštitúciami a orgánmi Únie, aby stanovila, či treba predložiť odporúčanie podľa článku 218 ods. 3.

4. EUCI sa nesmú vymieňať elektronickými prostriedkami, pokiaľ sa to výslovne nestanoví v dohode o bezpečnosti utajovaných skutočností alebo technických vykonávacích dojednaniach.

5. V Komisii je register EUCI, ktorý spravuje Generálny sekretariát, spravidla hlavným vstupným a výstupným bodom utajovaných skutočností s tretími štátmi a medzinárodnými organizáciami. Ak je to však z bezpečnostných, organizačných alebo prevádzkových dôvodov na ochranu EUCI vhodnejšie, miestne registre EUCI v oddeleniach Komisie v súlade s týmto rozhodnutím a jeho vykonávacími predpismi pôsobia ako vstupný a výstupný bod utajovaných skutočností, pokiaľ ide o záležitosti v rámci právomoci príslušných oddelení Komisie.

6. Na účely posúdenia účinnosti bezpečnostných predpisov, štruktúr a postupov v dotknutom treťom štáte alebo medzinárodnej organizácii sa Komisia v spolupráci s inými inštitúciami, agentúrami alebo orgánmi Únie zúčastní na hodnotiacich návštevách po vzájomnej dohode s dotknutým tretím štátom alebo medzinárodnou organizáciou. Počas týchto hodnotiacich návštev sa hodnotí:

a) regulačný rámec uplatniteľný na ochranu utajovaných skutočností;

b) všetky osobitné charakteristiky bezpečnostnej politiky a spôsobu organizácie bezpečnosti v treťom štáte alebo medzinárodnej organizácii, ktoré môžu mať vplyv na stupeň utajovaných skutočností, ktoré sa môžu vymieňať;

c) uplatňované bezpečnostné opatrenia a postupy a

d) postupy bezpečnostnej previerky pre stupeň utajenia EUCI, ktoré sa majú poskytnúť.

Článok 56

Administratívne dojednania

1. V prípade dlhodobej potreby výmeny utajovaných skutočností s tretím štátom alebo medzinárodnou organizáciou so stupňom utajenia spravidla nie vyšším ako RESTREINT UE/EU RESTRICTED v kontexte politického alebo právneho rámca Únie a v prípade, že bezpečnostný orgán Komisie po konzultácii so skupinou bezpečnostných expertov Komisie najmä stanovil, že daná strana nemá dostatočne rozvinutý bezpečnostný systém na to, aby sa s ňou mohla uzavrieť dohoda o bezpečnosti utajovaných skutočností, môže Komisia uzavrieť s príslušnými orgánmi daného tretieho štátu alebo medzinárodnej organizácie administratívne dojednanie.

2. Takéto administratívne dojednania majú spravidla formu výmeny listov.

3. Hodnotiaca návšteva sa uskutoční pred uzavretím dojednania. Výsledok hodnotiacej návštevy sa oznámi skupine bezpečnostných expertov Komisie. Ak však existujú výnimočné dôvody na naliehavú výmenu utajovaných skutočností, EUCI sa môžu poskytnúť, pokiaľ sa vynaloží maximálne úsilie, aby sa takáto hodnotiaca návšteva uskutočnila čo najskôr.

4. Elektronickými prostriedkami sa neuskutočňuje nijaká výmena EUCI, pokiaľ sa to v administratívnom dojednaní výslovne nestanoví.

Článok 57

Výnimočné *ad hoc* poskytnutie EUCI

1. Ak neexistuje dohoda o bezpečnosti utajovaných skutočností ani administratívne dojednanie a ak Komisia alebo jedno z jej oddelení zistí, že je mimoriadne potrebné v kontexte politického alebo právneho rámca Únie poskytnúť EUCI tretiemu štátu alebo medzinárodnej organizácii, bezpečnostný orgán Komisie v najvyššej možnej miere u bezpečnostných orgánov dotknutého tretieho štátu alebo medzinárodnej organizácie overí, že jeho alebo jej bezpečnostné predpisy, štruktúry a postupy zaručujú ochranu poskytnutých EUCI, ktorá zodpovedá normám, ktoré nie sú menej prísne ako normy stanovené v tomto rozhodnutí.

2. Rozhodnutie o poskytnutí EUCI dotknutému tretiemu štátu alebo medzinárodnej organizácii prijíma Komisia po konzultácii so skupinou bezpečnostných expertov Komisie na základe návrhu člena Komisie zodpovedného za bezpečnostné záležitosti.

3. Po rozhodnutí Komisie o poskytnutí EUCI a na základe predchádzajúceho písomného súhlasu pôvodcu, vrátane pôvodcov zdrojového materiálu, ktoré môžu obsahovať, príslušné oddelenie Komisie poskytne dotknutú skutočnosť, na ktorej sa uvedie rozsah jej možného postúpenia, ako aj tretí štát alebo medzinárodná organizácia, ktorým sa poskytla. Pred samotným poskytnutím alebo pri ňom sa dotknutá tretia strana písomne zaviaže, že bude EUCI, s ktorými sa oboznámi, chrániť v súlade so základnými zásadami a minimálnymi normami stanovenými v tomto rozhodnutí.

KAPITOLA 8

ZÁVEREČNÉ USTANOVENIA

Článok 58

Nahradenie predchádzajúceho rozhodnutia

Týmto rozhodnutím sa zrušuje a nahrádza rozhodnutie Komisie 2001/844/ES, ESUO, Euratom ([1]).

Článok 59

Utajované skutočnosti vytvorené pred nadobudnutím účinnosti tohto rozhodnutia

1. Všetky EUCI utajované v súlade s rozhodnutím Rady 2001/844/ES, EUSO, Euratom sú naďalej chránené v súlade s príslušnými ustanoveniami tohto rozhodnutia.

2. Všetky utajované skutočnosti, ktoré mala Komisia v držbe k dátumu nadobudnutia účinnosti rozhodnutia 2001/844/ES, ESUO, Euratom, s výnimkou utajovaných skutočností Euratomu:

a) ak boli vytvorené Komisiou, sa naďalej považujú za automaticky preradené do stupňa utajenia RESTREINT UE, pokiaľ ich autor do 31. januára 2002 nerozhodol o tom, že sa im pridelí iný stupeň utajenia, a neinformoval všetkých adresátov dotknutého dokumentu;

b) ak boli vytvorené pôvodcami mimo Komisie, si ponechajú svoj pôvodný stupeň utajenia, a preto sa budú považovať za EUCI rovnocenného stupňa, pokiaľ pôvodca nebude súhlasiť so zrušením stupňa utajenia alebo s pridelením nižšieho stupňa utajenia.

Článok 60

Vykonávacie predpisy a bezpečnostné oznámenia

1. Ak to bude potrebné, prijatie vykonávacích predpisov pre toto rozhodnutie bude predmetom osobitného rozhodnutia Komisie o splnomocnení člena Komisie zodpovedného za bezpečnostné záležitosti v plnom súlade s jej rokovacím poriadkom.

2. Potom, ako člen Komisie zodpovedný za bezpečnostné záležitosti dostal na základe uvedeného rozhodnutia Komisie splnomocnenie, môže vypracovať bezpečnostné oznámenia, v ktorých sa stanovia bezpečnostné usmernenia a najlepšie postupy v rámci rozsahu pôsobnosti tohto rozhodnutia a jeho vykonávacích predpisov.

3. Komisia môže v plnom súlade so svojím rokovacím poriadkom delegovať úlohy uvedené v prvom a druhom odseku tohto článku na generálneho riaditeľa pre ľudské zdroje a bezpečnosť prostredníctvom samostatného rozhodnutia o delegovaní.

Článok 61

Nadobudnutie účinnosti

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

V Bruseli 13. marca 2015

Za Komisiu

predseda

Jean-Claude JUNCKER

([1]) Rozhodnutie Komisie 2001/844/ES, ESUO, Euratom z 29. novembra 2001, ktorým sa mení a dopĺňa jej rokovací poriadok (Ú. v. ES L 317, 3.12.2001, s. 1).

PRÍLOHA I

EKVIVALENČNÁ TABUĽKA STUPŇOV UTAJENIA

EÚ	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Belgicko	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	pozri poznámku ([1])
Bulharsko	Строго секретно	Секретно	Поверително	За служебно ползване
Česká republika	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dánsko	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Nemecko	Streng geheim	Geheim	VS ([2]) — Vertraulich	VS — Nur für den Dienstgebrauch
Estónsko	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Írsko	Top Secret	Secret	Confidential	Restricted
Grécko	Άκρως Απόρρητο skratka: ΑΑΠ	Απόρρητο skratka: (ΑΠ)	Εμπιστευτικό skratka: (ΕΜ)	Περιορισμένης Χρήσης skratka: (ΠΧ)
Španielsko	Secreto	Reservado	Confidencial	Difusión Limitada
Francúzsko	Très Secret Défense	Secret Défense	Confidentiel Défense	pozri poznámku ([3])
Chorvátsko	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Taliansko	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο skratka: (ΑΑΠ)	Απόρρητο skratka: (ΑΠ)	Εμπιστευτικό skratka: (ΕΜ)	Περιορισμένης Χρήσης skratka: (ΠΧ)
Lotyšsko	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembursko	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Maďarsko	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Holandsko	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Rakúsko	Streng geheim	Geheim	Vertraulich	Eingeschränkt
Poľsko	Ściśle tajne	Tajne	Poufne	Zastrzeżone
Portugalsko	Muito secreto	Secreto	Confidencial	Reservado

EÚ	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Rumunsko	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovinsko	Strogo tajno	Tajno	Zaupno	Interno
Slovensko	Prísne tajné	Tajné	Dôverné	Vyhradené
Fínsko	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švédsko ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Spojené kráľovstvo	UK TOP SECRET	UK SECRET	Žiadny ekvivalent ([5])	UK OFFICIAL – SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding nie je v Belgicku stupňom utajenia. Belgicko manipuluje s utajovanými skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED a chráni ich spôsobom, ktorý nie je menej prísny, ako si vyžadujú normy a postupy uvedené v bezpečnostných predpisoch Rady Európskej únie.

([2]) Nemecko: VS = Verschlusssache.

([3]) Francúzsko vo svojom vnútroštátnom systéme nepoužíva stupeň utajenia RESTREINT. Francúzsko manipuluje s utajovanými skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED a chráni ich spôsobom, ktorý nie je menej prísny, ako si vyžadujú štandardy a postupy uvedené v bezpečnostných predpisoch Rady Európskej únie.

([4]) Švédsko: označenie stupňa utajenia v hornom riadku používajú orgány obrany a označenia v dolnom riadku ostatné orgány.

([5]) Spojené kráľovstvo manipuluje s utajovanými skutočnosťami EÚ so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a chráni ich v súlade s ochrannými bezpečnostnými požiadavkami pre stupeň utajenia UK SECRET.

PRÍLOHA II

ZOZNAM SKRATIEK

Akronym	Význam
CA	Crypto Authority (kryptografický orgán)
CAA	Crypto Approval Authority (kryptografický schvaľovací orgán)
CCTV	Closed Circuit Television (kamerový systém)
CDA	Crypto Distribution Authority (kryptografický distribučný orgán)
CIS	Communication and Information Systems handling EUCI (komunikačné a informačné systémy, ktorými sa manipuluje s utajovanými skutočnosťami EÚ)
DSA	Designated Security Authority (určený bezpečnostný orgán)
EUCI	EU Classified Information (utajované skutočnosti EÚ)
FSC	Facility Security Clearance (priemyselná bezpečnostná previerka)
IA	Information Assurance (informačná bezpečnosť)
IAA	Information Assurance Authority (orgán pre informačnú bezpečnosť)
IDS	Intrusion Detection System (systém detekcie narušenia)
IT	Information Technology (informačné technológie)
LSO	Local Security Officer (miestny bezpečnostný úradník)
NSA	National Security Authority (národný bezpečnostný orgán)
PSC	Personnel Security Clearance (personálna bezpečnostná previerka)
PSCC	Personnel Security Clearance Certificate (certifikát o personálnej bezpečnostnej previerke)
PSI	Programme/Project Security Instructions (bezpečnostné pokyny pre program/projekt)
RCO	Registry Control Officer (kontrolný úradník registra)
SAA	Security Accreditation Authority (bezpečnostný akreditačný orgán)
SAL	Security Aspects Letter (bezpečnostná doložka)
SCG	Security Classification Guide (sprievodca stupňami utajenia)
SecOPs	Security Operating Procedures (operačné bezpečnostné postupy)
TA	TEMPEST Authority (orgán pre TEMPEST)
ZFEÚ	Zmluva o fungovaní EÚ

PRÍLOHA III

ZOZNAM NÁRODNÝCH BEZPEČNOSTNÝCH ORGÁNOV

BELGICKO

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Telefón: sekretariát +32 25014542
Fax: +32 25014596
E-mail: nvo-ans@diplobel.fed.be

BULHARSKO

State Commission on Information Security
90 Cherkovna Str.
Sofia 1505
Telefón: +359 29333600
Fax: +359 29873750
E-mail: dksi@government.bg
webová stránka: www.dksi.bg

ČESKÁ REPUBLIKA

Národní bezpečnostní úřad
Na Popelce 2/16
150 06 Praha 56
Telefón: +420 257283335
Fax: +420 257283110
E-mail: czech.nsa@nbu.cz
Webová stránka: www.nbu.cz

DÁNSKO

Politiets Efterretningstjeneste
(dánska bezpečnostná spravodajská služba)
Klausdalsbrovej 1
2860 Søborg
Telefón: +45 33148888
Fax: +45 33430190

Forsvarets Efterretningstjeneste
(dánska obranná spravodajská služba)
Kastellet 30
2100 Copenhagen Ø
Telefón: +45 33325566
Fax: +45 33931320

NEMECKO

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
D-11014 Berlin
Telefón: +49 30186810
Fax: +49 30186811441
E-mail: oesIII3@bmi.bund.de

ESTÓNSKO

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn
Tel.: +372 7170113 0019, +372 7170117
Fax: +372 7170213
E-mail: nsa@mod.gov.ee

GRÉCKO

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Τηλ.: +30 2106572045 (ώρες γραφείου)
+ 30 2106572009 (ώρες γραφείου)
Φαξ: +30 2106536279; +30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos – Athens
Telefón: +30 2106572045
+ 30 2106572009
Fax: +30 2106536279, +30 2106577612

ŠPANIELSKO

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid
Telefón: +34 913725000
Fax: +34 913725808
E-mail: nsa-sp@areatec.com

FRANCÚZSKO

Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP
Telefón: +33 171758177
Fax: + 33 171758200

CHORVÁTSKO

Office of the National Security Council
(chorvátsky NSA)
Jurjevska 34
10 000 Zagreb
Chorvátsko
Telefón: +385 14681222
Fax: + 385 14686049
Webová stránka: www.uvns.hr

ÍRSKO

National Security Authority
Department of Foreign Affairs
76 – 78 Harcourt Street
Dublin 2
Telefón: +353 14780822
Fax: +353 14082959

TALIANSKO

Presidenza del Consiglio dei Ministri
D.I.S. – U.C.Se.
Via di Santa Susanna, 15
00187 Roma
Telefón: +39 0661174266
Fax: +39 064885273

CYPRUS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος
Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia
Telefón: +357 22807569, +357 22807643,
+357 22807764
Fax: +357 22302351
E-mail: cynsa@mod.gov.cy

LOTYŠSKO

National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
LV-1001 Riga
Telefón: +371 67025418
Fax: +371 67025454
E-mail: ndi@sab.gov.lv

LITVA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(komisia pre koordináciu ochrany tajomstiev Litovskej republiky – národný bezpečnostný orgán)
Gedimino 40/1
LT-01110 Vilnius
Telefón: +370 706 66701, +370 706 66702
Fax: Fax: +370 706 66700
E-mail: nsa@vsd.lt

LUXEMBURSKO

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Telefón: +352 24782210 central
+ 352 24782253 direct
Fax: +352 24782243

MAĎARSKO

Nemzeti Biztonsági Felügyelet
(národný bezpečnostný orgán Maďarska)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Telefón: +36 (1) 7952303
Fax: +36 (1) 7950344

Poštová adresa:
H-1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Webová stránka: www.nbf.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Telefón: +356 21249844
Fax: +356 25695321

HOLANDSKO

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Telefón: +31 703204400
Fax: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Telefón: +31 703187060
Fax: +31 703187522

RAKÚSKO

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien
Telefón: +43 1531152594
Fax: +43 1531152615
E-mail: ISK@bka.gv.at

POĽSKO

Agencja Bezpieczeństwa Wewnętrznego – ABW
(agentúra vnútornej bezpečnosti)
2A Rakowiecka St.
00-993 Warszawa
Telefón: +48 22 58 57 944
Fax: +48 22 58 57 443
E-mail: nsa@abw.gov.pl
Webová stránka: www.abw.gov.pl

PORTUGALSKO

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa
Telefón: +351 213031710
Fax: +351 213031711

RUMUNSKO

Oficiul Registrului Național al Informațiilor Secrete de Stat
(rumunský NSA – ORNISS národný registračný úrad pre utajované skutočnosti)
4 Mures Street
012275 București
Telefón: +40 212245830
Fax: +40 212240714
E-mail: nsa.romania@nsa.ro
Webová stránka: www.orniss.ro

SLOVINSKO

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Telefón: +386 14781390
Fax: +386 14781399
E-mail: gp.uvtp@gov.si

SLOVENSKO

Národný bezpečnostný úrad
Budatínska 30
P. O. Box 16
850 07 Bratislava
Telefón: +421 268692314
Fax: +421 263824005
Webová stránka: www.nbusr.sk

FÍNSKO

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Telefón: 16055890
Fax: +358 916055140
E-mail: NSA@formin.fi

ŠVÉDSKO

Utrikesdepartementet
(ministerstvo zahraničných vecí)
SSSB
SE-103 39 Stockholm
Telefón: +46 84051000
Fax: +46 87231176
E-mail: ud-nsa@foreign.ministry.se

SPOJENÉ KRÁĽOVSTVO

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS
Telefón 1: +44 2072765649
Telefón 2: +44 2072765497
Fax: +44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk