ROZHODNUTÍ KOMISE (EU, Euratom) 2015/444

ze dne 13. března 2015

o bezpečnostních pravidlech na ochranu utajovaných informací EU

EVROPSKÁ KOMISE,

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

s ohledem na Smlouvu o založení Evropského společenství pro atomovou energii, a zejména na článek 106 této smlouvy,

s ohledem na Protokol č. 7 o výsadách a imunitách Evropské unie připojený ke Smlouvám, a zejména na článek 18 uvedeného protokolu,

vzhledem k těmto důvodům:

(1) Bezpečnostní předpisy Komise týkající se ochrany utajovaných informací Evropské unie je třeba revidovat a aktualizovat, aby se zohlednil institucionální, organizační, provozní a technický vývoj.

(2) S vládou Belgie, Lucemburska a Itálie uzavřela Evropská komise dohody o bezpečnostních otázkách týkající se jejích hlavních sídel ([1]).

(3) Komise, Rada a Evropská služba pro vnější činnost se zavázaly k uplatňování rovnocenných bezpečnostních standardů pro ochranu utajovaných informací EU.

(4) Je důležité, aby zásady, standardy a pravidla pro ochranu utajovaných informací nezbytné pro ochranu zájmů Unie a jejích členských států v příslušných případech uplatňoval i Evropský parlament a další orgány, instituce a jiné subjekty Unie.

(5) Rizika související s utajovanými informacemi EU jsou řízena jako proces. Tento proces se zaměřuje na určení známých bezpečnostních rizik, na stanovení bezpečnostních opatření ke snížení těchto rizik na přijatelnou úroveň v souladu se základními zásadami a minimálními standardy stanovenými tímto rozhodnutím a na uplatňování těchto opatření v souladu s koncepcí hloubkové ochrany. Účinnost těchto opatření se průběžně vyhodnocuje.

(6) V rámci Komise se fyzickou bezpečností zaměřenou na ochranu utajovaných informací rozumí uplatňování fyzických a technických ochranných opatření s cílem předejít neoprávněnému přístupu k utajovaným informacím EU.

(7) Správou utajovaných informací EU se rozumí uplatňování administrativních opatření, která slouží ke kontrole těchto informací během celého jejich životního cyklu a která doplňují opatření stanovená v kapitolách 2, 3 a 5 tohoto rozhodnutí, a pomáhají tak zabránit úmyslnému či neúmyslnému ohrožení či ztrátě takových informací, jejich ohrožení nebo ztrátu zjistit a následně zajistit nápravu. Tato opatření se týkají zejména vytváření, uchovávání, evidence, kopírování, překladů, snižování stupně utajení, odtajňování, přenášení a ničení utajovaných informací EU a doplňují obecné předpisy pro správu dokumentů Komise (rozhodnutí 2002/47/ES ([2]), ESUO, Euratom a 2004/563/ES, Euratom ([3])).

([1]) Viz „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" ze dne 31. prosince 2004, „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois" ze dne 20. ledna 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" ze dne 22. července 1959.

([2]) Rozhodnutí Komise 2002/47/ES, ESUO, Euratom ze dne 23. ledna 2002 o doplnění jejího jednacího řádu (Úř. věst. L 21, 24.1.2002, s. 23).

([3]) Rozhodnutí Komise 2004/563/ES, ESUO, Euratom ze dne 7. července 2004, kterým se mění jednací řád Komise (Úř. věst. L 251, 27.7.2004, s. 9).

(8) Tímto rozhodnutím nejsou dotčeny:

a) nařízení (Euratom) č. 3 ([1]);

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

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

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

PŘIJALA TOTO ROZHODNUTÍ:

KAPITOLA 1

ZÁKLADNÍ ZÁSADY A MINIMÁLNÍ STANDARDY

Článek 1

Definice

Pro účely tohoto rozhodnutí se rozumí:

1) „útvarem Komise“ generální ředitelství či služba Komise nebo kabinet člena Komise;

2) „kryptografickými materiály“ šifrovací algoritmy, hardwarové a softwarové kryptografické moduly a prostředky, včetně prováděcích pravidel a související dokumentace, a klíčový materiál;

3) „odtajněním“ odstranění veškerých stupňů utajení;

4) „hloubkovou ochranou“ uplatňování řady bezpečnostních opatření, která jsou uspořádána jako několik obranných linií;

5) „dokumentem“ jakékoli zaznamenané informace bez ohledu na jejich fyzickou podobu či povahu;

6) „snížením stupně utajení“ označení informace nižším stupněm utajení;

7) „nakládáním“ s utajovanými informacemi EU veškeré možné činnosti, jimž mohou být podrobovány utajované informace EU během celého svého životního cyklu. K těmto činnostem patří vytváření, evidence, zpracovávání, přenášení, snižování stupně utajení, odtajňování a ničení informací. V souvislosti s komunikačními a informačními systémy tento pojem zahrnuje rovněž jejich shromažďování, zobrazování, přenos a uchovávání;

8) „držitelem“ řádně oprávněná osoba, která jednoznačně potřebuje znát utajované informace EU, má některé z nich v držení, a je tedy odpovědná za jejich ochranu;

9) „prováděcími pravidly“ soubor pravidel nebo bezpečnostních upozornění přijatý v souladu s kapitolou 5 rozhodnutí Komise (EU, Euratom) 2015/443 ([5]);

10) „materiálem“ jakékoli médium, datový nosič nebo část technického zařízení či vybavení, ať vyhotovené, či v procesu zhotovování;

11) „původcem“ orgán, instituce nebo jiný subjekt Unie, členský stát, třetí stát nebo mezinárodní organizace, z jejichž pověření byly utajované informace vytvořeny nebo uvedeny do struktur Unie;

12) „prostory“ všechny nemovitosti a přidružené věci ve vlastnictví či v držení Komise;

([1]) Nařízení Rady (Euratom) č. 3 ze dne 31. července 1958, kterým se provádí článek 24 Smlouvy o založení Evropského společenství pro atomovou energii (Úř. věst. 17, 6.10.1958, s. 406).

([2]) Nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise (Úř. věst. L 145, 31.5.2001, s. 43).

([3]) Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů (Úř. věst. L 8, 12.1.2001, s. 1).

([4]) Nařízení Rady (EHS, Euratom) č. 354/83 ze dne 1. února 1983 o otevření historických archivů Evropského hospodářského společenství a Evropského společenství pro atomovou energii veřejnosti (Úř. věst. L 43, 15.2.1983, s. 1).

([5]) Rozhodnutí Komise (EU, Euratom) 2015/443 ze dne 13. března 2015 o bezpečnosti v Komisi (viz strana 41 v tomto čísle Úředního věstníku).

13) „procesem řízení bezpečnostních rizik“ celý proces rozpoznávání, kontrolování a minimalizace nejistých událostí, které mohou ovlivnit bezpečnost organizace nebo jakýchkoli systémů, které používá. Zahrnuje všechny činnosti týkající se rizik, včetně hodnocení, řešení, přijímání a sdělování;

14) „služebním řádem“ služební řád úředníků Evropské unie a pracovní řád ostatních zaměstnanců Evropské unie stanovený nařízením Rady (EHS, Euratom, ESUO) č. 259/68 ([1]);

15) „hrozbou“ možná příčina nežádoucího incidentu, jež může vést k poškození určité organizace nebo jakéhokoli systému, který používá; hrozby mohou být neúmyslné či úmyslné (zlovolné) a vyznačují se ohrožujícími prvky, potenciálními cíli a metodami útoku;

16) „zranitelností“ jakákoli slabina, které může být využito v souvislosti s jednou či vícero hrozbami. Zranitelnost může být výsledkem opomenutí nebo může souviset s nedostatky v rámci kontrol, pokud jde o jejich intenzitu, úplnost nebo důslednost, a může být technické, procedurální, fyzické, organizační nebo provozní povahy.

Článek 2

Předmět a oblast působnosti

1. Toto rozhodnutí stanoví základní zásady a minimální bezpečnostní standardy pro ochranu utajovaných informací EU.

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

3. Bez ohledu na jakékoli zvláštní pokyny ohledně konkrétních skupin zaměstnanců se toto rozhodnutí použije na členy Komise, na zaměstnance Komise, na něž se vztahuje služební řád a pracovní řád ostatních zaměstnanců Evropských společenství, na národní odborníky vyslané do Komise, na poskytovatele služeb a jejich zaměstnance, na stážisty a na každého, kdo má přístup do budov či k majetku Komise nebo k informacím, s nimiž Komise nakládá.

4. Tímto rozhodnutím není dotčeno rozhodnutí 2002/47/ES, ESUO, Euratom a rozhodnutí 2004/563/ES, Euratom.

Článek 3

Definice utajovaných informací EU, stupně utajení a označení

1. „Utajovanými informacemi Evropské unie“ se rozumí jakékoli informace nebo materiály označené stupněm utajení EU, jejichž neoprávněné vyzrazení by mohlo různou měrou poškodit zájmy Evropské unie nebo jednoho či více členských států.

2. Utajované informace EU jsou utajovány jedním z následujících stupňů utajení:

a) TRES SECRET UE/EU TOP SECRET: informace a materiály, jejichž neoprávněné vyzrazení by mohlo vést k mimořádně závažnému poškození zásadních zájmů Evropské unie nebo jednoho či více členských států;

b) SECRET UE/EU SECRET: informace a materiály, jejichž neoprávněné vyzrazení by mohlo závažně poškodit podstatné zájmy Evropské unie nebo jednoho či více členských států;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informace a materiály, jejichž neoprávněné vyzrazení by mohlo poškodit podstatné zájmy Evropské unie nebo jednoho či více členských států;

d) RESTREINT UE/EU RESTRICTED: informace a materiály, jejichž neoprávněné vyzrazení by mohlo být nevýhodné pro zájmy Evropské unie nebo jednoho či více členských států.

3. Utajované informace EU jsou označeny stupněm utajení podle odstavce 2. Mohou nést doplňující označení, jež neoznačují stupeň utajení, ale mají uvést oblast činnosti, k níž se informace vztahují, identifikovat původce, omezovat distribuci či použití nebo uvádět informace o způsobilosti k předání.

([1]) Nařízení Rady (EHS, Euratom, ESUO) č. 259/68 ze dne 29. února 1968, kterým se stanoví služební řád úředníků Evropských společenství a pracovní řád ostatních zaměstnanců těchto Společenství a kterým se zavádějí zvláštní opatření dočasně použitelná na úředníky Komise (Úř. věst. L 56, 4.3.1968, s. 1).

Článek 4

Pravidla stanovování stupňů utajení

1. Každý člen Komise či útvaru Komise zajistí, aby utajované informace EU, jež vytváří, byly odpovídajícím způsobem utajeny, jasně označeny jako utajované informace EU a stupeň utajení si zachovaly pouze po nezbytnou dobu.

2. Aniž je dotčen článek 26, bez předchozího písemného souhlasu původce nelze snížit stupeň utajení utajovaných informací EU, odtajnit je a ani nelze změnit či zrušit žádné z označení stupně utajení uvedených v čl. 3 odst. 2.

3. Je-li to vhodné, přijmou se v souladu s článkem 60 prováděcí pravidla pro nakládání s utajovanými informacemi EU, včetně příručky pro stanovování stupňů utajení.

Článek 5

Ochrana utajovaných informací

1. Ochrana utajovaných informací EU se řídí tímto rozhodnutím a jeho prováděcími pravidly.

2. Držitel jakékoli utajované informace EU je odpovědný za její ochranu podle tohoto rozhodnutí a jeho prováděcích pravidel, v souladu s pravidly stanovenými v kapitole 4.

3. Pokud členské státy poskytnou do struktur či sítí Komise utajované informace označené vnitrostátním stupněm utajení, Komise tyto informace chrání v souladu s požadavky na ochranu utajovaných informací EU na odpovídající úrovni podle srovnávací tabulky stupňů utajení uvedené v příloze I.

4. Soubor shromážděných utajovaných informací EU může být důvodem pro úroveň ochrany odpovídající vyššímu stupni utajení než v případě jednotlivých složek takového souboru.

Článek 6

Řízení bezpečnostních rizik

1. Bezpečnostní opatření na ochranu utajovaných informací EU během celého jejich životního cyklu musí být přiměřená zejména stupni utajení, podobě a objemu informací nebo materiálů, umístění a konstrukci zařízení, v nichž jsou utajované informace EU uchovávány, a na místě vyhodnocené hrozbě zlovolných nebo trestných činností, včetně vyzvědačství, sabotáže nebo terorismu.

2. V pohotovostních plánech se zohlední potřeba chránit utajované informace EU v mimořádných situacích s cílem předejít neoprávněnému přístupu, vyzrazení nebo ztrátě integrity či dostupnosti.

3. Plány zajištění kontinuity provozu v každém útvaru zahrnují preventivní a nápravná opatření, která minimalizují dopad velkých selhání nebo incidentů na nakládání s utajovanými informacemi EU a na uchovávání těchto informací.

Článek 7

Provádění tohoto rozhodnutí

1. Je-li to nezbytné, přijmou se v souladu s článkem 60 prováděcí pravidla, která toto rozhodnutí doplní či podpoří.

2. Útvary Komise přijmou veškerá nezbytná opatření spadající do jejich pravomoci, aby zajistily, že se při nakládání s utajovanými informacemi EU či jinými utajovanými informacemi nebo při jejich uchovávání uplatňuje toto rozhodnutí a příslušná prováděcí pravidla.

3. Bezpečnostní opatření přijatá při provádění tohoto rozhodnutí musí být v souladu s bezpečnostními zásadami v Komisi stanovenými v článku 3 rozhodnutí (EU, Euratom) 2015/443.

4. Generální ředitel pro lidské zdroje a bezpečnost zřídí v rámci Generálního ředitelství pro lidské zdroje a bezpečnost bezpečnostní orgán Komise. Bezpečnostní orgán Komise má pravomoci, které mu ukládá toto rozhodnutí a jeho prováděcí pravidla.

5. V rámci každého útvaru Komise má místní bezpečnostní úředník (LSO), jak je uveden v článku 20 rozhodnutí (EU, Euratom) 2015/443, v úzké spolupráci s Generálním ředitelstvím pro lidské zdroje a bezpečnost při ochraně utajovaných informací EU v souladu s tímto rozhodnutím následující obecné úkoly:

a) vyřizovat žádosti o bezpečnostní oprávnění pro zaměstnance;

b) podílet se na bezpečnostním školení a informativních schůzích;

c) mít dohled nad vedoucím registru v daném útvaru;

d) podávat zprávy o případech narušení bezpečnosti a ohrožení utajovaných informací EU;

e) mít v držení náhradní klíče a písemné záznamy o nastavení každého kódu;

f) zastávat další úkoly související s ochranou utajovaných informací EU nebo vymezené v prováděcích pravidlech.

Článek 8

Narušení bezpečnosti a ohrožení utajovaných informací EU

1. K narušení bezpečnosti dochází v důsledku jednání nebo opomenutí určité osoby, jež je v rozporu s bezpečnostními pravidly stanovenými tímto rozhodnutím a jeho prováděcími pravidly.

2. K ohrožení utajovaných informací EU dochází, pokud byly tyto informace v důsledku narušení bezpečnosti zcela nebo zčásti zpřístupněny neoprávněným osobám.

3. Jakékoli narušení bezpečnosti nebo podezření na něj se neprodleně oznámí bezpečnostnímu orgánu Komise.

4. Je-li známo nebo existují-li oprávněné důvody se domnívat, že došlo k ohrožení či ztrátě utajovaných informací EU, provede se bezpečnostní šetření v souladu s článkem 13 rozhodnutí (EU, Euratom) 2015/443.

5. Přijmou se veškerá náležitá opatření, aby bylo možné:

a) informovat původce;

b) zajistit, aby za účelem zjištění faktů byla událost vyšetřena pracovníky, kteří nejsou za dané narušení bezpečnosti bezprostředně zapojeni;

c) posoudit možnou škodu z hlediska zájmů Unie nebo členských států;

d) přijmout vhodná opatření, která zabrání opakování události, a

e) oznámit přijatá opatření příslušným orgánům.

6. Vůči kterékoli osobě, která je odpovědná za porušení bezpečnostních pravidel stanovených tímto rozhodnutím, mohou být přijata disciplinární opatření v souladu se služebním řádem. Vůči kterékoli osobě, která je odpovědná za ohrožení či ztrátu utajovaných informací EU, se přijmou disciplinární opatření nebo právní kroky v souladu s příslušnými právními předpisy.

KAPITOLA 2

PERSONÁLNÍ BEZPEČNOST

Článek 9

Definice

Pro účely této kapitoly se použijí tyto definice:

1) „Oprávněním pro přístup k utajovaným informacím EU“ se rozumí rozhodnutí, jež na základě ujištění ze strany příslušného orgánu členského státu přijímá bezpečnostní orgán Komise a podle něhož může být úředníkovi Komise, jinému zaměstnanci nebo vyslanému národnímu odborníkovi, u něhož byla zjištěna potřeba znát utajované informace a jenž byl řádně informován o svých povinnostech, umožněn přístup k utajovaným informacím EU až do konkrétního stupně utajení (CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyššího) a do konkrétního data; osoba odpovídající tomuto popisu se označuje za „osobu s bezpečnostním oprávněním“.

2) „Personálním bezpečnostním opravňováním“ se rozumí uplatňování opatření, jež zajistí, že přístup k utajovaným informacím EU bude umožněn pouze osobám, které:

   a) utajované informace potřebují znát;

   b) případně mají bezpečnostní oprávnění pro odpovídající stupeň utajení a

   c) byly poučeny o svých povinnostech.

3) „Bezpečnostní prověrkou personálu“ se rozumí prohlášení příslušného orgánu členského státu, které je vydáno po skončení bezpečnostního řízení vedeného příslušnými orgány členského státu a kterým se osvědčuje, že určité osobě může být za podmínky, že bylo stanoveno, že utajované informace potřebuje znát, a že byla náležitě poučena o svých povinnostech, umožněn přístup k utajovaným informacím EU až do konkrétního stupně utajení (CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyššího) a do konkrétního data.

4) „Potvrzením o bezpečnostní prověrce personálu“ se rozumí osvědčení vydané příslušným orgánem, kterým se osvědčuje, že určitá osoba je držitelem platné bezpečnostní prověrky nebo bezpečnostního oprávnění vydaného bezpečnostním orgánem Komise, a které udává, k jakému stupni utajovaných informací EU může být dané osobě umožněn přístup (CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyššímu), uvádí dobu platnosti příslušné bezpečnostní prověrky či bezpečnostního oprávnění a datum skončení platnosti vlastního potvrzení.

5) „Bezpečnostním řízením“ se rozumí postupy šetření prováděné příslušným orgánem členského státu v souladu s jeho právními předpisy za účelem získání jistoty, že nejsou známy žádné negativní skutečnosti, které by bránily tomu, aby byla určité osobě udělena bezpečnostní prověrka až do konkrétního stupně utajení (CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyššího).

Článek 10

Základní principy

1. Určité osobě lze udělit přístup k utajovaným informacím EU pouze v případě, že:

1) byla zjištěna potřeba této osoby znát utajované informace;

2) tato osoba byla poučena o bezpečnostních pravidlech na ochranu utajovaných informací EU a o souvisejících bezpečnostních standardech a pokynech a vzala na vědomí své povinnosti ohledně ochrany těchto informací;

3) má v případě utajovaných informací se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším bezpečnostní oprávnění pro odpovídající stupeň utajení nebo jiné řádné oprávnění z titulu své funkce v souladu s vnitrostátními právními předpisy.

2. Všechny osoby, jejichž povinnosti mohou vyžadovat, aby měly přístup k utajovaným informacím EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším, musí předtím, než je jim k takovým utajovaným informacím EU umožněn přístup, získat bezpečnostní oprávnění pro odpovídající stupeň utajení. Dotčená osoba musí předložit písemný souhlas s tím, že podstoupí bezpečnostní prověrku personálu. Pokud tak neučiní, znamená to, že této osobě nemůže být přiděleno místo, funkce nebo úkol, které zahrnují přístup k informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším.

3. Bezpečnostní prověrka personálu je koncipována tak, aby určila, zda může být určitá osoba s přihlédnutím k její loajalitě, důvěryhodnosti a spolehlivosti oprávněna k přístupu k utajovaným informacím EU.

4. Loajalita, důvěryhodnost a spolehlivost určité osoby pro účely bezpečnostní prověrky pro přístup k informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším se ověřuje prostřednictvím bezpečnostního řízení, jež provádějí příslušné orgány členského státu v souladu se svými vnitrostátními předpisy.

5. Bezpečnostní orgán Komise nese výhradní odpovědnost za komunikaci s vnitrostátními bezpečnostními orgány nebo jinými příslušnými vnitrostátními orgány ohledně všech záležitostí týkajících se bezpečnostních prověrek. Veškeré kontakty mezi útvary Komise a jejich zaměstnanci a vnitrostátními bezpečnostními orgány a jinými příslušnými orgány probíhají prostřednictvím bezpečnostního orgánu Komise.

Článek 11

Udělování bezpečnostního oprávnění

1. Každý generální ředitel nebo vedoucí útvaru v Komisi určí v rámci svého útvaru pozice, jejichž držitelé potřebují mít k plnění svých úkolů přístup k informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším, a v důsledku toho potřebují mít bezpečnostní oprávnění.

2. Jakmile je známo, že bude určitá osoba jmenována na pracovní místo vyžadující přístup k utajovaným informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším, informuje LSO daného útvaru Komise bezpečnostní orgán Komise, který uvedené osobě předá dotazník bezpečnostní prověrky vydaný vnitrostátním bezpečnostním orgánem členského státu, jehož státní příslušnost má daná osoba při svém jmenování jako zaměstnanec evropských orgánů. Osoba vydá písemný souhlas s podstoupením bezpečnostní prověrky a vyplněný dotazník vrátí v co nejkratší lhůtě bezpečnostnímu orgánu Komise.

3. Bezpečnostní orgán Komise předá vyplněný dotazník bezpečnostní prověrky vnitrostátnímu bezpečnostnímu orgánu členského státu, jehož státní příslušnost má daná osoba při svém jmenování jako zaměstnanec evropských orgánů, a požádá o provedení bezpečnostního řízení pro stupeň utajení utajovaných informací EU, k nimž bude dotyčná osoba potřebovat přístup.

4. Jsou-li bezpečnostnímu orgánu Komise v souvislosti s osobou, která požádala o bezpečnostní prověrku, známy informace významné pro bezpečnostní řízení, oznámí je bezpečnostní orgán Komise postupem podle příslušných pravidel a předpisů příslušnému vnitrostátnímu bezpečnostnímu orgánu.

5. Po skončení bezpečnostního řízení a co nejdříve poté, co příslušný vnitrostátní bezpečnostní orgán oznámí svůj celkový posudek výsledků bezpečnostního řízení, bezpečnostní orgán Komise:

a) může dotyčné osobě vydat povolení pro přístup k utajovaným informacím EU a oprávnit ji k přístupu k utajovaným informacím EU až do odpovídajícího stupně a po dobu, kterou sám stanoví, nejdéle však na 5 let, pokud je výsledkem bezpečnostního řízení ujištění, že nejsou známy žádné nepříznivé skutečnosti, které by zpochybňovaly loajalitu, důvěryhodnost a spolehlivost dané osoby;

b) v případě, že z bezpečnostního řízení takové ujištění nevyplývá, oznámí tuto skutečnost v souladu s příslušnými pravidly a předpisy dotyčné osobě, která jej může požádat o slyšení, a pak má bezpečnostní orgán Komise možnost požádat příslušný vnitrostátní bezpečnostní orgán, aby v souladu s vnitrostátními právními předpisy poskytl veškerá další možná upřesnění. Je-li výsledek bezpečnostního řízení potvrzen, nelze oprávnění pro přístup k utajovaným informacím EU vydat.

6. Bezpečnostní řízení spolu se získanými výsledky podléhají příslušným právním předpisům platným v daném členském státě, včetně předpisů týkajících se opravných prostředků. Rozhodnutí bezpečnostního orgánu Komise podléhají opravným prostředkům v souladu se služebním řádem.

7. Komise uzná oprávnění pro přístup k utajovaným informacím EU udělené jakýmkoli jiným orgánem, institucí nebo jiným subjektem Unie, za předpokladu, že je toto oprávnění i nadále platné. Oprávnění se vztahují na veškeré úkoly přidělené dotyčné osobě v rámci Komise. Orgán, instituce nebo jiný subjekt Unie, kde dotyčná osoba nastupuje k výkonu zaměstnání, vyrozumí o změně zaměstnavatele příslušný vnitrostátní bezpečnostní orgán.

8. Nenastoupí-li dotyčná osoba do služby do 12 měsíců od oznámení výsledku bezpečnostního řízení bezpečnostnímu orgánu Komise nebo dojde-li k přerušení služby dotyčné osoby v délce 12 měsíců, během nichž není tato osoba zaměstnána v Komisi ani v žádném jiném orgánu, instituci či jiném subjektu Unie ani na pracovním místě ve vnitrostátních správních orgánech některého členského státu, oznámí bezpečnostní orgán Komise tuto skutečnost příslušnému vnitrostátnímu bezpečnostnímu orgánu za účelem potvrzení, že bezpečnostní prověrka je i nadále platná a odpovídající.

9. Pokud bezpečnostní orgán Komise zjistí informace týkající se bezpečnostního rizika, jež představuje osoba, která je držitelem platného bezpečnostního oprávnění, oznámí tuto skutečnost postupem podle příslušných pravidel a předpisů příslušnému vnitrostátnímu bezpečnostnímu orgánu.

10. Pokud vnitrostátní bezpečnostní orgán informuje bezpečnostní orgán Komise o tom, že v případě osoby, která je držitelem platného oprávnění pro přístup k utajovaným informacím EU, již není platné ujištění podle odst. 5 písm. a), může bezpečnostní orgán Komise vnitrostátní bezpečnostní orgán požádat, aby v souladu s vnitrostátními právními předpisy poskytl veškerá další možná upřesnění. Pokud vnitrostátní bezpečnostní orgán negativní skutečnosti potvrdí, zruší se výše uvedené oprávnění, dané osobě se zamezí v přístupu k utajovaným informacím EU a daná osoba je odvolána z pracovních míst, u nichž je přístup k utajovaným informacím EU možný nebo v jejichž rámci by mohla ohrožovat bezpečnost.

11. Jakékoli rozhodnutí zrušit či pozastavit oprávnění pro přístup k utajovaným informacím EU v případě osoby spadající do oblasti působnosti tohoto rozhodnutí a případné odůvodnění se oznámí dotyčné osobě, která může požádat bezpečnostní orgán Komise o slyšení. Informace poskytované vnitrostátním bezpečnostním orgánem podléhají příslušným právním předpisům platným v daném členském státě. Rozhodnutí bezpečnostního orgánu Komise učiněná v této souvislosti podléhají opravným prostředkům v souladu se služebním řádem.

12. Útvary Komise zajistí, aby národní odborníci vyslaní na pracovní místa v Komisi, jež vyžadují bezpečnostní oprávnění pro přístup k utajovaným informacím EU, před nástupem do služby předložili platnou bezpečnostní prověrku personálu nebo potvrzení o bezpečnostní prověrce personálu podle vnitrostátních právních předpisů bezpečnostnímu orgánu Komise, který jim na základě toho udělí bezpečnostní oprávnění pro přístup k utajovaným informacím EU až do stupně utajení rovnocenného stupni uvedenému ve vnitrostátní bezpečnostní prověrce, jež bude platné nejvýše po dobu jejich vyslání.

Přístup k utajovaným informacím EU pro jednotlivce řádně oprávněné z titulu své funkce

13. Členové Komise, kteří mají na základě smlouvy přístup k utajovaným informacím EU z titulu své funkce, musí být poučeni o svých bezpečnostních povinnostech při ochraně utajovaných informací EU.

Záznamy o bezpečnostní prověrce a bezpečnostním oprávnění

14. Záznamy o bezpečnostních prověrkách a oprávněních udělených pro přístup k utajovaným informacím EU vede bezpečnostní orgán Komise v souladu s tímto rozhodnutím. Tyto záznamy obsahují informace alespoň o stupni utajení utajovaných informací EU, k nimž může být dotčené osobě umožněn přístup, o datu vydání a době platnosti bezpečnostní prověrky.

15. Bezpečnostní orgán Komise může vydat potvrzení o bezpečnostní prověrce personálu, v němž uvede stupeň utajení utajovaných informací EU, k nimž může mít tato osoba přístup (stupeň utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšší), dobu platnosti příslušného oprávnění pro přístup k utajovaným informacím EU a datum skončení platnosti potvrzení.

Obnovení bezpečnostních oprávnění

16. Po počátečním udělení bezpečnostních oprávnění a za předpokladu, že daná osoba byla nepřetržitě ve službě v Evropské komisi nebo jiném orgánu, instituci nebo jiném subjektu Unie a nadále potřebuje přístup k utajovaným informacím EU, se bezpečnostní oprávnění pro přístup k utajovaným informacím EU přezkoumá za účelem obnovení zpravidla každých pět let ode dne oznámení výsledku posledního bezpečnostního řízení, na kterém bylo oprávnění založeno.

17. Pokud příslušný vnitrostátní bezpečnostní orgán nebo jiný příslušný vnitrostátní orgán ve lhůtě dvou měsíců ode dne, kdy mu byla předána žádost o obnovení platnosti a odpovídající dotazník bezpečnostní prověrky, neposkytne žádné nepříznivé informace, může bezpečnostní orgán Komise prodloužit platnost stávajícího bezpečnostního oprávnění na dobu až 12 měsíců. Pokud do konce tohoto dvanáctiměsíčního období příslušný vnitrostátní bezpečnostní orgán nebo jiný příslušný vnitrostátní orgán bezpečnostnímu orgánu Komise nepodá své stanovisko, přidělí se dotyčné osobě úkoly, které nevyžadují bezpečnostní oprávnění.

Článek 12

Informativní schůze o bezpečnostním oprávnění

1. Všechny osoby s bezpečnostním oprávněním poté, co se zúčastní informativní schůze o bezpečnostním oprávnění organizované bezpečnostním orgánem Komise, písemně potvrdí, že chápou své povinnosti, pokud jde o ochranu utajovaných informací EU, a jsou si vědomy důsledků v případě ohrožení utajovaných informací EU. Záznamy o těchto písemných potvrzeních vede bezpečnostní orgán Komise.

2. Všechny osoby, které jsou oprávněny přistupovat k utajovaným informacím EU nebo po nichž se vyžaduje, aby s nimi nakládaly, jsou nejprve poučeny a poté pravidelně informovány o možném ohrožení bezpečnosti a musí neprodleně informovat bezpečnostní orgán Komise o jakémkoli pokusu o kontakt nebo o činnosti, které považují za podezřelé nebo neobvyklé.

3. Všechny osoby, které přestanou vykonávat pracovní povinnosti vyžadující přístup k utajovaným informacím EU, musí být poučeny o své povinnosti utajované informace EU i nadále chránit a případně tuto skutečnost písemně potvrdí.

Článek 13

Dočasná bezpečnostní oprávnění

1. Ve výjimečných případech, pokud to vyžadují zájmy služby a není-li skončeno bezpečnostní řízení v plném rozsahu, může bezpečnostní orgán Komise, po konzultaci s vnitrostátním bezpečnostním orgánem členského státu, jehož je daná osoba státním příslušníkem, a pod podmínkou, že předběžné šetření potvrdí, že nejsou známy žádné negativní skutečnosti, vydat osobám dočasné oprávnění pro přístup k utajovaným informacím EU pro konkrétní funkci, aniž by tím byla dotčena ustanovení o obnově bezpečnostní prověrky. Dočasná oprávnění pro přístup k utajovaným informacím EU jsou platná jednorázově nejdéle po dobu šesti měsíců a neumožňují přístup k informacím se stupněm utajení TRES SECRET UE/EU TOP SECRET.

2. Všechny osoby, kterým bylo vydáno dočasné oprávnění, poté, co byly poučeny v souladu s čl. 12 odst. 1, písemně potvrdí, že rozumí tomu, jaké mají povinnosti, pokud jde o ochranu utajovaných informací EU, a jsou si vědomy důsledků v případě ohrožení utajovaných informací EU. Záznamy o těchto písemných potvrzeních vede bezpečnostní orgán Komise.

Článek 14

Účast na neveřejných jednáních organizovaných Komisí

1. Útvary Komise odpovědné za organizaci jednání, na niž se projednávají informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším, oznámí prostřednictvím svého LSO nebo prostřednictvím pořadatele jednání bezpečnostnímu orgánu Komise s dostatečným předstihem data, časy, místa a účastníky těchto jednání.

2. S výhradou ustanovení čl. 11 odst. 13 se osoby přizvané k účasti na jednáních organizovaných Komisí, na nichž se projednávají informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším, mohou zúčastnit, pouze pokud je potvrzen jejich status bezpečnostní prověrky nebo bezpečnostního oprávnění. Přístup k těmto neveřejným jednáním se zamítne osobám, které bezpečnostnímu orgánu Komise nepředložily potvrzení o bezpečnostní prověrce personálu ani jiný doklad o bezpečnostní prověrce, nebo účastníkům z Komise, kteří nejsou držiteli bezpečnostního oprávnění.

3. Před uspořádáním neveřejného jednání požádá odpovědný pořadatel či LSO útvaru Komise pořádajícího jednání externí účastníky, aby bezpečnostnímu orgánu Komise předložili potvrzení o bezpečnostní prověrce personálu či jiný doklad o bezpečnostní prověrce. Bezpečnostní orgán Komise informuje LSO či pořadatele jednání o tom, že potvrzení o bezpečnostní prověrce personálu nebo jiný doklad o bezpečnostní prověrce obdržel. Je-li to vhodné, lze použít společný jmenný seznam, v němž jsou příslušné informace o bezpečnostní prověrce uvedeny.

4. Oznámí-li příslušné orgány bezpečnostnímu orgánu Komise, že osobě, jejíž úkoly vyžadují účast na jednáních pořádaných Komisí, byla bezpečnostní prověrka odebrána, bezpečnostní orgán Komise o tom uvědomí LSO útvaru Komise, který je za pořádání daného jednání odpovědný.

Článek 15

Potenciální přístup k utajovaným informacím EU

Kurýři a členové ostrahy a doprovodu musí mít bezpečnostní oprávnění pro odpovídající stupeň utajení nebo musí být jinak vhodně prověřeni v souladu s vnitrostátními právními předpisy, musí být poučeni o bezpečnostních postupech pro ochranu utajovaných informací EU a musí být seznámeni se svými povinnostmi chránit jim svěřené utajované informace EU.

KAPITOLA 3

FYZICKÁ BEZPEČNOST ZAMĚŘENÁ NA OCHRANU UTAJOVANÝCH INFORMACÍ

Článek 16

Základní zásady

1. Opatření fyzické bezpečnosti mají znemožnit podloudné nebo násilné vniknutí narušitele, odradit od neoprávněné činnosti a takové činnosti zabránit a odhalit ji a umožnit rozdělení členů personálu, pokud jde o přístup k utajovaným informacím EU, v souladu se zásadou potřeby znát utajované informace. Tato opatření se stanoví na základě procesu řízení rizik v souladu s tímto rozhodnutím a s jeho prováděcími pravidly.

2. Opatření fyzické bezpečnosti mají zejména předejít neoprávněnému přístupu k utajovaným informacím EU tím, že:

a) zajišťují, aby s utajovanými informacemi EU bylo nakládáno a aby byly uchovávány vhodným způsobem;

b) umožňují rozdělení členů personálu, pokud jde o přístup k utajovaným informacím EU, na základě jejich potřeby znát utajované informace a případně i na základě jejich bezpečnostního oprávnění;

c) odrazují od neoprávněné činnosti a takové činnosti zabraňují a odhalují ji a

d) znemožňují nebo zpomalují podloudné nebo násilné vniknutí narušitelů.

3. Opatření fyzické bezpečnosti je třeba zavést pro všechny prostory, budovy, kanceláře, místnosti a další objekty, v nichž se nakládá s utajovanými informacemi EU nebo v nichž jsou takové informace uchovávány, včetně prostor, v nichž jsou umístěny komunikační a informační systémy uvedené v kapitole 5.

4. Prostory, v nichž jsou uchovávány utajované informace EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším, je třeba zřídit jako zabezpečené oblasti v souladu s touto kapitolou a musí je schválit orgán pro bezpečnostní akreditaci v Komisi.

5. Na ochranu utajovaných informací EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším se použijí pouze prostředky nebo zařízení schválené bezpečnostním orgánem Komise.

Článek 17

Požadavky na fyzickou bezpečnost a opatření fyzické bezpečnosti

1. Opatření fyzické bezpečnosti se vybírají na základě posouzení hrozeb provedeného bezpečnostním orgánem Komise a případně po konzultaci s dalšími útvary Komise, ostatními orgány, institucemi nebo jinými subjekty Unie a/nebo příslušnými orgány členských států. Komise uplatňuje ve svých prostorách proces řízení rizik na ochranu utajovaných informací EU, aby se vůči vyhodnocenému riziku poskytla přiměřená úroveň fyzické ochrany. V procesu řízení rizik se vezmou v úvahu veškeré důležité okolnosti, zejména:

a) stupeň utajení utajovaných informací EU;

b) podoba a objem utajovaných informací EU, přičemž je třeba brát v úvahu, že velké množství nebo kompilace utajovaných informací EU může vyžadovat použití přísnějších ochranných opatření;

c) okolní prostředí a uspořádání budov nebo prostor, v nichž jsou utajované informace EU uchovávány, a

d) vyhodnocené hrozby ze strany zpravodajských služeb zaměřených na Unii, její orgány, instituce či jiné subjekty nebo na členské státy a hrozba sabotáže a teroristických, podvratných nebo jiných trestných činností.

2. Bezpečnostní orgán Komise určí v souladu s koncepcí hloubkové ochrany vhodnou kombinaci opatření fyzické bezpečnosti, jež je třeba uplatňovat. Bezpečnostní orgán Komise za tímto účelem vypracuje minimální standardy, normy a kritéria stanovená v prováděcích pravidlech.

3. Bezpečnostní orgán Komise je oprávněn k provádění prohlídek při vstupu a odchodu, které mají odradit od nedovoleného vnášení materiálů nebo neoprávněného vynášení utajovaných informací EU z prostor nebo budov.

4. Hrozí-li nebezpečí, že by utajované informace EU být byť i neúmyslně zhlédnuty, příslušné útvary Komise přijmou vhodná opatření, jež definuje bezpečnostní orgán Komise, aby tomuto riziku zabránily.

5. U nových zařízení se požadavky na fyzickou bezpečnost a jejich funkční specifikace stanoví se souhlasem bezpečnostního orgánu Komise jako součást plánování a konstrukce zařízení. U stávajících zařízení se požadavky na fyzickou bezpečnost uplatňují v souladu s minimálními standardy, normami a kritérii stanovenými v prováděcích pravidlech.

Článek 18

Prostředky fyzické ochrany utajovaných informací EU

1. Pro fyzickou ochranu utajovaných informací EU se stanoví dva druhy fyzicky chráněných oblastí:

a) administrativní oblasti a

b) zabezpečené oblasti (včetně technicky zabezpečených oblastí).

2. Orgán pro bezpečnostní akreditaci v Komisi určí, zda daný prostor splňuje požadavky na to, aby mohl být označen jako administrativní oblast, zabezpečená oblast nebo technicky zabezpečená oblast.

3. U administrativních oblastí:

a) musí být viditelně vymezen obvod administrativní oblasti, který umožní kontrolu osob a pokud možno i vozidel;

b) je přístup bez doprovodu umožněn pouze osobám, které mají řádné oprávnění od bezpečnostního orgánu Komise či jiného příslušného orgánu, a

c) pro všechny jiné osoby je třeba zajistit nepřetržitý doprovod nebo rovnocenná kontrolní opatření.

4. U zabezpečených oblastí:

a) musí být viditelně vymezen a chráněn obvod zabezpečené oblasti, jejíž všechny vchody a východy jsou kontrolovány prostřednictvím průkazů nebo systému osobní identifikace;

b) lze přístup bez doprovodu umožnit pouze osobám, které jsou bezpečnostně prověřeny a jsou ke vstupu do dané oblasti výslovně oprávněny na základě potřeby znát utajované informace;

c) je pro všechny jiné osoby nutné zajistit nepřetržitý doprovod nebo rovnocenná kontrolní opatření.

5. Představuje-li vstup do zabezpečené oblasti *de facto* přímý přístup k utajovaným informacím, které se v ní nacházejí, musí být dále splněny tyto požadavky:

a) je třeba jasně uvést nejvyšší stupeň utajení informací, které jsou v dané oblasti zpravidla uchovávány, a

b) všichni návštěvníci musí být zvlášť oprávněni ke vstupu do dané oblasti, je třeba pro ně zajistit nepřetržitý doprovod a musí být náležitě bezpečnostně prověřeni, s výjimkou případů, kdy byla přijata opatření zajišťující, že k utajovaným informací EU není možný přístup.

6. Zabezpečené oblasti chráněné před odposlechem je třeba označit jako technicky zabezpečené oblasti. U těchto oblastí musí být dále splněny tyto požadavky:

a) tyto oblasti musí být vybaveny systémy detekce narušení, musí být uzamčeny v době, kdy nejsou obsazeny, a musí být střeženy v době, kdy obsazeny jsou. Všechny klíče musí být spravovány v souladu s článkem 20;

b) všechny osoby a materiály musí být při vstupu do těchto prostor kontrolovány;

c) tyto oblasti musí bezpečnostní orgán Komise pravidelně fyzicky a/nebo technicky kontrolovat. Tyto kontroly se rovněž provádějí po jakémkoli neoprávněném vstupu nebo podezření, že k takovému vstupu došlo, a

d) tyto oblasti nesmí obsahovat neschválené komunikační vedení, neschválené telefonní či jiné komunikační přístroje a neschválená elektrická nebo elektronická zařízení.

7. Bez ohledu na odst. 6 písm. d) předtím, než se komunikační přístroje a elektrická nebo elektronická zařízení jakéhokoli druhu použijí v oblastech, v nichž se konají zasedání nebo v nichž se pracuje s informacemi se stupněm utajení SECRET UE/EU SECRET nebo vyšším, a v případech, kdy je úroveň ohrožení utajovaných informací EU vyhodnocena jako vysoká, musí být veškeré přístroje a zařízení nejdříve prověřeny bezpečnostním orgánem Komise za tím účelem, aby prostřednictvím těchto zařízení nemohlo dojít k neúmyslnému či nezákonnému přenášení žádných srozumitelných informací mimo danou zabezpečenou oblast.

8. Zabezpečené oblasti, které nejsou 24 hodin denně obsazeny pracovníky ve službě, jsou podle potřeby kontrolovány na konci běžné pracovní doby a v náhodně zvolených intervalech mimo běžnou pracovní dobu, není-li zaveden systém detekce narušení.

9. Zabezpečené oblasti a technicky zabezpečené oblasti mohou být zřízeny dočasně v rámci administrativní oblasti pro uspořádání neveřejného jednání nebo pro jiný podobný účel.

10. LSO dotyčného útvaru Komise vypracuje pro každý zabezpečený prostor v jeho odpovědnosti bezpečnostní provozní postupy, které v souladu s ustanoveními tohoto rozhodnutí a jeho prováděcích pravidel stanoví:

a) stupeň utajení utajovaných informací EU, s nimiž se může nakládat nebo jež mohou být uchovávány v dané oblasti;

b) ostrahu a ochranná opatření, jež je třeba dodržovat;

c) osoby, které jsou oprávněny přistupovat do dané oblasti bez doprovodu vzhledem k tomu, že potřebují znát utajované informace a že mají bezpečnostní oprávnění;

d) případně postupy pro zajištění doprovodu nebo pro ochranu utajovaných informací EU, je-li přístup do dané oblasti umožněn jiným osobám;

e) veškerá jiná náležitá opatření a postupy.

11. Uvnitř zabezpečených oblastí se budují trezorové místnosti. Stěny, podlahy, stropy, okna a uzamykatelné dveře musí být schváleny bezpečnostním orgánem Komise a musí poskytovat ochranu na úrovni rovnocenné bezpečnostnímu úschovnému objektu schválenému pro uchovávání utajovaných informací EU se stejným stupněm utajení.

Článek 19

Opatření fyzické bezpečnosti pro nakládání s utajovanými informacemi EU a jejich uchovávání

1. S utajovanými informacemi EU se stupněm utajení RESTREINT UE/EU RESTRICTED lze nakládat:

a) v zabezpečené oblasti;

b) v administrativní oblasti za předpokladu, že utajované informace EU jsou chráněny před přístupem neoprávněných osob, nebo

c) mimo zabezpečenou oblast či mimo administrativní oblast za předpokladu, že držitel informací přenáší utajované informace EU v souladu s článkem 31 a že se zavázal k dodržování náhradních opatření stanovených v prováděcích předpisech tak, aby zajistil, že budou utajované informace EU chráněny před přístupem neoprávněných osob.

2. Utajované informace EU se stupněm utajení RESTREINT UE/EU RESTRICTED se uchovávají ve vhodném uzamčeném kancelářském nábytku v administrativní oblasti nebo v zabezpečené oblasti. Dočasně mohou být uchovávány mimo zabezpečenou oblast či mimo administrativní oblast za předpokladu, že se držitel informací zaváže k dodržování náhradních opatření stanovených v prováděcích pravidlech.

3. S utajovanými informacemi EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET lze nakládat:

a) v zabezpečené oblasti;

b) v administrativní oblasti za předpokladu, že utajované informace EU jsou chráněny před přístupem neoprávněných osob, nebo

c) mimo zabezpečenou oblast či mimo administrativní oblast za předpokladu, že držitel informací:

   i) se zavázal k dodržování náhradních opatření stanovených v prováděcích pravidlech tak, aby zajistil, že budou utajované informace EU chráněny před přístupem neoprávněných osob,

   ii) má utajované informace EU neustále pod osobním dohledem a

   iii) v případě dokumentů v tištěné podobě oznámil tuto skutečnost příslušnému registru.

4. Utajované informace EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET EU/EU SECRET se uchovávají v zabezpečené oblasti v bezpečnostním úschovném objektu nebo trezorové místnosti.

5. S utajovanými informacemi EU se stupněm utajení TRES SECRET UE/EU TOP SECRET se nakládá v zabezpečené oblasti zřízené a spravované bezpečnostním orgánem Komise a akreditované pro tento stupeň orgánem pro bezpečnostní akreditaci v Komisi.

6. Utajované informace EU se stupněm utajení TRES SECRET UE/EU TOP SECRET se uchovávají v zabezpečené oblasti akreditované pro tento stupeň orgánem pro bezpečnostní akreditaci v Komisi při dodržení jedné z těchto podmínek:

a) informace se uchovávají v bezpečnostním úschovném objektu v souladu s článkem 18, přičemž je třeba uplatňovat jedno nebo více těchto dodatečných kontrolních opatření:

   1) nepřetržitá ochrana nebo kontrola ze strany prověřeného bezpečnostního nebo službu konajícího personálu,

   2) schválený systém detekce narušení v kombinaci s pohotovostním bezpečnostním personálem;

   nebo

b) informace se uchovávají v trezorové místnosti vybavené systémem detekce narušení v kombinaci s pohotovostním bezpečnostním personálem.

Článek 20

Správa klíčů a kódů používaných pro ochranu utajovaných informací EU

1. Postupy pro správu klíčů a nastavení kódů pro kanceláře, místnosti, trezorové místnosti a bezpečnostní úschovné objekty jsou stanoveny v prováděcích pravidlech podle článku 60. Cílem těchto postupů je zabránit neoprávněnému přístupu.

2. Nastavení kódů zná zpaměti co nejmenší možný počet osob, které je znát potřebují. Nastavení kódů pro bezpečnostní úschovné objekty a trezorové místnosti, v nichž se uchovávají utajované informace EU, je třeba změnit:

a) při přijetí nového úschovného objektu;

b) kdykoli se změní personál, který kód zná;

c) kdykoli dojde k ohrožení informací nebo v případě podezření z ohrožení;

d) pokud došlo k údržbě či opravě zámku a

e) nejméně každých 12 měsíců.

KAPITOLA 4

SPRÁVA UTAJOVANÝCH INFORMACÍ EU

Článek 21

Základní zásady

1. Veškeré dokumenty s utajovanými informacemi EU by měly být spravovány v souladu s politikou Komise pro správu dokumentů, a proto by měly být zaevidovány, tříděny, uchovávány a nakonec odstraněny nebo zčásti či zcela převedeny do historických archivů v souladu se společným seznamem pro uchovávání spisů Evropské komise.

2. Informace stupně utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyššího je třeba po jejich obdržení a před jejich distribucí z bezpečnostních důvodů zaevidovat. Informace se stupněm utajení TRES SECRET UE/EU TOP SECRET musí být zaevidovány v určených registrech.

3. V rámci Komise se vytvoří systém evidence utajovaných informací EU v souladu s ustanoveními článku 27.

4. Útvary a prostory Komise, v nichž se nakládá s utajovanými informacemi EU nebo v nichž jsou takové informace uchovávány, podléhají pravidelné inspekci prováděné bezpečnostním orgánem Komise.

5. Mimo fyzicky chráněné oblasti se utajované informace EU mezi jednotlivými útvary a prostory přenášejí tímto způsobem:

a) utajované informace EU se obecně přenášejí elektronicky při zajištění ochrany kryptografickými prostředky schválenými v souladu s kapitolou 5;

b) pokud přenos není uskutečňován způsobem uvedeným v písmeni a), přenášejí se utajované informace EU:

   i) na elektronických nosičích informací (jako například USB paměti, kompaktní disky, pevné disky), které jsou chráněny kryptografickými prostředky schválenými v souladu s kapitolou 5, nebo

   ii) ve všech ostatních případech způsobem předepsaným v prováděcích pravidlech.

Článek 22

Stupně utajení a označení

1. Informace se utajují v případě, že vyžadují ochranu z důvodu své důvěrnosti v souladu s čl. 3 odst. 1.

2. Původce utajovaných informací EU odpovídá za stanovení stupně utajení podle příslušných prováděcích pravidel, standardů a pokynů pro utajování informací a za počáteční distribuci informací.

3. Stupeň utajení utajovaných informací EU se stanoví v souladu s čl. 3 odst. 2 a příslušnými prováděcími pravidly.

4. Stupeň utajení musí být jasně a správně označen bez ohledu na to, zda mají utajované informace EU tištěnou, ústní, elektronickou či jinou podobu.

5. Jednotlivé části daného dokumentu (tj. stránky, odstavce, oddíly, přílohy, dodatky a připojené části dokumentu) mohou vyžadovat různé stupně utajení a být podle toho označeny, a to i v případě, že jsou uloženy v elektronické podobě.

6. Stupeň utajení dokumentu nebo spisu jako celku musí být alespoň stejně vysoký jako u jeho části s nejvyšším stupněm utajení. Jestliže dokument vznikl sloučením informací z různých zdrojů, konečný produkt se přezkoumá za účelem stanovení celkového stupně utajení, neboť může vyžadovat vyšší stupeň utajení než jeho jednotlivé části.

7. Dokumenty obsahující části s různými stupni utajení musí být v co nejvyšší míře strukturovány tak, aby části s různým stupněm utajení mohly být v případě potřeby snadno rozpoznány a odděleny.

8. Stupeň utajení dopisu nebo průvodní poznámky k připojeným částem musí být stejně vysoký jako nejvyšší stupeň utajení těchto připojených částí. Původce jasně vyznačí jejich stupeň utajení, pokud budou odděleny od připojených částí, pomocí odpovídajícího označení, například:

CONFIDENTIEL UE/EU CONFIDENTIAL

Bez příloh(y) RESTREINT UE/EU RESTRICTED

Článek 23

Označení

Kromě jednoho z označení stupňů utajení uvedených v čl. 3 odst. 2 mohou utajované informace EU nést doplňující označení, například:

a) označení určující původce;

b) jakákoli upozornění, kódová slova nebo zkratky k upřesnění oblasti činnosti, k níž se daný dokument vztahuje, k označení zvláštního způsobu distribuce na základě potřeby znát utajované informace nebo k omezení použití;

c) označení týkající se způsobilosti k předání;

d) případně datum nebo určitou událost, po nichž lze stupeň utajení snížit nebo informace odtajnit.

Článek 24

Zkrácená označení stupňů utajení

1. Pro označení stupně utajení jednotlivých odstavců určitého textu lze použít standardizované zkratky. Tyto zkratky nenahrazují úplné označení stupňů utajení.

2. V utajovaných dokumentech EU je možné použít pro označení stupně utajení oddílů nebo částí textu kratších než jedna strana tyto standardní zkratky:

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

Článek 25

Vyhotovování utajovaných dokumentů EU

1. Při vyhotovování utajovaného dokumentu EU:

a) se na každé straně jasně vyznačí příslušný stupeň utajení;

b) se každá strana očísluje;

c) se na dokumentu uvede evidenční číslo a předmět, které samy o sobě nejsou utajovanými informacemi, pokud tak nejsou označeny;

d) se na dokumentu uvede datum;

e) se na dokumentech se stupněm utajení SECRET UE/EU SECRET nebo vyšším, které mají být distribuovány ve více výtiscích, na každé straně uvede číslo výtisku.

2. Nelze-li na utajované informace EU použít odstavec 1, přijmou se jiná patřičná opatření v souladu s prováděcími pravidly.

Článek 26

Snížení stupně utajení a odtajnění utajovaných informací EU

1. Je-li to možné, uvede původce v době vytvoření utajovaných informací EU, zda je k určitému datu nebo po určité události možné jejich stupeň utajení snížit nebo je odtajnit.

2. Každý útvar Komise pravidelně přezkoumává utajované informace EU, kterých je původcem, za účelem zjištění, zda je příslušný stupeň utajení stále odpovídající. Pomocí prováděcích pravidel se zavede systém, v rámci něhož budou stupně utajení evidovaných utajovaných informací EU, jež mají původ v Komisi, přezkoumávány nejméně jednou za pět let. Tento přezkum není třeba provést v případě, že původce na počátku uvedl, že u daných informací bude automaticky snížen stupeň utajení či budou odtajněny, a dané informace jsou odpovídajícím způsobem označeny.

3. Informace se stupněm utajení RESTREINT UE/EU RESTRICTED, jež mají původ v Komisi, se v souladu s nařízením Rady (EHS, Euratom) č. 354/83 ve znění nařízení Rady (ES, Euratom) č. 1700/2003 ([1]) považují za automaticky odtajněné po třiceti letech.

Článek 27

Systém evidence utajovaných informací EU v Komisi

1. Aniž je dotčen čl. 52 odst. 5, v každém útvaru Komise, v němž se nakládá s utajovanými informacemi EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET nebo v němž jsou tyto informace uchovávány, se určí odpovědný místní registr utajovaných informací EU s cílem zajistit, aby se s utajovanými informacemi EU nakládalo v souladu s tímto rozhodnutím.

2. Centrálním registrem Komise pro utajované informace EU je registr utajovaných informací EU spravovaný generálním sekretariátem. Působí jako:

— místní registr utajovaných informací EU pro generální sekretariát Komise,

— registr utajovaných informací EU pro soukromé kanceláře členů Komise, nemají-li tito členové zvláštní místní registr utajovaných informací EU,

— registr utajovaných informací EU pro generální ředitelství nebo služby, které nemají místní registr utajovaných informací EU,

— hlavní vstupní a výstupní místo pro všechny informace se stupněm utajení RESTREINT UE/EU RESTRICTED a až do stupně utajení SECRET UE/EU SECRET včetně, které si mezi sebou vyměňují Komise a její útvary, třetí státy a mezinárodní organizace, a stanoví-li tak zvláštní ujednání, též jako hlavní vstupní a výstupní místo pro ostatní orgány, agentury a instituce Unie.

3. Bezpečnostní orgán Komise určí v Komisi registr, který bude působit jako ústřední orgán pro příjem a odesílání informací se stupněm utajení TRES SECRET UE/EU TOP SECRET. V případě potřeby mohou být určeny podřízené registry pro nakládání s těmito informacemi za účelem evidence.

4. Podřízené registry nesmějí bez výslovného písemného souhlasu ústředního registru pro dokumenty se stupněm utajení TRES SECRET UE/EU TOP SECRET poskytovat dokumenty se stupněm utajení TRES SECRET UE/EU TOP SECRET přímo jiným registrům podřízeným stejnému ústřednímu registru ani externím subjektům.

5. Registry utajovaných informací EU se zřizují jako zabezpečené oblasti podle kapitoly 3 a jsou akreditovány orgánem pro bezpečnostní akreditaci v Komisi.

Článek 28

Vedoucí registru

1. Každý registr utajovaných informací EU spravuje vedoucí registru.

2. Vedoucí registru musí mít náležitou bezpečnostní prověrku.

3. Vedoucí registru podléhá dohledu LSO v daném útvaru Komise, pokud jde o uplatňování ustanovení o nakládání s dokumenty obsahujícími utajované informace EU a o dodržování příslušných bezpečnostních pravidel, standardů a pokynů.

4. V rámci své odpovědnosti za správu registru utajovaných informací EU, ke kterému byl přidělen, má vedoucí registru v souladu s tímto rozhodnutím a příslušnými prováděcími pravidly, standardy a pokyny následující okruhy úkolů:

— řídit operace, které se týkají evidence, uchovávání, reprodukce, překladu, přenosu, odesílání a ničení utajovaných informací EU či jejich převodu do oddělení historických archivů,

— pravidelně ověřovat, zda je nadále třeba uchovávat informace v utajení;

— zastávat další úkoly související s ochranou utajovaných informací EU vymezené v prováděcích pravidlech.

Článek 29

Evidence utajovaných informací EU z bezpečnostních důvodů

1. Pro účely tohoto rozhodnutí se evidencí z bezpečnostních důvodů (dále jen „evidence“) rozumí uplatňování postupů, kterými se zaznamenává životní cyklus utajovaných informací EU, včetně jejich distribuce.

([1]) Nařízení Rady (ES, Euratom) č. 1700/2003 ze dne 22. září 2003, kterým se mění nařízení (EHS, Euratom) č. 354/83 o otevření historických archivů Evropského hospodářského společenství a Evropského společenství pro atomovou energii veřejnosti (Úř. věst. L 243, 27.9.2003, s. 1).

2. Veškeré informace či materiál se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a vyšším je třeba evidovat v určených registrech, kdykoli jsou přijaty v určité organizační složce nebo kdykoli jsou z ní odeslány.

3. Při nakládání s utajovanými informacemi EU nebo jejich uchovávání pomocí komunikačního a informačního systému, mohou být evidenční postupy provedeny přímo v rámci systému.

4. Podrobnější ustanovení týkající se evidence utajovaných informací EU z bezpečnostních důvodů se určí v prováděcích pravidlech.

Článek 30

Kopírování a překládání dokumentů s utajovanými informacemi EU

1. Dokumenty se stupněm utajení TRES SECRET UE/EU TOP SECRET se nesmí kopírovat ani překládat bez předchozího písemného souhlasu původce.

2. Pokud původce dokumentů se stupněm utajení SECRET UE/EU SECRET a nižším nevydal upozornění týkající se jejich kopírování nebo překladu, mohou být tyto dokumenty kopírovány či překládány podle pokynů držitele.

3. Na kopie a překlady dokumentů se použijí bezpečnostní opatření platná pro původní dokument.

Článek 31

Přenos utajovaných informací EU

1. Utajované informace EU se přenášejí takovým způsobem, aby byly během přenosu chráněny před neoprávněným vyzrazením.

2. Přenos utajovaných informací EU podléhá ochranným opatřením, jež:

— jsou úměrná stupni utajení přenášených utajovaných informací EU a

— jsou přizpůsobena konkrétním podmínkám jejich přenosu, zejména v závislosti na tom, zda jsou utajované informace EU přenášeny:

  — uvnitř budovy Komise nebo uzavřené skupiny budov Komise,

  — mezi budovami Komise nacházejícími se ve stejném členském státě,

  — v rámci Unie,

  — z Unie na území třetího státu a

  — jsou přizpůsobena povaze a formě utajovaných informací EU.

3. Ochranná opatření jsou podrobně stanovena v prováděcích pravidlech, nebo jsou v případě projektů a programů uvedených v článku 42 nedílnou součástí bezpečnostních pokynů k příslušnému programu nebo projektu.

4. Prováděcí pravidla či bezpečnostní pokyny k programu/projektu obsahují ustanovení úměrná stupni utajení utajovaných informací EU, pokud jde o:

— druh přenosu, například ruční přenos, přepravu diplomatickým nebo vojenským kurýrem, poštovními službami či komerčními kurýrními službami,

— balení utajovaných informací EU,

— technická protiopatření pro utajované informace EU přenášené na elektronických nosičích,

— jakékoli další procedurální, fyzické nebo elektronické opatření,

— postup evidence,

— využití personálu s bezpečnostním oprávněním.

5. V případech, kdy jsou utajované informace EU přenášeny na elektronických nosičích, a to bez ohledu na čl. 21 odst. 5, mohou být ochranná opatření uvedená v prováděcích pravidlech doplněna vhodnými technickými protiopatřeními schválenými bezpečnostním orgánem Komise s cílem minimalizovat riziko ztráty nebo ohrožení.

Článek 32

Ničení utajovaných informací EU

1. Utajované dokumenty EU, které již nejsou potřebné, mohou být zničeny, se zohledněním nařízení o archivech a pravidel a předpisů Komise týkajících se správy dokumentů a archivace, a zejména společného seznamu pro uchovávání spisů Komise.

2. Utajované informace EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a vyšším zničí vedoucí příslušného registru utajovaných informací EU podle pokynů držitele nebo příslušného orgánu. Vedoucí registru odpovídajícím způsobem aktualizuje záznamy a jiné informace o evidenci.

3. Ničení dokumentů se stupněm utajení SECRET UE/EU SECRET nebo TRES SECRET UE/EU TOP SECRET provádí vedoucí registru za přítomnosti svědka, který je bezpečnostně prověřen alespoň pro stupeň utajení ničeného dokumentu.

4. Pracovník registru a svědek, pokud je přítomnost svědka vyžadována, podepíší zápis o zničení, který se uloží v registru. Vedoucí příslušného registru utajovaných informací EU uchovává zápisy o zničení dokumentů se stupněm utajení TRES SECRET UE/EU TOP SECRET alespoň po dobu deseti let a dokumentů se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET alespoň po dobu pěti let.

5. Ničení utajovaných dokumentů, včetně dokumentů se stupněm utajení RESTREINT UE/EU RESTRICTED, se provádí v souladu s postupy, které jsou vymezeny v prováděcích pravidlech a které splňují příslušné standardy EU či jim rovnocenné standardy.

6. Počítačová paměťová média používaná pro utajované informace EU se ničí v souladu s postupy stanovenými v prováděcích pravidlech.

Článek 33

Ničení utajovaných informací EU v mimořádných situacích

1. Útvary Komise, jež mají utajované informace EU v držení, vypracují s ohledem na místní podmínky plány pro zabezpečení utajovaných materiálů EU v případě krize včetně případných plánů na zničení a vyklizení v případech nouze. Vyhlásí pokyny, které považují za nezbytné pro zamezení tomu, aby se utajované informace EU dostaly do nepovolaných rukou.

2. Ustanovení přijatá pro zabezpečení a/nebo zničení materiálů se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET v případě krize nesmí za žádných okolností negativně ovlivnit zabezpečení nebo zničení materiálů se stupněm utajení TRES SECRET UE/EU TOP SECRET, včetně kódovacího zařízení, jejichž opatrování má přednost před všemi ostatními úkoly.

3. V mimořádné situaci, kdy hrozí bezprostřední riziko neoprávněného vyzrazení, zničí utajované informace EU jejich držitel tak, aby nebylo možné znovu sestavit celý dokument ani jeho část. O nouzovém zničení evidovaných utajovaných informací EU jsou informováni původce a příslušný registr.

4. Podrobnější ustanovení týkající se ničení utajovaných informací EU stanoví prováděcí pravidla.

KAPITOLA 5

OCHRANA UTAJOVANÝCH INFORMACÍ EU V KOMUNIKAČNÍCH A INFORMAČNÍCH SYSTÉMECH

Článek 34

Základní zásady zabezpečení informací

1. Zabezpečení informací v oblasti komunikačních a informačních systémů je jistota, že takové systémy ochrání informace, s nimiž nakládají, a že budou fungovat správně, když jsou zapotřebí, pod dohledem oprávněných uživatelů.

2. Účinné zabezpečení informací zajišťuje odpovídající úroveň:

autenticity: záruka, že informace jsou autentické a z důvěryhodných zdrojů;

dostupnosti: přístupnost a použitelnost informací na žádost oprávněného subjektu;

důvěrnosti: skutečnost, že informace se nezpřístupňují neoprávněným osobám a subjektům nebo pro nedovolené účely;

integrity: zajištění správnosti a úplnosti aktiv a informací;

nepopiratelnosti: schopnost prokázat zpětně jednání či událost tak, aby dané jednání či událost nemohly být následně popřeny.

3. Zabezpečení informací je založeno na procesu řízení rizik.

Článek 35

Definice

Pro účely této kapitoly se použijí tyto definice:

a) „akreditací“ se rozumí formální povolení nebo schválení, které orgán pro bezpečnostní akreditaci udělil komunikačnímu a informačnímu systému, aby ve svém provozním prostředí mohl zpracovávat utajované informace EU, a které následuje po formálním schválení a správném provádění bezpečnostního plánu;

b) „akreditačním řízením“ se rozumí nutné kroky a úkoly, jež je třeba provést předtím, než orgán pro bezpečnostní akreditaci udělí akreditaci. Tyto kroky a úkoly se upřesní ve standardu pro akreditační řízení;

c) „komunikačním a informačním systémem“ se rozumí jakýkoli systém, který umožňuje nakládat s informacemi v elektronické podobě. Komunikační a informační systém zahrnuje všechna aktiva nezbytná k jeho fungování, včetně infrastruktury, organizace, personálu a informačních zdrojů;

d) „zbytkovým rizikem“ se rozumí riziko, které přetrvává poté, co byla zavedena bezpečnostní opatření, neboť nelze čelit všem hrozbám a nelze odstranit všechna zranitelná místa;

e) „rizikem“ se rozumí možnost, že pro účely určité hrozby budou zneužita vnitřní a vnější zranitelná místa organizace nebo kteréhokoli ze systémů, jichž využívá, a dojde tak k poškození organizace a jejích hmotných či nehmotných aktiv. Měří se jako kombinace pravděpodobnosti hrozeb a jejich dopadu;

f) „přijetím rizika“ se rozumí rozhodnutí, kterým se vyjadřuje souhlas s tím, že po řešení rizika i nadále existuje zbytkové riziko;

g) „hodnocení rizika“ spočívá v rozpoznání hrozeb a zranitelných míst a v provádění analýzy souvisejícího rizika, tj. analýzy pravděpodobnosti a dopadu;

h) „sdělování rizika“ spočívá v rozvoji informovanosti o rizicích v rámci skupin uživatelů komunikačních a informačních systémů, v informování schvalovacích orgánů o těchto rizicích a podávání zpráv o těchto rizicích provozním orgánům;

i) „řešení rizika“ spočívá ve zmírnění, odstranění a omezení rizika (prostřednictvím vhodné kombinace technických, fyzických, organizačních nebo procedurálních opatření), přenesení rizika nebo jeho monitorování.

Článek 36

Komunikační a informační systémy nakládající s utajovanými informacemi EU

1. V komunikačních a informačních systémech se nakládá s utajovanými informacemi EU v souladu s koncepcí zabezpečení informací.

2. Pro komunikační a informační systémy, které nakládají s utajovanými informacemi EU, znamená dodržování politiky bezpečnosti informačních systémů Komise, uvedené v rozhodnutí Komise K(2006) 3602 ([1]), že:

a) během celého životního cyklu informačního systému se při provádění politiky bezpečnosti informačních systémů používá přístup „plánuj, udělej, zkontroluj, jednej“ (*Plan-Do-Check-Act*);

b) potřeby v oblasti bezpečnosti musí být určeny prostřednictvím posouzení hospodářského dopadu;

c) informační systém a údaje v něm obsažené musí projít formální klasifikací aktiv;

([1]) K(2006) 3602 ze dne 16. srpna 2006 o bezpečnosti informačních systémů užívaných v Evropské komisi.

d) všechna povinná bezpečnostní opatření, která jsou stanovena v politice bezpečnosti informačních systémů, musí být provedena;

e) musí proběhnout proces řízení rizik, který se skládá z těchto kroků: identifikace hrozeb a zranitelných míst, hodnocení rizika, řešení rizika, přijetí rizika a sdělování rizika;

f) je definován, prováděn, kontrolován a přezkoumáván bezpečnostní plán, včetně bezpečnostní politiky a bezpečnostních provozních postupů.

3. Všichni zaměstnanci, kteří se podílejí na návrhu, vývoji, zkoušení, provozu, řízení nebo používání komunikačních a informačních systémů nakládajících s utajovanými informacemi EU, oznámí orgánu pro bezpečnostní akreditaci všechny potenciální bezpečnostní nedostatky, incidenty, narušení bezpečnosti nebo ohrožení, které mohou mít dopad na ochranu daných systémů a/nebo utajovaných informací EU v nich obsažených.

4. Pokud je ochrana utajovaných informací EU zajišťována kryptografickými prostředky, tyto prostředky se schvalují tímto způsobem:

a) na základě doporučení skupiny odborníků pro bezpečnost v Komisi je třeba dát přednost výrobkům, které byly schváleny Radou nebo generálním tajemníkem Rady jakožto schvalovacím orgánem pro kryptografickou ochranu v Radě;

b) opravňují-li k tomu zvláštní provozní důvody, může schvalovací orgán pro kryptografickou ochranu v Komisi na základě doporučení skupiny odborníků pro bezpečnost v Komisi udělit výjimku z požadavků uvedených pod písmenem a) a udělit dočasné schválení na konkrétní období.

5. Během elektronického přenosu, zpracovávání a uchovávání utajovaných informací EU se použijí schválené kryptografické prostředky. Bez ohledu na tento požadavek se za mimořádných okolností nebo v případě zvláštních technických konfigurací mohou po schválení schvalovacím orgánem pro kryptografickou ochranu použít zvláštní postupy.

6. Komunikační a informační systémy nakládající s informacemi se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo vyšším jsou chráněny bezpečnostními opatřeními proti ohrožení dotyčných informací kompromitujícím elektromagnetickým vyzařováním („bezpečnostní opatření TEMPEST“). Tato bezpečnostní opatření jsou přiměřená riziku zneužití a stupni utajení daných informací.

7. Bezpečnostní orgán Komise působí jako:

— orgán pro zabezpečení informací,

— orgán pro bezpečnostní akreditaci,

— orgán TEMPEST,

— schvalovací orgán pro kryptografickou ochranu,

— orgán pro distribuci kryptografických materiálů.

8. Bezpečnostní orgán Komise jmenuje u každého systému provozní orgán pro zabezpečení informací.

9. Úkoly spojené s funkcemi popsanými v odstavcích 7 a 8 budou vymezeny v prováděcích pravidlech.

Článek 37

Akreditace komunikačních a informačních systémů nakládajících s utajovanými informacemi EU

1. Veškeré komunikační a informační systémy, které nakládají s utajovanými informacemi EU, podléhají akreditačnímu řízení, které vychází ze zásad zabezpečení informací a které musí být natolik podrobné, aby to odpovídalo požadované úrovni ochrany.

2. Akreditační řízení zahrnuje formální schválení bezpečnostního plánu komunikačního a informačního systému orgánem pro bezpečnostní akreditaci v Komisi, aby bylo zajištěno, že:

a) proces řízení rizik, jak je uveden v čl. 36 odst. 2, byl řádně proveden;

b) vlastník systému vědomě přijal zbytkové riziko a

c) bylo dosaženo dostatečné úrovně ochrany komunikačního a informačního systému a utajovaných informací EU, s nimiž se v něm nakládá, v souladu s tímto rozhodnutím.

3. Orgán pro bezpečnostní akreditaci v Komisi vydá rozhodnutí o akreditaci, které stanoví nejvyšší stupeň utajení informací EU, s nimiž lze v daném systému nakládat, a příslušné podmínky pro provoz. Tím nejsou dotčeny úkoly, které byly svěřeny radě pro bezpečnostní akreditaci podle článku 11 nařízení Evropského parlamentu a Rady (EU) č. 512/2014 ([1]).

4. Za akreditaci komunikačních a informačních systémů Komise, na nichž se podílí několik stran, odpovídá společná rada pro bezpečnostní akreditaci. Tato rada se skládá z jednoho zástupce orgánu pro bezpečnostní akreditaci každé zúčastněné strany a předsedá jí zástupce orgánu pro bezpečnostní akreditaci v Komisi.

5. Akreditační řízení zahrnuje řadu úkolů, které mají vykonat zúčastněné strany. Odpovědnost za přípravu akreditačních spisů a dokumentace nese v plné míře vlastník systému.

6. Za akreditaci je odpovědný orgán pro bezpečnostní akreditaci v Komisi, jenž má kdykoli během životního cyklu komunikačního a informačního systému právo:

a) požadovat, aby se použilo akreditační řízení;

b) provést audit či kontrolu systému;

c) tam, kde podmínky pro provoz již nejsou splněny, požadovat vypracování a účinné provádění plánu na zlepšení bezpečnosti v jasně vymezeném časovém horizontu, a případně odebrat povolení pro provoz systému do té doby, než budou podmínky pro provoz opět splněny.

7. Akreditační řízení se stanoví ve standardu pro akreditační řízení pro komunikační a informační systémy, které nakládají s utajovanými informacemi EU, jež bude přijat v souladu s čl. 10 odst. 3 rozhodnutí K(2006) 3602.

Článek 38

Mimořádné okolnosti

1. Bez ohledu na ustanovení této kapitoly mohou být za mimořádných okolností, například během hrozící nebo probíhající krize, konfliktu, války nebo za výjimečných provozních okolností, použity níže popsané zvláštní postupy.

2. Utajované informace EU mohou být přenášeny za použití kryptografických prostředků schválených pro nižší stupeň utajení nebo v nešifrované podobě se souhlasem příslušného orgánu, pokud by jakékoli zpoždění způsobilo škodu nepochybně převyšující škodu způsobenou případným vyzrazením utajovaných materiálů a pokud:

a) odesílatel a příjemce nemají požadované šifrovací zařízení a

b) utajované materiály nelze včas předat jiným způsobem.

3. Za okolností uvedených v odstavci 1 nenesou přenášené utajované informace žádná označení ani údaje, jež by je odlišovaly od informací, které nejsou utajované nebo které mohou být chráněny dostupným kryptografickým prostředkem. Příjemce informací je třeba neprodleně uvědomit o stupni utajení jiným způsobem.

4. Následně se podá zpráva příslušnému orgánu a skupině odborníků pro bezpečnost v Komisi.

KAPITOLA 6

PRŮMYSLOVÁ BEZPEČNOST

Článek 39

Základní zásady

1. Průmyslovou bezpečností se rozumí uplatňování opatření, s jejichž pomocí ochranu utajovaných informací EU zajišťují:

a) v rámci utajovaných smluv:

   i) zájemci nebo uchazeči po dobu nabídkového a zadávacího řízení;

   ii) dodavatelé či subdodavatelé po celý životní cyklus utajovaných smluv;

([1]) Nařízení Evropského parlamentu a Rady (EU) č. 512/2014 ze dne 16. dubna 2014, kterým se mění nařízení (EU) č. 912/2010 o zřízení Agentury pro evropský GNSS (Úř. věst. L 150, 20.5.2014, s. 72).

b) v rámci utajovaných grantových dohod:

i) žadatelé během řízení o udělování grantů;

ii) příjemci během celého životního cyklu utajovaných grantových dohod.

2. Tyto smlouvy či grantové dohody nesmí obsahovat informace se stupněm utajení TRES SECRET UE/EU TOP SECRET.

3. Není-li stanoveno jinak, ustanovení této kapitoly týkající se utajovaných smluv nebo dodavatelů se použijí také na utajované subdodavatelské smlouvy či subdodavatele.

Článek 40

Definice

Pro účely této kapitoly se rozumí:

a) „utajovanou smlouvou“ rámcová smlouva nebo smlouva podle nařízení Rady (ES, Euratom) č. 1605/2002 ([1]), kterou uzavírá Komise nebo jeden z jejích útvarů s určitým dodavatelem na dodání movitého nebo nemovitého majetku, provedení prací nebo poskytnutí služeb, jejichž plnění vyžaduje nebo zahrnuje vytváření a uchovávání utajovaných informací EU nebo nakládání s nimi;

b) „utajovanou subdodavatelskou smlouvou“ smlouva mezi dodavatelem Komise nebo jednoho z jejích útvarů a jiným dodavatelem (tj. subdodavatelem) o dodání movitého nebo nemovitého majetku, provedení prací nebo poskytnutí služeb, jejichž plnění vyžaduje nebo zahrnuje vytváření a uchovávání utajovaných informací EU nebo nakládání s nimi;

c) „utajovanou grantovou dohodou“ dohoda, na jejímž základě Komise udělí grant, jak je uvedeno v části I hlavě VI nařízení (ES, Euratom) č. 1605/2002, a jejíž plnění vyžaduje nebo zahrnuje vytváření a uchovávání utajovaných informací EU nebo nakládání s nimi;

d) „určeným bezpečnostním orgánem“ orgán, který podléhá vnitrostátnímu bezpečnostnímu orgánu členského státu a který odpovídá za informování průmyslových nebo jiných subjektů o vnitrostátní politice ohledně všech otázek průmyslové bezpečnosti a za poskytování pokynů a pomoci při jejím provádění. Funkci určeného bezpečnostního orgánu může vykonávat vnitrostátní bezpečnostní orgán nebo kterýkoli jiný příslušný orgán.

Článek 41

Postup v případě utajovaných smluv nebo utajovaných grantových dohod

1. Každý útvar Komise jakožto veřejný zadavatel zajistí, aby smlouva odkazovala na minimální standardy průmyslové bezpečnosti, které jsou stanoveny v této kapitole, či je obsahovala a aby tyto standardy byly při zadávání zakázek na základě utajovaných smluv či udělování grantů na základě utajovaných grantových dohod dodržovány.

2. Pro účely odstavce 1 příslušné útvary v rámci Komise konzultují Generální ředitelství pro lidské zdroje a bezpečnost, a zejména ředitelství pro bezpečnost, a zajistí, aby vzorové smlouvy a subdodavatelské smlouvy a vzorové grantové dohody obsahovaly ustanovení odrážející základní zásady a minimální standardy pro ochranu utajovaných informací EU, jež musí splňovat dodavatelé, subdodavatelé a příjemci grantových dohod.

3. Komise úzce spolupracuje s vnitrostátním bezpečnostním orgánem, určeným bezpečnostním orgánem nebo kterýmkoli jiným příslušným orgánem dotyčného členského státu.

4. Pokud veřejný zadavatel hodlá zahájit řízení, jehož cílem je uzavření utajované smlouvy nebo grantové dohody, vyžádá si poradenství bezpečnostního orgánu Komise ohledně otázek týkajících se povahy utajení a utajovaných prvků řízení ve všech jeho fázích.

5. Šablony a vzory utajovaných smluv, subdodavatelských smluv a grantových dohod, oznámení o zahájení zadávacího řízení, pokyny ohledně okolností, za nichž je vyžadováno osvědčení o bezpečnostní prověrce zařízení, bezpečnostní pokyny k programu nebo projektu, seznamy bezpečnostních požadavků, pravidla pro návštěvy, přenos a přepravu utajovaných informací EU v rámci utajovaných smluv nebo utajovaných grantových dohod se po konzultaci se skupinou odborníků pro bezpečnost v Komisi stanoví v prováděcích pravidlech pro průmyslovou bezpečnost.

([1]) Nařízení Rady (ES, Euratom) č. 1605/2002 ze dne 25. června 2002, kterým se stanoví finanční nařízení o souhrnném rozpočtu Evropských společenství (Úř. věst. L 248, 16.9.2002, s. 1).

6. Komise může uzavřít utajované smlouvy nebo grantové dohody, ve kterých plněním úkolů, které zahrnují nebo vyžadují přístup k utajovaným informacím EU nebo nakládání s nimi či jejich uchovávání, pověří hospodářské subjekty registrované v členském státě nebo ve třetím státě, s nímž byla uzavřena dohoda nebo správní ujednání podle kapitoly 7 tohoto rozhodnutí.

Článek 42

Bezpečnostní prvky v utajované smlouvě nebo utajované grantové dohodě

1. Utajované smlouvy nebo grantové dohody obsahují následující bezpečnostní prvky:

Bezpečnostní pokyny k programu nebo projektu

a) „Bezpečnostními pokyny k programu nebo projektu“ se rozumí seznam bezpečnostních postupů, které se uplatňují u konkrétního programu nebo projektu s cílem standardizovat bezpečnostní postupy. Tyto pokyny lze během celé doby trvání programu nebo projektu revidovat.

b) Generální ředitelství pro lidské zdroje a bezpečnost vypracuje obecné bezpečnostní pokyny k programu nebo projektu; útvary Komise odpovědné za programy nebo projekty zahrnující nakládání s utajovanými informacemi EU nebo jejich uchovávání mohou případně vypracovat konkrétní bezpečnostní pokyny k programu nebo projektu, které budou z obecných bezpečnostních pokynů vycházet.

c) Konkrétní bezpečnostní pokyny k programu nebo projektu se vypracují zejména pro programy a projekty, které se vyznačují značným rozsahem, měřítkem nebo složitostí nebo množstvím či rozmanitostí dodavatelů, příjemců a ostatních partnerů a zúčastněných stran, například pokud jde o jejich právní status. Konkrétní bezpečnostní pokyny k programu nebo projektu vypracuje útvar či útvary Komise, jež program nebo projekt řídí, v úzké spolupráci s Generálním ředitelstvím pro lidské zdroje a bezpečnost.

d) Generální ředitelství pro lidské zdroje a bezpečnost předloží obecné i konkrétní bezpečnostní pokyny k programu nebo projektu ke konzultaci skupině odborníků pro bezpečnost v Komisi.

Seznam bezpečnostních požadavků

a) „Seznamem bezpečnostních požadavků“ se rozumí soubor zvláštních smluvních podmínek vydaný veřejným zadavatelem, který je nedílnou součástí kterékoli utajované smlouvy, jejíž plnění vyžaduje přístup k utajovaným informacím EU nebo jejich vytváření, a který určí bezpečnostní požadavky a části smlouvy vyžadující bezpečnostní ochranu.

b) V seznamu bezpečnostních požadavků jsou popsány bezpečnostní požadavky pro konkrétní smlouvu. Seznam případně zahrnuje příručku pro stanovování stupně utajení a je nedílnou částí utajované smlouvy, subdodavatelské smlouvy nebo grantové dohody.

c) Seznam bezpečnostních požadavků obsahuje ustanovení, podle nichž musí dodavatel nebo příjemce dodržovat minimální standardy stanovené tímto rozhodnutím. Veřejný zadavatel zajistí, aby v seznamu bezpečnostních požadavků bylo uvedeno, že nedodržení těchto minimálních standardů může být dostatečným důvodem pro ukončení smlouvy nebo grantové dohody.

2. Jak bezpečnostní pokyny k programu nebo projektu, tak seznamy bezpečnostních požadavků obsahují jako povinný bezpečnostní prvek příručku pro stanovování stupně utajení:

a) „Příručkou pro stanovování stupně utajení“ se rozumí dokument popisující prvky programu, projektu, smlouvy nebo grantové dohody, které jsou utajované, přičemž stanoví použitelné stupně utajení. Příručka pro stanovování stupně utajení může být v průběhu realizace programu, projektu, smlouvy nebo grantové dohody rozšířena a stupně utajení informací mohou být změněny nebo sníženy; pokud existuje příručka pro stanovování stupně utajení, je součástí seznamu bezpečnostních požadavků.

b) Před zahájením nabídkového řízení na uzavření utajované smlouvy nebo před uzavřením takové smlouvy určí útvary Komise jakožto veřejný zadavatel stupeň utajení veškerých informací, které mají být poskytnuty zájemcům, uchazečům či dodavatelům, a rovněž stupeň utajení veškerých informací, které vytvoří dodavatel. Za tímto účelem připraví po konzultaci s bezpečnostním orgánem Komise příručku pro stanovování stupně utajení, jež se má používat pro provedení zakázky, podle tohoto rozhodnutí a jeho prováděcích pravidel.

c) Pro stanovení stupně utajení jednotlivých částí utajované smlouvy se použijí tyto zásady:

i) při přípravě příručky pro stanovování stupňů utajení bere útvar Komise jakožto veřejný zadavatel v úvahu veškeré důležité bezpečnostní aspekty, včetně stupně utajení, který poskytnutým informacím přidělil původce informací a který původce informací schválil pro danou smlouvu;

ii) stupeň utajení smlouvy jako celku nesmí být nižší než nejvyšší stupeň utajení kterékoli části smlouvy a

iii) dojde-li k jakýmkoli změnám ohledně stupně utajení informací vytvářených dodavateli nebo poskytovaných dodavatelům při plnění smlouvy a provádějí-li se jakékoli dodatečné změny v příručce pro stanovování stupňů utajení, veřejný zadavatel se případně prostřednictvím bezpečnostního orgánu Komise spojí s vnitrostátními bezpečnostními orgány, s určenými bezpečnostními orgány členských států nebo s jakýmkoli jiným příslušným bezpečnostním orgánem.

Článek 43

Přístup k utajovaným informacím EU pro zaměstnance dodavatelů a příjemců

Veřejný zadavatel či poskytovatel grantu zajistí, aby utajovaná smlouva nebo utajovaná grantová dohoda obsahovaly ustanovení o tom, že zaměstnanci dodavatele, subdodavatele nebo příjemce, kteří pro plnění utajované smlouvy, subdodavatelské smlouvy nebo grantové dohody potřebují přístup k utajovaným informacím EU, tento přístup získají, pouze pokud:

a) mají bezpečnostní oprávnění pro odpovídající stupeň utajení nebo jsou jinak řádně oprávněni a bylo rozhodnuto, že informace potřebují znát;

b) byli poučeni o příslušných bezpečnostních pravidlech pro ochranu utajovaných informací EU a vzali na vědomí své povinnosti ohledně ochrany těchto informací;

c) jedná-li se o informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET, prošli bezpečnostní prověrkou pro odpovídající stupeň utajení, kterou provedl příslušný vnitrostátní bezpečnostní orgán, určený bezpečnostní orgán nebo kterýkoli jiný příslušný orgán.

Článek 44

Bezpečnostní prověrka zařízení

1. „Bezpečnostní prověrkou zařízení“ se rozumí správní rozhodnutí vnitrostátního bezpečnostního orgánu, určeného bezpečnostního orgánu nebo jiného příslušného bezpečnostního orgánu, že určité zařízení může z hlediska bezpečnosti zajistit odpovídající úroveň ochrany utajovaných informací EU s určitým stupněm utajení.

2. Dříve, než mohou být zájemci, uchazeči či dodavateli nebo žadateli o grant či příjemci grantu poskytnuty utajované informace EU nebo než je mu k utajovaným informacím EU umožněn přístup, musí bezpečnostnímu orgánu Komise předložit osvědčení o bezpečnostní prověrce zařízení udělené vnitrostátním bezpečnostním orgánem nebo určeným bezpečnostním orgánem nebo jakýmkoli jiným příslušným bezpečnostním orgánem členského státu, které v souladu s vnitrostátními právními předpisy potvrzuje, že hospodářský subjekt je ve svých zařízeních schopen zajistit ochranu utajovaných informací EU na odpovídajícím stupni utajení (CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET), a bezpečnostní orgán Komise je předá útvaru Komise, jenž jedná jako veřejný zadavatel nebo poskytovatel grantu.

3. V příslušných případech veřejný zadavatel oznámí prostřednictvím bezpečnostního orgánu Komise příslušnému vnitrostátnímu bezpečnostnímu orgánu, určenému bezpečnostnímu orgánu nebo kterémukoli jinému příslušnému bezpečnostnímu orgánu, že pro účely plnění smlouvy je vyžadováno osvědčení o bezpečnostní prověrce zařízení. Osvědčení o bezpečnostní prověrce zařízení nebo osvědčení o bezpečnostní prověrce personálu je vyžadováno v případě, že je během zadávacího řízení či řízení o udělení grantu třeba poskytovat utajované informace EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET.

4. Veřejný zadavatel či poskytovatel grantu neuzavře utajovanou smlouvu či grantovou dohodu s upřednostňovaným uchazečem či účastníkem, dokud neobdrží od vnitrostátního bezpečnostního orgánu, určeného bezpečnostního orgánu nebo kteréhokoli jiného příslušného bezpečnostního orgánu členského státu, v němž je dotyčný dodavatel nebo subdodavatel registrován, potvrzení o tom, že bylo v případě, kdy je to vyžadováno, vydáno příslušné osvědčení o bezpečnostní prověrce zařízení.

5. Pokud vnitrostátní bezpečnostní orgán, určený bezpečnostní orgán nebo kterýkoli jiný příslušný bezpečnostní orgán, který vydal osvědčení o bezpečnostní prověrce zařízení, uvědomí bezpečnostní orgán Komise o změnách ovlivňujících toto osvědčení, bezpečnostní orgán Komise o tom uvědomí útvar Komise, který jedná jako veřejný zadavatel nebo poskytovatel grantu. V případě subdodavatelské smlouvy je odpovídajícím způsobem informován vnitrostátní bezpečnostní orgán, určený bezpečnostní orgán nebo kterýkoli jiný příslušný bezpečnostní orgán.

6. Zrušení osvědčení o bezpečnostní prověrce zařízení příslušným vnitrostátním bezpečnostním orgánem, určeným bezpečnostním orgánem nebo kterýmkoli jiným příslušným bezpečnostním orgánem je dostatečným důvodem k tomu, aby veřejný zadavatel či poskytovatel grantu vypověděl utajovanou smlouvu nebo aby vyloučil určitého zájemce, uchazeče nebo žadatele z nabídkového řízení. Ve vzorových smlouvách a grantových dohodách, jež mají být vypracovány, musí být obsaženo příslušné ustanovení.

Článek 45

Ustanovení týkající se utajovaných smluv a utajovaných grantových dohod

1. Pokud jsou během zadávacího řízení zájemci, uchazeči nebo žadateli poskytovány utajované informace EU, musí výzva k podávání nabídek či výzva k předkládání návrhů obsahovat ustanovení o tom, že zájemce, uchazeč nebo žadatel, který nabídku či návrh nepředloží nebo jehož nabídka či návrh nebudou vybrány, je povinen všechny utajované dokumenty ve stanovené lhůtě vrátit.

2. Veřejný zadavatel či poskytovatel grantu oznámí prostřednictvím bezpečnostního orgánu Komise příslušnému vnitrostátnímu bezpečnostnímu orgánu, určenému bezpečnostnímu orgánu nebo kterémukoli jinému příslušnému bezpečnostnímu orgánu skutečnost, že utajovaná smlouva nebo grantová dohoda byla uzavřena, a rovněž oznámí příslušné údaje, jako je název dodavatelů nebo příjemců, doba trvání smlouvy a maximální stupeň utajení.

3. Jakmile je taková smlouva či grantová dohoda ukončena, veřejný zadavatel či poskytovatel grantu o tom neprodleně prostřednictvím bezpečnostního orgánu Komise uvědomí příslušný vnitrostátní bezpečnostní orgán, určený bezpečnostní orgán nebo kterýkoli jiný příslušný bezpečnostní orgán členského státu, v němž je dodavatel nebo příjemce grantu registrován.

4. Obecně platí, že při ukončení utajované smlouvy či grantové dohody nebo ukončení účasti příjemce grantu musí dodavatel nebo příjemce grantu vrátit veřejnému zadavateli či poskytovateli grantu veškeré utajované informace EU, které má v držení.

5. V seznamu bezpečnostních požadavků se stanoví zvláštní ustanovení týkající se nakládání s utajovanými informacemi EU během plnění utajované smlouvy či grantové dohody nebo při jejím ukončení.

6. Pokud je dodavatel nebo příjemce grantu oprávněn ponechat si utajované informace EU po ukončení smlouvy či grantové dohody, dodavatel nebo příjemce grantu nadále dodržuje minimální standardy obsažené v tomto rozhodnutí a chrání důvěrnost utajovaných informací EU.

Článek 46

Zvláštní ustanovení týkající se utajovaných smluv

1. Podmínky týkající se ochrany utajovaných informací EU, za nichž může dodavatel uzavřít subdodavatelskou smlouvu, jsou stanoveny ve výzvě k předkládání nabídek a v utajované smlouvě.

2. Předtím, než dodavatel zadá jakékoli části utajované smlouvy subdodavateli, musí získat povolení od veřejného zadavatele. Subdodavatelská smlouva, s níž souvisí přístup k utajovaným informacím EU, nemůže být zadána subdodavatelům se sídlem ve třetí zemi, pokud neexistuje právní rámec pro bezpečnost informací stanovený v kapitole 7.

3. Dodavatel je povinen zajistit, aby veškeré subdodavatelské činnosti byly prováděny v souladu s minimálními standardy stanovenými tímto rozhodnutím, a nesmí subdodavateli poskytovat utajované informace EU bez předchozího písemného souhlasu veřejného zadavatele.

4. Pokud jde o utajované informace EU, které vytvořil nebo s nimiž nakládá dodavatel, pak se za původce považuje Komise a práva náležející původci vykonává veřejný zadavatel.

Článek 47

Návštěvy v souvislosti s utajovanými smlouvami

1. Pokud zaměstnanci Komise, dodavatelů či příjemců grantu potřebují pro plnění utajované smlouvy nebo grantové dohody přístup k informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET v prostorách druhé strany, sjednají se návštěvy ve spolupráci s příslušnými vnitrostátními bezpečnostními orgány, určenými bezpečnostními orgány nebo s kterýmkoli jiným příslušným bezpečnostním orgánem. O těchto návštěvách je vyrozuměn bezpečnostní orgán Komise. Vnitrostátní bezpečnostní orgány, určené bezpečnostní orgány nebo kterýkoli jiný příslušný bezpečnostní orgán se však mohou v rámci konkrétních programů nebo projektů dohodnout na postupu, podle kterého se mohou návštěvy sjednávat přímo.

2. Všechny navštěvující osoby musí být držiteli odpovídajícího osvědčení o bezpečnostní prověrce a musí mít potřebu znát utajované informace EU související s utajovanou smlouvou.

3. Navštěvujícím osobám je umožněn přístup pouze k utajovaným informacím EU souvisejícím s účelem návštěvy.

4. Podrobnější ustanovení se formulují v prováděcích pravidlech.

5. Dodržování ustanovení o návštěvách ve spojitosti s utajovanými smlouvami, stanovených v tomto rozhodnutí a v prováděcích pravidlech uvedených v odstavci 4, je povinné.

Článek 48

Přenos a přeprava utajovaných informací EU v rámci utajovaných smluv nebo utajovaných grantových dohod

1. Pokud jde o elektronický přenos utajovaných informací EU, použijí se příslušná ustanovení kapitoly 5 tohoto rozhodnutí.

2. Pokud jde o přepravu utajovaných informací EU, použijí se příslušná ustanovení kapitoly 4 tohoto rozhodnutí a jeho prováděcích pravidel v souladu s vnitrostátními právními předpisy.

3. V případě přepravy utajovaných materiálů jako nákladu se při určování bezpečnostních opatření uplatní tyto zásady:

a) bezpečnost musí být zajištěna během všech fází přepravy z místa původu až po konečné místo určení;

b) stupeň ochrany poskytovaný zásilce se stanoví podle nejvyššího stupně utajení materiálů, které jsou její součástí;

c) před jakoukoli přeshraniční přepravou materiálů se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET musí odesílatel vypracovat přepravní plán, který schválí příslušný vnitrostátní bezpečnostní orgán, určený bezpečnostní orgán nebo kterýkoli jiný příslušný bezpečnostní orgán;

d) materiály musí být převáženy v nejvyšší možné míře po přímé trase a přeprava musí být ukončena, jak nejrychleji to okolnosti umožní;

e) je-li to možné, přepravní trasy by měly vést pouze přes území členských států. Přeprava přes jiné než členské státy by se měla uskutečnit pouze v případě, kdy byla povolena vnitrostátním bezpečnostním orgánem, určeným bezpečnostním orgánem nebo kterýmkoli jiným příslušným bezpečnostním orgánem států odesílatele i příjemce zásilky.

Článek 49

Poskytování utajovaných informací EU dodavatelům nebo příjemcům grantů se sídlem ve třetích státech

Utajované informace EU jsou dodavatelům nebo příjemcům grantu se sídlem v třetích státech poskytovány v souladu s bezpečnostními opatřeními dohodnutými mezi bezpečnostním orgánem Komise, útvarem Komise jakožto veřejným zadavatelem či poskytovatelem grantu a vnitrostátním bezpečnostním orgánem, určeným bezpečnostním orgánem nebo jiným příslušným bezpečnostním orgánem dotyčného třetího státu, v němž je dodavatel nebo příjemce grantu registrován.

Článek 50

Nakládání s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED v rámci utajovaných smluv nebo utajovaných grantových dohod

1. Ochrana informací se stupněm utajení RESTREINT UE/EU RESTRICTED, s nimiž se nakládá nebo jež jsou uchovávány v rámci utajovaných smluv nebo grantových dohod se zakládá na zásadách přiměřenosti a efektivnosti nákladů.

2. Osvědčení o bezpečnostní prověrce zařízení nebo bezpečnostní prověrce personálu se v rámci utajovaných smluv nebo utajovaných grantových dohod zahrnujících nakládání s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED nevyžaduje.

3. Pokud smlouva nebo grantová dohoda zahrnuje nakládání s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED v komunikačním a informačním systému provozovaném dodavatelem nebo příjemcem grantu, veřejný zadavatel či poskytovatel grantu po konzultaci s bezpečnostním orgánem Komise zajistí, aby ve smlouvě nebo grantové dohodě byly uvedeny nezbytné technické a správní požadavky týkající se akreditace či schválení komunikačního a informačního systému, které budou přiměřené posouzenému riziku a zohlední všechny příslušné faktory. Na rozsahu akreditace či schválení takového komunikačního a informačního systému se dohodnou bezpečnostní orgán Komise a příslušný vnitrostátní bezpečnostní orgán nebo určený bezpečnostní orgán.

KAPITOLA 7

VÝMĚNA UTAJOVANÝCH INFORMACÍ S DALŠÍMI ORGÁNY, INSTITUCEMI NEBO JINÝMI SUBJEKTY UNIE, S ČLENSKÝMI STÁTY A SE TŘETÍMI STÁTY A MEZINÁRODNÍMI ORGANIZACEMI

Článek 51

Základní zásady

1. Pokud Komise nebo jeden z jejích útvarů rozhodne, že je třeba přistoupit k výměně utajovaných informací EU s jiným orgánem, institucí nebo jiným subjektem Unie, se třetím státem nebo s mezinárodní organizací, podniknou se nezbytné kroky k tomu, aby byl pro tento účel zaveden vhodný právní nebo správní rámec, jenž může zahrnovat ujednání o bezpečnosti informací nebo správní ujednání uzavřená v souladu s příslušnými právními předpisy.

2. Aniž je dotčen článek 57, vyměňují se utajované informace EU s jiným orgánem, institucí nebo jiným subjektem Unie, se třetím státem nebo mezinárodní organizací, pouze pokud je takový vhodný právní nebo správní rámec zaveden a pokud existují dostatečné záruky, že daný orgán, instituce nebo jiný subjekt Unie nebo třetí stát nebo mezinárodní organizace uplatňuje rovnocenné základní zásady a minimální standardy pro ochranu utajovaných informací.

Článek 52

Výměna utajovaných informací EU s dalšími orgány, institucemi nebo jinými subjekty Unie

1. Před uzavřením správního ujednání pro výměnu utajovaných informací EU s jiným orgánem, institucí nebo jiným subjektem Unie si Komise vyžádá ujištění, že daný orgán, instituce nebo jiný subjekt Unie:

a) má zaveden právní rámec pro ochranu utajovaných informací EU, který stanoví základní zásady a minimální standardy rovnocenné těm, které jsou stanoveny v tomto rozhodnutí a jeho prováděcích pravidlech;

b) uplatňuje bezpečnostní standardy a pokyny týkající se personální bezpečnosti, fyzické bezpečnosti, správy utajovaných informací EU a bezpečnosti komunikačních a informačních systémů, které zaručují úroveň ochrany utajovaných informací EU rovnocennou ochraně v Komisi;

c) označuje utajované informace, které vytváří, jako utajované informace EU.

2. Hlavním útvarem pro uzavírání správních ujednání o výměně utajovaných informací EU s dalšími orgány, institucemi nebo jinými subjekty Unie je v rámci Komise Generální ředitelství pro lidské zdroje a bezpečnost, které úzce spolupracuje s ostatními příslušnými útvary Komise.

3. Správní ujednání mají zpravidla formu výměny dopisů podepsaných jménem Komise generálním ředitelem pro lidské zdroje a bezpečnost.

4. Před uzavřením správního ujednání o výměně utajovaných informací EU provede bezpečnostní orgán Komise hodnoticí návštěvy s cílem posoudit regulační rámec pro ochranu utajovaných informací EU a ověřit účinnost opatření prováděných na ochranu utajovaných informací EU. Správní ujednání vstupuje v platnost a utajované informace EU se vyměňují, pouze pokud výsledky této hodnoticí návštěvy byly uspokojivé a bylo vyhověno doporučením učiněným v návaznosti na návštěvu. Pravidelně se provádějí následné hodnoticí návštěvy, jejichž účelem je ověřovat, zda je správní ujednání dodržováno a zda zavedená bezpečnostní opatření i nadále splňují dohodnuté základní zásady a minimální standardy.

5. Hlavním vstupním a výstupním místem všech utajovaných informací vyměňovaných s dalšími orgány, institucemi nebo jinými subjekty Unie je v rámci Komise zpravidla registr utajovaných informací EU spravovaný generálním sekretariátem. Pokud je to však pro ochranu utajovaných informací EU z bezpečnostních, organizačních či provozních důvodů vhodnější, fungují jako hlavní vstupní a výstupní místo všech utajovaných informací ohledně záležitostí, které spadají do pravomoci dotčených útvarů Komise, místní registry utajovaných informací EU zřízené v rámci útvarů Komise podle tohoto rozhodnutí a jeho prováděcích pravidel.

6. O procesu uzavírání správních ujednání podle odstavce 2 je informována skupina odborníků pro bezpečnost v Komisi.

Článek 53

Výměna utajovaných informací EU s členskými státy

1. Utajované informace EU mohou být předávány členským státům za předpokladu, že členské státy tyto informace chrání v souladu s požadavky použitelnými na utajované informace označené vnitrostátním stupněm utajení na rovnocenné úrovni podle srovnávací tabulky stupňů utajení uvedené v příloze I.

2. Pokud členské státy poskytnou do struktur či sítí Evropské unie utajované informace označené vnitrostátním stupněm utajení, Komise tyto informace chrání v souladu s požadavky na ochranu utajovaných informací EU na rovnocenné úrovni podle srovnávací tabulky stupňů utajení uvedené v příloze I.

Článek 54

Výměna utajovaných informací EU se třetími státy a mezinárodními organizacemi

1. Pokud Komise rozhodne, že je třeba dlouhodobě vyměňovat utajované informace se třetími státy nebo mezinárodními organizacemi, podniknou se nezbytné kroky k tomu, aby byl pro tento účel zaveden vhodný právní nebo správní rámec, jenž může zahrnovat ujednání o bezpečnosti informací nebo správní ujednání uzavřená v souladu s příslušnými právními předpisy.

2. Dohody o bezpečnosti informací a správní ujednání podle odstavce 1 musí obsahovat ustanovení, která zaručí, že třetí státy nebo mezinárodní organizace, obdrží-li utajované informace EU, zajistí ochranu těchto informací odpovídající jejich stupni utajení a v souladu s minimálními standardy, které jsou rovnocenné standardům stanoveným tímto rozhodnutím.

3. Komise může uzavřít správní ujednání v souladu s článkem 56, pokud stupeň utajení poskytovaných utajovaných informací EU není zpravidla vyšší než RESTREINT UE/EU RESTRICTED.

4. Správní ujednání o výměně utajovaných informací podle odstavce 3 musí obsahovat ustanovení, která zaručí, že třetí státy nebo mezinárodní organizace, obdrží-li utajované informace EU, zajistí ochranu těchto informací odpovídající jejich stupni utajení a v souladu s minimálními standardy, které jsou rovnocenné minimálním standardům stanoveným tímto rozhodnutím. Uzavření dohody o bezpečnosti informací nebo správního ujednání je třeba konzultovat se skupinou odborníků pro bezpečnost v Komisi.

5. Rozhodnutí o poskytnutí utajovaných informací EU, jejichž původcem je Komise, třetímu státu nebo mezinárodní organizaci přijímá příslušný útvar Komise (jakožto původce utajovaných informací EU v Komisi) případ od případu s ohledem na povahu a obsah těchto informací, na potřebu příjemce znát utajované informace a na míru prospěchu pro Unii. Není-li Komise původcem utajovaných informací, jejichž poskytnutí se požaduje, či zdrojového materiálu, jež mohou obsahovat, útvar Komise, jenž má tyto utajované informace v držení, nejdříve získá pro poskytnutí informací písemný souhlas původce. Nelze-li původce zjistit, převezme po konzultaci se skupinou odborníků pro bezpečnost v Komisi jeho odpovědnost útvar Komise, který má tyto utajované informace v držení.

Článek 55

Dohody o bezpečnosti informací

1. Dohody o bezpečnosti informací se třetími státy nebo mezinárodními organizacemi se uzavírají v souladu s článkem 218 SFEU.

2. Dohody o bezpečnosti informací:

a) stanoví základní zásady a minimální standardy upravující výměnu utajovaných informací mezi Unií a třetím státem nebo mezinárodní organizací;

b) stanoví, že se příslušné bezpečnostní orgány příslušných orgánů a institucí Unie a příslušný bezpečnostní orgán dotyčného třetího státu nebo mezinárodní organizace dohodnou na technických prováděcích pravidlech. Tato pravidla zohlední úroveň ochrany zajišťovanou zavedenými bezpečnostními předpisy, strukturami a postupy v dotyčném třetím státě nebo mezinárodní organizaci;

c) stanoví, že před zahájením výměny utajovaných informací v rámci dotyčné dohody je třeba se ujistit, že přijímající strana je schopna jí poskytované utajované informace řádným způsobem chránit a zabezpečit.

3. Pokud je v souladu s čl. 51 odst. 1 rozhodnuto, že je třeba utajované informace EU vyměňovat, konzultuje Komise, je-li to vhodné, Evropskou službu pro vnější činnost, generální sekretariát Rady a jiné orgány a instituce Unie s cílem určit, zda by mělo být předloženo doporučení podle čl. 218 odst. 3 Smlouvy o fungování EU.

4. Utajované informace EU nesmí být vyměňovány elektronickými prostředky, pokud tak výslovně není stanoveno v dohodě o bezpečnosti informací nebo v technických prováděcích pravidlech.

5. Hlavním vstupním a výstupním místem všech utajovaných informací vyměňovaných se třetími státy a mezinárodními organizacemi je v rámci Komise zpravidla registr utajovaných informací EU spravovaný generálním sekretariátem. Pokud je to však pro ochranu utajovaných informací EU z bezpečnostních, organizačních či provozních důvodů vhodnější, fungují jako hlavní vstupní a výstupní místo všech utajovaných informací ohledně záležitostí, které spadají do pravomoci dotčených útvarů Komise, místní registry utajovaných skutečností EU zřízené v rámci útvarů Komise podle tohoto rozhodnutí a jeho prováděcích pravidel.

6. Za účelem posouzení účinnosti bezpečnostních předpisů, struktur a postupů v dotyčném třetím státě nebo mezinárodní organizaci se Komise ve spolupráci s ostatními orgány, institucemi či jinými subjekty Unie a na základě vzájemné dohody s dotyčným třetím státem nebo mezinárodní organizací účastní hodnoticích návštěv. Cílem hodnoticích návštěv je vyhodnotit:

a) právní rámec použitelný pro ochranu utajovaných informací;

b) veškeré zvláštnosti bezpečnostní politiky a způsobu organizace bezpečnosti v dotyčném třetím státě nebo mezinárodní organizaci, které mohou mít dopad na stupeň utajení informací, jež mohou být vyměňovány;

c) již zavedená bezpečnostní opatření a postupy a

d) bezpečnostní prověrky pro stupeň utajovaných informací EU, které mají být poskytovány.

Článek 56

Správní ujednání

1. Pokud je třeba v kontextu politického či právního rámce Unie dlouhodobě vyměňovat se třetím státem nebo mezinárodní organizací informace, jejichž stupeň utajení není zpravidla vyšší než RESTREINT UE/EU RESTRICTED, a pokud bezpečnostní orgán Komise po konzultaci se skupinou odborníků pro bezpečnost v Komisi zejména potvrdí, že dotyčná strana nemá dostatečně rozvinutý bezpečnostní systém, který by jí umožnil uzavřít dohodu o bezpečnosti informací, může Komise uzavřít s příslušnými orgány dotyčného třetího státu nebo mezinárodní organizace správní ujednání.

2. Taková správní ujednání mají zpravidla formu výměny dopisů.

3. Před uzavřením ujednání se provede hodnoticí návštěva. O výsledku hodnoticí návštěvy se uvědomí skupina odborníků pro bezpečnost v Komisi. Pokud existují výjimečné důvody pro naléhavou výměnu utajovaných informací, mohou být utajované informace EU poskytnuty pod podmínkou, že bude učiněno vše pro to, aby hodnoticí návštěva byla vykonána co nejdříve.

4. Utajované informace EU nesmí být vyměňovány elektronickými prostředky, pokud tak správní ujednání výslovně nestanoví.

Článek 57

Výjimečné *ad hoc* poskytování utajovaných informací EU

1. Není-li uzavřena dohoda o bezpečnosti informací ani správní ujednání a pokud Komise nebo některý z jejích útvarů rozhodne, že je v kontextu politického nebo právního rámce Unie výjimečně třeba předat utajované informace EU třetímu státu nebo mezinárodní organizaci, bezpečnostní orgán Komise u bezpečnostních orgánů dotyčného třetího státu nebo mezinárodní organizace v možném rozsahu ověří, zda jsou jejich bezpečnostní předpisy, struktury a postupy takové, že poskytnuté utajované informace EU budou chráněny na úrovni standardů, které nejsou méně přísné než standardy stanovené v tomto rozhodnutí.

2. Rozhodnutí o poskytnutí utajovaných informací EU předmětnému třetímu státu nebo mezinárodní organizaci učiní po konzultaci se skupinou odborníků pro bezpečnost v Komisi Komise na základě návrhu člena Komise odpovědného za bezpečnostní záležitosti.

3. Poté, co Komise vydá své rozhodnutí o poskytnutí utajovaných informací EU, a s výhradou předchozího písemného souhlasu původce, včetně původců zdrojového materiálu, který mohou obsahovat, předá příslušný útvar Komise dotčené informace, které ponesou označení týkající se způsobilosti k předání uvádějící třetí stát nebo mezinárodní organizaci, jíž byly informace poskytnuty. Před vlastním poskytnutím informací nebo při jejich poskytnutí se dotyčná třetí strana písemně zaváže k ochraně obdržených utajovaných informací EU v souladu se základními zásadami a minimálními standardy stanovenými tímto rozhodnutím.

KAPITOLA 8

ZÁVĚREČNÁ USTANOVENÍ

Článek 58

Nahrazení předchozího rozhodnutí

Tímto rozhodnutím se zrušuje a nahrazuje rozhodnutí Komise 2001/844/ES, ESUO, Euratom ([1]).

Článek 59

Utajované informace vytvořené před vstupem tohoto rozhodnutí v platnost

1. Veškeré informace EU utajované podle rozhodnutí 2001/844/ES, ESUO, Euratom jsou nadále chráněny v souladu s příslušnými ustanoveními tohoto rozhodnutí.

2. Veškeré utajované informace v držení Komise ke dni, kdy rozhodnutí 2001/844/ES, ESUO, Euratom vstoupilo v platnost, s výjimkou utajovaných informací Euratom:

a) pokud je vytvořila Komise, se nadále považují za automaticky přeřazené do stupně utajení RESTREINT UE, ledaže se jejich autor do 31. ledna 2002 rozhodl udělit jim jiný stupeň utajení a informoval všechny subjekty, jimž je dotčený dokument určen;

b) pokud je vytvořily osoby mimo Komisi, si zachovávají svůj původní stupeň utajení, a považují se proto za utajované informace EU rovnocenného stupně, ledaže autor souhlasí s jejich odtajněním nebo se snížením stupně jejich utajení.

Článek 60

Prováděcí pravidla a bezpečnostní upozornění

1. Na přijetí prováděcích pravidel k tomuto rozhodnutí, je-li to zapotřebí, se v plném souladu s vnitřním jednacím řádem vztahuje zvláštní rozhodnutí Komise o zmocnění určené členovi Komise, který je odpovědný za bezpečnostní záležitosti.

2. Po svém zmocnění prostřednictvím výše uvedeného rozhodnutí Komise může člen Komise odpovědný za bezpečnostní záležitosti vypracovávat bezpečnostní upozornění, v nichž stanoví bezpečnostní pokyny a osvědčené postupy v oblasti působnosti tohoto rozhodnutí a jeho prováděcích pravidel.

3. Úkoly zmiňované v prvním a druhém odstavci tohoto článku může Komise plně v souladu s vnitřním jednacím řádem přenést na generálního ředitele pro lidské zdroje a bezpečnost prostřednictvím zvláštního rozhodnutí o přenesení pravomoci.

Článek 61

Vstup v platnost

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

V Bruselu dne 13. března 2015.

Za Komisi

předseda

Jean-Claude JUNCKER

([1]) Rozhodnutí Komise 2001/844/ES, ESUO, Euratom ze dne 29. listopadu 2001, kterým se mění její jednací řád (Úř. věst. L 317, 3.12.2001, s. 1).

PŘÍLOHA I

SROVNÁVACÍ TABULKA STUPŇŮ UTAJENÍ

EU	TRES 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
Belgie	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)	poznámka [1] níže
Bulharsko	Строго секретно	Секретно	Поверително	За служебно ползване
Česká republika	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dánsko	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Německo	Streng geheim	Geheim	VS [2] — Vertraulich	VS — Nur für den Dienstgebrauch
Estonsko	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Irsko	Top Secret	Secret	Confidential	Restricted
Řecko	Άκρως Απόρρητο Zkratka: ΑΑΠ	Απόρρητο Zkratka: (ΑΠ)	Εμπιστευτικό Zkratka: (ΕΜ)	Περιορισμένης Χρήσης Zkratka: (ΠΧ)
Španělsko	Secreto	Reservado	Confidencial	Difusión Limitada
Francie	Très Secret Défense	Secret Défense	Confidentiel Défense	poznámka [3] níže
Chorvatsko	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Itálie	Segretissimo	Segreto	Riservatissimo	Riservato
Kypr	Άκρως Απόρρητο Zkratka: (ΑΑΠ)	Απόρρητο Zkratka: (ΑΠ)	Εμπιστευτικό Zkratka: (ΕΜ)	Περιορισμένης Χρήσης Zkratka: (ΠΧ)
Lotyšsko	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Lucembursko	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Maďarsko	„Szigorúan titkos!“	„Titkos!“	„Bizalmas!“	„Korlátozott terjesztésű!“
Malta	L-Oghla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nizozemsko	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Rakousko	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polsko	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalsko	Muito Secreto	Secreto	Confidencial	Reservado

EU	TRES 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
Finsko	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 království	UK TOP SECRET	UK SECRET	Neexistuje ekvivalent ([5])	UK OFFICIAL – SENSITIVE

([1]) Diffusion Restreinte/Beperkte Verspreiding není v Belgii stupněm utajení. S informacemi se stupněm utajení „RESTREINT UE/EU RESTRICTED" Belgie nakládá a chrání je způsobem, který není méně přísný než standardy a postupy uvedené v bezpečnostních pravidlech Rady Evropské unie.

([2]) Německo: VS = Verschlusssache.

([3]) Francie ve svém vnitrostátním systému nepoužívá stupeň utajení „RESTREINT". S informacemi se stupněm utajení „RESTREINT UE/EU RESTRICTED" Francie nakládá a chrání je způsobem, který není méně přísný než standardy a postupy uvedené v bezpečnostních pravidlech Rady Evropské unie.

([4]) Švédsko: označení stupňů utajení uvedená v horní řadě jsou používána orgány v oblasti obrany a označení v dolní řadě jinými orgány.

([5]) S informacemi se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL Spojené království nakládá a chrání je způsobem, který je v souladu s ochrannými bezpečnostními požadavky pro stupeň utajení UK SECRET.

PŘÍLOHA II

SEZNAM ANGLICKÝCH ZKRATEK

Zkratka	Význam
CA	orgán pro šifrování
CAA	schvalovací orgán pro kryptografickou ochranu
CCTV	uzavřený televizní okruh
CDA	orgán pro distribuci kryptografických materiálů
CIS	komunikační a informační systémy, v nichž se nakládá s utajovanými informacemi EU
DSA	určený bezpečnostní orgán
EUCI	utajované informace EU
FSC	bezpečnostní prověrka zařízení
IA	zabezpečení informací
IAA	orgán pro zabezpečení informací
IDS	systém detekce narušení
IT	informační technologie
LSO	místní bezpečnostní úředník
NSA	vnitrostátní bezpečnostní orgán
PSC	bezpečnostní prověrka personálu
PSCC	potvrzení o bezpečnostní prověrce personálu
PSI	bezpečnostní pokyny k programu/projektu
RCO	vedoucí registru
SAA	orgán pro bezpečnostní akreditaci
SAL	seznam bezpečnostních požadavků
SCG	příručka pro stanovování stupňů utajení
SecOPs	bezpečnostní provozní postupy
TA	orgán TEMPEST
SFEU	Smlouva o fungování Evropské unie

PŘÍLOHA III

SEZNAM VNITROSTÁTNÍCH BEZPEČNOSTNÍCH ORGÁNŮ

BELGIE

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

BULHARSKO

State Commission on Information Security
90 Cherkovna S.
1505 Sofia
Tel. +359 29333600
Fax +359 29873750
E-mail: dksi@government.bg
Internetové stránky: www.dksi.bg

ČESKÁ REPUBLIKA

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tel. +420 257283335
Fax +420 257283110
E-mail: czech.nsa@nbu.cz
Internetové stránky: www.nbu.cz

DÁNSKO

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg
Tel. +45 33148888
Fax +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø
Tel. +45 33325566
Fax +45 33931320

NĚMECKO

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

ESTONSKO

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

ŘECKO

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
Tel. +30 2106572045
+ 30 2106572009
Fax +30 2106536279, +30 2106577612

ŠPANĚLSKO

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

FRANCIE

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
Tel. +33 171758177
Fax + 33 171758200

CHORVATSKO

Office of the National Security Council
Croatian NSA
Jurjevska 34
10000 Zagreb
Croatia
Tel. +385 14681222
Fax + 385 14686049
Internetové stránky: www.uvns.hr

IRSKO

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

ITÁLIE

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

KYPR

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
Tel. +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
Tel. +371 67025418
Fax +371 67025454
E-mail: ndi@sab.gov.lv

LITVA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania National Security Authority)
Gedimino 40/1
LT-01110 Vilnius
Tel. +370 70666701, +370 70666702
Fax +370 70666700
E-mail: nsa@vsd.lt

LUCEMBURSKO

Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg
Tel. +352 24782210 ústředna
+ 352 24782253 přímá linka
Fax +352 24782243

MAĎARSKO

Nemzeti Biztonsági Felügyelet
(National Security Authority of Hungary)
H-1024 Budapest, Szilágyi Erzsébet fasor 11/B
Tel. +36 17952303
Fax +36 17950344

Poštovní adresa:
H-1357 Budapest, PO Box 2
E-mail: nbf@nbf.hu
Internetové stránky: www.nbf.hu

MALTA

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

NIZOZEMSKO

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

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag
Tel. +31 703187060
Fax +31 703187522

RAKOUSKO

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

POLSKO

Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
2 A Rakowiecka St.
00-993 Warszawa
Tel. +48 225857944
Fax +48 225857443
E-mail: nsa@abw.gov.pl
Internetové stránky: www.abw.gov.pl

PORTUGALSKO

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

RUMUNSKO

Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest
Tel. +40 212245830
Fax +40 212240714
E-mail: nsa.romania@nsa.ro
Internetové stránky: www.orniss.ro

SLOVINSKO

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

SLOVENSKO

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Tel. +421 268692314
Fax +421 263824005
Internetové stránky: www.nbusr.sk

FINSKO

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

ŠVÉDSKO

Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
S-103 39 Stockholm
Tel. +46 84051000
Fax +46 87231176
E-mail: ud-nsa@foreign.ministry.se

UNITED KINGDOM

UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1 A 2AS
Tel. č. 1: +44 2072765649
Tel. č. 2: +44 2072765497
Fax +44 2072765651
E-mail: UK-NSA@cabinet-office.x.gsi.gov.uk