II

(Nelegislativní akty)

ROZHODNUTÍ

ROZHODNUTÍ RADY

ze dne 31. března 2011

o bezpečnostních pravidlech na ochranu utajovaných informací EU

(2011/292/EU)

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na čl. 240 odst. 3 této smlouvy,

s ohledem na rozhodnutí Rady 2009/937/EU ze dne 1. prosince 2009, kterým se přijímá její jednací řád [1], a zejména na článek 24 uvedeného rozhodnutí,

vzhledem k těmto důvodům:

(1) Aby bylo možno rozvíjet aktivity Rady ve všech oblastech, které vyžadují nakládání s utajovanými informacemi, je vhodné zavést komplexní bezpečnostní systém ochrany utajovaných informací vztahující se na Radu, její generální sekretariát a členské státy.

(2) Toto rozhodnutí by se mělo uplatňovat v případech, kdy Rada, její přípravné orgány a generální sekretariát Rady nakládají s utajovanými informacemi EU.

(3) V souladu s vnitrostátními právními předpisy a v míře nezbytné pro fungování Rady by členské státy měly dodržovat toto rozhodnutí v případech, kdy jejich příslušné orgány, pracovníci nebo dodavatelé nakládají s utajovanými informacemi EU, aby měl každý jistotu, že utajovaným informacím EU je poskytována rovnocenná úroveň ochrany.

(4) Rada a Komise se zavázaly k uplatňování rovnocenných bezpečnostních standardů pro ochranu utajovaných informací EU.

(5) Rada zdůrazňuje, že je důležité, aby se Evropský parlament a další orgány, agentury, instituce nebo úřady EU případně připojily k uplatňování zásad, standardů a pravidel pro ochranu utajovaných informací, které jsou nezbytné pro ochranu zájmů Unie a jejích členských států.

(6) Základní zásady a minimální standardy stanovené tímto rozhodnutím pro ochranu utajovaných informací EU uplatňují v rámci své vnitřní organizace agentury a subjekty EU zřízené podle hlavy V kapitoly 2 Smlouvy o Evropské unii, Europol a Eurojust podle ustanovení svých příslušných zřizovacích aktů.

(7) Bezpečnostní pravidla na ochranu utajovaných informací EU přijatá Radou jsou uplatňována v rámci operací pro řešení krizí zřízených podle hlavy V kapitoly 2 Smlouvy o Evropské unii a jejich pracovníky.

(8) Bezpečnostní pravidla na ochranu utajovaných informací EU přijatá Radou uplatňují zvláštní zástupci EU a členové jejich týmů.

(9) Tímto rozhodnutím nejsou dotčeny články 15 a 16 Smlouvy o fungování Evropské unie a jejich prováděcí akty.

(10) Tímto rozhodnutím nejsou dotčeny platné postupy členských států v oblasti informování jejich národních parlamentů o činnostech Unie,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Účel, oblast působnosti a definice

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

[1] Úř. věst. L 325, 11.12.2009, s. 35.

2. Tyto základní zásady a minimální standardy jsou použitelné pro Radu a generální sekretariát Rady a dodržují je členské státy v souladu se svými vnitrostátními právními předpisy tak, aby měl každý jistotu, že utajovaným informacím EU je poskytována rovnocenná úroveň ochrany.

3. Pro účely tohoto rozhodnutí se použijí definice uvedené v dodatku A.

Článek 2

Definice utajovaných informací EU, stupně utajení a označení

1. „Utajovanými informacemi EU" se rozumějí 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) TRÈS SECRET UE / EU TOP SECRET: informace a materiály, jejichž neoprávněné vyzrazení by mohlo vést k mimořádně závažnému poškození podstatných 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 uvádějící oblast činnosti, k níž se vztahují, identifikující původce, omezující distribuci či použití nebo uvádějící informace o způsobilosti k předání.

Článek 3

Pravidla stanovování stupňů utajení

1. Příslušné orgány zajistí odpovídající utajení utajovaných informací EU, jejich jasné označení jako utajované informace a zachování stupně utajení pouze po nezbytnou dobu.

2. Bez předchozího písemného souhlasu původce nelze snížit ani zrušit stupeň utajení utajovaných informací EU a ani nelze změnit či zrušit žádné z označení uvedených v čl. 2 odst. 3.

3. Rada schválí bezpečnostní politiku pro vytváření utajovaných informací EU, která zahrnuje praktickou příručku pro stanovování stupňů utajení.

Článek 4

Ochrana utajovaných informací

1. Ochrana utajovaných informací EU se řídí tímto rozhodnutím.

2. Držitel jakékoli utajované informace EU je odpovědný za její ochranu v souladu s tímto rozhodnutím.

3. Pokud členské státy poskytnou v rámci struktur či sítí Evropské unie utajované informace označené vnitrostátním stupněm utajení, Rada a generální sekretariát Rady tyto informace chrání v souladu s požadavky na ochranu utajovaných informací EU na odpovídající úrovni podle srovnávací tabulky stupňů utajení uvedené v dodatku B.

4. Velké množství či kompilace utajovaných informací EU mohou být důvodem pro úroveň ochrany odpovídající vyššímu stupni utajení.

Článek 5

Řízení bezpečnostních rizik

1. Bezpečnostní rizika související s utajovanými informacemi EU jsou řízena jako proces. Tento proces je zaměřen 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 podle dodatku A. Účinnost těchto opatření se průběžně vyhodnocuje.

2. 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 uloženy, a na místě vyhodnocené hrozby škodlivých nebo TRÈStných činností, včetně vyzvědačství, sabotáže nebo terorismu.

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

4. Plány zajištění kontinuity provozu zahrnují preventivní a nápravná opatření, která minimalizují dopad velkých selhání nebo incidentů na nakládání s utajovanými informacemi EU a na ukládání těchto informací.

Článek 6

Provádění tohoto rozhodnutí

1. V případě potřeby Rada na doporučení Bezpečnostního výboru schválí bezpečností politiky, kterými se stanoví prováděcí opatření k tomuto rozhodnutí.

2. Bezpečnostní výbor může na své úrovni schválit bezpečnostní pokyny, které doplní nebo podpoří toto rozhodnutí a veškeré bezpečnostní politiky schválené Radou.

Článek 7

Personální bezpečnost

1. Personální bezpečností se rozumí uplatňování opatření, jež zajistí, že přístup k utajovaným informacím EU je umožněn pouze osobám, které:

— potřebují znát utajované informace,

— jsou případně bezpečnostně prověřeny pro odpovídající stupeň utajení a

— byly poučeny o svých povinnostech.

2. Bezpečnostní prověrka slouží k tomu, aby určila, zda může být určitá osoba s přihlédnutím ke své loajalitě, důvěryhodnosti a spolehlivosti oprávněna k přístupu k utajovaným informacím EU.

3. Všechny osoby v generálním sekretariátu Rady, jejichž povinnosti mohou vyžadovat, aby měly přístup k utajovaným informacím EU se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším, musí být před umožněním přístupu k takovým utajovaným informacím EU bezpečnostně prověřeny pro odpovídající stupeň utajení. Bezpečnostní prověrka pro úředníky a ostatní zaměstnance generálního sekretariátu Rady je upravena v příloze I.

4. Pracovníci členských států uvedení v čl. 14 odst. 3, jejichž povinnosti mohou vyžadovat přístup k utajovaným informacím EU se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším, musí být před umožněním přístupu k takovým utajovaným informacím EU bezpečnostně prověřeni pro odpovídající stupeň utajení nebo musí být jinak řádně oprávněni z titulu své funkce v souladu s vnitrostátními právními předpisy.

5. Všechny osoby musí být před tím, než jim bude umožněn přístupu k utajovaným informacím EU, a poté v pravidelných intervalech poučeny o svých povinnostech souvisejících s ochranou utajovaných informací EU v souladu s tímto rozhodnutím; uvedené osoby tuto skutečnost potvrdí.

6. Prováděcí pravidla k tomuto článku jsou stanovena v příloze I.

Článek 8

Fyzická bezpečnost

1. Fyzickou bezpečností se rozumí uplatňování fyzických a technických ochranných opatření s cílem předejít neoprávněnému přístupu k utajovaným informacím EU.

2. Opatření fyzické bezpečnosti mají znemožnit neoprávněný nebo násilný vstup útočníka, 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.

3. Opatření fyzické bezpečnosti je třeba zavést pro všechny areály, budovy, kanceláře, místnosti a další prostory, v nichž se nakládá s utajovanými informacemi EU nebo v nichž jsou takové informace ukládány, včetně prostor, v nichž jsou umístěny komunikační a informační systémy podle čl. 10 odst. 2.

4. Prostory, v nichž jsou ukládány utajované informace EU se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším, je třeba zřídit jako zabezpečené oblasti v souladu s přílohou II a musí je schválit příslušný bezpečnostní orgán.

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

6. Prováděcí pravidla k tomuto článku jsou stanovena v příloze II.

Článek 9

Správa utajovaných informací

1. Správou utajovaných informací se rozumí uplatňování administrativních opatření, která slouží ke kontrole utajovaných informací EU během celého jejich životního cyklu a doplňují opatření stanovená v článcích 7, 8 a 10, a pomáhají tak zabránit úmyslnému či neúmyslnému ohrožení či ztrátě takových informací, zjistit takové ohrožení nebo ztrátu informací a následně zajistit nápravu. Tato opatření se týkají zejména vytváření, evidence, kopírování, překladů, přenášení a ničení utajovaných informací EU.

2. Informace stupně utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyššího je třeba po jejich obdržení a před jejich distribucí z bezpečnostních důvodů zaevidovat. Příslušné orgány generálního sekretariátu Rady a členských států zřídí za tímto účelem systém registrů. Informace se stupněm utajení TRÈS SECRET UE / EU TOP SECRET musí být zaevidovány v určených registrech.

3. Útvary a prostory, v nichž se nakládá s utajovanými informacemi EU nebo v nichž jsou takové informace ukládány, podléhají pravidelné inspekci prováděné příslušným bezpečnostním orgánem.

4. 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 čl. 10 odst. 6;

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 čl. 10 odst. 6, nebo

ii) ve všech ostatních případech podle pokynů stanovených příslušným bezpečnostním orgánem v souladu s příslušnými ochrannými opatřeními stanovenými v příloze III.

5. Prováděcí pravidla k tomuto článku jsou stanovena v příloze III.

Článek 10

Ochrana utajovaných informací EU, s nimiž se nakládá v komunikačních a informačních systémech

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. Účinné zabezpečení informací zajišťuje příslušnou míru důvěrnosti, integrity, dostupnosti, nepopiratelnosti a autenticity informací. Zabezpečení informací je založeno na procesu řízení rizik.

2. 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. Toto rozhodnutí se použije na komunikační a informační systémy, v nichž se nakládá s utajovanými informacemi EU.

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

4. Veškeré komunikační a informační systémy podléhají akreditačnímu řízení. Cílem akreditace je získat jistotu, že byla provedena veškerá vhodná bezpečnostní opatření a že byla dosažena dostatečná úroveň ochrany utajovaných informací EU a komunikačních a informačních systémů v souladu s tímto rozhodnutím. Rozhodnutí o akreditaci stanoví nejvyšší stupeň utajení informací, s nimiž lze v daném systému nakládat, a příslušné podmínky.

5. Komunikační a informační systémy nakládající s informacemi se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším jsou chráněny takovým způsobem, aby informace nemohly být ohroženy kompromitujícím elektromagnetickým vyzařováním („bezpečnostní opatření TEMPEST“).

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

a) Důvěrnost informací se stupněm utajení SECRET UE / EU SECRET a vyšším je chráněna kryptografickými prostředky schválenými Radou jakožto schvalovacím orgánem pro kryptografickou ochranu na základě doporučení Bezpečnostního výboru.

b) Důvěrnost informací se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo RESTREINT UE / EU RESTRICTED je chráněna kryptografickými prostředky schválenými generálním tajemníkem Rady jakožto schvalovacím orgánem pro kryptografickou ochranu na základě doporučení Bezpečnostního výboru.

Bez ohledu na písmeno b) může být důvěrnost utajovaných informací EU se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo RESTREINT UE / EU RESTRICTED v rámci vnitrostátních systémů členských států chráněna kryptografickými prostředky schválenými schvalovacím orgánem pro kryptografickou ochranu daného členského státu.

7. Během elektronického přenosu utajovaných informací EU se použijí schválené kryptografické prostředky. Bez ohledu na tento požadavek se za mimořádných okolností nebo v případě zvláštních technických konfigurací mohou použít zvláštní postupy, jak je uvedeno v příloze IV.

8. Příslušné orgány generálního sekretariátu Rady a členských států zřídí v souvislosti se zabezpečením informací tyto orgány:

a) orgán pro zabezpečení informací;

b) orgán TEMPEST;

c) schvalovací orgán pro kryptografickou ochranu;

d) orgán pro distribuci kryptografických materiálů.

9. Příslušné orgány generálního sekretariátu Rady a členských států zřídí pro každý systém:

a) orgán pro bezpečnostní akreditaci;

b) provozní orgán pro zabezpečení informací.

10. Prováděcí pravidla k tomuto článku jsou stanovena v příloze IV.

Článek 11

Průmyslová bezpečnost

1. Průmyslovou bezpečností se rozumí uplatňování opatření k zajištění ochrany utajovaných informací EU ze strany dodavatelů nebo subdodavatelů během jednání před uzavřením utajovaných smluv a během celého životního cyklu utajovaných smluv. Tyto smlouvy nesmí umožnit přístup k informacím se stupněm utajení TRÈS SECRET UE / EU TOP SECRET.

2. Generální sekretariát Rady může na základě smlouvy pověřit plněním úkolů, které zahrnují nebo vyžadují přístup k utajovaným informacím EU nebo nakládání s nimi či jejich ukládání, průmyslové nebo jiné subjekty registrované v členském státě nebo ve třetím státě, který uzavřel dohodu nebo správní ujednání podle čl. 12 odst. 2 písm. a) nebo b).

3. Generální sekretariát Rady jakožto zadavatel zajistí, aby při zadávání zakázek na základě utajovaných smluv průmyslovým nebo jiným subjektům byly dodržovány minimální standardy průmyslové bezpečnosti, které jsou stanoveny tímto rozhodnutím a na něž dotyčná smlouva odkazuje.

4. Vnitrostátní bezpečnostní orgán, určený bezpečnostní orgán nebo kterýkoli jiný příslušný orgán každého členského státu zajistí v rozsahu daném vnitrostátními právními předpisy, aby dodavatelé a subdodavatelé registrovaní na jejich území přijali všechna vhodná opatření na ochranu utajovaných informací EU během jednání před uzavřením smluv a při plnění utajované smlouvy.

5. Vnitrostátní bezpečnostní orgán, určený bezpečnostní orgán nebo kterýkoli jiný příslušný bezpečnostní orgán každého členského státu zajistí v souladu s vnitrostátními právními předpisy, aby dodavatelé a subdodavatelé registrovaní v daném členském státě a účastnící se zakázek na základě utajovaných smluv nebo utajovaných subdodavatelských smluv, které vyžadují přístup k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo SECRET UE / EU SECRET v jejich prostorách, buď při plnění takových smluv, nebo před jejich uzavřením, byli držiteli osvědčení o bezpečnostní prověrce zařízení pro požadovaný stupeň utajení.

6. Pracovníkům dodavatele či subdodavatele, kteří pro plnění utajované smlouvy potřebují přístup k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo SECRET UE / EU SECRET, vydá příslušný vnitrostátní bezpečnostní orgán, určený bezpečnostní orgán nebo kterýkoli jiný příslušný bezpečnostní orgán osvědčení o bezpečnostní prověrce personálu v souladu s vnitrostátními právními předpisy a s minimálními standardy stanovenými v příloze I.

7. Prováděcí pravidla k tomuto článku jsou stanovena v příloze V.

Článek 12

Výměna utajovaných informací se třetími státy a mezinárodními organizacemi

1. Pokud Rada určí, že je třeba přistoupit k výměně utajovaných informací EU s některým třetím státem nebo mezinárodní organizací, vytvoří se za tím účelem příslušný rámec.

2. S cílem vytvořit tento rámec a stanovit vzájemně uplatňovaná pravidla pro ochranu vyměňovaných utajovaných informací:

a) Rada uzavře dohody o bezpečnostních postupech pro výměnu a ochranu utajovaných informací (dále jen „dohody o bezpečnosti informací“) nebo

b) generální tajemník Rady může uzavřít správní ujednání v souladu s bodem 17 přílohy VI, pokud stupeň utajení poskytovaných utajovaných informací EU není zpravidla vyšší než RESTREINT UE / EU RESTRICTED.

3. Dohody o bezpečnosti informací nebo správní ujednání podle odstavce 2 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 nejsou méně přísné než minimální standardy stanovené tímto rozhodnutím.

4. Rozhodnutí o poskytnutí utajovaných informací EU, jejichž původcem je Rada, třetímu státu nebo mezinárodní organizaci přijímá Rada případ od případu s ohledem na povahu a obsah těchto informací, na potřebu příjemce znát utajované informace a na míru prospěchu pro EU. Není-li Rada původcem utajovaných informací, které mají být poskytnuty, generální sekretariát Rady nejdříve získá pro poskytnutí informací písemný souhlas původce. Nelze-li původce zjistit, převezme jeho odpovědnost Rada.

5. Za účelem zhodnocení účinnosti zavedených bezpečnostních opatření ve třetím státě nebo mezinárodní organizaci zajišťujících ochranu poskytovaných nebo vyměňovaných utajovaných informací EU se vykonají hodnotící návštěvy.

6. Prováděcí pravidla k tomuto článku jsou stanovena v příloze VI.

Článek 13

Narušení bezpečnosti a ohrožení utajovaných informací EU

1. K narušení bezpečnosti dochází v důsledku jednání nebo opomenutí určité osoby v rozporu s bezpečnostními pravidly stanovenými tímto rozhodnutím.

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 příslušnému bezpečnostnímu orgánu.

4. Je-li známo nebo existují-li oprávněné důvody domnívat se, že došlo k ohrožení či ztrátě utajovaných informací EU, přijme příslušný bezpečnostní orgán v souladu s příslušnými právními předpisy veškerá vhodná opatření s cílem:

a) informovat původce;

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

c) posoudit možnou škodu z hlediska zájmů EU a členských států;

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

e) oznámit přijatá opatření příslušným orgánům.

5. Vůči kterékoli osobě, která je odpovědná za porušení bezpečnostních pravidel stanovených tímto rozhodnutím, mohou být přijata disciplinární opatření v souladu s příslušnými pravidly a předpisy. 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.

Článek 14

Odpovědnost za provádění

1. Rada přijme veškerá nezbytná opatření, aby zajistila jednotné uplatňování tohoto rozhodnutí.

2. Generální tajemník Rady přijme veškerá nezbytná opatření, aby zajistil, že při nakládání s utajovanými informacemi EU nebo s jinými utajovanými informacemi nebo při jejich ukládání budou v prostorách využívaných Radou a v generálním sekretariátu Rady uplatňováno toto rozhodnutí, včetně styčných úřadů ve třetích státech a ze strany úředníků a ostatních zaměstnanců generálního sekretariátu Rady, pracovníků vyslaných ke generálnímu sekretariátu Rady a dodavatelů generálního sekretariátu Rady.

3. Členské státy přijmou v souladu se svými vnitrostátními právními předpisy veškerá vhodná opatření, aby zajistily, že při nakládání s utajovanými informacemi EU nebo při jejich ukládání bude toto rozhodnutí dodržováno:

a) pracovníky stálých zastoupení členských států při Evropské unii a členů jejich delegací, kteří se účastní zasedání Rady či jejích přípravných orgánů nebo jiných činností Rady;

b) jinými pracovníky správních orgánů členských států, včetně pracovníků vyslaných k těmto orgánům, bez ohledu na to, zda působí na území členských států nebo v zahraničí;

c) jinými osobami v členských státech, které jsou k přístupu k utajovaným informacím EU řádně oprávněny z titulu své funkce, a

d) dodavateli členských států, ať již působí na území členských států nebo v zahraničí.

Článek 15

Organizace bezpečnosti v rámci Rady

1. V rámci své úlohy při zajišťování jednotného uplatňování tohoto rozhodnutí Rada schválí:

a) dohody uvedené v čl. 12 odst. 2 písm. a);

b) rozhodnutí opravňující k poskytování utajovaných informací EU třetím státům a mezinárodním organizacím;

c) roční program inspekcí navržený generálním tajemníkem Rady a doporučený Bezpečnostním výborem pro inspekce orgánů a prostor členských států a agentur a subjektů EU zřízených podle hlavy V kapitoly 2 Smlouvy o Evropské unii, Europolu a Eurojustu, jakož i hodnotící návštěvy třetích států a mezinárodních organizací za účelem ověření účinnosti opatření zavedených na ochranu utajovaných informací EU a

d) bezpečnostní politiky podle čl. 6 odst. 1.

2. Bezpečnostním orgánem generálního sekretariátu Rady je generální tajemník Rady. Generální tajemník Rady v této funkci:

a) provádí bezpečnostní politiku Rady a její přezkum;

b) koordinuje s vnitrostátními bezpečnostními orgány členských států veškeré bezpečnostní otázky týkající se ochrany utajovaných informací souvisejících s činností Rady;

c) před umožněním přístupu k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším úředníkům a ostatním zaměstnancům generálního sekretariátu Rady vydává v souladu s čl. 7 odst. 3 těmto úředníkům a zaměstnancům osvědčení o bezpečnostní prověrce personálu EU;

d) podle potřeby nařizuje vyšetřování jakéhokoli faktického nebo možného ohrožení či ztráty utajovaných informací, jejichž držitelem nebo původcem je Rada, nebo v případě podezření z ohrožení či ztráty takových informací a žádá příslušné bezpečnostní orgány o spolupráci při tomto vyšetřování;

e) provádí pravidelné kontroly bezpečnostních opatření na ochranu utajovaných informací v prostorách generálního sekretariátu Rady;

f) provádí pravidelné kontroly bezpečnostních opatření na ochranu utajovaných informací EU v agenturách a subjektech EU zřízených podle hlavy V kapitoly 2 Smlouvy o Evropské unii, Europolu a Eurojustu, jakož i v rámci operací pro řešení krizí zřízených podle hlavy V kapitoly 2 Smlouvy o EU a ze strany zvláštních zástupců EU a členů jejich týmů;

g) ve spolupráci s příslušným vnitrostátním bezpečnostním orgánem a po dohodě s ním provádí pravidelné kontroly bezpečnostních opatření na ochranu utajovaných informací EU v orgánech a prostorách členských států;

h) koordinuje bezpečnostní opatření s příslušnými orgány členských států, které odpovídají za ochranu utajovaných informací, a případně se třetími státy nebo mezinárodními organizacemi, mimo jiné s ohledem na povahu ohrožení bezpečnosti utajovaných informací EU a způsoby ochrany před tímto ohrožením;

i) uzavírá správní ujednání podle čl. 12 odst. 2 písm. b) a

j) provádí úvodní a pravidelné hodnotící návštěvy třetích států a mezinárodních organizací za účelem ověření účinnosti opatření zavedených na ochranu utajovaných informací EU, jež jim jsou poskytovány nebo jež jsou s nimi vyměňovány.

Při plnění těchto povinností je generálnímu tajemníkovi Rady nápomocna bezpečnostní kancelář generálního sekretariátu Rady.

3. Pro účely provádění čl. 14 odst. 3 by členské státy měly:

a) určit vnitrostátní bezpečnostní orgán odpovědný za bezpečnostní opatření na ochranu utajovaných informací EU, aby:

i) utajované informace EU v držení kteréhokoli vnitrostátního orgánu, veřejnoprávního či soukromoprávního, subjektu nebo agentury, na domácí půdě či v zahraničí, byly chráněny v souladu s tímto rozhodnutím,

ii) bezpečnostní opatření na ochranu utajovaných informací EU byla pravidelně kontrolována,

iii) všechny osoby, které jsou zaměstnány ve správních orgánech daného členského státu nebo dodavatelem a kterým může být umožněn přístup k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším, byly bezpečnostně prověřeny nebo jinak řádně oprávněny z titulu své funkce v souladu s vnitrostátními právními předpisy,

iv) byly podle potřeby zavedeny bezpečnostní programy, aby se minimalizovalo riziko, že utajované informace EU budou ohroženy či ztraceny,

v) bezpečnostní otázky týkající se ochrany utajovaných informací EU byly koordinovány s ostatními příslušnými bezpečnostními orgány, včetně orgánů uvedených v tomto rozhodnutí a

vi) byly vyřízeny příslušné žádosti o provedení bezpečnostní prověrky podané ze strany agentur a subjektů EU zřízených podle hlavy V kapitoly 2 Smlouvy o Evropské unii, Europolu a Eurojustu, jakož i ze strany operací pro řešení krizí zřízených podle hlavy V kapitoly 2 Smlouvy o EU nebo zvláštních zástupců EU a členů jejich týmů;

Seznam vnitrostátních bezpečnostních orgánů je uveden v dodatku C.

b) zajistit, aby příslušné orgány poskytovaly informace a poradenství svým vládám a jejich prostřednictvím Radě o povaze ohrožení bezpečnosti utajovaných informací EU a o způsobech ochrany před tímto ohrožením.

Článek 16

Bezpečnostní výbor

1. Zřizuje se Bezpečnostní výbor. Tento výbor přezkoumává a posuzuje veškeré bezpečnostní otázky v oblasti působnosti tohoto rozhodnutí a podle potřeby poskytuje doporučení Radě.

2. Bezpečnostní výbor se skládá ze zástupců vnitrostátních bezpečnostních orgánů členských států a jeho zasedání se účastní zástupce Komise a Evropské služby pro vnější činnost. Předsedá mu generální tajemník Rady nebo osoba pověřená jej zastupovat. Bezpečností výbor se schází podle pokynů Rady nebo na žádost generálního tajemníka Rady či některého vnitrostátního bezpečnostního orgánu.

Zástupci agentur a subjektů EU zřízených podle hlavy V kapitoly 2 Smlouvy o Evropské unii, jakož i Europolu a Eurojustu, mohou být přizváni k účasti na zasedání, jestliže se jich týkají projednávané otázky.

3. Bezpečnostní výbor organizuje svou činnost tak, aby mohl poskytovat doporučení týkající se určitých oblastí bezpečnosti. Zřídí odbornou podskupinu pro otázky zabezpečení informací a podle potřeby další odborné podskupiny. Pro tyto odborné podskupiny vypracuje statut a ty mu následně předkládají zprávy o své činnosti, případně doporučení určená Radě.

Článek 17

Nahrazení předchozích rozhodnutí

1. Toto rozhodnutí zrušuje a nahrazuje rozhodnutí 2001/264/ES ze dne 19. března 2001, kterým se přijímají bezpečnostní předpisy Rady ([1]).

2. Veškeré utajované informace EU podle rozhodnutí Rady 2001/264/ES jsou nadále chráněny v souladu s příslušnými ustanoveními tohoto rozhodnutí.

Článek 18

Vstup v platnost

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

V Bruselu dne 31. března 2011.

Za Radu
předseda
VÖLNER P.

([1]) Úř. věst. L 101, 11.4.2001, s. 1.

PŘÍLOHY

PŘÍLOHA I

Personální bezpečnost

PŘÍLOHA II

Fyzická bezpečnost

PŘÍLOHA III

Správa utajovaných informací

PŘÍLOHA IV

Ochrana utajovaných informací EU, s nimiž se nakládá v komunikačních a informačních systémech

PŘÍLOHA V

Průmyslová bezpečnost

PŘÍLOHA VI

Výměna utajovaných informací se třetími státy a mezinárodními organizacemi

PŘÍLOHA I

PERSONÁLNÍ BEZPEČNOST

I. ÚVOD

1. Tato příloha stanoví prováděcí pravidla k článku 7. Stanoví zejména kritéria určující, zda určitá osoba může s přihlédnutím k její loajalitě, důvěryhodnosti a spolehlivosti získat oprávnění k přístupu k utajovaným informacím EU, a postupy šetření a správní postupy, jež je třeba za tímto účelem dodržovat.

2. V celé této příloze (kromě případů, kdy je rozlišení důležité) se pojmem „ osvědčením o bezpečnostní prověrce personálu" rozumí vnitrostátní osvědčení o bezpečnostní prověrce personálu nebo osvědčení o bezpečnostní prověrce personálu EU, jak jsou vymezena v dodatku A.

II. OPRÁVNĚNÍ K PŘÍSTUPU K UTAJOVANÝM INFORMACÍM EU

3. Určitou osobu lze oprávnit k přístupu k utajovaným informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším pouze v případě, že:

   a) byla zjištěna potřeba této osoby znát utajované informace;

   b) je tato osoba držitelem osvědčení o bezpečnostní prověrce personálu pro odpovídající stupeň utajení nebo je jinak řádně oprávněna z titulu své funkce v souladu s vnitrostátními právními předpisy a

   c) tato osoba byla poučena o bezpečnostních pravidlech a postupech na ochranu utajovaných informací EU a vzala na vědomí své povinnosti ohledně ochrany těchto informací.

4. Každý členský stát a generální sekretariát Rady určí ve svých strukturách pracovní místa, která vyžadují přístup k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším, a tedy i osvědčení o bezpečnostní prověrce personálu pro odpovídající stupeň utajení.

III. PODMÍNKY PRO VYDÁNÍ OSVĚDČENÍ O BEZPEČNOSTNÍ PROVĚRCE PERSONÁLU

5. Poté co vnitrostátní bezpečnostní orgány nebo jiné příslušné vnitrostátní orgány obdrží žádost se všemi náležitostmi, odpovídají za zajištění toho, že budou provedena bezpečnostní šetření týkající se státních příslušníků daného členského státu, kteří žádají o přístup k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším. Pravidla upravující toto šetření musí být v souladu s vnitrostátními právními předpisy.

6. Pokud má žádající osoba bydliště na území jiného členského státu nebo třetího státu, příslušné vnitrostátní orgány požádají o spolupráci příslušný orgán státu bydliště v souladu s vnitrostátními právními předpisy. Členské státy jsou si při provádění bezpečnostních šetření vzájemně nápomocny v souladu s vnitrostátními právními předpisy.

7. Pokud to vnitrostátní právní předpisy dovolují, mohou vnitrostátní bezpečnostní orgány nebo jiné příslušné vnitrostátní orgány provádět bezpečnostní šetření týkající se osob, které nejsou státními příslušníky daného členského státu a žádají o přístup k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším. Pravidla upravující toto šetření musí být v souladu svnitrostátními právními předpisy.

Kritéria bezpečnostního šetření

8. Loajalita, důvěryhodnost a spolehlivost určité osoby pro účely vydání osvědčení o bezpečnostní prověrce personálu pro přístup k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším se ověřuje prostřednictvím bezpečnostního šetření. Příslušný vnitrostátní orgán provede celkové hodnocení na základě zjištění tohoto bezpečnostního šetření. Žádné jednotlivé negativní zjištění nemusí být nutně důvodem k odmítnutí vydánío-svědčení o bezpečnostní prověrce personálu. Základní kritéria používaná pro tento účel by měla v rozsahu daném vnitrostátními právními předpisy zahrnovat posouzení, zda dotyčná osoba:

   a) spáchala nebo se pokusila spáchat některý s těchto činů: vyzvědačství, teroristický útok, sabotáž, vlastizrada nebo pobuřování, nebo se spikla s jinou osobou nebo napomáhala jiné osobě nebo jinou osobu naváděla ke spáchání takového činu;

   b) je nebo byla spojena s vyzvědači, teroristy, sabotéry nebo osobami důvodně podezřelými, že jimi jsou, nebo se zástupci organizací nebo cizích států, včetně cizích zpravodajských služeb, které mohou ohrožovat bezpečnost EU nebo členských států, pokud nebyla k těmto spojením oprávněna v rámci svých služebních povinností;

c) je nebo byla členem jakékoli organizace, která násilnými, podvratnými nebo jinými protiprávními způsoby usiluje mimo jiné o svržení vlády některého členského státu, o změnu ústavního pořádku některého členského státu nebo o změnu formy nebo politik jeho vlády;

d) je či byla stoupencem jakékoli organizace popsané v písmenu c) nebo je či byla úzce spojena se členy takových organizací;

e) úmyslně zatajila, zkreslila nebo zfalšovala významné informace, zejména informace bezpečnostní povahy, nebo úmyslně lhala při vyplňování bezpečnostního dotazníku personálu nebo v průběhu bezpečnostního pohovoru;

f) byla odsouzena za TRÈStný čin nebo činy;

g) je či byla závislá na alkoholu, užívá či užívala nedovolené omamné látky nebo zneužívá či zneužívala běžně dostupné omamné látky y;

h) chová se nebo se chovala způsobem, který může vyvolat riziko, že dotyčná osoba podlehne vydírání nebo nátlaku;

i) svými činy nebo projevy se ukázala být nečestnou, neloajální, nespolehlivou nebo nedůvěryhodnou;

j) vážným nebo opakovaným způsobem porušila bezpečnostní předpisy nebo se pokusila o neoprávněnou činnost ve vztahu ke komunikačním a informačním systémům či takovou činnost dokonala;

k) může být náchylná k podlehnutí nátlaku (například tím, že je státním příslušníkem jednoho nebo více států, které nejsou členskými státy EU, či prostřednictvím příbuzných nebo blízkých osob, kteří by mohli být ovlivnitelní cizími zpravodajskými službami, teroristickými skupinami nebo jinými podvratnými organizacemi nebo osobami, jejichž úmysly mohou ohrožovat bezpečnostní zájmy EU nebo členských států).

9. Podle okolností a v souladu s vnitrostátními právními předpisy mohou být při bezpečnostním šetření považovány za významné i finanční situace a zdravotní stav dotyčné osoby.

10. Podle okolností a v souladu s vnitrostátními právními předpisy mohou být při bezpečnostním šetření považovány za významné i povaha, chování a situace manžela nebo manželky, osoby žijící ve společné domácnosti nebo blízkého člena rodiny.

Požadavky na bezpečnostní šetření týkající se přístupu k utajovaným informacím EU

První vydání osvědčení o bezpečnostní prověrce personálu

11. První osvědčení o bezpečnostní prověrce personálu pro přístup k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL a SECRET UE /EU SECRET vychází z bezpečnostního šetření zahrnujícího období alespoň posledních pěti let, nebo období od dosažení věku 18 let do současnosti, podle toho, které z nich je kratší, a zahrnuje tato opatření:

a) vyplnění vnitrostátního bezpečnostního dotazníku personálu odpovídajícího stupni utajení utajovaných informací EU, k nimž může dotyčná osoba potřebovat přístup; po vyplnění se tento dotazník předá příslušnému bezpečnostnímu orgánu;

b) ověření totožnosti / občanství / státní příslušnosti – ověří se datum a místo narození dotyčné osoby a její totožnost. Prokáže se minulé i současné občanství nebo státní příslušnost dotyčné osoby; to zahrnuje vyhodnocení rizika podlehnutí nátlaku ze zahraničí, například v souvislosti s dřívějším pobytem nebo s kontakty v minulosti; a

c) kontrolu celostátních a místních rejstříků – prověří se celostátní bezpečnostní a ústřední TRÈStní rejstříky, pokud existují, nebo jiné srovnatelné vládní a policejní rejstříky. Prověří se záznamy donucovacích orgánů místně příslušných tam, kde měla dotyčná osoba bydliště nebo kde byla zaměstnána.

12. První osvědčení o bezpečnostní prověrce personálu pro přístup k informacím se stupněm utajení TRÈS SECRET UE / EU TOP SECRET vychází z bezpečnostního šetření zahrnujícího období alespoň posledních deseti let, nebo období od dosažení věku 18 let do současnosti, podle toho, které z nich je kratší. Provádějí-li se pohovory podle písmene e), zahrnuje šetření období alespoň posledních sedmi let, nebo období od dosažení věku 18 let do současnosti, podle toho, které z nich je kratší. Kromě kritérií uvedených v bodě 8 jsou před vydáním bezpečnostní prověrky personálu pro stupeň utajení TRÈS SECRET UE / EU TOP SECRET v rozsahu daném vnitrostátními právními předpisy prošetřovány níže uvedené skutečnosti; mohou být rovněž prošetřovány před vydáním osvědčení o bezpečnostní prověrce personálu pro stupeň utajení CONFIDENTIEL UE / EU CONFIDENTIAL a SECRET UE / EU SECRET, pokud to vnitrostátní právní předpisy vyžadují:

a) finanční situace – zjišťují se informace o finanční situaci dotyčné osoby za účelem posouzení rizika podlehnutí nátlaku ze zahraničí či domova z důvodu závažných finančních potíží nebo za účelem odhalení nevysvětlených majetkových nebo finančních poměrů;

b) vzdělání – zjišťují se informace za účelem ověření vzdělání dotyčné osoby dosaženého na školách, vysokých školách a v jiných vzdělávacích zařízeních, které tato osoba navštěvovala od svých 18. narozenin nebo po dobu, kterou orgán provádějící šetření považuje za příměřenou;

c) zaměstnání – zjišťují se informace o současném a dřívějším zaměstnání s odkazem na zdroje, jako jsou záznamy o zaměstnání nebo pracovní posudky, a na zaměstnavatele či nadřízené;

d) vojenská služba – ověří se služba dotyčné osoby v ozbrojených silách, byla-li vykonávána, a forma jejího ukončení, a

e) pohovory – pohovor nebo pohovory se vedou s dotyčnou osobou v případě, že tak stanoví a dovoluje vnitrostátní právo. Pohovory se vedou rovněž s dalšími osobami, které jsou schopny poskytnout nezaujaté hodnocení dotyčné osoby, její minulosti, činností, loajality, důvěryhodnosti a spolehlivosti. Pokud vnitrostátní praxe požaduje od osoby, která je předmětem šetření, uvedení referenčních osob, uskuteční se s těmito osobami pohovory, pokud neexistují pádné důvody tak neučinit.

13. V případě potřeby a v souladu s vnitrostátními právními předpisy může být vedeno doplňující šetření s cílem propracovat veškeré významné informace, jež jsou o dotyčné osobě dostupné, a negativní informace potvrdit, nebo vyvrátit.

Obnovení platnosti osvědčení o bezpečnostní prověrce personálu

14. Po prvním vydání osvědčení o bezpečnostní prověrce personálu a za předpokladu, že dotyčná osoba vykonávala nepřetržitou službu ve vnitrostátních správních orgánech nebo v generálním sekretariátu Rady a potřebuje i nadále mít přístup k utajovaným informacím EU, se osvědčení o bezpečnostní prověrce personálu přezkoumá za účelem obnovení jeho platnosti v intervalech, které nepřekročí dobu pěti let u osvědčení pro stupeň utajení TRÈS SECRET UE / EU TOP SECRET a dobu deseti let u osvědčení pro stupeň utajení SECRET UE / EU SECRET a CONFIDENTIEL UE / EU CONFIDENTIAL, s účinkem ode dne oznámení výsledku posledního bezpečnostního šetření, které vedlo k jeho vydání. Veškerá bezpečnostní šetření za účelem obnovení platnosti osvědčení obezpečnostní prověrce personálu zahrnují období od předchozího bezpečnostního šetření.

15. Za účelem obnovení platnosti osvědčení o bezpečnostní prověrce personálu se prošetřují skutečnosti uvedené v bodech 11 a 12.

16. Žádosti o obnovení platnosti osvědčení o bezpečnostní prověrce personálu je třeba předkládat včas a zohlednit dobu nezbytnou pro bezpečnostní šetření. Pokud však příslušný vnitrostátní bezpečnostní orgán nebo jiný příslušný vnitrostátní orgán obdrží příslušnou žádost o obnovení platnosti osvědčení o bezpečnostní prověrce personálu a odpovídající bezpečnostní dotazník personálu před skončením platnosti stávající bezpečnostní prověrky personálu a nezbytné bezpečnostní šetření zatím nebylo skončeno, může příslušný vnitrostátní orgán, pokud to dovolují vnitrostátní právní předpisy, prodloužit platnost stávajícího osvědčení o bezpečnostní prověrce personálu o období až 12 měsíců. Nedojde-li k dokončení bezpečnostního šetření do konce této dvanáctiměsíční lhůty, přidělí se dotyčné osobě úkoly, které nevyžadují bezpečnostní prověrku personálu.

Bezpečnostní prověrky personálu v generálním sekretariátu Rady

17. V případě úředníků a ostatních zaměstnanců generálního sekretariátu Rady předá bezpečnostní orgán generálního sekretariátu Rady vyplněný bezpečnostní dotazník personálu vnitrostátnímu bezpečnostnímu orgánu členského státu, jehož je dotyčná osoba státním příslušníkem, a požádá o provedení bezpečnostního šetření pro stupeň utajení utajovaných informací EU, k nimž bude dotyčná osoba potřebovat přístup.

18. Pokud generální sekretariát Rady zjistí v souvislosti s osobou, která požádala o vydání osvědčení o bezpečnostní prověrce personálu EU, informace významné pro bezpečnostní šetření, oznámí tuto skutečnost postupem podle příslušných pravidel a předpisů příslušnému vnitrostátnímu bezpečnostnímu orgánu.

19. Příslušný vnitrostátní bezpečnostní orgán informuje po skončení bezpečnostního šetření bezpečnostní orgán generálního sekretariátu Rady o výsledku šetření standardní formou stanovenou pro korespondenci Bezpečnostním výborem.

a) V případech, kdy bezpečnostní šetření dojde k závěru, že nejsou známy žádné negativní skutečnosti, které by zpochybnily loajalitu, důvěryhodnost a spolehlivost určité osoby, může orgán generálního sekretariátu Rady oprávněný ke jmenování vydat dotyčné osobě osvědčení o bezpečnostní prověrce personálu EU a oprávnit ji k přístupu k utajovaným informacím EU až do odpovídajícího stupně utajení a do konkrétně stanoveného data;

b) Pokud nelze v rámci bezpečnostního šetření dojít k závěru, že nejsou známy tyto negativní skutečnosti, orgán generálního sekretariátu Rady oprávněný ke jmenování uvědomí dotyčnou osobu, která může tento orgán požádat o slyšení. Orgán oprávněný ke jmenování může požádat příslušný vnitrostátní bezpečnostní orgán, aby v souladu s vnitrostátními právními předpisy poskytl veškerá další možná upřesnění. Je-li výsledek potvrzen, nelze osvědčení o bezpečnostní prověrce personálu EU vydat.

20. Bezpečnostní šetření spolu se získanými výsledky podléhají příslušným právním předpisům platným v daném členském státě, včetně předpisů týkajících se opravných prostředků. Rozhodnutí orgánu generálního sekretariátu Rady oprávněného ke jmenování podléhají opravným prostředkům v souladu se služebním řádem úředníků Evropské unie a pracovním řádem ostatních zaměstnanců Evropské unie stanoveným nařízením (EHS, Euratom, ESUO) č. 259/68 ([1]) (dále jen „služební a pracovní řád“).

21. Závěry, z nichž vychází dané osvědčení o bezpečnostní prověrce personálu EU, za předpokladu, že jsou i nadále platné, se vztahují na veškeré úkoly přidělené dotyčné osobě v rámci generálního sekretariátu Rady nebo Evropské komise.

22. Nenastoupí-li dotyčná osoba do služby do 12 měsíců od oznámení výsledku bezpečnostního šetření orgánu generálního sekretariátu Rady oprávněnému ke jmenování nebo dojde-li k přerušení služby dotyčné osoby v délce 12 měsíců, během nichž není tato osoba zaměstnána v generálním sekretariátu Rady nebo na pracovním místě ve vnitrostátních správních orgánech některého členského státu, oznámí se tato skutečnost příslušnému vnitrostátnímu bezpečnostnímu orgánu za účelem potvrzení, že je i nadále platná a aktuální.

23. Pokud generální sekretariát Rady zjistí informace týkající se bezpečnostního rizika, jež představuje osoba, která je držitelem platného osvědčení o bezpečnostní prověrce personálu EU, oznámí tuto skutečnost postupem podle příslušných pravidel a předpisů příslušnému vnitrostátnímu bezpečnostnímu orgánu. Pokud vnitrostátní bezpečnostní orgán informuje generální sekretariát Rady o tom, že již nejsou platné závěry podle bodu 19 písm. a) v případě osoby, která je držitelem platného osvědčení o bezpečnostní prověrce personálu EU, může orgán generálního sekretariátu Rady oprávněný ke jmenování požádat vnitrostátní bezpečnostní orgán, aby v souladu s vnitrostátními právními předpisy poskytl veškerá další možná upřesnění. Pokud se negativní skutečnosti potvrdí, zruší se osvědčení o bezpečnostní prověrce personálu EU a 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.

24. Jakékoli rozhodnutí o zrušení osvědčení obezpečnostní prověrce personálu EU v případě úředníka nebo jiného zaměstnance generálního sekretariátu Rady a případné příslušné odůvodnění se oznámí dotyčné osobě, která může požádat o slyšení orgán generálního sekretariátu Rady oprávněný ke jmenování. Informace poskytované vnitrostátním bezpečnostním orgánem podléhají příslušným právním předpisům platným v daném členském státě, včetně předpisů týkajících se opravných prostředků. Rozhodnutí orgánu generálního sekretariátu Rady oprávněného ke jmenování podléhají opravným prostředkům v souladu se služebním řádem a pracovním řádem.

25. Národní odborníci vyslaní ke generálnímu sekretariátu Rady na pracovní místa vyžadující osvědčení o bezpečnostní prověrce personálu EU předloží bezpečnostnímu orgánu generálního sekretariátu Rady před nástupem do služby platné vnitrostátní osvědčení o bezpečnostní prověrce personálu pro přístup k utajovaným informacím EU.

Záznamy o osvědčeních o bezpečnostní prověrce personálu

26. Každý členský stát vede záznamy o vnitrostátních osvědčeních o bezpečnostní prověrce personálu a generální sekretariát Rady vede záznamy o osvědčeních o bezpečnostní prověrce personálu EU, která byla vydána pro přístup k utajovaným informacím EU. Tyto záznamy obsahují informace alespoň o stupni utajení utajovaných informací EU, k nimž může být dotčené osobě umožněn přístup (stupeň utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšší) a o datu vydání a době platnosti osvědčení o bezpečnostní prověrce personálu.

27. Příslušný bezpečnostní orgán 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 vnitrostátního osvědčení o bezpečnostní prověrce personálu pro přístup k utajovaným informacím EU nebo osvědčení o bezpečnostní prověrce personálu EU a datum, do kdy je platné samotné potvrzení.

Výjimky z požadavku mít osvědčení o bezpečnostní prověrce personálu

28. Přístup k utajovaným informacím EU v členských státech ze strany osob, které jsou k tomuto přístupu řádně oprávněny z titulu své funkce, se řídí vnitrostátními právními předpisy; tyto osoby je třeba poučit o jejich bezpečnostních povinnostech ohledně ochrany utajovaných informací EU.

IV. BEZPEČNOSTNÍ VZDĚLÁVÁNÍ A POVĚDOMÍ

29. Všechny osoby, které jsou držiteli osvědčení o bezpečnostní prověrce personálu, písemně potvrdí, že chápou, jaké mají povinnosti, pokud jde o ochranu utajovaných informací EU, a jsou si vědomy důsledků v případě ohrožení utajovaných informací EU. Daný členský stát a generální sekretariát Rady vedou záznamy o těchto písemných potvrzeních.

30. Všechny osoby, které jsou oprávněny k přístupu 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 příslušné bezpečnostní orgány o jakémkoli pokusu o kontakt nebo o činnosti, které považují za podezřelé nebo neobvyklé.

31. 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.

([1]) Úř. věst. L 56, 4.3.1968, s.1.

V. VYJÍMEČNÉ OKOLNOSTI

32. Pokud to dovolují vnitrostátní právní předpisy, osvědčení o bezpečnostní prověrce personálu vydané příslušným vnitrostátním orgánem členského státu pro přístup k utajovaným informacím daného státu, může dočasně do vydání vnitrostátního osvědčení o bezpečnostní prověrce personálu pro přístup k utajovaným informacím EU umožnit státním úředníkům přístup k utajovaným informacím EU až do rovnocenné úrovně podle srovnávací tabulky uvedené v dodatku B v případech, kdy je dočasný přístup vyžadován v zájmu EU. Vnitrostátní bezpečnostní orgány informují Bezpečnostní výbor, pokud vnitrostátní právní předpisy dočasný přístup k utajovaným informacím EU nedovolují.

33. Z naléhavých důvodů, pokud to vyžadují služební zájmy a není-li skončeno bezpečnostní šetření v plném rozsahu, může orgán generálního sekretariátu Rady oprávněný ke jmenování, po konzultaci vnitrostátního bezpečnostního orgánu členského státu, jehož je daná osoba státním příslušníkem, a pod podmínkou, že předběžné šetření potvrdí, že nejsou známy žádné negativní skutečnosti, vydat dočasné oprávnění úředníkům a ostatním zaměstnancům generálního sekretariátu Rady k přístupu k utajovaným informacím EU pro konkrétní úkoly. Dočasná oprávnění jsou platná nejdéle po dobu šesti měsíců a neumožňují přístup k informacím se stupněm utajení TRÈS SECRET UE / EU TOP SECRET. Všechny osoby, kterým bylo vydáno dočasné oprávnění, písemně potvrdí, že chápou, jaké mají povinnosti, pokud jde o ochranu utajovaných informací EU, a a jsou si vědomy důsledků v případě ohrožení utajovaných informací EU. Generální sekretariát Rady vede záznamy o těchto písemných potvrzeních.

34. Má-li být určitá osoba zařazena na pracovní místo, které vyžaduje osvědčení o bezpečnostní prověrce personálu pro přístup k utajovaným informacím o jeden stupeň utajení vyšší, než je stupeň, pro nějž bylo této osobě vydáno současné osvědčení o bezpečnostní prověrce personálu, lze tuto osobu prozatímně zařadit na toto místo za těchto podmínek:

a) nadřízený dotyčné osoby písemně odůvodní naléhavou potřebu přístupu k utajovaným informacím EU s vyšším stupněm utajení;

b) přístup je omezen na konkrétní utajované informace EU nezbytné pro plnění úkolů v rámci daného pracovního místa;

c) dotyčná osoba je držitelem platného vnitrostátního osvědčení o bezpečnostní prověrce personálu nebo osvědčení o bezpečnostní prověrce personálu EU;

d) byly zahájeny kroky k získání oprávnění k přístupu k informacím se stupněm utajení, který vyžaduje dané pracovní místo;

e) příslušný orgán s uspokojivým výsledkem prověřil, že dotyčná osoba neporušila závažným nebo opakovaným způsobem bezpečnostní předpisy;

f) zařazení dotyčné osoby schválí příslušný orgán; a

g) v příslušném registru nebo podřízeném registru jsou vedeny záznamy o udělených výjimkách, včetně popisu informací, pro něž byl přístup schválen.

35. Výše uvedený postup se použije pro jednorázový přístup k utajovaným informacím EU se stupněm utajení o jeden stupeň vyšším, než je stupeň, pro který byla dotyčná osoba bezpečnostně prověřena. Tento postup nelze použít opakovaně.

36. Za velmi vyjímečných okolností,jako například během plnění úkolů v nepřátelském prostředí nebo v obdobích stoupajícího mezinárodního napětí, kdy to vyžadují mimořádná opatření, zejména pro záchranu životů, mohou členské státy a generální tajemník Rady, je-li to možné, písemně povolit přístup k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo SECRET UE / EU SECRET osobám, které nejsou držiteli potřebného osvědčení o bezpečnostní prověrce personálu, pokud je takové povolení bezpodmínečně nutné a neexistují důvodné pochybnosti o loajalitě, důvěryhodnosti a spolehlivosti dotyčné osoby. O povolení včetně popisu informací, k nimž byl přístup povolen, musí být veden záznam.

37. V případě informací se stupněm utajení TRÈS SECRET UE / EU TOP SECRET je přístup v mimořádných situacích omezen na státní příslušníky EU, jimž byl povolen přístup k informacím se stupněm utajení rovnocenným na vnitrostátní úrovni stupni utajení TRÈS SECRET UE / EU TOP SECRET nebo k informacím se stupněm utajení SECRET UE / EU SECRET.

38. O případech, kdy se použije postup stanovený v bodech 36 a 37, je informován Bezpečnostní výbor.

39. Pokud vnitrostátní právní předpisy daného členského státu stanoví přísnější pravidla ohledně dočasného oprávnění, prozatímního zařazení, jednorázového přístupu osob k utajovaným informacím nebo přístupu osob k utajovaným informacím v mimořádných situacích, použijí se postupy stanovené v tomto oddílu pouze v mezích stanovených příslušnými vnitrostátními právními předpisy.

40. Bezpečnostní výbor obdrží výroční zprávu o použití postupů uvedených v tomto oddíle.

VI. ÚČAST NA ZASEDÁNÍCH V RADĚ

41. Osoby, které se mají účastnit zasedání Rady nebo přípravných orgánů Rady, v nichž se projednávají informace se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL a vyšším, tak mohou činit pouze po potvrzení statusu svého osvědčení o bezpečnostní prověrce personálu, s výhradou bodu 28. Pokud jde o delegáty, příslušné orgány doručí bezpečnostní kanceláři generálního sekretariátu Rady potvrzení o bezpečnostní prověrce personálu nebo jiný doklad o vydání osvědčení o bezpečnostní prověrce personálu nebo jej ve vyjímečných případech předloží dotyčný delegát. Tam kde je to vhodné, lze použít společný jmenný seznam, v němž jsou uvedeny příslušné informace o osvědčeních o bezpečnostní prověrce personálu.

42. Pokud je z bezpečnostních důvodů zrušeno vnitrostátní osvědčení o bezpečnostní prověrce personálu pro přístup k utajovaným informacím EU v případě osoby, jejíž povinnosti vyžadují účast na zasedáních Rady nebo přípravných orgánů Rady, oznámí to příslušný orgán generálnímu sekretariátu Rady.

VII. POTENCIÁLNÍ PŘÍSTUP K UTAJOVANÝM INFORMACÍM EU

43. Pokud mají být zaměstnány osoby za situace, v níž by mohly mít případně přístup k informacím se stupněm utajení CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšším, musí být náležitě bezpečnostně prověřeny nebo je třeba pro ně zajistit nepřetržitě doprovod.

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

PŘÍLOHA II

FYZICKÁ BEZPEČNOST

I. ÚVOD

1. Tato příloha stanoví prováděcí pravidla k článku 8. Stanoví minimální požadavky na fyzickou ochranu areálů, budov, kanceláří, místností a dalších prostor, v nichž se nakládá s utajovanými informacemi EU a v nichž jsou takové informace ukládány, včetně prostor, v nichž jsou umístěny komunikační a informační systémy.

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

   a) zajišťují, aby s utajovanými informacemi bylo nakládáno a aby byly ukládány 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 bezpečnostní prověrky;

   c) odrazujíod neoprávněné činnosti a takové činnosti zabraňují a odhalují ji; a

   d) znemožňují nebo zpomalují nepovolený nebo násilný vstup útočníků.

II. POŽADAVKY NA FYZICKOU BEZPEČNOST A OPATŘENÍ FYZICKÉ BEZPEČNOSTI

3. Výběr opatření fyzické bezpečnosti se provede na základě hodnocení rizika ze strany příslušných orgánů. Generální sekretariát Rady a členské státy uplatňují ve svých prostorách proces řízení rizik na ochranu utajovaných informací EU, aby se poskytla přiměřená úroveň fyzické ochrany vůči vyhodnocenému riziku. V procesu řízení rizik se vezmou v úvahu veškeré důležité okolnosti, zejména:

   a) stupeň utajení utajovaných informací EU;

   b) podoba a objem dotčených 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 ukládány; a

   d) vyhodnocené hrozby ze strany zpravodajských služeb zaměřených na EU nebo na členské státy a hrozba sabotáže a teroristických, podvratných nebo jiných trestných činností.

4. Příslušný bezpečnostní orgán určí v souladu s koncepcí hloubkové ochrany vhodnou kombinaci opatření fyzické bezpečnosti, jež je třeba uplatňovat. Zahrnují jedno nebo více z těchto opatření:

   a) obvodová bariéra: fyzické ohraničení, které chrání hranici prostoru, jenž vyžaduje ochranu;

   b) systémy detekce narušení: systém detekce narušení může být používán ke zvýšení úrovně bezpečnosti, kterou poskytuje obvodová bariéra, nebo v místnostech a budovách místo bezpečnostního personálu nebo jako podpůrný prostředek bezpečnostního personálu;

   c) kontrola vstupu: kontrola vstupu se může týkat určitého areálu, budovy nebo budov v daném areálu nebo prostor či místností uvnitř budovy. Kontrola může být prováděna elektronickými či elektromechanickými prostředky bezpečnostním personálem nebo pracovníkem recepce nebo jakýmikoli jinými fyzickými prostředky;

   d) bezpečnostní personál: vyškolený a kontrolovaný bezpečnostní personál, který je podle potřeby náležitě bezpečnostně prověřen, může být využit mimo jiné s cílem odradit osoby plánující tajné vniknutí;

   e) uzavřený televizní okruh (CCTV): uzavřený televizní okruh může být používán bezpečnostním personálem za účelem ověřování incidentů a signalizace systémů detekce narušení v případě rozsáhlých areálů nebo po obvodu určitého prostoru;

   f) bezpečnostní osvětlení: bezpečnostní osvětlení může být používáno s cílem odradit případného útočníka a zajistit osvětlení potřebné pro účinnou ostrahu přímo ze strany bezpečnostního personálu nebo nepřímo prostřednictvím uzavřeného televizního okruhu a

   g) jakákoli jiná vhodná fyzická opatření, která mají zabránit neoprávněnému přístupu či takový přístup odhalit nebo předejít ztrátě či poškození utajovaných informací EU.

5. Příslušný orgán může být oprávněn k provádění prohlídek při vstupu a odchodu, které mají odradit od nedovoleného vnášení materiálů nebo neoprávněného vynášení utajovaných informací EU z areálů nebo budov.

6. Hrozí-li nebezpečí, že by utajované informace EU mohly být, i neúmyslně, odezírány, přijmou se vhodná opatření, kterými se tomuto riziku zamezí.

7. U nových zařízení se požadavky na fyzickou bezpečnost a jejich funkční specifikace stanoví jako součást plánování a konstrukce zařízení. U stávajících zařízení se požadavky na fyzickou bezpečnost uplatňují v nejvyšší možné míře.

III. PROSTŘEDKY FYZICKÉ OCHRANY UTAJOVANÝCH INFORMACÍ EU

8. Při pořizování prostředků fyzické ochrany utajovaných informací EU (například bezpečnostních úschovných objektů, skartovacích přístrojů, dveřních zámků, elektronických systémů kontroly vstupu, systémů detekce narušení, poplašných systémů) zajistí příslušný bezpečnostní orgán, aby tyto prostředky splňovaly schválené technické standardy a minimální požadavky.

9. Technické specifikace prostředků používaných pro fyzickou ochranu utajovaných informací EU se stanoví v bezpečnostních pokynech, které schválí Bezpečnostní výbor.

10. Kontrola bezpečnostních systémů a údržba prostředků fyzické ochrany se provádí pravidelně. Při údržbě se zohlední výsledek kontrol, aby se i nadále zajistilo optimální fungování těchto prostředků.

11. Účinnost jednotlivých bezpečnostních opatření a celého bezpečnostního systému se znovu hodnotí při každé kontrole.

IV. FYZICKY CHRÁNĚNÉ OBLASTI

12. Pro fyzickou ochranu utajovaných informací EU se stanoví dva druhy fyzicky chráněných oblastí nebo jejich vnitrostátní ekvivalenty:

    a) administrativní oblasti a

    b) zabezpečené oblasti (včetně technicky zabezpečených oblastí).

    V tomto rozhodnutí je třeba všechny odkazy na administrativní oblasti a zabezpečené oblasti včetně technicky zabezpečených oblastí chápat také jako odkazy na jejich vnitrostátní ekvivalenty.

13. Příslušný bezpečnostní orgán určí, zda daný prostor splňuje požadavky na to, aby mohl být označen jako administrativní oblast, zabezpečená oblast nebo technicky zabezpečená oblast.

14. U administrativních oblastí:

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

    b) je přístup bez doprovodu umožněn pouze osobám, které mají řádné oprávnění od příslušného orgánu; a

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

15. U zabezpečených oblastí:

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

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

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

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

a) je třeba jasně stanovit nejvyšší stupeň utajení informací, které jsou v dané oblasti zpravidla ukládány; 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.

17. 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, být uzamčeny v době, kdy nejsou obsazeny, a střeženy v době, kdy obsazeny jsou. Všechny klíče musí být kontrolovány v souladu s částí VI;

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

c) tyto oblasti musí být předmětem pravidelných fyzických nebo technických kontrol podle požadavků příslušného bezpečnostního orgánu. 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.

18. Bez ohledu na bod 17 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 příslušným bezpečnostním orgánem za tím účelem, aby prostřednictvím těchto zařízení nemohlo dojít k neúmyslnému či nezákonnému přenášení žádných srozumitelných informací mimo danou zabezpečenou oblast.

19. 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.

20. Zabezpečené oblasti a technicky zabezpečené oblasti mohou být zřízeny dočasně v rámci administrativní oblasti pro uspořádání tajného zasedání nebo pro jiný podobný účel.

21. Pro každou zabezpečenou oblast se vypracují bezpečnostní provozní směrnice, v nichž se stanoví:

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

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

c) osoby, které jsou k přístupu do dané oblasti bez doprovodu oprávněny vzhledem k tomu, že potřebují znát utajované informace a že jsou bezpečnostně prověřeny;

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.

22. Trezorové místnosti se budují uvnitř zabezpečených oblastí. Stěny, podlahy, stropy, okna a uzamykatelné dveře musí být schváleny příslušným bezpečnostním orgánem a musí poskytovat ochranu na úrovni rovnocenné s bezpečnostním úschovným objektem schváleným pro ukládání utajovaných informací EU se stejným stupněm utajení.

V. OPATŘENÍ FYZICKÉ BEZPEČNOSTI PRO NAKLÁDÁNÍ S UTAJOVANÝMI INFORMACEMI EU A JEJICH UKLÁDÁNÍ

23. 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 body 28 až 40 přílohy III a že se zavázal k dodržování náhradních opatření stanovených bezpečnostními pokyny vydanými příslušným bezpečnostním orgánem s cílem zajistit, aby utajované informace EU byly chráněny před přístupem neoprávněných osob.

24. Utajované informace EU se stupněm utajení RESTREINT UE / EU RESTRICTED se ukládají ve vhodném uzamčeném kancelářském nábytku v administrativní oblasti nebo v zabezpečené oblasti. Dočasně mohou být ukládány mimo zabezpečenou oblast či mimo administrativní oblast za předpokladu, že se držitel informací zavázal k dodržování náhradních opatření stanovených bezpečnostními pokyny vydanými příslušným bezpečnostním orgánem.

25. 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) přenáší utajované informace EU v souladu s body 28 až 40 přílohy III,

        ii) zavázal se k dodržování náhradních opatření stanovených bezpečnostními pokyny vydanými příslušným bezpečnostním orgánem s cílem zajistit, aby utajované informace EU byly chráněny před přístupem neoprávněných osob,

        iii) má utajované informace EU neustále pod osobním dohledem, a

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

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

27. S utajovanými informacemi EU se stupněm utajení TRÈS SECRET UE / EU TOP SECRET se nakládá v zabezpečené oblasti.

28. Utajované informace EU se stupněm utajení TRÈS SECRET UE / EU TOP SECRET se ukládají v zabezpečené oblasti při dodržení jedné z těchto podmínek:

    a) informace se ukládají v bezpečnostním úschovném objektu v souladu s bodem 8, přičemž je třeba uplatňovat jedno nebo více těchto dodatečných kontrolních opatření:

        i) nepřetržitá ochrana nebo kontrola ze strany prověřeného bezpečnostního nebo služebního personálu,

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

    nebo

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

29. Pravidla pro přenos utajovaných informací EU mimo fyzicky chráněné oblasti jsou stanovena v příloze III.

VI. KONTROLA KLÍČŮ A KÓDŮ POUŽÍVANÝCH PRO OCHRANU UTAJOVANÝCH INFORMACÍ EU

30. Příslušný bezpečnostní orgán stanoví postupy pro správu klíčů a nastavení kódů pro kanceláře, místnosti, bezpečnostní trezorové místnosti a bezpečnostní úschovné objekty. Tyto postupy zabrání neoprávněnému přístupu.

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

    a) kdykoli se změní personál, který kombinaci zná;

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

    c) pokud došlo k údržbě či opravě zámku; a

    d) nejméně každých 12 měsíců.

PŘÍLOHA III

SPRÁVA UTAJOVANÝCH INFORMACÍ

I. ÚVOD

1. Tato příloha stanoví prováděcí pravidla k článku 9. Stanoví administrativní opatření, která slouží ke kontrolování utajovaných informací EU během celého jejich životního cyklu, a napomáhají tak zabránit úmyslnému či neúmyslnému ohrožení či ztrátě informací, zjistit takové ohrožení nebo ztrátu informací a následně zajistit nápravu.

II. PRAVIDLA UTAJOVÁNÍ

Stupně utajení a označení

2. Informace se utajují pouze v případě, že vyžadují ochranu z důvodu jejich důvěrnosti.

3. Původce utajovaných informací EU odpovídá za stanovení stupně utajení podle příslušných pokynů pro utajení informací a za počáteční distribuci informací.

4. Stupeň utajení utajovaných informací EU se stanoví v souladu s čl. 2 odst. 2 a na základě bezpečnostní politiky schválené v souladu s čl. 3 odst. 3.

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

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

7. 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.

8. 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.

9. 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

Označení

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

a) označení určující původce;

b) jakákoli výstražná označení, 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 informací snížit nebo zrušit.

Zkratky označení stupňů utajení

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

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

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

Vyhotovování utajovaných dokumentů EU

13. Při vyhotovování utajovaného dokumentu EU:

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

b) každá strana se očísluje;

c) informacemi, pokud tak nejsou označeny;

d) na dokumentu se uvede datum;

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

14. Nelze-li na utajované informace EU použít bod 13, přijmou se jiná patřičná opatření podle bezpečnostních pokynů, které se vypracují v souladu s čl. 6 odst. 2.

Snížení a zrušení stupně utajení utajovaných informací EU

15. Je-li to možné, a zejména jedná-li se o informace se stupněm utajení RESTREINT UE/EU RESTRICTED, uvede původce v době vytvoření utajovaných informací EU, zda je možné snížit nebo zrušit jejich stupeň utajení k určitému datu nebo po určité události.

16. Generální sekretariát Rady pravidelně přezkoumává utajované informace EU, které jsou v jeho držení, za účelem zjištění, zda je příslušný stupeň utajení stále odpovídající. Generální sekretariát Rady zavede systém přezkumu stupně utajení evidovaných utajovaných informací EU, jichž je původcem, který je prováděn nejméně jednou za pět let. Tento přezkum není třeba provést v případě, že původce na počátku uvedl, že u daných informací bude automaticky snížen nebo zrušen stupeň utajení a dané informace jsou odpovídajícím způsobem označeny.

III. EVIDENCE UTAJOVANÝCH INFORMACÍ EU Z BEZPEČNOSTNÍCH DŮVODŮ

17. Pro každou organizační složku v rámci generálního sekretariátu Rady a správních orgánů členských států, v nichž se nakládá s utajovanými informacemi EU, se určí odpovědný registr s cílem zajistit, aby se s utajovanými informacemi EU nakládalo v souladu s tímto rozhodnutím. Registry se zřizují jako zabezpečené oblasti podle přílohy II.

18. Pro účely tohoto rozhodnutí se evidencí z bezpečnostních důvodů (dále jen „evidence“) rozumí uplatňování postupů, kterými se zaznamenává životní cyklus daného materiálu, včetně jeho distribuce a zničení.

19. Veškerý materiál se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a vyšším nebo s rovnocenným stupněm utajení je třeba evidovat v určených registrech, kdykoli je doručen určité organizační složce nebo kdykoli ji opouští.

20. Ústřední registr generálního sekretariátu Rady vede záznamy o všech utajovaných informacích předaných Radou a generálním sekretariátem Rady třetím státům a mezinárodním organizacím a všech utajovaných informacích, které od třetích států a mezinárodních organizací obdrží.

21. V případě komunikačního a informačního systému mohou být evidenční postupy provedeny přímo v rámci systému.

22. Rada schválí bezpečnostní politiku pro evidenci utajovaných informací EU z bezpečnostních důvodů.

Registry pro dokumenty se stupněm utajení TRÈS SECRET UE/EU TOP SECRET

23. V členských státech a v generálním sekretariátu Rady se určí registr, který je ústředním orgánem pro příjem a odesílání informací se stupněm utajení TRÈS SECRET UE/EU TOP SECRET. V případě potřeby mohou být určeny podřízené registry pro nakládání s těmito informacemi z důvodů evidence.

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

IV. KOPÍROVÁNÍ A PŘEKLÁDÁNÍ UTAJOVANÝCH DOKUMENTŮ EU

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

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

27. Pro kopie a překlady dokumentů se použijí bezpečnostní opatření použitá pro původní dokument.

IV. PŘENOS UTAJOVANÝCH INFORMACÍ EU

28. Přenos utajovaných informací EU podléhá ochranným opatřením stanoveným v bodech 30 až 40. V případech, kdy jsou utajované informace EU přenášeny na elektronických záznamových médiích, a to bez ohledu na čl. 9 odst. 4 mohou níže uvedená ochranná opatření doplňovat vhodná technická protiopatření podle pokynů stanovených příslušným bezpečnostním orgánem s cílem minimalizovat riziko ztráty nebo ohrožení.

29. Příslušné bezpečnostní orgány generálního sekretariátu Rady a členských států vydají pokyny týkající se přenosu utajovaných informací EU v souladu s tímto rozhodnutím.

Přenos uvnitř budovy nebo uzavřené skupiny budov

30. Utajované informace EU přenášené uvnitř budovy nebo uzavřené skupiny budov musí být zakryty, aby se zamezilo odpozorování jejich obsahu.

31. Informace se stupněm utajení TRÈS SECRET UE/EU TOP SECRET musí být při přenosu uvnitř budovy nebo uzavřené skupiny budov uloženy v zabezpečené obálce označené pouze jménem příjemce.

Přenos v rámci EU

32. Utajované informace EU přenášené mezi budovami či areály v rámci EU jsou uloženy v takovém obalu, aby byly chráněny před neoprávněným vyzrazením.

33. Přenos informací se stupněm utajení nejvýše SECRET UE/EU SECRET v rámci EU se provádí jedním z těchto způsobů:

a) vojenským, vládním nebo případně diplomatickým kurýrem;

b) osobním přenosem za těchto podmínek:

i) osoba, která utajované informace EU přenáší, je má stále u sebe, pokud nejsou uloženy v souladu s požadavky stanovenými v příloze II,

ii) utajované informace EU nesmí být během přenosu otevřeny ani čteny na veřejných místech,

iii) dotčené osoby jsou poučeny o svých povinnostech týkajících se bezpečnosti,

iv) dotčené osoby musí být v případě potřeby držiteli kurýrního listu;

c) vnitrostátními poštovními službami nebo komerčními kurýrními službami za těchto podmínek:

i) příslušný vnitrostátní bezpečnostní orgán je schválil v souladu s vnitrostátními právními předpisy,

ii) uplatňují odpovídající ochranná opatření v souladu s minimálními požadavky, které budou stanoveny v bezpečnostních pokynech podle čl. 6 odst. 2.

V případě přenosu z jednoho členského státu do jiného se ustanovení písmene e) budou vztahovat pouze na informace až do stupně utajení CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Materiál se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET (například vybavení nebo technické zařízení), který nemůže být přenášen způsoby uvedenými v bodě 33, přepravují v souladu s přílohou V obchodní přepravci jako náklad.

35. Přenos informací se stupněm utajení TRÈS SECRET UE/EU TOP SECRET mezi budovami či areály v rámci EU se provádí vojenským, vládním nebo případně diplomatickým kurýrem.

Přenos z EU na území třetího státu

36. Utajované informace EU přenášené z EU na území třetího státu jsou uloženy v takovém obalu, aby byly chráněny před neoprávněným vyzrazením.

37. Přenos informací se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET z EU na území třetího státu se provádí jedním z těchto způsobů:

a) vojenským nebo diplomatickým kurýrem;

b) osobním přenosem za těchto podmínek:

i) balíček je opatřen úřední pečetí nebo je zabalen tak, aby bylo zřejmé, že se jedná o úřední zásilku, která by neměla být předmětem celní nebo bezpečnostní kontroly,

ii) dotčené osoby jsou držiteli kurýrního listu, který obsahuje identifikační údaje balíčku a opravňuje tyto osoby k jeho přenosu,

iii) osoba, která utajované informace EU přenáší, je má stále u sebe, pokud nejsou uloženy v souladu s požadavky stanovenými v příloze II,

iv) utajované informace EU nesmí být na cestě otevřeny ani čteny na veřejných místech,

v) dotčené osoby jsou poučeny o svých povinnostech týkajících se bezpečnosti.

38. Přenos informací se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET, které EU předává třetímu státu nebo mezinárodní organizaci, musí splňovat příslušná ustanovení dohody o bezpečnosti informací či správního ujednání v souladu s čl. 12 odst. 2 písm. a) nebo b).

39. Informace se stupněm utajení RESTREINT UE/EU RESTRICTED lze přenášet také poštovními službami či komerčními kurýrními službami.

40. Přenos informací se stupněm utajení TRÈS SECRET UE/EU TOP SECRET z EU na území třetího státu se provádí vojenským nebo diplomatickým kurýrem.

VI. NIČENÍ UTAJOVANÝCH INFORMACÍ EU

41. Utajované dokumenty EU, které již nejsou potřebné, mohou být zničeny, aniž jsou dotčena příslušná pravidla a předpisy o archivování.

42. Ničení dokumentů podléhajících evidenci v souladu s čl. 9 odst. 2 provádí odpovědný registr podle pokynů držitele nebo příslušného orgánu. Administrativní pomůcky a jiné informace o evidenci musí být odpovídajícím způsobem aktualizovány.

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

44. Pracovník registru a svědek, pokud je přítomnost svědka vyžadována, podepíší zápis o zničení, který se uloží v registru. V registru jsou ukládány zápisy o zničení dokumentů se stupněm utajení TRÈS 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.

45. Ničení utajovaných dokumentů, včetně dokumentů se stupněm utajení RESTREINT UE/EU RESTRICTED, se provádí postupy, které splňují příslušné normy EU či rovnocenné normy nebo které byly schváleny členskými státy v souladu s vnitrostátními technickými normami tak, aby nebylo možné znovu sestavit celý dokument nebo jeho část.

46. Ničení počítačových paměťových médií používaných pro utajované informace EU se provádí v souladu s bodem 36 přílohy IV.

VII. INSPEKCE A HODNOTÍCÍ NÁVŠTĚVY

47. Pojem „inspekce“ se dále použije k označení jakékoli

a) inspekce či kontroly v souladu s čl. 9 odst. 3, čl. 15 odst. 2 písm. e), f) a g); nebo

b) hodnotící návštěvy v souladu s čl. 12 odst. 5,

která má vyhodnotit účinnost opatření zavedených na ochranu utajovaných informací EU.

48. Inspekce se mimo jiné provádějí s cílem:

a) zajistit dodržování požadovaných minimálních standardů pro ochranu utajovaných informací EU stanovených tímto rozhodnutím;

b) zdůraznit význam bezpečnosti a účinného řízení rizik u kontrolovaných subjektů;

c) doporučit protiopatření za účelem zmírnění konkrétních dopadů, které může přinášet ztráta důvěrnosti, integrity nebo dostupnosti utajovaných informací; a

d) posilovat probíhající programy bezpečnostních orgánů v oblasti bezpečnostního vzdělávání a povědomí.

49. Před koncem každého kalendářního roku přijme Rada program inspekcí na další rok podle čl. 15 odst. 1 písm. c). Konkrétní data jednotlivých inspekcí se určí po dohodě s dotyčnou agenturou nebo institucí EU, členským státem, třetím státem nebo mezinárodní organizací.

Provádění inspekcí

50. Inspekce se provádějí s cílem prověřit příslušná pravidla, předpisy a postupy v kontrolovaném subjektu a ověřit, zda jsou praktické postupy daného subjektu v souladu se základními zásadami a minimálními standardy stanovenými tímto rozhodnutím a předpisy upravujícími výměnu utajovaných informací s daným subjektem.

51. Inspekce se provádějí ve dvou fázích. Před vlastní inspekcí je v případě potřeby uspořádáno přípravné jednání s příslušným subjektem. Po tomto přípravném jednání stanoví inspekční tým se souhlasem dotyčného subjektu podrobný program inspekce zahrnující všechny oblasti bezpečnosti. Inspekční tým má přístup do jakéhokoli prostoru, v němž se nakládá s utajovanými informacemi EU, zejména do registrů a k přístupovým bodům komunikačních a informačních systémů.

52. Inspekce ve správních orgánech členských států jsou prováděny pod vedením společného inspekčního týmu generálního sekretariátu Rady a Evropské komise v plné spolupráci s úředníky kontrolovaného subjektu.

53. Inspekce ve třetích státech a v mezinárodních organizacích jsou prováděny pod vedením společného inspekčního týmu generálního sekretariátu Rady a Evropské komise v plné spolupráci s úředníky kontrolovaného třetího státu nebo mezinárodní organizace.

54. Inspekce v agenturách a subjektech EU zřízených podle hlavy V kapitoly 2 Smlouvy o EU, jakož i v Europolu a Eurojustu provádí bezpečnostní kancelář generálního sekretariátu Rady za pomoci odborníků z vnitrostátního bezpečnostního orgánu státu, na jehož území se daná agentura či instituce nachází. Zapojeno může být i bezpečnostní ředitelství Evropské komise, pokud si pravidelně vyměňuje utajované informace EU s danou agenturou nebo subjektem.

55. V případě inspekcí v agenturách a institucích EU zřízených podle hlavy V kapitoly 2 Smlouvy o EU, jakož i v Europolu a Eurojustu a ve třetích státech a mezinárodních organizacích se o pomoc a příspěvky odborníků z vnitrostátního bezpečnostního orgánu žádá v souladu s podrobnými ujednáními, která schválí Bezpečnostní výbor.

Inspekční zprávy

56. Na konci inspekce jsou kontrolovanému subjektu předloženy hlavní závěry a doporučení. Poté je v rámci pravomocí bezpečnostního orgánu generálního sekretariátu Rady (bezpečnostní kanceláře) vypracována inspekční zpráva. Pokud byla navržena nápravná opatření a doporučení, je třeba do zprávy zahrnout dostatečná odůvodnění závěrů inspekce. Inspekční zpráva se předá příslušnému orgánu kontrolovaného subjektu.

57. U inspekcí prováděných ve správních orgánech členských států:

a) se návrh inspekční zprávy předloží příslušnému vnitrostátnímu bezpečnostnímu orgánu, který ověří, že zpráva je věcně správná a že neobsahuje žádné informace s vyšším stupněm utajení než RESTREINT UE/EU RESTRICTED;

b) pokud vnitrostátní bezpečnostní orgán daného členského státu nepožádá o zamezení všeobecné distribuce zprávy, jsou inspekční zprávy zaslány členům Bezpečnostního výboru a bezpečnostnímu ředitelství Evropské komise; zpráva musí být utajena stupněm utajení RESTREINT UE/EU RESTRICTED.

V rámci pravomocí bezpečnostního orgánu generálního sekretariátu Rady (bezpečnostní kanceláře) se vypracovává pravidelná zpráva, v níž se zdůrazní poznatky získané z inspekcí provedených v členských státech za určité období; tuto zprávu posoudí Bezpečnostní výbor.

58. U hodnotících návštěv třetích států a mezinárodních organizací je zpráva zaslána Bezpečnostnímu výboru a bezpečnostnímu ředitelství Evropské komise. Zpráva musí být utajena alespoň stupněm utajení RESTREINT UE/EU RESTRICTED. Veškerá nápravná opatření jsou ověřena během následné návštěvy a oznámena Bezpečnostnímu výboru.

59. U hodnotících návštěv agentur a subjektů EU zřízených podle hlavy V kapitoly 2 Smlouvy o EU, jakož i Europolu a Eurojustu jsou inspekční zprávy zaslány členům Bezpečnostního výboru a bezpečnostnímu ředitelství Evropské komise. Návrh inspekční zprávy je předložen příslušné agentuře nebo subjektu, která ověří, že zpráva je věcně správná a že neobsahuje žádné informace s vyšším stupněm utajení než RESTREINT UE/EU RESTRICTED. Veškerá nápravná opatření jsou ověřena během následné návštěvy a oznámena Bezpečnostnímu výboru.

60. Bezpečnostní orgán generálního sekretariátu Rady provádí pravidelné inspekce organizačních složek v rámci generálního sekretariátu Rady pro účely stanovené v bodě 48.

Kontrolní seznam pro účely inspekcí

61. Bezpečnostní orgán generálního sekretariátu Rady (bezpečnostní kancelář) vypracuje a aktualizuje kontrolní seznam pro účely inspekcí obsahující položky, které je třeba ověřit během inspekce. Tento seznam se zasílá Bezpečnostnímu výboru.

62. Informace pro vyplnění kontrolního seznamu lze získat zejména během inspekce od pracovníků odpovědných za řízení bezpečnosti subjektu, v němž je inspekce prováděna. Jakmile je seznam podrobně vyplněn, stanoví se po dohodě s kontrolovaným subjektem stupeň jeho utajení. Seznam není součástí inspekční zprávy.

PŘÍLOHA IV

OCHRANA UTAJOVANÝCH INFORMACÍ EU, S NIMIŽ SE NAKLÁDÁ V KOMUNIKAČNÍCH A INFORMAČNÍCH SYSTÉMECH

I. ÚVOD

1. Tato příloha stanoví prováděcí pravidla k článku 10.

2. Pro bezpečné a správné fungování komunikačních a informačních systémů jsou zásadní tyto vlastnosti a koncepce zabezpečení informací:

Autenticita:	záruka, že informace jsou autentické a z důvěryhodných zdrojů;
Dostupnost:	přístupnost a použitelnost informací na žádost oprávněného subjektu;
Důvěrnost:	skutečnost, že informace nejsou zpřístupněny neoprávněným osobám a subjektům a pro nedovolené účely;
Integrita:	zajištění přesnosti a úplnosti informací a aktiv;
Nepopiratelnost:	schopnost prokázat zpětně jednání či událost tak, aby dané jednání či událost nemohly být následně popřeny.

II. ZÁSADY ZABEZPEČENÍ INFORMACÍ

3. Níže uvedená ustanovení tvoří minimální požadavky na bezpečnost veškerých komunikačních a informačních systémů nakládajících s utajovanými informacemi EU. Podrobné požadavky na provádění těchto ustanovení se stanoví v bezpečnostních politikách a bezpečnostních pokynech pro zabezpečení informací.

Řízení bezpečnostních rizik

4. Řízení bezpečnostních rizik je nedílnou součástí vytváření, vývoje, provozování a údržby komunikačních a informačních systémů. Řízení rizik (hodnocení, řešení, přijetí a sdělování) probíhá jako cyklický proces a je prováděno společně zástupci vlastníků systémů, projektovými a provozními orgány a orgány pro schvalování bezpečnosti za využití osvědčeného, transparentního a zcela srozumitelného procesu hodnocení rizika. Oblast působnosti komunikačního a informačního systému a jeho aktiv je třeba jasně určit na počátku procesu řízení rizik.

5. Příslušné orgány přezkoumají možné hrozby pro komunikační a informační systémy a vypracovávají aktualizovaná a přesná hodnocení hrozeb, která odpovídají stávajícímu provoznímu prostředí. Neustále si doplňují znalosti o otázkách zranitelnosti a pravidelně přezkoumávají hodnocení zranitelnosti, aby mohly odpovídajícím způsobem reagovat na měnící se prostředí informačních technologií.

6. Cílem řešení bezpečnostních rizik je uplatňovat soubor bezpečnostních opatření, jejichž výsledkem je uspokojivá rovnováha mezi požadavky uživatelů, náklady a zbytkovým bezpečnostním rizikem.

7. Specifické požadavky, rozsah a míra podrobnosti stanovená příslušným orgánem pro bezpečnostní akreditaci k akreditaci komunikačního a informačního systému musí být přiměřená posouzenému riziku při zohlednění všech příslušných faktorů, včetně stupně utajení utajovaných informací EU, s nimiž se v komunikačním a informačním systému nakládá. Akreditace komunikačního a informačního systému zahrnuje formální prohlášení o zbytkovém riziku a přijetí zbytkového rizika ze strany odpovědného orgánu.

Bezpečnost během celého životního cyklu komunikačního a informačního systému

8. Zajištění bezpečnosti zůstává požadavkem po celý životní cyklus daného komunikačního a informačního systému od uvedení do provozu až do ukončení provozu.

9. Pro každou fázi životního cyklu komunikačního a informačního systému je třeba v oblasti bezpečnosti stanovit úlohu a způsob zapojení každého aktéra spojeného s daným systémem.

10. Každý komunikační a informační systém, včetně jeho technických i netechnických bezpečnostních opatření, musí být během akreditačního řízení podroben bezpečnostním testům s cílem zajistit odpovídající úroveň zabezpečení a ověřit, zda je řádně zprovozněn, zapojen a konfigurován.

11. Hodnocení, kontroly a přezkumy bezpečnosti se provádějí pravidelně během provozu a údržby komunikačního a informačního systému a rovněž za vyjímečných okolností.

12. Bezpečnostní dokumentace pro daný komunikační a informační systém se vyvíjí během jeho celého životního cyklu jakožto nedílná součást procesu řízení změn a konfigurací.

Osvědčené postupy

13. Generální sekretariát Rady a členské státy spolupracují na vývoji osvědčených postupů na ochranu utajovaných informací EU, s nimiž se nakládá v komunikačních a informačních systémech. Pokyny týkající se osvědčených postupů stanoví technická, fyzická, organizační a procedurální bezpečnostní opatření pro komunikační a informační systémy, která se ukázala jako účinná v boji proti určitým hrozbám a zranitelným místům.

14. Pro ochranu utajovaných informací EU, s nimiž se nakládá v komunikačních a informačních systémech, se využijí získané poznatky subjektů, které působí v oblasti zabezpečení informací v EU i mimo EU.

15. Šíření a následné uplatňování osvědčených postupů má napomoci dosažení rovnocenné úrovně zabezpečení jednotlivých komunikačních a informačních systémů, které jsou provozovány generálním sekretariátem Rady a členskými státy a v nichž se nakládá s utajovanými informacemi EU.

Hloubková ochrana

16. V zájmu zmírnění rizika pro komunikační a informační systémy se provádí řada technických a netechnických bezpečnostních opatření, která jsou uspořádána jako několik obranných linií. Tyto linie zahrnují:

a) *odstrašování:* bezpečnostní opatření, jež mají odradit od jakéhokoli nepřátelského plánování útoku na komunikační a informační systém;

b) *prevence:* bezpečnostní opatření, jež mají zabránit útoku na komunikační a informační systém nebo takový útok znemožnit;

c) *odhalování:* bezpečnostní opatření, jež mají odhalit uskutečnění útoku na komunikační a informační systém;

d) *odolnost:* bezpečnostní opatření, která mají omezit dopad útoku na co nejmenší soubor informací nebo aktiv komunikačního a informačního systému a předcházet další škodě, a

e) *náprava:* bezpečnostní opatření, jež mají vést k obnovení bezpečného stavu systému.

Míra přísnosti bezpečnostních opatření se stanoví na základě hodnocení rizik.

17. Příslušné orgány zajistí, aby byly schopny reagovat na mimořádné události, které mohou přesahovat organizační a státní hranice, s cílem koordinovat reakce a sdílet informace o těchto mimořádných událostech a souvisejícím riziku (schopnost reakce na počítačové hrozby).

Zásada minimality a co nejomezenějších práv

18. Aby se předešlo zbytečnému riziku, budou prováděny nebo provozovány pouze funkce, zařízení a služby, které jsou nezbytné pro splnění provozních požadavků.

19. Aby se omezila jakákoli škoda způsobená v důsledku nepředvídaných událostí, chyb nebo neoprávněného používání zdrojů komunikačních a informačních systémů, mají mít uživatelé systémů a automatizované procesy přístup, práva nebo oprávnění pouze v rozsahu nezbytném k plnění svých úkolů.

20. Je-li v komunikačním a informačním systému vyžadováno provádění evidenčních procedur, musí být tyto procedury ověřeny v akreditačním řízení.

Povědomí o zabezpečení informací

21. Povědomí o rizicích a dostupných bezpečnostních opatřeních je první obrannou linií zajišťující bezpečnost komunikačních a informačních systémů. Zejména všichni členové personálu zasahující do životního cyklu komunikačního a informačního systému, včetně uživatelů, si musí být vědomi:

a) že selhání bezpečnosti může významně poškodit komunikační a informační systémy;

b) možné újmy způsobené jiným subjektům z důvodu vzájemného propojení a vzájemné závislosti; a

c) svých individuálních povinností a odpovědnosti za bezpečnost komunikačního a informačního systému v závislosti na svých konkrétních úlohách v rámci daných systémů a procesů.

22. Aby se zajistilo pochopení povinností souvisejících s bezpečností, je pro veškerý dotčený personál, včetně vedoucích pracovníků a uživatelů komunikačních a informačních systémů povinné vzdělávání v oblasti zabezpečení informací a školení zaměřené na zvyšování povědomí o zabezpečení informací.

Hodnocení a schvalování bezpečnostních prostředků informačních technologií

23. Požadovaná míra důvěry v bezpečnostní opatření, vymezená jako úroveň zabezpečení, se stanoví na základě výsledku procesu řízení rizik a v souladu s příslušnými bezpečnostními politikami a bezpečnostními pokyny.

24. Úroveň zabezpečení se ověří pomocí mezinárodně uznávaných nebo na vnitrostátní úrovni schválených postupů a metod. To zahrnuje zejména hodnocení, kontroly a audity.

25. Kryptografické prostředky na ochranu utajovaných informací EU hodnotí a schvaluje vnitrostátní schvalovací orgán členského státu pro kryptografickou ochranu.

26. Předtím než jsou kryptografické prostředky doporučeny ke schválení Radou nebo generálním tajemníkem Rady v souladu s čl. 10 odst. 6, musí být úspěšné vyhodnoceny druhou stranou, jíž je orgán s odpovídající kvalifikací členského státu, který se nepodílí na vývoji ani výrobě zařízení. Rozsah informací vyžadovaný během hodnocení druhou stranou závisí na předpokládaném nejvyšším stupni utajení utajovaných informací EU, které mají být danými prostředky chráněny. Rada schválí bezpečnostní politiku pro hodnocení a schvalování kryptografických prostředků.

27. Opravňují-li k tomu zvláštní provozní důvody, může Rada nebo případně generální tajemník Rady na doporučení Bezpečnostního výboru od požadavků podle odstavce 25 nebo 26 upustit a postupem podle čl. 10 odst. 6 udělit dočasné schválení na konkrétní období.

28. Orgánem s odpovídající kvalifikací je schvalovací orgán členského státu pro kryptografickou ochranu, který byl akreditován na základě kritérií stanovených Radou k provádění druhého hodnocení kryptografických prostředků na ochranu utajovaných informací EU.

29. Rada schválí bezpečnostní politiku pro způsobilost a schvalování nekryptografických bezpečnostních prostředků informačních technologií.

Přenos v zabezpečených oblastech

30. Bez ohledu na ustanovení tohoto rozhodnutí, je-li přenos utajovaných informací EU omezen na zabezpečené oblasti, může být na základě výsledku procesu řízení rizik a se souhlasem orgánu pro bezpečnostní akreditaci použit přenos nešifrovaný nebo šifrovaný na nižší úrovni.

Bezpečné propojení komunikačních a informačních systémů

31. Pro účely tohoto rozhodnutí se propojením rozumí přímé spojení dvou nebo více informačních systémů za účelem jednosměrného či vícesměrného sdílení údajů a dalších informačních zdrojů (například komunikace).

32. Komunikační a informační systém považuje každý propojený informační systém za nedůvěryhodný a uplatní ochranná opatření pro kontrolu výměny utajovaných informací.

33. U všech propojení komunikačních a informačních systémů s jiným systémem informačních technologií je třeba splnit tyto základní požadavky:

a) pracovní či provozní požadavky na tato propojení stanoví a schválí příslušné orgány;

b) propojení je předmětem procesu řízení rizik a akreditačního řízení a je schváleno ze strany příslušných orgánů pro bezpečnostní akreditaci; a

c) na vnější hranici všech systémů se použijí funkce ochrany (Boundary Protection Services, BPS).

34. Certifikovaný komunikační a informační systém nesmí být propojen s nechráněnou nebo veřejnou sítí, s výjimkou případů, kdy má komunikační a informační systém schválené funkce BPS instalované pro tento účel mezi daným systémem a nechráněnou či veřejnou sítí. Bezpečnostní opatření pro taková propojení přezkoumá příslušný orgán pro zabezpečení informací a schválí je příslušný orgán pro bezpečnostní akreditaci.

Pokud je nechráněná nebo veřejná síť využívána výhradně k přenosu dat a informace jsou zašifrovány pomocí kryptografického prostředku schváleného v souladu s článkem 10, nepovažuje se takové spojení za propojení.

35. Komunikační a informační systém certifikovaný pro nakládání s informacemi se stupněm utajení TRÈS SECRET UE/EU TOP SECRET nesmí být přímo ani kaskádou propojen s nechráněnou nebo veřejnou sítí.

Počítačová paměťová média

36. Počítačová paměťová média se ničí postupy schválenými příslušným bezpečnostním orgánem.

37. Počítačová paměťová média se znovu použijí nebo se u nich sníží či zruší stupeň utajení v souladu s bezpečnostní politikou, která bude vypracována podle čl. 6 odst. 1.

Mimořádné okolnosti

38. Bez ohledu na ustanovení tohoto rozhodnutí mohou být za mimořádných okolností, například během hrozící nebo probíhající krize, konfliktu, války nebo za vyjímečných provozních okolností, použity níže popsané zvláštní postupy.

39. 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 nebo nemají žádné šifrovací zařízení; a

b) utajované materiály nelze včas předat jiným způsobem.

40. Za okolností uvedených v bodě 38 nenesou přenášené utajované informace žádná označení ani údaje, které by je odlišovaly od informací, které nejsou utajované nebo mohou být chráněny dostupným kryptografickým prostředkem. Příjemce informací je třeba neprodleně uvědomit o stupni utajení jiným způsobem.

41. Pokud se použije postup podle bodu 38, podá se následně zpráva příslušnému orgánu a Bezpečnostnímu výboru.

III. FUNKCE A ORGÁNY V OBLASTI ZABEZPEČENÍ INFORMACÍ

42. V členských státech a v rámci generálního sekretariátu Rady je třeba zajistit výkon níže uvedených funkcí v oblasti zabezpečení informací. Tyto funkce nevyžadují zřízení samostatných organizačních složek. Jsou plněny v rámci oddělených mandátů. Tyto funkce a související povinnosti mohou být ovšem kombinovány nebo spojeny ve stejné organizační složce nebo rozděleny do různých organizačních složek za podmínky, že se zamezí vnitřním střetům zájmů nebo úkolů.

Orgán pro zabezpečení informací

43. Orgán pro zabezpečení informací je povinen:

a) vypracovat politiky v oblasti zabezpečení informací a bezpečnostní pokyny pro zabezpečení informací a monitorovat jejich účinnost a vhodnost;

b) zajistit a spravovat technické informace týkající se kryptografických prostředků;

c) zajistit, aby opatření na zabezpečení informací zvolená pro ochranu utajovaných informací EU byla v souladu s příslušnými politikami, jimiž se řídí jejich způsobilost a výběr;

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

e) koordinovat školení a zvyšování povědomí o zabezpečení informací;

f) konzultovat s poskytovatelem komunikačního a informačního systému, s aktéry v oblasti bezpečnosti a se zástupci uživatelů otázky týkající se politik v oblasti zabezpečení informací a bezpečnostních pokynů pro zabezpečení informací; a

g) zajistit, aby v odborné podskupině Bezpečnostního výboru pro otázky zabezpečení informací byly k dispozici odpovídající odborné znalosti.

Orgán TEMPEST

44. Orgán TEMPEST je povinen zajistit, aby komunikační a informační systémy byly v souladu s politikami a pokyny TEMPEST. Schvaluje protiopatření TEMPEST pro zařízení a prostředky na ochranu utajovaných informací EU do určitého stupně utajení v jeho provozním prostředí.

Schvalovací orgán pro kryptografickou ochranu

45. Schvalovací orgán pro kryptografickou ochranu je povinen zajistit, aby kryptografické prostředky byly v souladu s vnitrostátní politikou v oblasti kryptografické ochrany nebo s politikou Rady v této oblasti. Schvaluje konkrétní kryptografický prostředek na ochranu utajovaných informací EU do určitého stupně utajení v jeho provozním prostředí. Pokud jde o členské státy, odpovídá schvalovací orgán pro kryptografickou ochranu rovněž za hodnocení kryptografických prostředků.

Orgán pro distribuci kryptografických materiálů

46. Orgán pro distribuci kryptografických materiálů je povinen:

a) spravovat a dokládat kryptografické materiály EU;

b) zajistit, aby byly uplatňovány příslušné postupy a stanoveny způsoby dokládání veškerých kryptografických materiálů EU, bezpečného nakládání s nimi a jejich ukládání a distribuce; a

c) zajišťovat distribuci kryptografických materiálů EU osobám či orgánům, které je využívají, a zpětné převzetí.

Orgán pro bezpečnostní akreditaci

47. Orgán pro bezpečnostní akreditaci je povinen:

a) zajistit, aby komunikační a informační systémy byly v souladu s příslušnými bezpečnostními politikami a bezpečnostními pokyny, vydávat rozhodnutí o schválení komunikačních a informačních systémů pro nakládání s utajovanými informacemi EU do určitého stupně utajení v jejich provozním prostředí, v nichž uvede podmínky akreditace a kritéria, na jejichž základě se vyžaduje opakované schválení;

b) zajistit v souladu s příslušnými politikami bezpečnostní akreditační řízení, přičemž jasně uvede podmínky pro schválení komunikačních a informačních systémů v rámci svých pravomocí;

c) vymezit strategii bezpečnostní akreditace stanovující míru podrobností vyžadovaných v akreditačním řízení, která je přiměřená požadované úrovni zabezpečení;

d) posuzovat a schvalovat bezpečnostní dokumentaci, včetně prohlášení o řízení rizik a zbytkovém riziku, bezpečnostních požadavků pro konkrétní systém (SSRS), dokumentace týkající se ověřování provádění bezpečnostních opatření a bezpečnostních provozních směrnic (SecOPs), a zajistit, aby tato dokumentace byla v souladu s bezpečnostními pravidly a politikami Rady;

e) kontrolovat provádění bezpečnostních opatření souvisejících s komunikačními a informačními systémy tím, že uskuteční nebo zadá bezpečnostní hodnocení, kontroly či revize;

f) stanovovat bezpečnostní požadavky (například stupně utajení informací, pro něž je personál bezpečnostně prověřen) pro pracovní místa citlivá z hlediska bezpečnosti daného komunikačního a informačního systému;

g) potvrzovat výběr schválených kryptografických prostředků a prostředků TEMPEST používaných k zajištění bezpečnosti určitého komunikačního a informačního systému;

h) schvalovat propojení určitého komunikačního a informačního systému s jiným nebo se případně účastnit společného schvalování; a

i) konzultovat s poskytovatelem systému, s aktéry v oblasti bezpečnosti a se zástupci uživatelů otázky týkající se řízení bezpečnostních rizik, zejména zbytkového rizika, a podmínek vydání rozhodnutí o schválení.

48. Orgán pro bezpečnostní akreditaci generálního sekretariátu Rady odpovídá za akreditaci všech komunikačních a informačních systémů provozovaných v rámci generálního sekretariátu Rady.

49. Příslušný orgán pro bezpečnostní akreditaci členského státu odpovídá za akreditaci komunikačních a informačních systémů a jejich komponent provozovaných v daném členském státě.

50. Společná komise pro bezpečnostní akreditaci odpovídá za akreditaci komunikačních a informačních systémů v pravomoci orgánu pro bezpečnostní akreditaci generálního sekretariátu Rady i orgánů pro bezpečnostní akreditaci členských států. Každý členský stát je v této komisi zastoupen jedním zástupcem vnitrostátního orgánu pro bezpečnostní akreditaci a jejích zasedání se účastní zástupce orgánu Komise pro bezpečnostní akreditaci. K účasti jsou přizvány také jiné subjekty s uzlovými body připojení k určitému komunikačnímu a informačnímu systému, který je předmětem jednání.

Komisi pro bezpečnostní akreditaci předsedá zástupce orgánu pro bezpečnostní akreditaci generálního sekretariátu Rady. Komise pro bezpečnostní akreditaci jedná na základě shody zástupců orgánů pro bezpečnostní akreditaci orgánů, členských států a jiných subjektů s uzlovými body připojení k danému komunikačnímu a informačnímu systému. Komise pro bezpečnostní akreditaci předkládá pravidelné zprávy o své činnosti Bezpečnostnímu výboru a oznamuje mu veškerá rozhodnutí o akreditaci.

Provozní orgán pro zabezpečení informací

51. Provozní orgán pro zabezpečení informací každého systému je povinen:

a) vypracovat v rámci akreditačního řízení bezpečnostní dokumentaci v souladu s bezpečnostními politikami a bezpečnostními pokyny, zejména bezpečnostní požadavky pro daný systém, včetně prohlášení o zbytkovém riziku, bezpečnostních provozních směrnic a plánu kryptografické ochrany;

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

c) účastnit se výběru bezpečnostních opatření a zařízení TEMPEST, pokud jsou vyžadovány v bezpečnostní požadavcích pro daný systém, a ve spolupráci s orgánem TEMPEST zajistit jejich bezpečnou instalaci a údržbu;

d) monitorovat provádění a uplatňování bezpečnostních provozních směrnic a může případně plněním povinností souvisejících s provozní bezpečností pověřit vlastníka systému;

e) spravovat kryptografické prostředky a nakládat s nimi, zajistit ochranu kryptografických a kontrolovaných materiálů a případně zajistit vytváření kryptografických proměnných;

f) podle požadavků orgánu pro bezpečnostní akreditaci provádět bezpečnostní analýzy, přezkumy a testování, zejména vypracovávat příslušné zprávy o riziku;

g) poskytovat školení o zabezpečení informací u konkrétních komunikačních a informačních systémů;

h) zavádět bezpečnostní opatření u konkrétních komunikačních a informačních systémů a řídit jejich uplatňování.

PŘÍLOHA V

PRŮMYSLOVÁ BEZPEČNOST

I. ÚVOD

1. Tato příloha stanoví prováděcí pravidla k článku 11. Stanoví obecná bezpečnostní pravidla použitelná pro průmyslové nebo jiné subjekty pro jednání před uzavřením utajovaných smluv a během celého životního cyklu utajovaných smluv uzavíraných generálním sekretariátem Rady.

2. Rada schválí politiku v oblasti průmyslové bezpečnosti, v níž stanoví zejména podrobné požadavky, pokud jde o osvědčení o bezpečnostní prověrce zařízení, seznamy bezpečnostních požadavků, návštěvy, přenos a přenášení utajovaných informací EU.

II. PRVKY UTAJOVANÉ SMLOUVY TÝKAJÍCÍ SE BEZPEČNOSTI

Příručka pro stanovování stupňů utajení

3. Před zahájením nabídkového řízení na uzavření utajované smlouvy nebo před uzavřením takové smlouvy určí generální sekretariát Rady jakožto zadavatel stupeň utajení veškerých informací, které mají být poskytnuty uchazečům a dodavatelům, a rovněž stupeň utajení veškerých informací, které vytvoří dodavatel. Generální sekretariát Rady k tomuto účelu připraví příručku pro stanovování stupňů utajení, která bude použita pro plnění smlouvy.

4. Pro stanovení stupně utajení jednotlivých částí utajované smlouvy se použijí tyto zásady:

   a) při přípravě příručky pro stanovování stupňů utajení bere generální sekretariát Rady v úvahu veškeré důležité bezpečnostní aspekty, včetně stupně utajení, který poskytnutým informacím přidělil původce informací a který původce informací schválil pro danou smlouvu;

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

   c) generální sekretariát Rady se případně spojí s vnitrostátními bezpečnostními orgány/s určenými bezpečnostními orgány členských států nebo s jakýmkoli jiným příslušným bezpečnostním orgánem, dojde-li k jakýmkoli změnám ohledně stupně utajení informací vytvářených dodavateli nebo poskytovaných dodavatelům při plnění smlouvy a provádějí-li se jakékoli dodatečné změny příručky pro stanovování stupňů utajení.

Seznam bezpečnostních požadavků

5. Bezpečnostní požadavky pro konkrétní smlouvu jsou popsány v seznamu bezpečnostních požadavků. Seznam bezpečnostních požadavků případně zahrnuje příručku pro stanovování stupňů utajení a je nedílnou částí utajované smlouvy nebo utajované subdodavatelské smlouvy.

6. Seznam bezpečnostních požadavků obsahuje ustanovení, podle nichž musí dodavatel nebo subdodavatel dodržovat minimální standardy stanovené tímto rozhodnutím. Nedodržení těchto minimálních standardů může být dostatečným důvodem k vypovězení smlouvy.

Bezpečnostní pokyny k programu/projektu

7. V závislosti na rozsahu programů nebo projektů, které zahrnují přístup k utajovaným informacím EU nebo nakládání s nimi či jejich ukládání, může orgán zadávající zakázku a pověřený řízením programu nebo projektu připravit zvláštní bezpečnostní pokyny k programu/projektu. Tyto pokyny vyžadují schválení ze strany vnitrostátních bezpečnostních orgánů/určených bezpečnostních orgánů členských států nebo kteréhokoli jiného příslušného bezpečnostního orgánu, který se účastní daného programu/projektu, a mohou obsahovat další bezpečnostní požadavky.

III. OSVĚDČENÍ O BEZPEČNOSTNÍ PROVĚRCE ZAŘÍZENÍ

8. Osvědčení o bezpečnostní prověrce zařízení vydává vnitrostátní bezpečnostní orgán nebo určený bezpečnostní orgán nebo jakýkoli jiný příslušný bezpečnostní orgán členského státu v souladu s vnitrostátními právními předpisy jako potvrzení o tom, že průmyslový nebo jiný subjekt může ve svých prostorách zajistit ochranu utajovaných informací EU na odpovídajícím stupni utajení (CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET). Je třeba ji předložit generálnímu sekretariátu Rady jakožto zadavateli předtím, než mohou být dodavateli či subdodavateli nebo možnému dodavateli či subdodavateli poskytnuty utajované informace EU nebo než mu je k utajovaným informacím EU umožněn přístup.

9. Před vydáním osvědčení o bezpečnostní prověrce zařízení vnitrostátní bezpečnostní orgán nebo určený bezpečnostní orgán alespoň:

   a) posoudí integritu průmyslového nebo jiného subjektu;

   b) posoudí vlastnické vztahy, kontrolu nebo možný nepatřičný vliv, které by mohly být považovány za bezpečnostní riziko;

c) ověří, že průmyslový nebo jiný subjekt zavedl v daném zařízení bezpečnostní systém, který zahrnuje všechna vhodná bezpečnostní opatření nezbytná pro ochranu informací nebo materiálů se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET v souladu s požadavky stanovenými tímto rozhodnutím;

d) ověří, že byla zajištěna personální bezpečnost u vedoucích pracovníků, vlastníků a zaměstnanců, kteří potřebují mít přístup k informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET, v souladu s požadavky stanovenými v příloze I;

e) ověří, že průmyslový nebo jiný subjekt jmenoval osobu odpovědnou za bezpečnost zařízení, která je odpovědná vedení subjektu za plnění bezpečnostních závazků v prostorách daného subjektu.

10. Generální sekretariát Rady jakožto zadavatel oznámí, pokud to bude nutné, příslušnému vnitrostátnímu bezpečnostnímu orgánu/určenému bezpečnostnímu orgánu nebo kterémukoli jinému příslušnému bezpečnostnímu orgánu, že v předsmluvní fázi nebo při plnění smlouvy bude vyžadováno osvědčení o bezpečnostní prověrce zařízení. V případě, že je během nabídkového řízení třeba poskytovat utajované informace EU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET, je v předsmluvní fázi vyžadováno osvědčení o bezpečnostní prověrce zařízení nebo osvědčení o bezpečnostní prověrce personálu.

11. Zadavatel neuzavře utajovanou smlouvu s upřednostňovaným uchazečem, 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.

12. Vnitrostátní bezpečnostní orgán/určený bezpečnostní orgán nebo kterýkoli jiný příslušný bezpečnostní orgán, který vydal osvědčení o bezpečnostní prověrce zařízení, oznamuje generálnímu sekretariátu Rady jakožto zadavateli změny týkající se osvědčení o bezpečnostní prověrce zařízení. V případě subdodavatelské smlouvy je odpovídajícím způsobem informován vnitrostátní bezpečnostní orgán/určený bezpečnostní orgán nebo kterýkoli jiný příslušný bezpečnostní orgán.

13. 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 generální sekretariát Rady jakožto zadavatel vypověděl utajovanou smlouvu nebo aby vyloučil určitého uchazeče z nabídkového řízení.

IV. UTAJOVANÉ SMLOUVY A UTAJOVANÉ SUBDODAVATELSKÉ SMLOUVY

14. Pokud jsou utajované informace EU poskytovány uchazeči v předsmluvní fázi, musí výzva k předkládání nabídek obsahovat ustanovení o tom, že uchazeč, který nepředloží nabídku nebo jehož nabídka není vybrána, je povinen vrátit ve stanovené lhůtě všechny utajované dokumenty.

15. Jakmile je zadána zakázka na základě utajované smlouvy nebo utajované subdodavatelské smlouvy, generální sekretariát Rady jakožto zadavatel informuje vnitrostátní bezpečnostní orgán/určený bezpečnostní orgán příslušný pro daného dodavatele nebo subdodavatele nebo jakýkoli jiný příslušný bezpečnostní orgán o bezpečnostních ustanoveních utajované smlouvy.

16. V případě ukončení platnosti těchto smluv generální sekretariát Rady jakožto zadavatel (nebo v případě subdodavatelské smlouvy případně vnitrostátní bezpečnostní orgán/určený bezpečnostní orgán nebo kterýkoli jiný příslušný bezpečnostní orgán) uvědomí neprodleně vnitrostátní bezpečnostní orgán/určený bezpečnostní orgán nebo kterýkoli jiný příslušný bezpečnostní orgán členského státu, v němž je dodavatel nebo subdodavatel registrován.

17. Obecně platí, že při ukončení utajované smlouvy nebo utajované subdodavatelské smlouvy musí dodavatel nebo subdodavatel vrátit zadavateli veškeré utajované informace EU v jeho držení.

18. Zvláštní ustanovení týkající se nakládání s utajovanými informacemi EU během plnění smlouvy nebo při jejím ukončení se stanoví v seznamu bezpečnostních požadavků.

19. Pokud je dodavatel nebo subdodavatel oprávněn ponechat si utajované informace EU po ukončení smlouvy, dodavatel nebo subdodavatel nadále dodržuje minimální standardy obsažené v tomto rozhodnutí a chrání důvěrnost utajovaných informací EU.

20. Podmínky, za nichž může dodavatel uzavřít subdodavatelskou smlouvu, jsou stanoveny ve výzvě k předkládání nabídek a ve smlouvě.

21. Předtím než dodavatel zadá jakékoli části utajované smlouvy subdodavateli, musí získat povolení od generálního sekretariátu Rady jakožto zadavatele. Žádná subdodavatelská smlouva nesmí být uzavřena s průmyslovými nebo jinými subjekty registrovanými ve státě, který není členským státem EU a který s EU neuzavřel smlouvu o bezpečnosti informací.

22. 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 zadavatele.

23. Pokud jde o utajované informace EU, které vytvořil nebo s nimiž nakládá dodavatel nebo subdodavatel, pak práva náležející původci vykonává zadavatel.

V. NÁVŠTĚVY V SOUVISLOSTI S UTAJOVANÝMI SMLOUVAMI

24. Pokud generální sekretariát Rady, dodavatelé či subdodavatelé potřebují pro plnění utajované smlouvy 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. Vnitrostátní bezpečnostní orgány/určené bezpečnostní orgány se však mohou v rámci konkrétních projektů dohodnout na postupu, kterým se mohou návštěvy sjednávat přímo.

25. Všechny navštěvující osoby musí být držiteli odpovídajícího osvědčení o bezpečnostní prověrce personálu a musí mít potřebu znát utajované informace EU související se smlouvou uzavřenou generálním sekretariátem Rady.

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

VI. PŘENOS A PŘENÁŠENÍ UTAJOVANÝCH INFORMACÍ EU

27. Pokud jde o elektronický přenos utajovaných informací EU, použijí se příslušná ustanovení článku 10 a přílohy IV.

28. Pokud jde o přenos utajovaných informací EU, použijí se příslušná ustanovení přílohy III v souladu s vnitrostátními právními předpisy.

29. V případě přepravy utajovaných materiálů jako nákladu se při stanovení 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) společnosti zajišťující přepravu jsou držiteli osvědčení o bezpečnostní prověrce zařízení na patřičné úrovni. V takových případech musí být pracovníci nakládající se zásilkou bezpečnostně prověřeni v souladu s přílohou I;

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

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

f) 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.

VII. POSKYTOVÁNÍ UTAJOVANÝCH INFORMACÍ EU DODAVATELŮM SE SÍDLEM V TŘETÍCH STÁTECH

30. Utajované informace EU jsou dodavatelům a subdodavatelům se sídlem v třetích státech poskytovány v souladu s bezpečnostními opatřeními dohodnutými mezi generálním sekretariátem Rady jakožto zadavatelem a vnitrostátním bezpečnostním orgánem/určeným bezpečnostním orgánem dotyčného třetího státu, v němž je dodavatel registrován.

VIII. NAKLÁDÁNÍ S INFORMACEMI SE STUPNĚM UTAJENÍ REISTREINT UE/EU RESTRICTED A JEJICH UKLÁDÁNÍ

31. Generální sekretariát Rady jakožto zadavatel je oprávněn případně ve spojení s vnitrostátním bezpečnostním orgánem/určeným bezpečnostním orgánem dotčeného členského státu vykonávat na základě smluvních ustanovení návštěvy v zařízeních dodavatelů/subdodavatelů s cílem ověřit, že byla zavedena příslušná bezpečnostní opatření na ochranu utajovaných informací EU se stupněm utajení RESTREINT UE/EU RESTRICTED podle požadavků smlouvy.

32. Generální sekretariát Rady jakožto zadavatel informuje vnitrostátní bezpečnostní orgány/určené bezpečnostní orgány nebo kterýkoli jiný bezpečnostní orgán v rozsahu nezbytném podle vnitrostátních právních předpisů o smlouvách či subdodavatelských smlouváchobsahujících informace se stupněm utajení RESTREINT UE/EU RESTRICTED.

33. U smluv zadaných generálním sekretariátem Rady a obsahujících informace se stupněm utajení RESTREINT UE/EU RESTRICTED se pro dodavatele nebo subdodavatele a jejich pracovníky nevyžaduje osvědčení o bezpečnostní prověrce zařízení ani osvědčení o bezpečnostní prověrce personálu.

34. Generální sekretariát Rady jakožto zadavatel posoudí odpovědi na výzvy k předkládání nabídek v souvislosti se zakázkami, které vyžadují přístup k informacím se stupněm utajení RESTREINT UE/EU RESTRICTED, bez ohledu na požadavky týkající se osvědčení o bezpečnostní prověrce zařízení nebo osvědčení o bezpečnostní prověrce personálu, které mohou být stanoveny vnitrostátními právními předpisy.

35. Podmínky, za nichž může dodavatel uzavřít subdodavatelskou smlouvu, se stanoví v souladu s bodem 21.

36. Pokud smlouva zahrnuje nakládání s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED v komunikačním a informačním systému provozovaném dodavatelem, generální sekretariát Rady jakožto zadavatel zajistí, aby ve smlouvě nebo subdodavatelské smlouvě byly uvedeny nezbytné technické a správní požadavky týkající se akreditace komunikačního a informačního systému, které budou přiměřené posouzenému riziku a zohlední všechny příslušné faktory. Zadavatel a příslušný vnitrostátní bezpečnostní orgán/určený bezpečnostní orgán se dohodnou na rozsahu akreditace takového komunikačního a informačního systému.

PŘÍLOHA VI

VÝMĚNA UTAJOVANÝCH INFORMACÍ S TŘETÍMI STÁTY A MEZINÁRODNÍMI ORGANIZACEMI

I. ÚVOD

1. Tato příloha stanoví prováděcí pravidla k článku 12.

II. RÁMCE UPRAVUJÍCÍ VÝMĚNU UTAJOVANÝCH INFORMACÍ

2. Pokud Rada rozhodne, že existuje dlouhodobá potřeba výměny utajovaných informací,

— uzavře se dohoda o bezpečnosti informací, nebo

— uzavře se správní ujednání

v souladu s čl. 12 odst. 2 a s oddíly III a IV a na základě doporučení Bezpečnostního výboru.

3. Pokud mají být utajované informace EU, které byly vytvořeny pro účely operace SBOP, poskytnuty třetím státům nebo mezinárodním organizacím účastnícím se dané operace a neexistuje-li žádný z rámců uvedených v bodě 2, v souladu s oddílem V bude výměna utajovaných informací EU s přispívajícím třetím státem nebo mezinárodní organizací upravena:

— rámcovou dohodou o účasti,

— *ad hoc* dohodou o účasti, nebo

— neexistují-li výše uvedené dohody, *ad hoc* správním ujednáním.

4. Neexistuje-li rámec podle bodů 2 a 3 a rozhodne-li se o vyjímečném *ad hoc* poskytnutí utajovaných informací EU třetímu státu nebo mezinárodní organizaci v souladu s oddílem VI, vyžádá se od daného třetího státu nebo mezinárodní organizace písemné prohlášení o zárukách s cílem zajistit, že budou poskytnuté utajované informace EU chránit v souladu se základními zásadami a minimálními standardy stanovenými tímto rozhodnutím.

III. DOHODY O BEZPEČNOSTI INFORMACÍ

5. Dohody o bezpečnosti informací stanoví základní zásady a minimální standardy upravující výměnu utajovaných informací mezi EU a třetím státem nebo mezinárodní organizací.

6. Dohody o bezpečnosti informací stanoví, že bezpečnostní kancelář generálního sekretariátu Rady, bezpečnostní ředitelství Evropské komise a příslušný bezpečnostní orgán dotyčného třetího státu nebo mezinárodní organizace se dohodnou na technických prováděcích pravidlech. Tato pravidla zohlední úroveň ochrany zajišťovanou platnými bezpečnostními předpisy, strukturami a postupy v dotyčném třetím státě nebo mezinárodní organizaci. Schválí je Bezpečnostní výbor.

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

8. Dohody o bezpečnosti informací stanoví, že před zahájením výměny utajovaných informací v rámci dotyčné dohody se bezpečnostní kancelář generálního sekretariátu Rady a bezpečnostní ředitelství Evropské komise musí shodnout na tom, že přijímající strana je schopna jí poskytované informace řádným způsobem chránit a zabezpečit.

9. Pokud Rada uzavře dohodu o bezpečnosti informací, každá strana zřídí registr, který je při výměně utajovaných informací hlavním přijímacím a odbavovacím místem.

10. Za účelem posouzení účinnosti bezpečnostních předpisů, struktur a postupů v dotyčném třetím státě nebo mezinárodní organizaci vykonává bezpečnostní kancelář generálního sekretariátu Rady spolu s bezpečnostním ředitelstvím Evropské komise na základě vzájemné dohody s dotyčným třetím státem nebo mezinárodní organizací hodnotící návštěvy. Hodnotící návštěvy jsou vykonávány v souladu s příslušnými ustanoveními přílohy III a v jejich průběhu se hodnotí:

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 ovlivnit stanovení stupně utajení informací, jež mohou být vyměňovány;

c) již uplatňovaná bezpečnostní opatření a postupy a

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

11. Tým vykonávající hodnotící návštěvu jménem EU posoudí, zda jsou bezpečnostní předpisy a postupy v dotyčném třetím státě nebo mezinárodní organizaci přiměřené pro zajištění ochrany utajovaných informací EU na příslušné úrovni.

12. Závěry těchto návštěv se uvedou ve zprávě, na jejímž základě stanoví Bezpečnostní výbor nejvyšší stupeň utajovaných informací EU, které mohou být v tištěné podobě nebo případně elektronicky vyměňovány s dotyčnou třetí stranou, a jakékoli zvláštní podmínky upravující výměnu informací s dotyčnou stranou.

13. Předtím než Bezpečnostní výbor schválí prováděcí pravidla, učiní se vše pro vykonání hodnotící návštěvy dotyčného třetího státu nebo mezinárodní organizace za účelem podrobného vyhodnocení bezpečnosti, aby se posoudila povaha a účinnost již zavedeného bezpečnostního systému. Pokud však toto není možné, obdrží Bezpečnostní výbor od bezpečnostní kanceláře generálního sekretariátu Rady co nejpodrobnější zprávu vypracovanou na základě jí dostupných informací, v níž Bezpečnostnímu výboru poskytne informace o příslušných bezpečnostních předpisech a o způsobu organizace bezpečnosti v dotyčném třetím státě nebo mezinárodní organizaci.

14. Bezpečnostní výbor může rozhodnout, že až do posouzení výsledku hodnotící návštěvy nemohou být poskytovány žádné utajované informace EU nebo že mohou být poskytovány utajované informace EU jen do určitého stupně utajení, nebo může stanovit jiné zvláštní podmínky upravující poskytování utajovaných informací EU dotyčnému třetímu státu nebo mezinárodní organizaci. Tuto skutečnost oznámí bezpečnostní kancelář generálního sekretariátu Rady dotyčnému třetímu státu nebo mezinárodní organizaci.

15. Po vzájemné dohodě s dotyčným třetím státem nebo mezinárodní organizací provádí bezpečnostní kancelář generálního sekretariátu Rady pravidelně následné hodnotící návštěvy s cílem ověřit, že uplatňovaná opatření i nadále splňují dohodnuté minimální standardy.

16. Poté co dohoda o bezpečnosti informací vstoupí v platnost a s dotyčným třetím státem nebo mezinárodní organizací jsou vyměňovány utajované informace, může Bezpečnostní výbor rozhodnout, že změní nejvyšší stupeň utajení informací EU, které mohou být vyměňovány v tištěné podobě či elektronicky, zejména s ohledem na některou následnou hodnotící návštěvu.

IV. SPRÁVNÍ UJEDNÁNÍ

17. Pokud v případě třetího státu nebo mezinárodní organizace existuje dlouhodobá potřeba výměny informací, jejichž nejvyšší stupeň utajení není zpravidla vyšší než RESTREINT UE/EU RESTRICTED, a pokud Bezpečnostní výbor potvrdil, že dotyčná strana nemá dostatečně rozvinutý bezpečnostní systém, který by jí umožnil uzavřít dohodu o bezpečnosti informací, může generální tajemník Rady s výhradou souhlasu Rady uzavřít s příslušnými orgány dotyčného třetího státu nebo mezinárodní organizace správní ujednání.

18. Pokud je z naléhavých operativních důvodů třeba urychleně vytvořit rámec pro výměnu utajovaných informací, může Rada ve vyjímečných případech rozhodnout, že správní ujednání lze uzavřít pro výměnu informací s vyšším stupněm utajení.

19. Správní ujednání mají zpravidla formu výměny dopisů.

20. Před zahájením vlastního poskytování utajovaných informací EU dotyčnému třetímu státu nebo mezinárodní organizaci je třeba vykonat hodnotící návštěvu uvedenou v bodě 10 a předložit zprávu Bezpečnostnímu výboru, který ji musí vyhodnotit jako uspokojivou. Pokud však existují vyjímečné důvody pro naléhavou výměnu utajovaných informací, na něž je upozorněna Rada, mohou být utajované informace EU poskytovány pod podmínkou, že bude učiněno vše pro to, aby hodnotící návštěva byla vykonána co nejdříve.

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

V. VÝMĚNA UTAJOVANÝCH INFORMACÍ V RÁMCI OPERACÍ SBOP

22. Účast třetích států nebo mezinárodních organizací na operacích SBOP upravují rámcové dohody o účasti. Tyto dohody obsahují ustanovení o poskytování utajovaných informací EU vytvořených pro účely operací SBOP přispívajícím třetím státům nebo mezinárodním organizacím. Nejvyšší stupeň utajení utajovaných informací EU, které mohou být vyměňovány, je RESTREINT UE/EU RESTRICTED pro civilní operace SBOP a CONFIDENTIEL UE/EU CONFIDENTIAL pro vojenské operace SBOP, pokud rozhodnutí o zřízení jednotlivé operace SBOP nestanoví jinak.

23. *Ad hoc* dohody o účasti uzavřené pro konkrétní operaci SBOP obsahují ustanovení o poskytování utajovaných informací EU vytvořených pro účely dané operace přispívajícímu třetímu státu nebo mezinárodní organizaci. Nejvyšší stupeň utajení utajovaných informací EU, které mohou být vyměňovány, je RESTREINT UE/EU RESTRICTED pro civilní operace SBOP a CONFIDENTIEL UE/EU CONFIDENTIAL pro vojenské operace SBOP, pokud společná akce o zřízení jednotlivé operace SBOP nestanoví jinak.

24. *Ad hoc* správní ujednání o účasti třetího státu nebo mezinárodní organizace na konkrétní operaci SBOP mohou mimo jiné upravovat poskytování utajovaných informací EU vytvořených pro účely dané operace dotyčnému třetímu státu nebo mezinárodní organizaci. Tato *ad hoc* správní ujednání se uzavírají v souladu s postupy uvedenými v bodech 17 a 18 oddílu IV. Nejvyšší stupeň utajení utajovaných informací EU, které mohou být vyměňovány, je RESTREINT UE/EU RESTRICTED pro civilní operace SBOP a CONFIDENTIEL UE/EU CONFIDENTIAL pro vojenské operace SBOP, pokud rozhodnutí o zřízení jednotlivé operace SBOP nestanoví jinak.

25. Ustanovení o poskytování utajovaných informací EU podle bodů 22, 23 a 24 nevyžadují, aby byly před jejich prováděním přijata prováděcí pravidla nebo uskutečněny hodnotící návštěvy.

26. Pokud hostitelský stát, na jehož území je operace SBOP vedena, nemá s EU uzavřenou dohodu o bezpečnosti informací ani správní ujednání o výměně utajovaných informací, může být v případě zvláštní nebo okamžité operační potřeby uzavřeno *ad hoc* správní ujednání. Tato možnost se stanoví v rozhodnutí o zřízení dané operace SBOP. Poskytování utajovaných informací EU za těchto okolností se omezí na informace vytvořené pro účely dané operace SBOP se stupněm utajení nejvýše RESTREINT UE/EU RESTRICTED. V rámci *ad hoc* správního ujednání se hostitelský stát zaváže k ochraně utajovaných informací EU v souladu s minimálními standardy, které nejsou méně přísné než minimální standardy stanovené v tomto rozhodnutí.

27. Podle ustanovení o utajovaných informacích, která jsou součástí rámcových dohod o účasti, *ad hoc* dohod o účasti a *ad hoc* správních ujednání podle bodů 22 až 24, zajistí dotyčný třetí stát nebo mezinárodní organizace, aby jejich personál vyslaný v rámci kterékoli operace chránil utajované informace EU v souladu s bezpečnostními pravidly Rady a s dalšími pokyny vydanými příslušnými orgány, včetně linie velení operace.

28. Pokud je mezi EU a přispívajícím třetím státem nebo mezinárodní organizací následně uzavřena dohoda o bezpečnosti informací, nahradí tato dohoda o bezpečnosti informací v otázkách výměny utajovaných informací EU a nakládání s nimi jakoukoli rámcovou dohodu o účasti, *ad hoc* dohodu o účasti nebo *ad hoc* správní ujednání.

29. Podle rámcové dohody o účasti, *ad hoc* dohody o účasti nebo *ad hoc* správního ujednání s třetím státem nebo mezinárodní organizací není dovolena žádná výměna utajovaných informací EU elektronicky, pokud tak výslovně nestanoví dotyčná dohoda nebo ujednání.

30. Utajované informace EU vytvořené pro účely konkrétní operace SBOP mohou být zpřístupněny pracovníkům vyslaným v rámci dané operace třetími státy nebo mezinárodními organizacemi v souladu s body 22 až 29. Při povolování přístupu těchto pracovníků k utajovaným informacím EU v prostorách nebo v komunikačních a informačních systémech dané operace SBOP je třeba uplatňovat opatření (včetně záznamů o zpřístupněných utajovaných informacích EU) ke zmírnění rizika ztráty nebo ohrožení těchto informací. Tato opatření se stanoví v příslušných plánovacích dokumentech nebo v dokumentech mise.

VI. VYJÍMEČNÉ *AD HOC* POSKYTOVÁNÍ UTAJOVANÝCH INFORMACÍ EU

31. Pokud neexistuje žádný rámec v souladu s oddíly III až V a Rada nebo jeden z jejích přípravných orgánů rozhodne, že je vyjímečně třeba poskytnout utajované informace EU třetímu státu nebo mezinárodní organizaci, generální sekretariát Rady:

a) v možném rozsahu ověří u bezpečnostních orgánů dotyčného třetího státu nebo mezinárodní organizace, že jejich bezpečnostní předpisy, struktury a postupy jsou takové, aby jím poskytnuté utajované informace EU byly chráněny na základě standardů, které nejsou méně přísné než standardy stanovené tímto rozhodnutím;

b) požádá Bezpečnostní výbor, aby na základě dostupných informací vydal doporučení s ohledem na míru důvěry, která může být vložena v bezpečnostní předpisy, struktury a postupy v třetím státě nebo mezinárodní organizaci, jimž mají být poskytnuty utajované informace EU.

32. Pokud Bezpečnostní výbor vydá ohledně poskytnutí utajovaných informací EU kladné doporučení, postoupí se tato záležitost Výboru stálých zástupců, který přijme rozhodnutí o poskytnutí informací.

33. Pokud Bezpečnostní výbor ve svém doporučení vyjádří nesouhlas s poskytnutím utajovaných informací EU:

a) v případě otázek týkajících se SZBP/SBOP projedná záležitost Politický a bezpečnostní výbor, který vypracuje doporučení, jež předloží k rozhodnutí Výboru stálých zástupců;

b) v případě všech ostatních otázek záležitost projedná a rozhodnutí přijme Výbor stálých zástupců.

34. Je-li to považováno za vhodné a vyjádří-li předem písemně souhlas původce, může Výbor stálých zástupců rozhodnout, že utajované informace mohou být poskytnuty pouze v částečném rozsahu nebo za podmínky, že u nich bude nejdříve snížen nebo zrušen stupeň utajení, nebo že informace určené k poskytnutí budou připraveny bez odkazu na zdroj nebo původní stupeň utajení EU.

35. Po rozhodnutí o poskytnutí utajovaných informací EU předá generální sekretariát Rady dotyčný dokument, který nese označení týkající se způsobilosti k poskytnutí 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.

VII. ZMOCNĚNÍ K POSKYTOVÁNÍ UTAJOVANÝCH INFORMACÍ EU TŘETÍM STÁTŮM NEBO MEZINÁRODNÍM ORGANIZACÍM

36. Pokud existuje rámec pro výměnu utajovaných informací se třetím státem nebo mezinárodní organizací v souladu s bodem 2, přijme Rada rozhodnutí o zmocnění generálního tajemníka Rady k poskytování utajovaných informací EU dotyčnému třetímu státu nebo mezinárodní organizaci při dodržení zásady souhlasu původce.

37. Pokud existuje rámec pro výměnu utajovaných informací se třetím státem nebo mezinárodní organizací v souladu s bodem 3, je generální tajemník Rady zmocněn k poskytování utajovaných informací EU v souladu s rozhodnutím o zřízení operace SBOP a při dodržení zásady souhlasu původce.

38. Generální tajemník Rady může přenést tato pověření na vyšší úředníky generálního sekretariátu Rady nebo na jiné jemu podřízené osoby.

Dodatky

Dodatek A

DEFINICE

Pro účely tohoto rozhodnutí se použijí tyto definice:

„akreditací“ se rozumí postup, jehož výsledkem je formální rozhodnutí orgánu pro bezpečnostní akreditaci, že určitý systém se schvaluje do provozu s určitým stupněm utajení, v určitém bezpečnostním módu v jeho provozním prostředí a s přijatelnou úrovní rizika na základě předpokladu, že je uplatňován schválený soubor technických, fyzických, organizačních a procedurálních bezpečnostních opatření;

„aktivem“ se rozumí cokoli s významem pro organizaci, její činnosti a jejich kontinuitu, včetně informačních zdrojů podporujících poslání organizace;

„bezpečnostním provozním módem“ se rozumí vymezení podmínek provozu určitého komunikačního a informačního systému na základě stupňů utajení informací, s nimiž se nakládá, a stupňů bezpečnostní prověrky, formálních schválení přístupu a potřeby jeho uživatelů znát utajované informace. Pro nakládání s utajovanými informacemi nebo pro jejich přenos existují čtyři provozní módy: bezpečnostní provozní mód vyhrazený, bezpečnostní provozní mód s nejvyšší úrovní, bezpečnostní provozní mód s nejvyšší úrovní s formálním řízením přístupu k informacím a bezpečnostní provozní mód víceúrovňový;

— „módem vyhrazeným“ se rozumí provozní mód, v jehož rámci jsou všechny osoby, které mají přístup k určitému komunikačnímu a informačnímu systému, bezpečnostně prověřeny pro nejvyšší stupeň utajení informací, s nimiž daný systém nakládá, a všechny osoby mají společnou potřebu znát všechny informace, s nimiž daný systém nakládá,

— „módem s nejvyšší úrovní“ se rozumí provozní mód, v jehož rámci jsou všechny osoby, které mají přístup k určitému komunikačnímu a informačnímu systému, bezpečnostně prověřeny pro nejvyšší stupeň utajení informací, s nimiž daný systém nakládá, avšak nikoli všechny osoby mající přístup k danému systému mají společnou potřebu znát informace, s nimiž daný systém nakládá; přístup k informacím může schválit jedna určitá osoba,

— „módem s nejvyšší úrovní s formálním řízením přístupu k informacím“ se rozumí provozní mód, v jehož rámci jsou všechny osoby, které mají přístup k určitému komunikačnímu a informačnímu systému, bezpečnostně prověřeny pro nejvyšší stupeň utajení informací, s nimiž daný systém nakládá, avšak nikoli všechny osoby mající přístup k danému systému jsou formálně oprávněny k přístupu ke VŠEM informacím, s nimiž daný systém nakládá; na rozdíl od pravomoci rozhodovat o umožnění přístupu, kterou vykonává jedna určitá osoba, formální oprávnění předpokládá formální centrální správu kontroly přístupu,

— „módem víceúrovňovým“ se rozumí provozní mód, v jehož rámci jsou nikoli všechny osoby s přístupem k určitému komunikačnímu a informačnímu systému bezpečnostně prověřeny pro nejvyšší stupeň utajení informací, s nimiž daný systém nakládá, a nikoli všechny osoby s přístupem k danému systému mají společnou potřebu znát utajované informace, s nimiž daný systém nakládá;

„bezpečnostním šetřením“ se rozumějí postupy šetření prováděné příslušným orgánem členského státu v souladu s jeho právními předpisy za účelem získání záruky, že nejsou známy žádné negativní skutečnosti, které by bránily tomu, aby bylo určité osobě vydáno vnitrostátní osvědčení o o bezpečnostní prověrce personálu nebo o bezpečnostní prověrce personálu EU pro přístup k utajovaným informacím EU až do konkrétního stupně utajení (CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyššího);

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

„dodavatelem“ se rozumí fyzická nebo právnická osoba právně způsobilá k uzavírání smluv;

„dokumentem“ se rozumějí jakékoli zaznamenané informace bez ohledu na jejich fyzickou podobu či povahu;

„držitelem“ se rozumí řádně oprávněná osoba, která jednoznačně potřebuje znát utajované informace EU a má v držení utajované informace EU, a je tedy odpovědná za jejich ochranu;

„evidence“ – viz příloha III bod 18;

„fyzická bezpečnost“ – viz čl. 8 odst. 1;

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

„hrozbou“ se rozumí 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;

„komunikační a informační systém“ – viz čl. 10 odst. 2;

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

„materiálem“ se rozumí jakýkoli dokument nebo část technického zařízení či vybavení, ať vyhotovené, či v procesu zhotovování;

„nakládáním“ s utajovanými informacemi EU se rozumí veškeré možné činnosti, jejichž předmětem mohou být utajované informace EU během celého svého životního cyklu. Zahrnuje jejich vytváření, zpracovávání, přenášení, snížení a zrušení jejich stupně utajení a ničení. V souvislosti s komunikačními a informačními systémy zahrnuje rovněž jejich shromažďování, zobrazení, přenos a ukládání;

„opatřeními TEMPEST“ se rozumí zjišťování, zkoumání a kontrola v souvislosti s kompromitujícím elektromagnetickým vyzařováním a opatření k jeho potlačení;

„operací SBOP“ se rozumí vojenská nebo civilní operace pro řešení krize zřízená podle hlavy V kapitoly 2 Smlouvy o EU;

„osvědčením o bezpečnostní prověrce personálu“ se rozumí jedno z těchto osvědčení nebo obě tato osvědčení:

„osvědčením o bezpečnostní prověrce zařízení“ se rozumí správní rozhodnutí vnitrostátního bezpečnostního orgánu nebo určeného bezpečnostního orgánu, že určité zařízení může z hlediska bezpečnosti zajistit odpovídající úroveň ochrany utajovaných informací EU s určitým stupněm utajení a že pracovníci zařízení, kteří potřebují přístup k utajovaným informacím EU, jsou náležitě bezpečnostně prověřeni a byli poučeni o příslušných bezpečnostních požadavcích nezbytných pro přístup k utajovaným informacím EU a k jejich ochraně;

„personální bezpečnost“ – viz čl. 7 odst. 1;

— „osvědčením o bezpečnostní prověrce personálu EU“ pro přístup k utajovaným informacím EU se rozumí osvědčení vydané orgánem generálního sekretariátu Rady oprávněným ke jmenování přijaté v souladu s tímto rozhodnutím po skončení bezpečnostního šetření vedeného příslušnými orgány členského státu, kterým se osvědčuje, že určité osobě může být za podmínky, že byla zjištěna její potřeba znát utajované informace, 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, která je „bezpečnostně prověřena“,

— „vnitrostátním osvědčením o bezpečnostní prověrkce personálu“ pro přístup k utajovaným informacím EU se rozumí osvědčení vydané příslušným orgánem členského státu přijaté po skončení bezpečnostního šetření prováděného příslušnými orgány členského státu, kterým se osvědčuje, že určité osobě může být za podmínky, že byla zjištěna její potřeba znát utajované informace, 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, která je „bezpečnostně prověřena“;

„potvrzením o bezpečnostní prověrce personálu“ se rozumí potvrzení vydané příslušným orgánem, v němž se uvede, že určitá osoba je bezpečnostně prověřena a je držitelem platného vnitrostátního osvědčení o bezpečnostní prověrce personálu nebo o bezpečnostní prověrce personálu EU, a z něhož je zřejmý stupeň utajení utajovaných informací EU, k nimž může mít tato osoba přístup (CONFIDENTIEL UE / EU CONFIDENTIAL nebo vyšší), doba platnosti příslušného osvědčení o bezpečnostní prověrce personálu a datum, do kdy je platné samotné potvrzení;

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

„propojení“ – viz příloha IV bod 31;

„průmyslová bezpečnost“ – viz čl. 11 odst. 1;

„průmyslovým nebo jiným subjektem“ se rozumí subjekt zapojený do dodávek zboží, provádění prací nebo poskytování služeb; může se jednat o subjekt působící v oblasti průmyslu, obchodu, služeb, vědy, výzkumu, vzdělávání či vývoje nebo o samostatně výdělečně činnou osobu;

„původcem“ se rozumí orgán, agentura nebo instituce EU, členský stát, třetí stát nebo mezinárodní organizace, z jejichž pověření byly utajované informace vytvořeny nebo uvedeny do struktur EU;

„příručkou pro stanovování stupňů utajení“ se rozumí dokument popisující prvky programu nebo smlouvy, které jsou utajované, přičemž stanoví použitelné stupně utajení. Příručka pro stanovování stupňů utajení může být rozšiřována během celé doby trvání programu nebo smlouvy a u jednotlivých prvků informací může dojít ke změně stupně utajení nebo ke snížení stupně utajení; pokud existuje příručka pro stanovování stupňů utajení, je součástí seznamu bezpečnostních požadavků;

„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, že dojde k ohrožením, a dopadu těchto ohrožení;

— „přijetí rizika“ je rozhodnutí, kterým se vyjadřuje souhlas s tím, že po řešení rizika i nadále existuje zbytkové riziko,

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

— „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,

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

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

„snížením stupně utajení“ se rozumí označení informace nižším stupněm utajení;

„správa utajovaných informací“ – viz čl. 9 odst. 1;

„určeným bezpečnostním orgánem“ se rozumí orgán podléhající vnitrostátnímu bezpečnostnímu orgánu členského státu, 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;

„utajované informace EU“ – viz čl. 2 odst. 1;

„utajovanou smlouvou“ se rozumí smlouva mezi generálním sekretariátem Rady a určitým dodavatelem o dodání zboží, provedení prací nebo poskytnutí služeb, jejíž plnění vyžaduje nebo zahrnuje přístup k utajovaným informacím EU nebo jejich vytváření;

„utajovanou subdodavatelskou smlouvou“ se rozumí smlouva mezi dodavatelem generálního sekretariátu Rady a jiným dodavatelem (tj. subdodavatelem) o dodání zboží, provedení prací nebo poskytnutí služeb, jejíž plnění vyžaduje nebo zahrnuje přístup k utajovaným informacím EU nebo jejich vytváření;

„zabezpečení informací“ – viz čl. 10 odst. 1;

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

„zranitelným místem“ se rozumí slabé místo jakékoli povahy, které může být zneužito pro účely jedné nebo několika hrozeb. 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;

„zrušením stupně utajení“ se rozumí odstranění veškerých stupňů utajení;

„životním cyklem komunikačního a informačního systému“ se rozumí celé období existence komunikačního a informačního systému, které zahrnuje uvedení do provozu, vytvoření koncepce, plánování, analýzu požadavků, vytvoření návrhu, vývoj, testování, zavedení, provoz, údržbu a vyřazení z provozu.

Dodatek B

SROVNÁVACÍ TABULKA STUPŇŮ UTAJENÍ

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU 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)	*viz poznámka níže (1)*
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 Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Španělsko	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Francie	Très Secret Défense	Secret Défense	Confidentiel Défense	*viz poznámka níže (3)*
Itálie	Segretissimo	Segreto	Riservatissimo	Riservato
Kypr	Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (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-Ogħla 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
Rumunsko	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu

EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Slovinsko	Strogo tajno	Tajno	Zaupno	Interno
Slovensko	Prísne tajné	Tajné	Dôverné	Vyhradené
Finsko	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÄNG
Švédsko (4)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Spojené království	Top Secret	Secret	Confidential	Restricted

(1) Diffusion Restreinte/Beperkte Verspreiding není v Belgii stupněm utajení. Belgie nakládá s informacemi se stupněm utajení „RESTREINT UE/EU RESTRICTED“ 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“. Francie nakládá s informacemi se stupněm utajení „RESTREINT UE/EU RESTRICTED“ 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.

Dodatek C

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

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
DK-2100 Copenhagen Ø

Tel.: +45 3332 55 66
Fax: +45 339313 20

BULHARSKO
State Commission on Information Security
90 Cherkovna Str.
1505 Sofia

Tel.: +359 29215911
Fax: +359 29873750
E-mail: dksi@government.bg
Website: www.dksi.bg

NĚMECKO
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
11014 Berlin

Tel.: +49 30186810
Fax: +49 3018 6811441
E-mail: oesIII3@bmi.bund.de

ČESKÁ REPUBLIKA
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56 ČESKÁ REPUBLIKA

Tel.: +420 257283335
Fax: +420 257283110
E-mail: czech.nsa@nbu.cz
Website: www.nbu.cz

ESTONSKO
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Tel.: +372 7170113, +372 7170117
Fax: +372 7170213
E-mail: nsa@kmin.ee

IRSKO
National Security Authority
Department of Foreign Affairs
76-78 Harcourt Street
Dublin 2 Ireland

Tel.: +353 14780822
Fax: +353 14082959

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

ŘECKO
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλέφωνα: +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 210652045
+30 2106572009
Fax: +30 2106536279
+30 2106577612

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

ITÁLIE
Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
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 2287643,
+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

LUXEMBURSKO
Autorité nationale de Sécurité
Boîte postale 2379
L-1023 Luxembourg

Tel.: +352 24782210 central
+352 24782253 direct
Fax: +352 24782243

MAĎARSKO
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
1357 Budapest

Tel.: +361 3469652
Fax: +361 3469658
E-mail: nbf@nbf.hu
Website: www.nbf.hu

MALTA
Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta

Tel.: +356 21249844
Fax: +356 25695321

LOTYŠSKO
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
Riga, LV- 001

Tel.: +371 67025418
Fax: +371 67025454
Email: 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 52663201,
+370 52663202
Fax: +370 52663200
E-mail: nsa@vsd.lt

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
NL-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)
2A Rakowiecka St.
00-993 Warszawa

Tel.: +48 225857360
Fax: +48 225858509
E-mail: nsa@abw.gov.pl
Website: www.abw.gov.pl

Służba Kontrwywiadu Wojskowego
(Military Counter-Intelligence Service)
Classified Information Protection Bureau
Oczki 1
PL-02-007 Warszawa

Tel.: +48 226841247
Fax: +48 226841076
E-mail: skw@skw.gov.pl

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
Website: www.orniss.ro

PORTUGALSKO
Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa

Tel: +351 213031710
Fax: +351 213031711

SLOVINSKO
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
Sl-1000 Ljubljana

Tel.: +386 14781390
Fax: +386 14781399

SLOVENSKO
Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava

Tel.: +421 268692314
Fax: +421 26864005
Website: www.nbusr.sk

ŠVÉDSKO
Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
SE-103 39 Stockholm

Tel.: +46 84051000
Fax: +46 87231176
E-mail: ud-nsa@foreign.ministry.se

FINSKO
National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

Telephone 1: +358 916056487
Telephone 2: +358 916056484
Fax: +358 916055140
E-mail: NSA@formin.fi

SPOJENÉ KRÁLOVSTVÍ
UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS

Telephone 1: +44 2072765649
Telephone 2: +44 2072765497
Fax: +44 2072765651
Email: UK-NSA@cabinet-office.x.gsi.gov.uk

Dodatek D

SEZNAM ZKRATEK

SBOP	Společná bezpečnostní a obranná politika
SZBP	Společná bezpečnostní a zahraniční politika