Úřední věstník C 96

Evropské unie

České vydání

Informace a oznámení

Svazek 57

1. dubna 2014

Obsah

II *Sdělení*

SDĚLENÍ ORGÁNŮ, INSTITUCÍ A JINÝCH SUBJEKTŮ EVROPSKÉ UNIE

Evropský parlament

2014/C 96/01 Rozhodnutí předsednictva Evropského parlamentu ze dne 15. dubna 2013 týkající se pravidel pro nakládání s důvěrnými informacemi ze strany Evropského parlamentu 1

CS

II

(Sdělení)

SDĚLENÍ ORGÁNŮ, INSTITUCÍ A JINÝCH SUBJEKTŮ EVROPSKÉ UNIE

EVROPSKÝ PARLAMENT

ROZHODNUTÍ PŘEDSEDNICTVA EVROPSKÉHO PARLAMENTU

ze dne 15. dubna 2013

týkající se pravidel pro nakládání s důvěrnými informacemi ze strany Evropského parlamentu

(2014/C 96/01)

PŘEDSEDNICTVO EVROPSKÉHO PARLAMENTU,

s ohledem na čl. 23 odst. 12 jednacího řádu Evropského parlamentu,

vzhledem k těmto důvodům:

(1) Na základě nové rámcové dohody o vztazích mezi Evropským parlamentem a Evropskou komisí ([1]) podepsané dne 20. října 2010 (dále jen rámcová dohoda) a na základě interinstitucionální dohody mezi Evropským parlamentem a Radou o předávání utajovaných informací Rady v záležitostech, které nespadají do oblasti společné zahraniční a bezpečnostní politiky, Evropskému parlamentu a o jeho nakládání s nimi ([2]) podepsané dne 12. března 2014, (dále jen interinstitucionální dohoda) je nezbytné stanovit zvláštní pravidla pro nakládání s důvěrnými informacemi ze strany Evropského parlamentu.

(2) Lisabonská smlouva ukládá Evropskému parlamentu nové úkoly, a aby mohl Parlament vyvíjet činnost v oblastech vyžadujících určitý stupeň utajení, je nutné stanovit základní zásady, minimální bezpečnostní normy a vhodné postupy pro nakládání s důvěrnými informacemi ze strany Evropského parlamentu, včetně informací utajovaných.

(3) V zájmu hladkého fungování rozhodovacího procesu v Evropské unii mají pravidla stanovená v tomto rozhodnutí zajistit stejnou úroveň ochrany, jako zajišťují pravidla přijatá ostatními orgány, institucemi, úřady a agenturami zřízenými na základě Smluv či členskými státy, a být s těmito pravidly slučitelná.

(4) Ustanoveními tohoto rozhodnutí nejsou dotčeny současné ani budoucí předpisy upravující přístup k dokumentům přijaté v souladu s článkem 15 Smlouvy o fungování Evropské unie (dále jen Smlouva o fungování EU).

([1]) Úř. věst. L 304, 20.11.2010, s. 47.
([2]) Úř. věst. C 95, 1.4.2014, s. 1.

(5) Ustanoveními tohoto rozhodnutí nejsou dotčeny současné ani budoucí předpisy upravující ochranu osobních údajů přijaté v souladu s článkem 16 Smlouvy o fungování EU,

PŘIJALO TOTO ROZHODNUTÍ:

Článek 1

Cíl

Toto rozhodnutí upravuje správu a nakládání s důvěrnými informacemi ze strany Evropského parlamentu, mj. vznik, přijímání, předávání a uchovávání těchto informací s cílem zajistit odpovídající ochranu důvěrné povahy těchto informací. Provádí interinstitucionální dohodu a rámcovou dohodu a zejména přílohu II této dohody.

Článek 2

Definice

Pro účely tohoto rozhodnutí se:

a) informacemi rozumějí jakékoli písemné nebo ústně předané informace, bez ohledu na druh nosiče, na kterém jsou uchovávány, a bez ohledu na jejich původce;

b) důvěrnými informacemi rozumějí utajované informace a jiné důvěrné informace nepodléhající utajení;

c) utajovanými informacemi rozumějí utajované informace EU (UIEU) a rovnocenné utajované informace;

d) utajovanými informacemi EU (UIEU) rozumějí jakékoli informace a materiály označené stupněm utajení TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL nebo RESTREINT UE/EU RESTRICTED, jejichž neoprávněné vyzrazení by mohlo na různých stupních ohrozit zájmy Unie nebo zájmy jednoho či více jejích členských států, bez ohledu na to, zda tyto informace a materiály pocházejí od orgánů, institucí, úřadů nebo agentur zřízených na základě Smluv. V tomto ohledu jsou informace a materiály označené stupněm:

— TRÈS SECRET UE/EU TOP SECRET informace a materiály, jejichž neoprávněné vyzrazení by mohlo mimořádně závažně poškodit základní zájmy Unie nebo jednoho či více jejích členských států;

— SECRET UE/EU SECRET informacemi a materiály, jejichž neoprávněné vyzrazení by mohlo vážně poškodit základní zájmy Unie nebo jednoho či více jejích členských států;

— CONFIDENTIEL UE/EU CONFIDENTIAL informace a materiály, jejichž neoprávněné vyzrazení by mohlo poškodit základní zájmy Unie nebo jednoho či více jejích členských států;

— RESTREINT UE/EU RESTRICTED informace a materiály, jejichž neoprávněné vyzrazení by mohlo být nevýhodné vzhledem k zájmům Unie nebo jednoho či více jejích členských států;

e) rovnocennými utajovanými informacemi rozumějí utajované informace od členských států, třetích států nebo mezinárodních organizací, které mají stupeň utajení rovnocenný jednomu ze stupňů utajení používaných pro UIEU a které byly předány Evropskému parlamentu Radou nebo Komisí;

f) jinými důvěrnými informacemi rozumějí jakékoli jiné důvěrné informace nepodléhající utajení, včetně informací, na něž se vztahují právní předpisy na ochranu údajů nebo profesní tajemství, které vzniknou v Evropském parlamentu nebo jsou Evropskému parlamentu předány jinými orgány, institucemi, úřady a agenturami zřízenými na základě Smluv či členskými státy;

g) dokumentem rozumí jakékoli zaznamenané informace, bez ohledu na jejich fyzickou podobu nebo vlastnosti;

h) materiálem rozumí jakýkoli dokument nebo část technického zařízení či vybavení, ať vyhotovené, či v procesu zhotovování;

i) potřebou vědět rozumí potřeba určité osoby mít přístup k důvěrným informacím, aby byla schopna vykonávat úřední funkci nebo provést úkol;

j) osvědčením rozumí rozhodnutí, které v případě poslanců Evropského parlamentu přijímá jeho předseda nebo v případě úředníků Evropského parlamentu a ostatních zaměstnanců Evropského parlamentu pracujících pro politické skupiny generální tajemník a na jehož základě se jednotlivcům povoluje přístup k utajovaným informacím až do určitého stupně utajení, a to poté, co projdou bezpečnostní prověrkou provedenou vnitrostátním orgánem v souladu s vnitrostátním právem a s ustanoveními obsaženými v příloze I části 2;

k) snížením stupně utajení rozumí přiřazení nižšího stupně utajení;

l) odtajněním rozumí odstranění jakéhokoli utajení;

m) označením rozumí značka, jíž jsou opatřeny jiné důvěrné informace a podle níž se pozná, jakými předem stanovenými specifickými pokyny se má řídit nakládání s těmito informacemi nebo jaké oblasti se daný dokument týká. Mohou jí být opatřeny rovněž utajované informace na znamení toho, že nakládání s nimi podléhá ještě dalším požadavkům.

n) zrušením označení rozumí odstranění jakéhokoli označení;

o) původcem rozumí řádně zmocněný autor důvěrných informací;

p) bezpečnostním upozorněním rozumějí prováděcí opatření stanovená v příloze II;

q) pokyny pro nakládání rozumějí technické pokyny vydané pro útvary Parlamentu týkající se správy důvěrných informací.

Článek 3

Základní zásady a minimální normy

1. Nakládání s důvěrnými informacemi ze strany Evropského parlamentu se řídí základními zásadami a minimálními normami stanovenými v příloze I části 1.

2. Evropský parlament na základě uvedených základních zásad a minimálních norem stanoví systém pro řízení bezpečnosti informací (ISMS). ISMS sestává z bezpečnostních upozornění, pokynů pro nakládání a příslušných ustanovení jednacího řádu. Cílem ISMS je usnadňovat parlamentní a správní činnost a zajišťovat ochranu veškerých důvěrných informací, s nimiž Evropský parlament pracuje, přičemž budou plně dodržována pravidla, jež původce daných informací stanoví v bezpečnostních upozorněních.

Zpracovávání důvěrných informací automatickými komunikačními a informačními systémy (CIS) Evropského parlamentu stanovené v bezpečnostním upozornění 3 se provádí v souladu s koncepcí zabezpečení informací (IA).

3. Poslanci Evropského parlamentu se mohou seznámit s utajovanými informacemi až do stupně utajení RESTREINT UE/EU RESTRICTED včetně, aniž by prošli bezpečnostní prověrkou.

4. Pokud je dotčená informace označená stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo se stupněm rovnocenným, přístup se umožní těm poslancům Evropského parlamentu, kteří obdrželi osvědčení od předsedy Parlamentu podle odstavce 5 nebo předem podepsali čestné prohlášení, že nevyzradí obsah těchto informací třetím osobám, že dodrží povinnost chránit informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a že jsou si vědomi důsledků v případě opačného jednání.

5. Pokud je dotčená informace označená stupněm utajení SECRET UE/EU SECRET nebo TRÈS SECRET/EU TOP SECRET nebo se stupněm rovnocenným, přístup se umožní těm poslancům Evropského parlamentu, kteří obdrželi osvědčení od předsedy Parlamentu poté, co:

a) prošli bezpečnostní prověrkou v souladu s přílohou I částí 2 tohoto rozhodnutí, nebo

b) příslušný vnitrostátní orgán oznámil, že jsou k tomu dotčení poslanci řádně oprávněni z titulu své funkce v souladu s vnitrostátními právními předpisy.

6. Před poskytnutím přístupu k utajovaným informacím musí být poslanci Evropského parlamentu seznámeni se svou odpovědností za ochranu těchto informací a musí prohlásit, že si jsou vědomi odpovědnosti ohledně ochrany těchto informací v souladu s přílohou I. Rovněž musí být seznámeni s tím, jakými prostředky se tato ochrana zajišťuje.

7. Úředníci Evropského parlamentu a ostatní zaměstnanci Parlamentu, kteří pracují pro politické skupiny, mohou pracovat s důvěrnými informacemi, mají-li prokazatelnou potřebu vědět, a s informacemi označenými vyšším stupněm utajení než RESTREINT UE/EU RESTRICTED, mají-li odpovídající bezpečnostní prověrku. Přístup k utajovaným informacím je poskytnut, pouze pokud byli seznámeni se svou odpovědností za ochranu těchto informací a s prostředky, kterými se tato ochrana zajišťuje, a obdrželi v tomto směru písemné pokyny a pokud podepsali prohlášení, v němž potvrzují převzetí těchto pokynů a zavazují se je dodržovat v souladu se stávajícími pravidly.

Článek 4

Vznik důvěrných informací a nakládání s nimi na administrativní úrovni Evropského parlamentu

1. Předseda Evropského parlamentu, předsedové příslušných parlamentních výborů a generální tajemník nebo jakákoli osoba, která jimi byla řádně písemně oprávněna, může být původcem důvěrných informací a utajovaných informací, které jsou popsány v bezpečnostních upozorněních.

2. Původce utajovaných informací při jejich vzniku použije vhodný stupeň utajení v souladu s mezinárodními normami a definicemi uvedenými v příloze I. Původce utajovaných informací při jejich vzniku rovněž zpravidla určí osoby, které jsou oprávněny se seznámit s informacemi odpovídajícími danému stupni utajení. Tyto informace jsou předány oddělení pro důvěrné informace (CIU) v okamžiku, kdy je dokument v CIU uložen.

3. S jinými důvěrnými informacemi, na které se vztahuje profesní tajemství, se nakládá v souladu s přílohami I a II a s příslušnými pokyny.

Článek 5

Přijímání důvěrných informací ze strany Evropského parlamentu

1. Důvěrné informace, které Evropský parlament obdrží, jsou sděleny:

a) sekretariátu orgánu či funkcionáři Parlamentu, který podal žádost, nebo přímo oddělení CIU, jedná-li se o informace se stupněm utajení RESTREINT UE/EU RESTRICTED nebo se stupněm rovnocenným a jiné důvěrné informace;

b) oddělení CIU, jedná-li se o informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE / EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET nebo se stupni jim rovnocennými.

2. Registraci, uchovávání a vysledovatelnost důvěrných informací zajišťuje případ od případu buď sekretariát orgánu nebo funkcionáře Parlamentu, kteří tyto informace obdrželi, nebo oddělení CIU.

3. Dohodnutá ujednání, která mají být stanovená společnou dohodou s cílem zajištit zachování důvěrnosti informací jsou v případě důvěrných informací, které sděluje Komise podle bodu 3.2 přílohy II rámcové dohody, nebo v případě utajovaných informací, které předává Rada podle čl. 5 odst. 4 interinstitucionální dohody, uložena společně s důvěrnými informacemi na sekretariátu orgánu nebo funkcionáře Parlamentu, popřípadě na oddělení CIU.

4. Opatření uvedené v odstavci 3 mohou být obdobně použita i pro sdělování důvěrných informací ze strany jiných institucí a orgánů EU, úřadů a agentur zřízených na základě Smluv nebo členskými státy.

5. S cílem zajistit úroveň ochrany odpovídající stupni utajení TRÈS SECRET UE/EU TOP SECRET nebo stupni rovnocennému zřídí Konference předsedů výbor pro dohled. Informace se stupněm utajení TRÈS SECRET UE/EU TOP SECRET nebo se stupněm rovnocenným se sdělují Evropskému parlamentu v souladu s dalšími ujednáními mezi Evropským parlamentem a orgánem Unie, od které byly tyto informace obdrženy.

Článek 6

Předávání utajovaných informací Evropským parlamentem třetím stranám

S předchozím souhlasem původce příslušných utajovaných informací, popřípadě orgány Unie, která je Evropskému parlamentu sdělila, může Evropský parlament předat tyto utajované informace třetím stranám pod podmínkou, že tyto strany zajistí, aby byla při nakládání s těmito informacemi v rámci jejich útvarů a v jejich prostorách dodržována pravidla rovnocenná pravidlům uvedeným v tomto rozhodnutí.

Článek 7

Zabezpečené prostory

1. Pro účely správy důvěrných informací zřídí Evropský parlament zabezpečený prostor a zabezpečené čítárny.

2. V zabezpečeném prostoru je k dispozici zařízení a vybavení pro registraci, prohlížení, archivaci a předávání důvěrných informací a nakládání s nimi. Je v něm mimo jiné čítárna a zasedací místnost, v nichž se lze seznámit s utajovanými informacemi, a spravuje jej oddělení CIU.

3. Mimo tento zabezpečený prostor mohou být zřízeny zabezpečené čítárny, v nichž se lze seznámit s informacemi až do stupně utajení RESTREINT UE/EU RESTRICTED nebo stupně rovnocenného a s jinými důvěrnými informacemi. Tyto zabezpečené čítárny spravují příslušné útvary sekretariátů orgánu nebo funkcionářů Parlamentu, popřípadě oddělení CIU. Nesmějí v nich být k dispozici kopírky, telefony, faxy, skenery nebo jakékoli jiné technické vybavení k rozmnožování nebo předávání dokumentů.

Článek 8

Registrace důvěrných informací, nakládání s nimi a jejich uchovávání

1. Informace se stupněm utajení RESTREINT UE/EU RESTRICTED nebo se stupněm rovnocenným a jiné důvěrné informace registrují a uchovávají příslušné útvary sekretariátů orgánu nebo funkcionáře Parlamentu nebo oddělení CIU, podle toho, kdo dané informace obdržel.

2. Na nakládání s informacemi se stupněm utajení RESTREINT EU/EU RESTRICTED nebo se stupněm rovnocenným a s jinými důvěrnými informacemi se vztahují tyto podmínky:

a) dokumenty se předávají osobně předány vedoucímu sekretariátu, který je zaregistruje a vydá potvrzení o přijetí;

b) pokud tyto dokumenty nejsou právě používány, sekretariát je na svou odpovědnost uschová na uzamčeném místě;

c) dané informace nesmějí být v žádném případě uloženy na jiný nosič ani předány jiné osobě. Takovéto dokumenty smí být kopírovány pouze na zařízení s příslušným oprávněním vymezeném v bezpečnostních upozorněních;

d) přístup k těmto informacím je omezen na osoby, které určil jejich původce nebo orgán Unie, která je Evropskému parlamentu sdělila, v souladu s ujednáními uvedenými v čl. 4 odst. 2 nebo čl. 5 odst. 3, 4 a 5;

e) sekretariát orgánu nebo funkcionáře Parlamentu vede záznamy o osobách, které se seznámily s příslušnými informacemi, a datech a hodinách, kdy se tak stalo. Sekretariáty daného orgánu nebo funkcionáře Parlamentu předají tyto záznamy oddělení CIU v okamžiku ukládání daných informací v oddělení CIU.

3. Informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET nebo se stupněm rovnocenným registruje, nakládá s nimi a uchovává oddělení CIU v zabezpečeném prostoru, v souladu s konkrétním stupněm utajení a tak, jak stanoví bezpečnostní upozornění.

4. V případě porušení pravidel uvedených v odstavcích 1 až 3 informuje příslušného pracovníka sekretariátu orgánu nebo funkcionáře Parlamentu, popřípadě oddělení CIU generálního tajemníka, který v případě, že se jedná o poslance Evropského parlamentu, záležitost postoupí předsedovi Parlamentu.

Článek 9

Přístup do zabezpečených prostor

1. Přístup do zabezpečeného prostoru mají pouze:

a) osoby, které jsou podle čl. 3 odst. 3 až 7 oprávněné seznamovat se s informacemi tam uchovávanými a které předložily žádost podle čl. 10 odst. 1;

b) osoby, které jsou podle čl. 4 odst. 1 oprávněny vytvářet utajované informace a které předložily žádost podle čl. 10 odst. 1;

c) úředníci Evropského parlamentu z oddělení CIU;

d) úředníci Evropského parlamentu odpovědní za řízení oddělení CIS;

e) v případě potřeby úředníci Evropského parlamentu odpovědní za obecnou a požární bezpečnost;

f) pracovníci úklidu, ale pouze v přítomnosti a pod dohledem úředníka pracujícího v oddělení CIU.

2. Oddělení CIU může odepřít přístup do zabezpečeného prostoru komukoli, kdo nemá oprávnění do něj vstoupit. Jakákoli námitka proti odepření vstupu se předkládá v případě žádosti o přístup podané poslanci Evropského parlamentu předsedovi Parlamentu a v ostatních případech generálnímu tajemníkovi.

3. Generální tajemník může povolit schůzi omezeného počtu osob v zasedací místnosti nacházející se v zabezpečeném prostoru.

4. Přístup do zabezpečené čítárny mají pouze:

a) poslanci Evropského parlamentu, úředníci Evropského parlamentu a ostatní zaměstnanci Evropského parlamentu pracující pro politické skupiny, kteří se řádně prokáží oprávněním pro účely seznámení se s důvěrnými informacemi nebo jejich vytváření;

b) úředníci Evropského parlamentu odpovědní za řízení oddělení CIS, úředníci sekretariátu orgánu nebo funkcionáře Parlamentu, který dané informace obdržel, a úředníci oddělení CIU;

c) v případě potřeby úředníci Evropského parlamentu odpovědní za obecnou a požární bezpečnost;

d) pracovníci úklidu, ale pouze v přítomnosti a pod dohledem úředníka pracujícího v sekretariátu orgánu nebo funkcionáře Parlamentu, popřípadě v oddělení CIU.

5. Příslušný sekretariát orgánu nebo funkcionáře Parlamentu, popřípadě oddělení CIU mohou odepřít přístup do zabezpečené čítárny komukoli, kdo nemá oprávnění do něj vstoupit. Jakákoli námitka proti odepření vstupu se předkládá v případě žádosti o přístup podané poslanci Evropského parlamentu předsedovi Parlamentu a v ostatních případech generálnímu tajemníkovi.

Článek 10

Seznámení se s důvěrnými informacemi a jejich vytváření v zabezpečených prostorách

1. Každá osoba, která má zájem se v zabezpečeném prostoru seznámit s důvěrnými informacemi nebo je vytvářet, sdělí předem své jméno oddělení CIU. Oddělení CIS zkontroluje totožnost každé osoby, která podá žádost, a ověří, zda je daná osoba oprávněna podle ujednání uvedených v čl. 3 odst. 3 až 7, v čl. 4 odst. 1 nebo v čl. 5 odst. 3, 4 a 5 se s důvěrnými informacemi seznámit nebo je vytvářet.

2. Každá osoba, která má zájem v souladu s čl. 3 odst. 3 až 7 seznámit se v zabezpečené čítárně s důvěrnými informacemi se stupněm utajení RESTREINT EU/EU RESTRICTED nebo se stupněm rovnocenným a s jinými důvěrnými informacemi, sdělí předem své jméno příslušným útvarům sekretariátů orgánu nebo funkcionáře Parlamentu nebo oddělení CIU.

3. S výjimkou mimořádných okolností (např. v případě četných žádostí o zpřístupnění podaných během krátké doby) smějí být důvěrné informace zpřístupněny v zabezpečeném prostoru vždy jen jedné osobě v přítomnosti úředníka sekretariátu daného orgánu nebo funkcionáře Parlamentu nebo oddělení CIU.

4. Během čtení jsou zakázány kontakty s vnějším prostředím (mimo jiné prostřednictvím telefonů nebo jiných technologických zařízeních), pořizování si poznámek, kopírování a fotografování zpřístupněných důvěrných informací.

5. Dříve, než bude osobě povoleno opustit zabezpečený prostor, se odpovědný úředník sekretariátu daného orgánu nebo funkcionáře Parlamentu nebo oddělení CIU přesvědčí, zda jsou důvěrné informace, s kterými se osoba seznamovala, na místě, a zkontroluje, zda jsou neporušené a úplné.

6. V případě porušení výše uvedených pravidel informuje úředník sekretariátu daného orgánu nebo funkcionáře Parlamentu nebo oddělení CIU generálního tajemníka, který v případě, že se jedná o poslance Evropského parlamentu, záležitost postoupí předsedovi Parlamentu.

Článek 11

Minimální standardy pro jiné zpřístupnění důvěrných informací na neveřejné schůzi mimo zabezpečené prostory

1. S informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED nebo se stupněm rovnocenným a s jinými důvěrnými informacemi se mohou poslanci parlamentních výborů nebo jiných politických a administrativních orgánů Evropského parlamentu seznámit na neveřejné schůzi mimo zabezpečené prostory.

2. V případě uvedeném v odstavci 1 zajistí sekretariát orgánu nebo funkcionáře Parlamentu odpovědný za toto jednání, aby byly dodrženy tyto podmínky:

a) do zasedací místnosti, v níž se koná toto jednání, mají přístup pouze osoby určené předsedajícím příslušného výboru či orgánu;

b) veškeré dokumenty jsou očíslovány, rozdány na začátku schůze a na jejím konci opět vybrány a na jejich základě nejsou pořizovány žádné poznámky, ani nejsou pořizovány žádné jejich fotokopie či fotografie;

c) zápis ze schůze neobsahuje žádnou zmínku o obsahu diskuse týkající se informací projednávaných důvěrným postupem. Zaznamená se pouze příslušné rozhodnutí, pokud bylo přijato;

d) důvěrné informace poskytované příjemcům v Evropském parlamentu ústně podléhají stejné míře ochrany jako důvěrné informace poskytované písemnou formou;

e) v zasedacích místnostech nesmí být žádný další soubor dokumentů;

f) na začátku schůze se účastníkům a tlumočníkům rozdá pouze nezbytně nutný počet výtisků dokumentů;

g) na začátku schůze předsedající jasně sdělí, jaký stupeň utajení a jaké označení příslušné dokumenty mají;

h) účastníci neodnášejí dokumenty ze zasedací místnosti;

i) na konci schůze sekretariát orgánu nebo funkcionáře Parlamentu vybere všechny výtisky dokumentů a vykázat jejich úplný počet; a

j) do zasedací místnosti, v níž se mají seznámit s danými důvěrnými informacemi nebo o nich mají jednat, s sebou účastníci schůze ne neberou žádná elektronická komunikační zařízení ani jiná elektronická zařízení.

3. Pokud se v souladu s výjimkami uvedenými v bodě 3.2.2 přílohy II rámcové dohody a v čl. 6 odst. 5 interinstitucionální dohody projednávají na neveřejné schůzi informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo se stupněm rovnocenným, sekretariát orgánu nebo funkcionáře Parlamentu odpovědný za toto jednání kromě ustanovení stanovených v odstavci 2 zajistí, aby určené osoby, které se mohou dané schůze zúčastnit, splňovaly požadavky čl. 3 odst. 3 a 7.

4. V případě uvedeném v odstavci 3 poskytne oddělení CIU sekretariátu orgánu nebo funkcionáře Parlamentu odpovědnému za dané neveřejné jednání požadovaný počet výtisků dokumentů, které mají být předmětem jednání, a tyto výtisky musí být po schůzi vráceny oddělení CIU.

Článek 12

Archivování důvěrných informací

1. Bezpečný systém archivování je zajištěn v zabezpečeném prostoru. Správu zabezpečených archivů zajišťuje oddělení CIU podle standardních kritérií pro archivování.

2. Utajované informace, které byly s konečnou platností uloženy na oddělení CIU a informace se stupněm utajení RESTREINT UE/EU RESTRICTED nebo se stupněm rovnocenným uložené na sekretariátu orgánu či funkcionáře Parlamentu, jsou šest měsíců poté, co byly naposledy zpřístupněny, nejpozději však jeden rok po uložení, přemístěny do zabezpečeného archivu v zabezpečeném prostoru. Jiné důvěrné informace, nejsou-li uloženy na oddělení CIU, jsou archivovány dotčeným sekretariáty příslušného orgánu či funkcionáře Parlamentu v souladu s obecnými předpisy pro správu dokumentů.

3. Do zabezpečených archivů obsahujících důvěrné informace lze nahlížet za následujících podmínek:

a) jsou k tomu oprávněny pouze osoby, které jsou v průvodním výkazu vyplněném při uložení důvěrných informací identifikovány na základě jména, pracovní pozice nebo své funkce;

b) žádost o nahlédnutí musí být předložena oddělení CIU, které zajistí dodání příslušného dokumentu do zabezpečené čítárny a;

c) použijí se postupy a podmínky pro zpřístupnění důvěrných informací stanovené v článku 10.

Článek 13

Snížení stupně utajení, odtajnění a zrušení označení důvěrných informací

1. Snížit stupeň utajení důvěrných informací, odtajnit je nebo zrušit jejich označení lze pouze s předchozím souhlasem jejich původce a, je-li to nezbytné, po konzultaci s ostatními zúčastněnými stranami.

2. Snížení stupně utajení nebo odtajnění musí být potvrzeno písemně. Původce odpovídá za to, že příjemci dokumentu budou informováni o změně stupně utajení, a příjemci jsou povinni na tuto změnu upozornit další příjemce, kterým předali originál dokumentu nebo jeho kopii. Je-li to možné, uvede původce na utajovaný dokument datum, lhůtu či událost, po jejichž uplynutí lze snížit stupeň utajení nebo odtajnit skutečnosti, které obsahuje. Jinak posuzuje tuto otázku nejpozději každých pět let, aby zjistil, zda je původní utajení nadále nezbytné.

3. Důvěrné informace v zabezpečených archivech jsou po patřičné době, a to nejpozději 25. rok po datu jejich vzniku, prozkoumány s cílem rozhodnout, zda by neměly být odtajněny, neměl by být snížen stupeň jejich utajení nebo by nemělo být zrušeno jejich označení. K prozkoumání a zveřejnění takových informací dojde v souladu s ustanoveními nařízení Rady (EHS, Euratom) č. 354/83 ze dne 1. února 1983 o otevření historických archivů Evropského hospodářského společenství a Evropského společenství pro atomovou energii veřejnosti ([1]). Odtajnění provede původce utajovaných informací nebo útvar, který bude v té době k dané věci příslušný, v souladu s přílohou I částí 1 oddílem 10.

4. Po odtajnění jsou dříve utajené informace uložené v zabezpečeném archivu přemístěny do historických archivů Evropského parlamentu k trvalému uchování a dalšímu zpracování podle příslušných předpisů.

5. Po zrušení označení se na dřívější jiné důvěrné informace vztahují předpisy Evropského parlamentu pro správu dokumentů.

Článek 14

Narušení bezpečnosti, ztráta nebo ohrožení důvěrných informací

1. V případě, že se narušení důvěrnosti v obecném smyslu a konkrétně porušení tohoto rozhodnutí dopustí poslanec Evropského parlamentu, použijí se příslušná ustanovení jednacího řádu Evropského parlamentu týkající se sankcí.

2. V případě porušení těchto pravidel ze strany zaměstnanců se použijí postupy a sankce stanovené ve služebním řádu úředníků a v pracovním řádu ostatních zaměstnanců Evropské unie, stanovené v nařízení (EHS, Euratom, ESUO) č. 259/68 ([2]) (dále jen služební řád).

([1]) Úř. věst. L 43, 15.2.1983, s. 1.
([2]) Úř. věst. L 56, 4.3.1968, s. 1.

3. Nezbytná šetření v případě narušení či porušení vymezeného v bezpečnostním upozornění 6 zajistí předseda Parlamentu nebo generální tajemník.

4. Pokud byly důvěrné informace sděleny Evropskému parlamentu orgánem Unie nebo členským státem, předseda Parlamentu nebo generální tajemník informují daný orgán Unie nebo členský stát o jakékoli prokázané či domnělé ztrátě nebo ohrožení utajovaných informací a o výsledcích příslušného vyšetřování a opatřeních, která byla přijata, aby se taková situace neopakovala.

Článek 15

Úpravy tohoto rozhodnutí a jeho prováděcích pravidel a podávání výročních zpráv o uplatňování tohoto rozhodnutí

1. Generální tajemník podává návrh na veškeré nezbytné úpravy tohoto rozhodnutí a prováděcích pravidel stanovených v přílohách a předává tyto návrhy předsednictvu ke schválení.

2. Generální tajemník odpovídá za provedení tohoto rozhodnutí v útvarech Evropského parlamentu a vydá pokyny pro nakládání s důvěrnými informacemi, pokud jde o záležitosti, na něž se vztahuje systém pro řízení bezpečnosti informací (ISMS), v souladu se zásadami stanovenými v tomto rozhodnutí.

3. Generální tajemník předkládá předsednictvu výroční zprávu o uplatňování tohoto rozhodnutí.

Článek 16

Přechodná a závěrečná ustanovení

1. Informace nepodléhající utajení, které jsou v držení oddělení pro důvěrné informace (CIU) nebo jakéhokoli jiného archívu Evropského parlamentu, jež jsou považovány za důvěrné a datovány před 1. dubna 2014, se pro účely tohoto rozhodnutí považují za jiné důvěrné informace. Původce může stupeň důvěrnosti kdykoliv přehodnotit.

2. Odchylně od čl. 5 odst. 1 písm. a) a čl. 8 odst. 1 tohoto rozhodnutí budou po dobu dvanácti měsíců od 1. dubna 2014 informace poskytnuté Radou v souladu s interinstitucionální dohodou označeny stupněm utajení RESTREINT UE/EU RESTRICTED, nebo rovnocenným stupněm utajení, a předány, zaregistrovány a uloženy na oddělení pro důvěrné informace (CIU). S těmito informacemi je možno se seznámit v souladu s čl. 4 odst. 2 písm. a) a c) a čl. 5 odst. 4 interinstitucionální dohody.

3. Rozhodnutí předsednictva ze dne 6. června 2011, kterým se stanoví pravidla pro nakládání s důvěrnými informacemi ze strany Evropského parlamentu, se zrušuje.

Článek 17

Vstup v platnost

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

PŘÍLOHA I

Část 1

ZÁKLADNÍ ZÁSADY A MINIMÁLNÍ BEZPEČNOSTNÍ NORMY NA OCHRANY DŮVĚRNÝCH INFORMACÍ

1. **ÚVOD**

Tato ustanovení vymezují základní zásady a minimální bezpečnostní normy na ochranu důvěrných informací, které Evropský parlament respektuje a dodržuje ve všech svých pracovních místech a rovněž všichni příjemci utajovaných informací a jiných důvěrných informací tak, aby byla zajištěna bezpečnost a aby měly všechny dotčené osoby jistotu, že byly vytvořeny společné normy ochrany. Doplňují je bezpečnostní upozornění obsažená v příloze II a jiná ustanovení upravující nakládání s důvěrnými informacemi ze strany parlamentních výborů a jiných orgánů a funkcionářů Parlamentu.

2. **OBECNÉ ZÁSADY**

Politika Evropského parlamentu v oblasti bezpečnosti je nedílnou součástí jeho obecné politiky vnitřního řízení, a vychází tedy ze zásad upravujících tuto obecnou politiku. Mezi tyto zásady patří legalita, transparentnost, odpovědnost, subsidiarita a proporcionalita.

Legalita znamená nezbytnost přísného dodržování právního rámce při výkonu bezpečnostních funkcí a nutnost dodržovat platné požadavky právních norem. Mimoto odpovědnost v oblasti bezpečnosti musí být založena na řádných právních ustanoveních. V tomto případě plně uplatní ustanovení služebního řádu, zejména článek 17 týkající se povinnosti úředníků zachovávat mlčenlivost o informacích obdržených v souvislosti s výkonem svých služebních povinností a hlava VI tohoto řádu týkající se disciplinárních opatření. Konečně to znamená, že porušení bezpečnosti v rámci odpovědnosti Evropského parlamentu se posoudí způsobem, který odpovídá jeho jednacímu řádu a koncepci disciplinárních opatření Evropského parlamentu.

Transparentnost znamená jednoduchost všech bezpečnostních pravidel a ustanovení, nezbytnost vyváženosti mezi různými odděleními a různými oblastmi (fyzická bezpečnost versus ochrana informací atd.) a nezbytnost důsledné a strukturované bezpečnostní politiky. Krom toho jsou nezbytné srozumitelné písemné pokyny pro uplatňování bezpečnostních opatření.

Odpovědnost znamená, že se jasně definují úkoly ve sféře bezpečnosti. Navíc znamená nutnost pravidelného prověřování, zda se tyto úkoly plní správným způsobem.

Subsidiarita znamená, že se bezpečnost musí být zaručena na nejnižší možné úrovni a co nejblíže generálním ředitelstvím a oddělením Evropského parlamentu. Proporcionalita znamená, že se bezpečnostní činnosti musí omezit pouze na ty prvky, které jsou skutečně nezbytné, a že bezpečnostní opatření musí být přiměřená zájmům, které mají chránit, a skutečnému nebo potenciálnímu ohrožení těchto zájmů a umožňují jejich obranu způsobem, která zajišťuje co nejmenší rušivé vlivy.

3. **ZÁKLADY BEZPEČNOSTI INFORMACÍ**

Základem pro zajištění spolehlivé bezpečnosti informací je/jsou:

a) řádné komunikační a informační systémy (CIS). Ty spadají do kompetence bezpečnostního orgánu Evropského parlamentu (jak je vymezeno v bezpečnostním upozornění 1).

b) v rámci Evropského parlamentu orgán pro zabezpečení informací (vymezený v bezpečnostním upozornění 1), který je pověřen spoluprací s dotčeným bezpečnostním orgánem při poskytování informací o technickém ohrožení bezpečnosti systémů CIS a při poskytování rad o prostředcích pro ochranu před tímto ohrožením;

c) úzká spolupráce mezi odpovědnými odděleními v Evropského parlamentu a bezpečnostními odděleními ostatních orgánů Unie;

4. **ZÁSADY BEZPEČNOSTI INFORMACÍ**

4.1 ***Cíle***

Zajištění bezpečnosti informací má tyto základní cíle:

a) ochrana utajovaných informací a jiných důvěrných informací před špionáží, zneužitím nebo nepovoleným zveřejněním;

b) ochrana utajovaných informací, které jsou používány v komunikačních a informačních systémech a sítích, před ohrožením jejich utajení, celistvosti a dostupnosti;

c) ochrana prostor Evropského parlamentu, v nichž jsou utajované informace uloženy, před pokusy o sabotáž a úmyslnými snahami o poškození;

d) v případě selhání bezpečnosti zhodnocení způsobené škody, omezení jejích důsledků, provedení bezpečnostních šetření a přijetí všech nezbytných nápravných opatření.

4.2 ***Utajení***

4.2.1 V oblasti důvěrných informací jsou pro výběr informací a materiálů, které mají být chráněny, a pro stanovení potřebného stupně ochrany nezbytné opatrnost a zkušenost. Je zásadně důležité, aby stupeň ochrany odpovídal citlivosti ve smyslu bezpečnosti, jednotlivých informací nebo materiálů, které mají být chráněny. S cílem zajistit řádný tok informací musí být přijata opatření, aby se zabránilo zařazení na příliš vysoký nebo příliš nízký stupeň utajení.

4.2.2 Systém utajení představuje nástroj, který umožňuje uplatňovat zásady stanovené v této části. Obdobný systém utajení by měl být použit pro plánování a organizaci boje proti špionáži, sabotáži, terorismu a jiným hrozbám tak, aby byla nejvíce chráněna nejdůležitější zařízení, v nichž se nacházejí utajované informace, a nejcitlivější části těchto zařízení.

4.2.3 Za utajení informací odpovídá výlučně původce dotyčných informací.

4.2.4 Při stanovení stupně utajení se vychází výlučně z obsahu daných informací.

4.2.5 V případech spojení několika informací do jednoho celku musí stupeň utajení, který se vztahuje na tento celek, odpovídat informaci s nejvyšším stupněm utajení. Soubor informací může ale získat vyšší klasifikaci, než mají jeho dílčí části.

4.2.6 Zařazení do stupně utajení se provádí pouze v nezbytných případech a po dobu nezbytně nutnou.

4.3 ***Cíle bezpečnostních opatření***

Bezpečnostní opatření:

a) se vztahují na všechny osoby, které mají přístup k utajovaným informacím, k prostředkům přenosu utajovaných informací a k jiným důvěrným informacím, do všech prostor obsahujících takové informace a k významným zařízením;

b) jsou vytvořena tak, aby určila osoby, jejichž postavení (pokud jde o přístup, vztahy nebo jiné záležitosti) by mohlo ohrozit bezpečnost utajovaných informací a významných zařízení obsahujících takové informace, a zamezila jejich přístupu nebo změnila jejich místo;

c) brání přístupu všech neoprávněných osob k utajovaným informacím nebo zařízením, která je obsahují;

d) zajistí, aby utajované informace byly šířeny výlučně v souladu se zásadou potřeby vědět, která je zásadní pro všechna hlediska bezpečnosti;

e) zajistí celistvost (tj. zabrání poškození nebo neoprávněné změně nebo neoprávněnému zničení) a dostupnost (tj. přístup nesmí být odmítnut osobám, které se potřebují s informacemi seznámit a jsou k tomu oprávněny) všech důvěrných informací, a zejména informací uložených, zpracovávaných nebo přenášených v elektromagnetické formě.

5. SPOLEČNÉ MINIMÁLNÍ NORMY

Evropský parlament zajistí, aby všichni příjemci utajovaných informací, a to jak vnitřní, tak i ti, kteří spadají do jeho odpovědnosti, a to všechna oddělení a smluvní partneři, dodržovali společné minimální normy bezpečnosti, aby takto utajované informace mohly být předávány s důvěrou, že všichni s nimi budou nakládat stejně obezřetně. Tyto minimální normy musí zahrnovat kritéria pro bezpečnostní prověrky úředníků Evropského parlamentu a ostatních zaměstnanců Parlamentu pracujících pro politické skupiny a opatření na ochranu důvěrných informací.

Přístup třetích stran k důvěrným informacím povolí Evropský parlament pouze pod podmínkou, že tyto subjekty zaručí, že při nakládání s těmito informacemi dodrží pravidla přinejmenším odpovídající těmto společným minimálním normám.

Tyto společné minimální normy se použijí i v případě, že Evropský parlament prostřednictvím smlouvy nebo grantu svěří průmyslovým nebo jiným subjektům úkoly, které zahrnují důvěrné informace.

6. BEZPEČNOSTNÍ OPATŘENÍ TÝKAJÍCÍ SE ÚŘEDNÍKŮ EVROPSKÉHO PARLAMENTU A OSTATNÍCH ZAMĚSTNANCŮ PARLAMENTU PRACUJÍCÍCH PRO POLITICKÉ SKUPINY

6.1 *Bezpečnostní školení úředníků Evropského parlamentu a ostatních zaměstnanců Parlamentu pracujících pro politické skupiny*

Úředníci Evropského parlamentu a jiní zaměstnanci Parlamentu pracující pro politické skupiny v postavení, ve kterém mohou mít přístup k utajovaným informacím, musí před nástupem do funkce a poté v pravidelných intervalech získat podrobný výklad o nezbytných bezpečnostních opatřeních a souvisejících postupech. Tyto osoby musí písemně potvrdit, že si přečetly tyto platné bezpečnostní předpisy a plně jim porozuměly.

6.2 *Odpovědnost vedoucích pracovníků*

Součástí povinností vedoucích pracovníků musí být to, aby věděli, kteří z jejich pracovníků nakládají s utajovanými informacemi a kteří mají přístup k zabezpečeným komunikačním a informačním systémům, a musí zaznamenávat a hlásit všechny události nebo zřejmá ohrožení, která by mohla ovlivnit bezpečnost.

6.3 *Bezpečnostní status úředníků Evropského parlamentu a ostatních zaměstnanců Parlamentu pracujících pro politické skupiny*

Měly by být stanoveny postupy umožňující určit, jsou-li zjištěny nepříznivé informace o určitém úředníkovi Evropského parlamentu nebo ostatním zaměstnanci Parlamentu pracujícím pro politické skupiny, zda jeho funkce vyžaduje přístup k utajovaným informacím nebo zda má přístup k zabezpečeným komunikačním nebo informačním systémům, a uvědomit příslušné oddělení Evropského parlamentu. Uvede-li příslušný vnitrostátní bezpečnostní orgán, že tato osoba představuje bezpečnostní riziko, bude odvolána nebo vyřazena z plnění úkolů, při kterém by mohla ohrožovat bezpečnost.

7. FYZICKÁ BEZPEČNOST

Fyzická bezpečnost znamená používání fyzických a technických ochranných opatření k zamezení neoprávněného přístupu k utajovaným informacím.

7.1 ***Potřeba ochrany***

Stupeň fyzické ochrany, který má být použit pro zajištění ochrany utajovaných informací, musí odpovídat stupni utajení držených informací a materiálu, jejich objemu a ohrožení, kterému jsou vystaveny. Všichni držitelé utajovaných informací se řídí jednotnými pravidly pro utajování informací a dodržují společné normy ochrany týkající se úschovy, přenosu a ničení informací a materiálů vyžadujících ochranu.

7.2 ***Kontrola***

Osoby, které odcházejí z prostor, v nichž se nacházejí jim svěřené utajované informace, se musí ujistit, že jsou bezpečně uloženy a že jsou aktivována všechna bezpečnostní zařízení (zámky, poplašná zařízení atd.). Po pracovní době se provádějí další nezávislé kontroly.

7.3 ***Bezpečnost budov***

Budovy, v nichž se nacházejí utajované informace nebo zabezpečené komunikační a informační systémy, musí být chráněny před neoprávněným vstupem.

Povaha této ochrany utajovaných informací (např. mříže na oknech, zámky na dveřích, stráže u vchodů, automatické systémy kontroly přístupu, bezpečnostní inspekce a hlídky, poplašné systémy, systémy pro odhalování neoprávněného vniknutí a hlídací psi) závisí na:

a) stupni utajení, objemu a umístění chráněných informací a materiálů v budově;

b) kvalitě bezpečnostních schránek obsahujících dotyčné informace a materiály; a dále

c) technických vlastnostech a umístění budovy.

Povaha ochrany poskytované komunikačním a informačním systémům závisí na určení hodnoty ohrožených informací a materiálů a na případné škodě v případě ohrožení bezpečnosti, na technických vlastnostech a na umístění budovy, v níž se systém nachází, a na umístění tohoto systému v budově.

7.4 ***Nouzové plány***

Je třeba předem připravit podrobné plány s cílem zajistit ochranu utajovaných informací v nouzových případech.

8. **STUPNĚ UTAJENÍ, BEZPEČNOSTNÍ SPECIFIKACE, ZNAČKY, VYZNAČENÍ A PRAVIDLA UTAJOVÁNÍ**

8.1 ***Bezpečnostní specifikace***

Jiný způsob utajování než ten, který je uveden v čl. 2 písm. d) tohoto rozhodnutí, není povolen.

Za účelem stanovení mezí platnosti utajení (což pro utajované informace udává automatické snížení stupně utajení nebo odtajnění) se může použít smluvená bezpečnostní specifikace.

Bezpečnostní specifikace se mohou použít pouze v kombinaci se stupněm utajení.

Bezpečnostní specifikace dále upravuje bezpečnostní upozornění 2 a jsou definovány v pokynech pro nakládání s důvěrnými informacemi.

8.2 ***Značky***

Značka se používá k upřesnění předem stanovených konkrétních pokynů pro nakládání s důvěrnými informacemi. Značky mohou rovněž sloužit k označení oblasti, které se týká daný dokument, nebo k označení zvláštního rozšiřování na základě potřeby vědět nebo (u informací nepodléhajících utajení) k označení konce embarga.

Značka se nepovažuje za stupeň utajení a nesmí se používat místo něj.

Značky dále upravuje bezpečnostní upozornění 2 a jsou definovány v pokynech pro nakládání s důvěrnými informacemi.

8.3 ***Vyznačení stupně utajení a bezpečnostní specifikace***

Vyznačení stupně utajení a bezpečnostní specifikace a značek se provede v souladu s bezpečnostním upozorněním 2, oddíl E, a s pokyny pro nakládání s důvěrnými informacemi.

8.4 ***Pravidla utajování***

8.4.1 *Obecně*

Informace podléhají utajení pouze tehdy, je-li to nezbytné. Stupeň utajení je jasně a řádně vyznačen a trvá pouze po dobu, po kterou daná informace vyžaduje ochranu.

Odpovědnost za utajení informací a za jakékoli následné snížení stupně utajení nebo odtajnění má výlučně původce.

Úředníci Evropského parlamentu a ostatní zaměstnanci Parlamentu provedou utajení informací, snížení stupně jejich utajení nebo jejich odtajnění na pokyn generálního tajemníka nebo s jeho souhlasem.

Podrobné postupy upravující nakládání s utajovanými dokumenty jsou vypracovávány tak, aby umožnily těmto dokumentům ochranu odpovídající informacím, které obsahují.

Počet osob oprávněných vypracovat informace označené stupněm TRÈS SECRET UE / EU TOP SECRET musí být omezen na minimum a jména těchto osob musí být uvedena na seznamu vytvořeném oddělením pro důvěrné informace (CIU).

8.4.2 *Stanovení stupně utajení*

Stupeň utajení dokumentu se určí podle úrovně citlivosti jeho obsahu v souladu s definicí v čl. 2 odst. d). Stupně utajení je nutno používat správně a střídmě.

Stupeň utajení průvodního dopisu nebo sdělení k připojeným částem musí být stejně vysoký jako nejvyšší stupeň utajení jedné z těchto částí. Původce jasně uvede jejich stupeň utajení, pokud dopis nebo sdělení budou odděleny od připojených částí.

Původce dokumentu, pro který má být stanoven stupeň utajení, musí přihlížet k výše zmíněným pravidlům a potlačit jakoukoli snahu o stanovení příliš vysokého stupně utajení nebo příliš nízkého stupně utajení.

Jednotlivé stránky, odstavce, oddíly, přílohy, dodatky a připojené části dokumentu mohou vyžadovat různý stupeň utajení a musí být podle toho označeny. Stupeň utajení dokumentu jako celku je stanoven podle části s nejvyšším stupněm utajení.

9. **KONTROLY**

Ředitelství pro bezpečnost a posuzování rizik Evropského parlamentu provádí pravidelné interní kontroly bezpečnostních opatření přijatých na ochranu utajovaných informací, přičemž může požádat o pomoc bezpečnostní orgány Komise nebo Rady.

Bezpečnostní orgány a příslušné útvary orgánů Unie mohou provádět v rámci dohodnutého postupu zahájeného kteroukoli stranou vzájemné hodnocení bezpečnostních opatření na ochranu utajovaných informací, jejichž výměna se provádí podle příslušných interinstitucionálních dohod.

10. **POSTUPY ODTAJNĚNÍ A ZRUŠENÍ ZNAČEK**

10.1 Oddělení CIU přezkoumá důvěrné informace obsažené v jeho registru a v každém případě nejpozději v 25. roce od vytvoření dokumentu předloží původci příslušné návrhy na odtajnění nebo zrušení značek. Dokumenty, které nebyly odtajněny – nebo u nichž nebyly zrušeny značky – při prvním přezkumu, budou pravidelně znovu hodnoceny nejméně každých pět let. Vedle dokumentů, které jsou uloženy v zabezpečených archivech v zabezpečeném prostoru a řádně utajeny, se může postup zrušení označení týkat také jiných důvěrných informací v držení buď na oddělení Parlamentu nebo funkcionáře Parlamentu nebo na oddělení Parlamentu, které má na starosti historické archivy Parlamentu.

10.2 Rozhodnutí týkající se odtajnění dokumentu nebo zrušení jeho označení musí přijmout zpravidla pouze původce, nebo může být výjimečně přijato ve spolupráci se správcem těchto informací, a to předtím, než jsou informace, které obsahuje, postoupeny oddělení nebo funkcionáři Parlamentu, které má na starosti historické archivy Parlamentu. K odtajnění utajovaných informací nebo zrušení jejich označení může dojít pouze po předchozím písemném souhlasu původce. V případě jiných důvěrných informací sekretariát oddělení /funkcionář Parlamentu, které má tyto informace ve správě, rozhodne ve spolupráci s původcem o tom, zda může být označení tohoto dokumentu zrušeno.

10.3 Oddělení CIU bude jménem původce odpovědné za to, aby uvědomilo příjemce dokumentu o změně stupně utajení nebo o zrušení značky, a příjemci jsou povinni na to upozornit další příjemce, kterým předali originál dokumentu nebo jeho kopii.

10.4 Odtajnění nemá vliv na jakékoli bezpečnostní specifikace nebo označení uvedená na dokumentu.

10.5 V případě odtajnění se původní stupeň utajení v horní a dolní části každé stránky škrtne. První (úvodní) strana dokumentu se orazítkuje a doplní se na ni poznámka oddělení CIU. V případě zrušení označení se původní označení v horní části každé stránky škrtne.

10.6 Text odtajněného dokumentu – nebo dokumentu, u něhož bylo zrušeno označení – se přiloží k elektronickému listu nebo podobnému systému, v němž byl registrován.

10.7 V případě dokumentů, pro něž platí výjimka ochrany soukromí a osobnosti nebo obchodních zájmů fyzické či právnické osoby, a v případě citlivých dokumentů se použije článek 2 nařízení (EHS, Euratom) č. 354/83.

10.8 Kromě ustanovení uvedených v bodech 10.1. až 10.7. se použijí následující pravidla:

a) u dokumentů třetích osob konzultuje oddělení CIU s danou třetí osobou předtím, než přistoupí k odtajnění nebo ke zrušení označení;

b) co se týče výjimky ohledně soukromí a integrity jednotlivce, je při odtajnění nebo zrušení označení třeba zohlednit především souhlas dotčené osoby, nebo případně nemožnost identifikovat dotčenou osobu;

c) co se týče výjimky ohledně obchodních zájmů fyzické či právnické osoby, lze dotčenou osobu informovat zveřejněním v *Úředním věstníku Evropské unie* a dát jí čtyři týdny ode dne zveřejnění k vyslovení připomínek.

Část 2

POSTUP BEZPEČNOSTNÍCH PROVĚREK

11. **BEZPEČNOSTNÍ PROVĚRKY POSLANCŮ EVROPSKÉHO PARLAMENTU**

11.1 Chtějí-li mít poslanci Evropského parlamentu přístup k informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, nebo se stupněm rovnocenným, musí získat osvědčení buď v souladu s postupem uvedeným v bodech 11.3 a 11.4 této přílohy, nebo na základě čestného prohlášení o zachování důvěrnosti podle čl. 3 odst. 4 tohoto rozhodnutí.

11.2 Pro přístup k informacím označeným stupněm utajení SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET a SECRET UE / EU SECRET, nebo stupněm rovnocenným, musí poslanci Evropského parlamentu získat osvědčení v souladu s postupem uvedeným v bodech 11.3. a 11.14.

11.3 Osvědčení se uděluje pouze poslancům Evropského parlamentu, kteří prošli bezpečnostní prověrkou příslušných vnitrostátních orgánů členských států v souladu s postupem uvedeným v bodech 11.9 až 11.14. Osvědčení poslancům uděluje předseda Parlamentu.

11.4 Předseda může udělit písemné osvědčení po obdržení stanoviska příslušných vnitrostátních orgánů členských států na základě bezpečnostní prověrky provedené v souladu s body 11.8 až 11.13.

11.5 Ředitelství pro bezpečnost a posuzování rizik Evropského parlamentu vede aktualizovaný seznam všech poslanců Evropského parlamentu, jimž bylo uděleno osvědčení, včetně dočasného osvědčení ve smyslu bodu 11.15.

11.6 Osvědčení je platné na dobu pět let nebo na dobu výkonu funkcí odůvodňujících jeho udělení, pokud je tato doba kratší. Může být obnoveno v souladu s postupem uvedeným v bodu 11.4.

11.7 Předseda osvědčení odejme, má-li za to, že jsou k tomu oprávněné důvody. Jakékoli rozhodnutí o odnětí osvědčení je sděleno danému poslanci Evropského parlamentu, který může žádat o vyslechnutí předsedou předtím, než k odnětí osvědčení dojde, a rovněž příslušnému vnitrostátnímu orgánu.

11.8 Bezpečnostní prověrka se provádí s pomocí dotčeného poslance Evropského parlamentu a na žádost předsedy Parlamentu. Za příslušný vnitrostátní orgán, který je oprávněn prověrku provádět, se považuje orgán toho členského státu, jehož je dotčený poslanec státním příslušníkem.

11.9 V rámci této prověrky je dotčený poslanec Evropského parlamentu povinen vyplnit formulář s osobními informacemi.

11.10 Předseda Parlamentu ve své žádosti adresované příslušným vnitrostátním orgánům upřesní stupeň utajení utajovaných informací, které mají být dotčenému poslanci Evropského parlamentu zpřístupněny, aby tyto orgány mohly provést prověrku.

11.11 Celá bezpečnostní prověrka prováděná příslušnými vnitrostátními orgány i její výsledky musí být v souladu s příslušnými pravidly a předpisy platnými v dotčeném členském státu včetně pravidel a předpisů pro opravné prostředky.

11.12 Vydají-li příslušné vnitrostátní orgány členského státu kladné stanovisko, může předseda Parlamentu udělit dotčenému poslanci Evropského parlamentu osvědčení.

11.13 Vydají-li příslušné vnitrostátní orgány záporné stanovisko, oznámí se smysl tohoto stanoviska dotčenému poslanci Evropského parlamentu, který může požádat předsedu Parlamentu o slyšení. Považuje-li to předseda Parlamentu za nezbytné, může požádat příslušné vnitrostátní orgány o doplňující vysvětlení. Je-li záporné stanovisko potvrzeno, nelze osvědčení udělit.

11.14 Všichni poslanci Evropského parlamentu, jimž bylo uděleno osvědčení ve smyslu bodu 11.3., dostanou v okamžiku udělení osvědčení a poté v pravidelných intervalech nezbytné pokyny týkající se ochrany utajovaných informací a způsobu zajištění této ochrany. Tito poslanci podepíší prohlášení potvrzující, že dané pokyny obdrželi.

11.15 Za výjimečných okolností může předseda poté, co uvědomí příslušné vnitrostátní orgány, a pokud od nich nezíská ve lhůtě jednoho měsíce žádnou reakci, udělit poslanci Evropského parlamentu dočasné osvědčení na dobu nepřesahující šest měsíců, dokud nebude znám výsledek prověrky uvedené v bodě 11.11. Takto udělená dočasná osvědčení neumožňují přístup k informacím označeným stupněm utajení TRÈS SECRET UE/EU TOP SECRET nebo nesoucím rovnocenné označení.

12. BEZPEČNOSTNÍ PROVĚRKY ÚŘEDNÍKŮ EVROPSKÉHO PARLAMENTU A OSTATNÍCH ZAMĚSTNANCŮ PARLAMENTU PRACUJÍCÍCH PRO POLITICKÉ SKUPINY

12.1 Přístup k utajovaným informacím smějí mít pouze úředníci Evropského parlamentu a ostatní zaměstnanci Parlamentu pracující pro politické skupiny, kteří mají z důvodu svých funkcí a pro splnění požadavků spojených s pracovní činností znát utajované informace nebo je používat.

12.2 Pro přístup k informacím označeným jako CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET,, nebo s rovnocenným označením, musí úředníci Evropského parlamentu a ostatní zaměstnanci Parlamentu, kteří pracují pro dotčené politické skupiny, získat osvědčení v souladu s postupem uvedeným v bodech 12.3 a 12.4.

12.3 Osvědčení se uděluje pouze osobám uvedeným v bodu 12.1, které prošly bezpečnostní prověrkou příslušných vnitrostátních orgánů členských států postupem uvedeným v bodech 12.9 až 12.14. Za udělování osvědčení úředníkům Evropského parlamentu a zaměstnancům Parlamentu pracujícím pro politické skupiny je odpovědný generální tajemník.

12.4 Písemné osvědčení může udělit generální tajemník po obdržení stanoviska příslušných vnitrostátních orgánů členských států na základě bezpečnostní prověrky provedené v souladu s body 12.8 až 12.13.

12.5 Ředitelství pro bezpečnost a posuzování rizik Evropského parlamentu vede aktualizovaný seznam veškerých pracovních míst vyžadujících bezpečnostní prověrku, o nichž ho informují příslušná oddělení Evropského parlamentu, a všech osob, jimž bylo uděleno osvědčení, včetně dočasného osvědčení ve smyslu bodu 12.15.

12.6 Osvědčení je platné na dobu pět let nebo na dobu výkonu funkcí odůvodňujících jeho udělení, pokud je tato doba kratší. Může být obnoveno v souladu s postupem uvedeným v bodu 12.4.

12.7 Generální tajemník osvědčení odejme, má-li za to, že jsou k tomu oprávněné důvody. Jakékoli rozhodnutí o odnětí osvědčení je sděleno danému úředníkovi Evropského parlamentu nebo jinému zaměstnanci Parlamentu pracujícímu pro politické skupiny, který může žádat o vyslechnutí generálním tajemníkem předtím, než k odnětí osvědčení dojde, a rovněž příslušnému vnitrostátnímu orgánu.

12.8 Bezpečnostní prověrka se provádí s pomocí úředníka Evropského parlamentu nebo jiného zaměstnance Parlamentu pracujícího pro politické skupiny a na žádost generálního tajemníka. Za příslušný vnitrostátní orgán, který je oprávněn prověrku provádět, se považuje orgán toho členského státu, jehož je dotčená osoba státním příslušníkem. V případě, že to umožňují vnitrostátní právní a správní předpisy, mohou příslušné vnitrostátní orgány osoby, které nejsou jejich státními příslušníky a žádají o přístup k informacím se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET, prošetřit.

12.9 V rámci této prověrky je úředník Evropského parlamentu nebo jiný zaměstnanec Parlamentu pracující pro politické skupiny povinen vyplnit formulář s osobními informacemi.

12.10 Generální tajemník ve své žádosti zaslané příslušným vnitrostátním orgánům upřesní typ a stupeň utajení informací, které mají být úředníkovi Evropského parlamentu nebo jinému zaměstnanci Parlamentu pracujícímu pro politické skupiny zpřístupněny, aby příslušné vnitrostátní orgány mohly provést prověrku a vydat své stanovisko k úrovni osvědčení, které má být dotčené osobě uděleno.

12.11 Celá bezpečnostní prověrka prováděná příslušnými vnitrostátními orgány i její výsledky musí být v souladu s příslušnými pravidly a předpisy platnými v dotčeném členském státu včetně pravidel a předpisů pro opravné prostředky.

12.12 Vydají-li příslušné vnitrostátní orgány členského státu kladné stanovisko, může generální tajemník udělit dotčenému úředníkovi Evropského parlamentu nebo jinému zaměstnanci Parlamentu pracujícímu pro politické skupiny osvědčení.

12.13 Vydají-li příslušné vnitrostátní orgány záporné stanovisko, oznámí se toto stanovisko úředníkovi Evropského parlamentu nebo jinému zaměstnanci Parlamentu pracujícímu pro politické skupiny, který může požádat generálního tajemníka o slyšení. Považuje-li to generální tajemník za nezbytné, může požádat příslušné vnitrostátní orgány o doplňující vysvětlení. Je-li záporné stanovisko potvrzeno, nelze osvědčení udělit.

12.14 Všichni úředníci Evropského parlamentu a zaměstnanci Parlamentu pracující pro politické skupiny, jimž bylo uděleno osvědčení ve smyslu bodů 12.4 a 12.5, obdrží v okamžiku udělení osvědčení a poté v pravidelných intervalech nezbytné pokyny týkající se ochrany utajovaných informací a způsobu zajištění této ochrany. Tito úředníci a zaměstnanci podepíší prohlášení potvrzující, že obdrželi pokyny a že se zavazují je dodržovat.

12.15 Za výjimečných okolností může generální tajemník poté, co uvědomí příslušné vnitrostátní orgány, a pokud od nich nezíská ve lhůtě jednoho měsíce žádnou reakci, udělit úředníkovi Evropského parlamentu nebo ostatnímu zaměstnanci Parlamentu pracujícímu pro politické skupiny dočasné osvědčení na dobu nepřesahující šest měsíců, dokud nebude znám výsledek prověrky uvedené v bodu 12.11 tohoto oddílu. Takto udělená dočasná osvědčení neumožňují přístup k informacím označeným stupněm utajení TRÈS SECRET UE/EU TOP SECRET nebo nesoucím rovnocenné označení.

PŘÍLOHA II

ÚVOD

Tato ustanovení stanoví bezpečnostní upozornění, která upravují a zajišťují bezpečné nakládání s důvěrnými informacemi a správu těchto informací v Evropském parlamentu. Uvedená bezpečnostní upozornění spolu s pokyny pro nakládání s důvěrnými informacemi vytváří systém pro řízení bezpečnosti informací (ISMS) Evropského parlamentu, o němž se zmiňuje čl. 3 odst. 2 tohoto rozhodnutí:

BEZPEČNOSTNÍ UPOZORNĚNÍ 1

Organizace zajištění bezpečnosti v Evropském parlamentu při ochraně důvěrných informací

BEZPEČNOSTNÍ UPOZORNĚNÍ 2

Správa důvěrných informací

BEZPEČNOSTNÍ UPOZORNĚNÍ 3

Zpracovávání důvěrných informací automatickými komunikačními a informačními systémy (CIS)

BEZPEČNOSTNÍ UPOZORNĚNÍ 4

Fyzická bezpečnost

BEZPEČNOSTNÍ UPOZORNĚNÍ 5

Průmyslová bezpečnost

BEZPEČNOSTNÍ UPOZORNĚNÍ 6

Narušení bezpečnosti, ztráta nebo ohrožení důvěrných informací

BEZPEČNOSTNÍ UPOZORNĚNÍ 1

ORGANIZACE ZAJIŠTĚNÍ BEZPEČNOSTI V EVROPSKÉM PARLAMENTU PŘI OCHRANĚ DŮVĚRNÝCH INFORMACÍ

1. Za celkové a jednotné uplatňování tohoto rozhodnutí odpovídá generální tajemník.

Generální tajemník přijme veškerá nezbytná opatření s cílem zajistit, aby pro účely nakládání s důvěrnými informacemi a jejich uchovávání bylo v prostorách Parlamentu uplatňováno toto rozhodnutí poslanci Evropského parlamentu, úředníky Evropského parlamentu, ostatními zaměstnanci Parlamentu pracujícími pro politické skupiny a smluvními dodavateli.

2. Generální tajemník plní funkci bezpečnostního orgánu. Generální tajemník Rady v této funkci odpovídá za:

2.1 koordinaci veškerých záležitostí ohledně bezpečnosti v souvislosti s činnostmi Parlamentu ve vztahu k ochraně důvěrných informací;

2.2 schvalování zřízení zabezpečeného prostoru, zabezpečených čítáren a zabezpečeného zařízení a vybavení;

2.3 provádění rozhodnutí, kterými se podle článku 6 tohoto rozhodnutí povoluje předávání utajovaných informací Evropským parlamentem třetím stranám;

2.4 vyšetření nebo nařízení vyšetření jakéhokoli úniku důvěrných informací, k němuž prvoplánově došlo v Parlamentu, a to v součinnosti s předsedou Evropského parlamentu, pokud se záležitost týká poslance Evropského parlamentu;

2.5 udržování úzkých kontaktů s bezpečnostními orgány jiných orgánů Unie a s vnitrostátními bezpečnostními orgány v členských státech s cílem zajistit optimální koordinaci bezpečnostní politiky v souvislosti s utajovanými informacemi;

2.6 neustálé přezkoumávání bezpečnostní politiky a postupů Parlamentu a vydávání z toho vyplývajících náležitých doporučení;

2.7 vyrozumění vnitrostátního bezpečnostního orgánu, který provedl bezpečnostní prověrku, v souladu s přílohou I částí 2 bodem 11.3, v případech jakýchkoli nepříznivých informací, které se mohou tohoto orgánu týkat.

3. Pokud že se záležitost týká poslance Evropského parlamentu, postupuje generální tajemník v rámci svých odpovědností v úzké součinnosti s předsedou Evropského parlamentu.

4. Při plnění jeho odpovědností podle bodů 2 a 3 jsou generálnímu tajemníkovi nápomocni zástupce generálního tajemníka, ředitelství pro bezpečnost a posuzování rizik, ředitelství pro informační technologie (DIT) a oddělení pro důvěrné informace (CIU).

4.1 Ředitelství pro bezpečnost a posuzování rizik odpovídá za opatření osobní ochrany, a zejména za bezpečnostní prověrku stanovenou v příloze I části 2. Ředitelství pro bezpečnost a posuzování rizika konkrétně:

a) funguje jako kontaktní partner pro bezpečnostní orgány ostatních orgánů Unie a pro vnitrostátní bezpečnostní orgány v záležitostech týkajících se bezpečnostních prověrek poslanců Evropského parlamentu, úředníků Evropského parlamentu a ostatních zaměstnanců Parlamentu pracujících pro politické skupiny;

b) poskytuje nezbytné obecné bezpečnostní školení seznamující s povinnostmi v zájmu ochrany důvěrných informací a s důsledky jejich nesplnění;

c) sleduje, jak funguje zabezpečený prostor a zabezpečené čítárny v prostorách Parlamentu, v případě potřeby ve spolupráci s bezpečnostními útvary jiných orgánů Unie a členských států;

d) ve spolupráci s bezpečnostními útvary jiných orgánů Unie a členských států provádí audit postupů správy a uchovávání utajovaných informací a fungování zabezpečeného prostoru a zabezpečených čítáren v prostorách Parlamentu, v nichž se nakládá s utajovanými informacemi;

e) navrhuje generálnímu tajemníkovi vhodné pokyny pro nakládání s důvěrnými informacemi.

4.2 DIT odpovídá za bezpečné IT systémy pro nakládání s důvěrnými informacemi ze strany Evropského parlamentu.

4.3 Oddělení CIU odpovídá za:

a) zjišťování potřeb v oblasti bezpečnosti v zájmu účinné ochrany důvěrných informací, a to v úzké spolupráci s ředitelstvím pro bezpečnost a posouzení rizik a DIT a bezpečnostními útvary jiných orgánů Unie;

b) postižení veškerých aspektů správy a uchovávání důvěrných informací v Parlamentu, jak jsou stanoveny v pokynech pro nakládání s důvěrnými informacemi;

c) fungování zabezpečeného prostoru;

d) za správu a seznamování se s důvěrnými informacemi v zabezpečeném prostoru nebo v zabezpečené čítárně spravované oddělením CIU, v souladu s čl. 7 odst. 2 a 3 tohoto rozhodnutí;

e) správu registru CIU;

f) hlášení bezpečnostnímu orgánu v případě jakéhokoli prokázaného nebo domnělého narušení bezpečnosti, ztráty nebo ohrožení důvěrných informací uložených v oddělení CIU a uchovávaných v zabezpečeném prostoru nebo v zabezpečené čítárně spravované oddělením CIU.

5. Generální tajemník jako bezpečnostní orgán dále jmenuje tyto orgány:

a) orgán pro bezpečnostní akreditaci;

b) provozní orgán pro zabezpečení informací;

c) orgán pro distribuci kryptografických materiálů;

d) orgán TEMPEST;

e) orgán pro zabezpečení informací.

Výkon těchto funkcí nevyžaduje 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 nedochází ke střetům zájmů a zdvojování úkolů.

6. Orgán pro bezpečnostní akreditaci radí ve všech bezpečnostních otázkách v souvislosti s akreditací každého IT systému a sítě v Parlamentu tak, že:

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

6.2 vytváří proces bezpečnostní akreditace v souladu s příslušnými politikami, přičemž jasně stanoví podmínky pro schválení komunikačních a informačních systémů pod jeho dohledem;

6.3 vymezí strategii bezpečnostní akreditace stanovující míru podrobností vyžadovaných v akreditačním řízení, která je přiměřená požadované úrovni zabezpečení;

6.4 posuzuje a schvaluje bezpečnostní dokumentaci, včetně prohlášení o řízení rizik a zbytkovém riziku, dokumentace týkající se ověřování provádění bezpečnostních opatření a bezpečnostních provozních postupů, a zajišťuje, aby tato dokumentace byla v souladu s bezpečnostními pravidly a politikami Parlamentu;

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

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

6.7 schvaluje, popřípadě se účastní společného schvalování propojení určitého komunikačního a informačního systému s jinými komunikačními a informačními systémy;

6.8 schvaluje bezpečnostní normy technického zařízení plánovaného pro bezpečné nakládání s utajovanými informacemi a jejich ochranu;

6.9 zajišťuje, aby kryptografické produkty používané v Parlamentu byly zařazeny na seznam produktů schválených EU; a

6.10 konzultuje 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.

7. Provozní orgán pro zabezpečení informací odpovídá za:

7.1 vypracování 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 v rámci akreditačního řízení pro komunikační a informační systémy;

7.2 účast při výběru a testování technických bezpečnostních opatření, zařízení a softwaru pro konkrétní systémy, dohled nad jejich používáním a zajištění jejich bezpečné instalace, konfigurace a údržby v souladu s příslušnou bezpečnostní dokumentací;

7.3 monitorování provádění a uplatňování bezpečnostních provozních směrnic a případně za pověření vlastníka systému, zejména CIU, plněním povinností souvisejících s provozní bezpečností;

7.4 správu kryptografických prostředků a nakládání s nimi, zajištění ochrany kryptografických a kontrolovaných materiálů a případně zajištění vytváření kryptografických proměnných;

7.5 provádění bezpečnostních analýz, přezkumy a testování, zejména vypracovávání příslušných zpráv o riziku, a to podle požadavků orgánu pro bezpečnostní akreditaci;

7.6 zajišťování školení na téma zabezpečení informací u konkrétních komunikačních a informačních systémů;

7.7 zavádění bezpečnostních opatření u konkrétních komunikačních a informačních systémů a řízení jejich uplatňování.

8. Orgán pro distribuci kryptografických materiálů odpovídá za:

8.1 správu a dokládání kryptografických materiálů EU;

8.2 zajištění – v úzké spolupráci s orgánem pro bezpečnostní akreditaci –, aby byly zavedeny příslušné postupy a stanoveny plány pro dokládání veškerých kryptografických materiálů EU, bezpečného nakládání s nimi a jejich ukládání a distribuce; a

8.3 zajištění distribuce kryptografických materiálů EU osobám či orgánům, které je využívají, a jejich zpětné převzetí.

9. Orgán TEMPEST odpovídá za zajištění toho, aby byly komunikační a informační systémy v souladu s politikami a pokyny TEMPEST. Schvaluje protiopatření TEMPEST pro instalace a produkty s cílem chránit utajované informace do určitého stupně utajení v jejich provozním prostředí.

10. Orgán pro zabezpečení informací odpovídá za veškeré aspekty správy důvěrných informací a nakládání s nimi v Parlamentu a konkrétně za:

10.1 vypracování politiky v oblasti zabezpečení informací a bezpečnostních pokynů pro zabezpečení informací a monitorování jejich účinnosti a vhodnosti;

10.2 zajištění a spravování technických informací týkajících se kryptografických prostředků;

10.3 zajištění toho, aby opatření pro zabezpečení informací zvolená pro ochranu utajovaných informací byla v souladu s příslušnými politikami, jimiž se řídí jejich způsobilost a výběr;

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

10.5 konzultace s poskytovatelem systému, s aktéry v oblasti bezpečnosti a se zástupci uživatelů ve věci zabezpečení informací;

BEZPEČNOSTNÍ UPOZORNĚNÍ 2

SPRÁVA DŮVĚRNÝCH INFORMACÍ

A. **ÚVOD**

1. Toto bezpečnostní upozornění obsahuje ustanovení pro správu důvěrných informací ze strany Parlamentu.

2. Při vytváření důvěrných informací zváží původce míru důvěrnosti a rozhodne se na základě zásad uvedených v tomto bezpečnostním upozornění pro utajení nebo označení příslušných informací.

B. **UTAJENÍ UIEU**

3. O tom, že určitému dokumentu bude přiřazen stupeň utajení, se rozhodne před jeho vytvořením. Pro tento účel zahrnuje označení informací UIEU předchozí určení míry jejich důvěrnosti a rozhodnutí původce, že jejichž neoprávněné vyzrazení by mohlo různou měrou poškodit zájmy Evropské unie nebo jednoho či více členských států nebo jednotlivců.

4. Jakmile je rozhodnuto o označení daných informací za utajované, proběhne druhé předchozí posouzení, tentokrát s cílem určit odpovídající stupeň utajení. Stupeň utajení dokumentu se určí podle úrovně citlivosti jeho obsahu.

5. Za utajení informací odpovídá výlučně původce dotyčných informací. Úředníci Parlamentu a ostatní zaměstnanci Parlamentu provedou utajení informací, snížení stupně jejich utajení nebo jejich odtajnění na pokyn generálního tajemníka nebo s jeho souhlasem.

6. Stupně utajení je nutno používat správně a střídmě. Původce dokumentu, jemuž má být přiřazen stupeň utajení, musí potlačit jakoukoli snahu o stanovení příliš vysokého nebo příliš nízkého stupně utajení.

7. Stupeň utajení přiřazený daným informacím je určující pro úroveň ochrany těchto informací v oblasti personální bezpečnosti, fyzické bezpečnosti, procedurální bezpečnosti a zabezpečení informací.

8. Informace, které vyžadují utajení, musí být jako takové označeny a musí s nimi tak být nakládáno bez ohledu na jejich fyzickou podobu. Příjemci musí být jasně seznámeni s tím, že jde o utajované informace, buď tím, že jsou označeny stupněm utajení (mají-li písemnou formu, ať již jsou tištěné nebo v komunikačním a informačním systému), nebo formou sdělení (jsou-li podávány ústně, například v rozhovoru nebo na neveřejné schůzi). Utajované materiály musí být fyzicky označeny, aby bylo umožněno snadno rozpoznat stupeň jejich utajení.

9. UIEU v elektronické formě lze vytvářet pouze v akreditovaném komunikačním a informačním systému. Samy utajované informace a také název souboru a zařízení, na němž jsou uloženy (pokud jde o externí zařízení, jako je CD-ROM nebo USB klíč) musí být označeny příslušným stupněm utajení.

10. Informace musí být označeny za utajované, jakmile získají určitou podobu. Například soukromé poznámky, návrhy dokumentů nebo e-mailové zprávy obsahující informace, které vyžadují utajení, musí být již v prvopočátku označeny za UIEU a musí být vypracovány a musí se s nimi nakládat v souladu s tímto rozhodnutím a s příslušnými pokyny jako po fyzické, tak po technické stránce. Tyto informace se mohou přeměnit v úřední dokument, který ovšem bude odpovídajícím způsobem označen a bude s ním patřičně nakládáno. Může se stát, že v průběhu vypracovávání úředního dokumentu se ukáže, že je nutno náhled přehodnotit a přiřadit mu podle situace vyšší či nižší stupeň utajení.

11. Původce se může rozhodnout přiřazovat určitý standardní stupeň utajení kategoriím informací, které pravidelně vytváří. Musí však zajistit, aby při takovémto přístupu soustavně nenadhodnocoval či nepodhodnocoval stupeň utajení jednotlivých informací.

12. UIEU musí být vždy označeny označením stupně utajení odpovídajícím stupni jejich utajení.

B.1. ***Stupně utajení***

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

— TRÈS SECRET UE/EU TOP SECRET, definovaným v čl. 2 písm. d) tohoto rozhodnutí; ohrožení takto označených informací by pravděpodobně:

a) přímo ohrozilo vnitřní stabilitu Unie nebo jednoho či více jejích členských států nebo třetích států nebo mezinárodních organizací,

b) mimořádně závažně poškodilo vztahy se třetími zeměmi nebo mezinárodními organizacemi,

c) přímo zapříčinilo rozsáhlé ztráty na životech,

d) mimořádně závažně poškodilo operační účinnost či bezpečnost nasazených sil členských států nebo sil jiných přispěvatelů nebo trvalou účinnost mimořádně významných bezpečnostních či zpravodajských operací,

e) dlouhodobě závažně poškodilo hospodářství Unie nebo členských států;

— SECRET UE/EU SECRET, definovaným v čl. 2 písm. d) tohoto rozhodnutí; ohrožení takto označených informací by pravděpodobně:

a) významnou měrou zvýšilo mezinárodní napětí,

b) závažně poškodilo vztahy se třetími zeměmi nebo mezinárodními organizacemi,

c) přímo ohrozilo životy nebo závažně narušilo veřejný pořádek nebo osobní bezpečnost či svobodu,

d) ublížilo zásadním obchodním nebo politickým jednáním, a tím by způsobilo značné operační problémy Unie nebo členským státům,

e) závažně poškodilo operační bezpečnost jednoho či více členských států nebo účinnost vysoce významných bezpečnostních či zpravodajských operací,

f) způsobilo Unii nebo jednomu či více členským státům značnou materiální škodu v oblasti finančních, měnových, hospodářských a obchodních zájmů,

g) podstatně narušilo finanční životaschopnost významných organizací nebo subjektů,

h) závažným způsobem bránilo rozvoji nebo fungování politik Unie, což by mělo značné ekonomické, obchodní nebo finanční důsledky;

— CONFIDENTIEL UE/EU CONFIDENTIAL, definovaným v čl. 2 písm. d) tohoto rozhodnutí; ohrožení takto označených informací by pravděpodobně:

a) výrazně poškodilo diplomatické vztahy, tj. mohlo by vést k oficiálnímu protestu nebo k jiným sankcím,

b) ohrozilo osobní bezpečnost či svobodu jednotlivců,

c) vážně ohrozilo výsledek obchodních nebo politických jednání, a tím by způsobilo operační problémy Unii nebo jednomu či více členským státům,

d) poškodilo operační bezpečnost jednoho či více členských států nebo účinnost bezpečnostních či zpravodajských operací,

e) podstatně narušilo finanční životaschopnost významných organizací nebo subjektů,

f) bránilo vyšetřování trestného činu nebo teroristických činností nebo napomohlo spáchání takového činu a provádění takových činností,

g) bylo zásadním způsobem v rozporu s finančními, měnovými, hospodářskými a obchodními zájmy Unie nebo jednoho či více členských států, nebo

h) závažným způsobem bránilo rozvoji nebo fungování politik Unie, což by mělo značné ekonomické, obchodní nebo finanční důsledky;

— RESTREINT UE/EU RESTRICTED, definovaným v čl. 2 písm. d) tohoto rozhodnutí; ohrožení takto označených informací by pravděpodobně:

a) bylo nevýhodné vzhledem k zájmům Unie,

b) nepříznivě ovlivnilo diplomatické vztahy,

c) způsobilo značné nesnáze jednotlivcům nebo společnostem,

d) uvedlo Unii nebo jeden či více členských států do nevýhodného postavení při obchodních nebo politických jednáních,

e) znesnadnilo zachování účinné bezpečnosti v Unii nebo v jednom či více členských státech,

f) bránilo účinnému rozvoji nebo fungování politik Unie,

g) narušilo řádné řízení Unie a jejích operací,

h) znamenalo porušení závazků Parlamentu zachovávat utajovanou povahu informací poskytnutých třetími stranami,

i) bylo porušením statutárních omezení týkajících se vyzrazení informací,

j) způsobilo finanční ztrátu nebo umožnilo nepatřičné zisky nebo výhody pro jednotlivce či společnosti,

k) ovlivnilo vyšetřování trestného činu nebo napomohlo jeho spáchání.

B.2. ***Utajení kompilací, obálek dokumentů a výtahů***

14. Stupeň utajení průvodního dopisu nebo sdělení obsahujících připojené části musí být stejně vysoký jako nejvyšší stupeň utajení jedné z těchto připojených částí. Původce jasně uvede jejich stupeň utajení, pokud dopis nebo sdělení budou odděleny od připojených částí. Pokud není třeba, aby bylo průvodní sdělení nebo dopis tajným dokumentem, musí v něm být uvedena tato závěrečná věta: Samostatně bez svých příloh není toto sdělení/tento dopis tajným dokumentem.

15. Dokumenty nebo soubory obsahující části s různými stupni utajení musí být pokud možno strukturovány tak, aby části s různým stupněm utajení mohly být v případě potřeby snadno rozpoznány a odděleny. Stupeň utajení dokumentu nebo spisu jako celku musí být alespoň stejně vysoký jako u jeho části s nejvyšším stupněm utajení.

16. Jednotlivé stránky, odstavce, oddíly, přílohy, dodatky a připojené části dokumentu mohou vyžadovat různý stupeň utajení a musí být podle toho označeny. V dokumentech obsahujících utajované informace EU je pro označení stupně utajení oddílů nebo částí textu kratších než jedna strana možné použít standardní zkratky.

17. 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.

C. **JINÉ DŮVĚRNÉ INFORMACE**

18. Jiné důvěrné informace musí být označeny v souladu s písmenem E tohoto bezpečnostního upozornění a pokynů pro nakládání s důvěrnými informacemi.

D. **VYTVÁŘENÍ DŮVĚRNÝCH INFORMACÍ**

19. Pouze osoby oprávněné na základě tohoto rozhodnutí nebo osoby, které k tomu mají povolení od bezpečnostního orgánu, mohou vytvářet důvěrné informace.

20. Důvěrné informace nesmějí být přidávány do systémů pro správu dokumentů na internetu nebo intranetu.

D.1. ***Vytváření utajovaných informací EU***

21. K vytvoření UIEU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET musí být příslušná osoba pověřena podle tohoto rozhodnutí nebo musí mít v první řadě osvědčení podle čl. 4 odst. 1 tohoto rozhodnutí.

22. UIEU se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET musí být vytvářeny pouze v zabezpečeném prostoru.

23. Vytváření UIEU se řídí těmito pravidly:

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

b) každá strana musí být očíslována a musí být uveden celkový počet stran;

c) na první straně dokumentu musí být uvedeno referenční číslo a téma, kterého se týká, což samo o sobě není utajovanou informací, pokud za takovou informaci není označeno;

d) dokument musí být na první straně opatřen datem;

e) na první straně každého dokumentu se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET musí být uveden seznam všech příloh a připojených částí;

f) na dokumentech se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET, které mají být distribuovány ve více výtiscích, se na každé straně uvede číslo výtisku. U každého výtisku musí být také na první straně uveden celkový počet výtisků a počet stran, a

g) pokud dokument odkazuje na jiné dokumenty obsahující utajované informace, které Parlament obdržel od jiných orgánů Unie, nebo pokud obsahuje utajované informace vyplývající z těchto dokumentů, musí mít stejný stupeň utajení jako tyto dokumenty a nesmí být bez předchozího písemného souhlasu jeho původce být distribuován nikomu jinému než osobám vyjmenovaným na distribučním seznamu k původnímu dokumentu nebo původním dokumentům obsahujícím utajované informace.

24. Původce si musí uchovat kontrolu na utajovanými informacemi EU, které vytvořil. Je nutno předem získat jeho písemný souhlas k tomu, aby utajované informace EU:

a) byly označeny nižším stupněm utajení nebo odtajněny;

b) byly použity k jiným účelům než k těm, které původce stanovil;

c) byly vyzrazeny jakémukoli třetímu státu nebo mezinárodní organizaci;

d) byly vyzrazeny jakékoli osobě, orgánu, zemi nebo mezinárodní organizaci jiné než adresátům, jimž původce původně povolil se s danými informacemi seznámit;

e) byly vyzrazeny smluvnímu dodavateli nebo budoucímu dodavateli se sídlem ve třetím státě;

f) byly zkopírovány nebo přeloženy, pokud mají dané informace stupeň utajení TRES SECRET UE/EU TOP SECRET;

g) byly zničeny.

D.2. ***Vytváření jiných důvěrných informací***

25. Generální tajemník se jako bezpečnostní orgán může rozhodnout, zda povolí, aby určitý útvar, oddělení nebo jednotlivec vytvořili jiné důvěrné informace.

26. Jiné důvěrné informace musí být označeny jedním ze způsobů stanovených v pokynech pro nakládání s důvěrnými informacemi.

27. Na vytvoření jiných důvěrných informací se použijí tato pravidla:

a) v horní části první strany daného dokumentu musí být uvedeno jejich označení;

b) každá strana se očísluje a uvede se celkový počet stran;

c) na první straně dokumentu musí být uvedeno referenční číslo a téma, kterého se týká;

d) dokument musí být na první straně opatřen datem a;

e) na poslední straně dokumentu musí být uveden seznam všech příloh a připojených dokumentů.

28. Vytvoření jiných důvěrných informací podléhá zvláštním pravidlům a postupům, jež jsou stanoveny v pokynech pro nakládání s důvěrnými informacemi.

E. **BEZPEČNOSTNÍ SPECIFIKACE A OZNAČENÍ**

29. Bezpečnostní specifikace a označení na dokumentech jsou určeny k usměrňování toku informací a k omezení přístupu k důvěrným informacím na základě zásady potřeba vědět.

30. Při používání bezpečnostních specifikací nebo označení je třeba dbát na to, aby nedošlo k záměně se stupni utajení užívanými u EUCI: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET a TRÈS SECRET UE/EU TOP SECRET.

31. V pokynech pro nakládání s důvěrnými informacemi se stanoví zvláštní pravidla týkající se používání bezpečnostních specifikací a označení, a to spolu se seznamem schválených bezpečnostních označení v Evropském parlamentu.

E.1. ***Bezpečnostní specifikace***

32. Bezpečnostní specifikace se mohou u dokumentů používat pouze ve spojení se stupněm utajení a nesmí být používány samostatně. Bezpečnostní specifikace může být u EUCI použita s cílem:

a) stanovit meze platnosti utajení (což pro utajované informace znamená automatické snížení stupně utajení nebo odtajnění);

b) omezit šíření EUCI;

c) zavést zvláštní opatření pro nakládání s utajovanými informacemi vedle těch, která odpovídají stupni bezpečnostního utajení.

33. Zvláštní kontroly týkající se nakládání s dokumenty obsahujícími EUCI a jejich ukládání představují pro všechny zúčastněné dodatečnou zátěž. Chceme-li minimalizovat práci požadovanou v této souvislosti, patří mezi osvědčené metody stanovit při vytváření takového dokumentu časovou hranici nebo událost, po které má utajení pozbýt automaticky platnosti, přičemž se stupeň utajení informací obsažených v tomto dokumentu sníží, nebo se má dokument úplně odtajnit.

34. Pokud se dokument zabývá specifickou oblastí práce a jeho šíření je třeba omezit nebo má podléhat zvláštním opatřením pro nakládání s informacemi, může být za tímto účelem k jeho stupni utajení připojeno prohlášení s cílem pomoci určit jeho cílovou skupinu.

E.2. ***Označení***

35. Označení nejsou stupněm utajení. Mají sloužit pouze k poskytnutí konkrétních pokynů o nakládání s dokumentem a nesmí být používána k popisu obsahu tohoto dokumentu.

36. Označení mohou být u dokumentů používána samostatně nebo ve spojení se stupněm utajení.

37. Jako obecné pravidlo platí, že označení se použijí u informací, jež podléhají služebnímu tajemství uvedenému v článku 287 Smlouvy o fungování EU, článek 17 služebního řádu, nebo to, co má být chráněno Parlamentem z právních důvodů, ale nemusí nebo nemohou být utajeny.

E.3. ***Užívání označení v komunikačních a informačních systémech (CIS)***

38. Pravidla pro používání označení jsou rovněž použitelná pro akreditované CIS.

39. Orgán pro bezpečnostní akreditaci stanovil zvláštní pravidla pro používání označení u akreditovaných CIS.

F. **PŘÍJÍMÁNÍ INFORMACÍ**

40. V Parlamentu je pouze oddělení CIU oprávněno přijímat od třetích stran utajené informace označené jako CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET nebo rovnocenným stupněm utajení.

41. Pokud jde o informace utajované na stupeň utajení RESTREINT UE/EU RESTRICTED, nebo s rovnocenným stupněm utajení, a o jiné důvěrné informace, může za jejich obdržení od třetích stran a za uplatnění zásad stanovených v tomto bezpečnostním upozornění odpovídat CIU nebo příslušný orgán/funkcionář Parlament.

G. **REGISTRACE**

42. Registrací se rozumí uplatňování postupů, kterými se zaznamenává životní cyklus důvěrných informací, včetně jejich šíření, seznamování se s nimi a zničení.

43. Pro účely tohoto bezpečnostního upozornění se slovem deník (logbook) rozumí registr, v němž jsou zaznamenána zejména data a časy, kdy důvěrné informace:

a) vstupují do příslušného sekretariátu orgánu nebo funkcionáře Parlamentu, popřípadě do oddělení CIU, nebo z něj vystupují;

b) byly zpřístupněny nebo předány osobě s bezpečnostní prověrkou; a

c) byly zničeny.

44. Původce utajovaných informací je odpovědný za označení původního prohlášení po vytvoření dokumentu obsahujícího tyto informace. Toto prohlášení je předáno oddělení CIU v okamžiku, kdy je dokument vytvořen.

45. Informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET nebo se stupněm rovnocenným může zaregistrovat pouze oddělení CIU pro bezpečnostní účely. Informace utajované na stupeň RESTREINT UE/EU RESTRICTED, nebo s rovnocenným stupněm utajení, a jiné důvěrné informace zaregistruje pro správní účely oddělení odpovědné za úřední přijetí daného dokumentu, což je buď oddělení CIU nebo sekretariát parlamentního orgánu / funkcionáře Parlamentu. Jiné důvěrné informace, které byly vypracovány v Parlamentu, zaregistruje pro správní účely původce.

46. Jedná-li se o informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET nebo se stupni jim rovnocennými, zaregistrují se zejména v okamžiku, kdy:

a) byly vypracovány;

b) byly doručeny do oddělení CIU nebo jej opouštějí; a

c) vstupují do komunikačního a informačního systému, nebo z něj vystupují.

47. Jedná-li se o informace se stupněm utajení RESTREINT UE/EU RESTRICTED nebo se stupni jim rovnocennými, zaregistrují se zejména v okamžiku, kdy:

a) byly vypracovány;

b) byly doručeny do příslušného sekretariátu orgánu nebo funkcionáře Parlamentu, popřípadě do oddělení CIU; a

c) vstoupily do komunikačního a informačního systému nebo z něj vystoupily.

48. Registrace důvěrných informací může být provedena v tištěném nebo elektronickém deníku/CIS.

49. U informací označených na stupeň utajení RESTREINT UE/EU RESTRICTED, nebo rovnocenným stupněm utajení, a u jiných důvěrných informací se zaznamenají přinejmenším tyto údaje:

a) datum a doba, kdy vstoupily do příslušného sekretariátu orgánu nebo funkcionáře Parlamentu, popřípadě do oddělení CIU, nebo kdy z něj vystoupily;

b) název dokumentu, stupeň utajení nebo označení, datum ukončení utajení nebo označení a jakékoli referenční číslo přidělené tomuto dokumentu.

50. U informací označených na stupeň utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET a vyšším nebo rovnocenným stupněm utajení se zaznamenají přinejmenším tyto údaje:

a) datum a doba, kdy vstoupily do oddělení CIU nebo z něj vystoupily;

b) název dokumentu, stupeň utajení nebo označení, jakékoli referenční číslo přidělené tomuto dokumentu a datum ukončení utajení nebo označení;

c) údaje o původci;

d) záznam o totožnosti kterékoliv osoby, které byl umožněn přístup k dokumentu, a o datu, kdy do dokumentu tato osoba nahlížela;

e) záznam o provedení jakékoli kopie nebo překladu tohoto dokumentu;

f) datum a doba, kdy kopie nebo překlady tohoto dokumentu opustily oddělení CIU nebo se do něj vrátily, a podrobné informace o tom, kam byly zaslány nebo kdo je vrátil zpět;

g) datum a doba, kdy byl dokument skartován v souladu s bezpečnostními pravidly pro skartaci dokumentů, a kdo jej skartoval; a

h) zrušení utajení nebo snížení stupně utajení dokumentu.

51. Deníky jsou v případě potřeby označeny stupněm utajení. Deníky, v nichž jsou registrovány informace označené na stupeň utajení TRES SECRET UE/EU TOP SECRET nebo rovnocenným stupněm utajení, se zaregistrují na stejném stupni.

52. Utajované informace mohou být registrovány:

a) v jediném deníku; nebo

b) v oddělených denících podle stupně utajení, podle toho zda vstupují do registru nebo jej opouštějí a podle jejich původu či určení.

53. Pokud je využíváno elektronického způsobu registrace v rámci komunikačního a informačního systému, postupy registrace mohou probíhat v rámci tohoto systému, který splňuje požadavky, jež jsou rovnocenné požadavkům stanoveným výše. Kdykoli utajované informace EU opustí oblast komunikačního a informačního systému, vztahuje se na ně výše uvedený postup registrace.

54. Oddělení CIU vede záznamy o všech utajovaných informacích, které Parlament poskytl třetím stranám, a o všech utajovaných informacích, které Parlament od třetích stran obdržel.

55. Jakmile je registrace informací označených na stupeň utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET nebo rovnocenným stupněm dokončena, oddělení CIU zkontroluje, zda má adresát platné bezpečnostní osvědčení. Pokud tomu tak je, oddělení CIU o tom adresáta zpraví. K seznámení se s utajovanými informacemi může dojít až po zaregistrování dokumentu, který takové informace obsahuje.

H. **DISTRIBUCE INFORMACÍ**

56. Původce sestaví počáteční distribuční seznam pro dokument obsahující utajované informace EU, který vytvořil.

57. Informace označené na stupeň utajení RESTREINT UE/EU RESTRICTED a jiné důvěrné informace, které Parlament vypracoval, rozesílá v Parlamentu původce v souladu s příslušnými pokyny pro nakládání s důvěrnými informacemi a na základě zásady potřeba vědět. Jedná-li se o informace označené na stupeň utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET, které Parlament vytvořil v zabezpečeném prostoru, bude oddělení CIU, jež odpovídá za nakládání s takovým dokumentem, poskytnut distribuční seznam (a jakékoli další pokyny týkající se distribuce dokumentu).

58. Utajované informace EU, které Parlament vypracoval, může rozesílat třetím stranám pouze oddělení CIU na základě zásady potřeba vědět.

59. Důvěrné informace, které získalo buď oddělení CIU nebo jakýkoli sekretariát parlamentního orgánu/funkcionáře, který předložil žádost, jsou rozesílány v souladu s pokyny obdrženými od původce.

I. **NAKLÁDÁNÍ S INFORMACEMI, JEJICH UKLÁDÁNÍ A SEZNAMOVÁNÍ SE S NIMI**

60. Nakládání s informacemi, jejich ukládání a seznamování se s nimi se provádí v souladu s bezpečnostním upozorněním 4 a s pokyny pro nakládání s důvěrnými informacemi.

J. **KOPÍROVÁNÍ, PŘEKLAD A TLUMOČENÍ UTAJOVANÝCH INFORMACÍ**

61. Dokumenty obsahující informace se stupněm utajení TRÈS SECRET UE/EU TOP SECRET, nebo s rovnocenným stupněm utajení, se nesmí kopírovat ani překládat bez předchozího písemného souhlasu původce. Dokumenty se stupněm utajení SECRET UE/EU SECRET, nebo s rovnocenným stupněm utajení, nebo se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, nebo s rovnocenným stupněm utajení, se mohou kopírovat nebo překládat podle pokynů jejich držitele, pokud to původce nezakázal.

62. Všechny kopie dokumentu obsahujícího informace se stupněm utajení TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET nebo CONFIDENTIEL UE/EU CONFIDENTIAL, nebo s rovnocenným stupněm utajení, musí být pro účely bezpečnosti registrovány.

63. Na kopie a překlady dokumentů se vztahují bezpečnostní opatření použitá pro původní dokument obsahující utajované informace.

64. Dokumenty poskytnuté Radou by měly být zaslány ve všech úředních jazycích.

65. Kopie nebo překlady dokumentů obsahujících utajované informace si může vyžádat původce nebo držitel kopie. Kopie dokumentů obsahujících informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a se stupněm utajení vyšším nebo rovnocenným mohou být zhotoveny pouze v zabezpečeném prostoru na kopírkách, které jsou součástí akreditovaného komunikačního a informačního systému. Kopie dokumentů obsahujících informace se stupněm utajení RESTREINT UE/EU RESTRICTED, nebo s rovnocenným stupněm utajení, a jiných důvěrných informací se zhotovují pomocí akreditovaného reprodukčního zařízení v prostorách Parlamentu.

66. Všechny kopie a překlady jakéhokoli dokumentu nebo části kopií dokumentů obsahujících důvěrné informace musí být odpovídajícím způsobem označeny, očíslovány a zaregistrovány.

67. Nezhotoví se více kopií, než je nezbytně nutné. Všechny kopie se skartují v souladu s pokyny pro nakládání s důvěrnými informacemi po skončení období, kdy bylo možné se s nimi seznámit.

68. Přístup k utajovaným informacím bude umožněn pouze těm tlumočníkům a překladatelům, kteří jsou úředníky Parlamentu.

69. Tlumočníci a překladatelé s přístupem k dokumentům obsahujícím informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET nebo rovnocenným stupněm utajení musí mít odpovídající bezpečnostní prověrku.

70. Při práci s dokumenty obsahujícími informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET nebo rovnocenným stupněm utajení musí tlumočníci a překladatelé pracovat v zabezpečeném prostoru.

K. SNÍŽENÍ STUPNĚ UTAJENÍ, ODTAJNĚNÍ A ZRUŠENÍ OZNAČENÍ DŮVĚRNÝCH INFORMACÍ

K.1. *Obecné zásady*

71. Důvěrné informace se odtajní, sníží se jejich stupeň utajení nebo se zruší jejich označení v případě, že není potřeba je nadále chránit nebo není nutná jejich ochrana na původní úrovni.

72. Rozhodnutí o snížení stupně utajení, odtajnění nebo zrušení označení informací obsažených v dokumentech, které byly vypracovány v Parlamentu, může být rovněž učiněno na *ad hoc* základě, například v reakci na žádost o přístup ze strany veřejnosti nebo jiného orgánu Unie, nebo z podnětu oddělení CIU nebo orgánu/funkcionáře Parlamentu.

73. Je-li to možné, uvede původce utajovaných informací EU v době vytvoření informace, zda je možné snížit stupeň utajení dotčených informací nebo je odtajnit k určitému datu nebo po určité události. Pokud není možné takovou informaci poskytnout, provede původce, oddělení CIU nebo orgán/funkcionář Parlamentu minimálně jednou za pět let přezkum stupně utajení utajovaných informací EU, které uchovává. V každém případě lze stupeň utajení utajovaných informací EU snížit nebo informace odtajnit pouze s předchozím písemným souhlasem původce.

74. V případě, že nelze určit nebo vysledovat původce utajovaných informací EU, které byly vypracovány v Parlamentu, přezkoumá bezpečnostní orgán stupeň utajení dotčených utajovaných informací EU na základě návrhu orgánu/funkcionáře Parlamentu, který informace uchovává, přičemž se může v této souvislosti obrátit na oddělení CIU.

75. Oddělení CIU nebo orgán/funkcionář Parlamentu, který informace uchovává, je odpovědný za to, že oznámí adresátovi/adresátům, že informace byly odtajněny nebo přeřazeny do nižšího stupně utajení, a dotyčný adresát/dotyční adresáti jsou zase odpovědní za to, že totéž oznámí jakémukoli následnému adresátovi/jakýmkoli následným adresátům, kterým byly zaslán nebo zkopírován dokument.

76. O odtajnění informací obsažených v dokumentu, snížení stupně jejich utajení nebo zrušení jejich označení se provede záznam.

K.2. *Odtajnění*

77. Utajované informace EU mohou být odtajněny v plném rozsahu nebo částečně. Utajované informace EU mohou být odtajněny částečně tehdy, když se již utajení nepovažuje za nezbytné pro určitou část dokumentu, který je obsahuje, ale je nadále odůvodněné pro zbytek dokumentu.

78. Pokud se při přezkoumávání utajovaných informací EU, které obsahuje dokument vytvořený v Parlamentu, dojde k rozhodnutí, že jej lze odtajnit, je nutno zvážit otázku, zda může být dokument zveřejněn, nebo zda má být označen pro distribuci (tj., že se nezveřejní).

79. V případě odtajnění utajovaných informací EU musí být tato skutečnost zaznamenána v deníku, včetně těchto údajů: datum odtajnění, jména osob, které o toto odtajnění požádaly, a kdo je schválil, referenční číslo odtajněného dokumentu a jeho konečné místo určení.

80. Veškerá označení předchozího stupně utajení musí být v dokumentu, jenž byl odtajněn, a ve všech jeho kopiích proškrtnuta. Tento dokument a veškeré jeho kopie musí být odpovídajícím způsobem uloženy.

81. Po odtajnění části dokumentu obsahujícího utajované informace se vyjme jeho část, jež byla odtajněna, a uloží se odpovídajícím způsobem. Příslušné oddělení zaregistruje:

a) datum částečného odtajnění;

b) jména osob, které o toto odtajnění požádaly, a kdo je schválil; a

c) referenční číslo dané části dokumentu.

K.3. ***Snížení stupně utajení***

82. Následně po snížení stupně utajení utajených informací se příslušný dokument, které tyt informace obsahuje, zaregistruje v denících odpovídajících jeho předchozí i nové úrovni utajení. Datum snížení stupně utajení se zaznamená, stejně jako jméno osoby, která je schválila.

83. Dokument obsahující informace, jejichž stupeň utajení byl snížen, a všechny jeho kopie musí být označeny novým stupněm utajení a uloženy odpovídajícím způsobem.

L. **SKARTACE DŮVĚRNÝCH INFORMACÍ**

84. Důvěrné informace (buď v tištěné či elektronické podobě), které již nejsou zapotřebí, se skartují nebo odstraní v souladu s pokyny pro nakládání s důvěrnými informacemi a platnými pravidly pro archivaci.

85. Skartaci utajovaných informací se stupněm utajení TRES SECRET UE/EU TOP SECRET nebo SECRET UE/EU SECRET, nebo s rovnocenným stupněm utajení, provádí oddělení CIU. Tato skartace se provádí za přítomnosti svědka, který má bezpečnostní prověrku alespoň pro stupeň utajení skartovaných informací.

86. Informace se stupněm utajení TRÈS SECRET UE/EU TOP SECRET, nebo s rovnocenným stupněm utajení, se skartují pouze s předchozím písemným souhlasem původce.

87. Informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET or TRÈS SECRET UE/EU TOP SECRET nebo rovnocenným, skartuje a odstraňuje oddělení CIU na pokyn původce nebo příslušného orgánu. Deníky a ostatní registry se odpovídajícím způsobem aktualizují. Informace se stupněm utajení RESTREINT UE/EU RESTRICTED, nebo s rovnocenným stupněm utajení, skartuje a odstraňuje oddělení CIU nebo příslušný orgán/funkcionář Parlamentu.

88. Úředník odpovědný za skartaci a příslušný svědek podepíší zápis o skartaci, který je zaregistrován a archivován v oddělení CIU. Oddělení CIU uchovává – spolu s formuláři pro distribuci dokumentů – zápisy o skartaci utajovaných informací se stupněm utajení TRES SECRET UE/EU TOP SECRET, nebo s rovnocenným stupněm utajení, po dobu nejméně deseti let, a o skartaci informací se stupněm utajení SECRET UE/EU SECRET, nebo s rovnocenným stupněm utajení, a se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, nebo s rovnocenným stupněm utajení, po dobu nejméně pěti let.

89. Dokument obsahující utajované informace se skartuje způsobem, který splňuje příslušné normy Unie nebo normy rovnocenné tak, aby nebylo možné znovu sestavit celý dokument nebo jeho část.

90. Skartace nosičů dat použitých pro uložení utajovaných informací se provádí v souladu s příslušnými pokyny pro nakládání s důvěrnými informacemi.

91. Skartace utajovaných informací se zaznamená v příslušném deníku, a to včetně těchto údajů:

a) datum a doba skartace;

b) jméno úředníka odpovědného za skartaci;

c) označení skartovaného dokumentu nebo jeho kopií;

d) původní fyzická podoba skartovaných utajovaných informací EU;

e) způsob skartace; a

f) místo skartace.

M. **ARCHIVACE**

92. Utajované informace, včetně jakýchkoliv průvodních poznámek/dopisu, příloh, potvrzení o předání nebo jiných částí spisu, jsou šest měsíců poté, co byly naposledy zpřístupněny, nejpozději však jeden rok po uložení, přemístěny do zabezpečeného archivu v zabezpečeném prostoru. Podrobná pravidla pro archivaci utajovaných informací jsou stanovena v pokynech pro nakládání s důvěrnými informacemi.

93. U jiných důvěrných informací se použijí obecná pravidla o správě dokumentů, aniž by tím byla dotčena další zvláštní ustanovení o nakládání s dokumenty.

BEZPEČNOSTNÍ UPOZORNĚNÍ 3

ZPRACOVÁVÁNÍ DŮVĚRNÝCH INFORMACÍ AUTOMATICKÝMI KOMUNIKAČNÍMI A INFORMAČNÍMI SYSTÉMY (CIS)

A. **INFORMAČNÍ ZABEZPEČENÍ UTAJOVANÝCH INFORMACÍ ZPRACOVÁVANÝCH V INFORMAČNÍCH SYSTÉMECH**

1. Zabezpečení informací v oblasti informačních systémů je jistota, že takové systémy ochrání utajované informace, s nimiž nakládají, a že budou fungovat správně a když je to 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 (CIS) pro nakládání s utajovanými informacemi se rozumí systém, který umožňuje nakládání s informacemi v elektronické podobě. Takový informační systém zahrnuje všechny složky nezbytné k fungování, včetně infrastruktury, organizace, personálu a informačních zdrojů.

3. V komunikačním a informačním systému se nakládá s utajovanými informacemi v souladu s koncepcí zabezpečení informací.

4. Komunikační a informační systém podléhá akreditačnímu řízení. Cílem akreditace je získat jistotu, že byla provedena veškerá vhodná bezpečnostní opatření a že byla dosažena dostatečná úroveň ochrany utajovaných informací a komunikačního a informačního systému v souladu s tímto bezpečnostním upozorněním. Rozhodnutí o akreditaci stanoví nejvyšší stupeň utajení informací, s nimiž lze v komunikačním a informačním systému nakládat, a příslušné podmínky.

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

a) autenticita: záruka, že informace jsou autentické a pochází od důvěryhodných zdrojů;

b) dostupnost: přístupnost a použitelnost informací na žádost oprávněného subjektu;

c) důvěrnost: skutečnost, že informace nejsou vyzrazeny neoprávněným osobám a subjektům a pro nedovolené účely;

d) integrita: zajištění přesnosti a úplnosti informací a aktiv;

e) nepopiratelnost: schopnost prokázat zpětně jednání či událost tak, aby dané jednání či událost nemohly být následně jakkoliv popřeny.

B. ZÁSADY ZABEZPEČENÍ INFORMACÍ

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

B.1. *Řízení bezpečnostních rizik*

7. 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 uvedené v bezpečnostním upozornění 1 za využití osvědčeného, transparentního a srozumitelného procesu hodnocení rizika. Oblast působnosti komunikačního a informačního systému a jeho aktiv je třeba jasně určit na počátku procesu řízení rizik.

8. Příslušné orgány uvedené v bezpečnostním upozornění 1 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.

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

10. Akreditace komunikačního a informačního systému zahrnuje formální prohlášení o zbytkovém riziku a přijetí zbytkového rizika ze strany odpovědného orgánu. 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, s nimiž se v komunikačním a informačním systému nakládá.

B.2. *Bezpečnost během celého životního cyklu komunikačního a informačního systému*

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

12. 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.

13. 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, že komunikační a informační systém, včetně technických a netechnických bezpečnostních opatření, je řádně zprovozněn, zapojen a konfigurován.

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

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

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

B.3. ***Osvědčené postupy***

17. Orgán pro zabezpečení informací vyvine osvědčené postupy na ochranu utajovaných informací, s nimiž se v komunikačním a informačním systému nakládá. 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.

18. Pro ochranu utajovaných informací, s nimiž se nakládá v komunikačním a informačním systému, se využijí získané poznatky subjektů, které působí v oblasti zabezpečení informací.

19. Šíření a následné uplatňování osvědčených postupů má napomoci dosažení rovnocenné úrovně zabezpečení komunikačních a informačních systémů, které jsou provozovány sekretariátem Parlamentu a v nichž se nakládá s utajovanými informacemi.

B.4. ***Hloubková ochrana***

20. 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 komunikačního a informačního systému.

Míra přísnosti bezpečnostních opatření se stanoví na základě hodnocení rizik.

21. Příslušné orgány uvedené v bezpečnostním upozornění 1 zajistí, aby byly schopny reagovat na mimořádné události, které mohou přesahovat organizační hranice, s cílem koordinovat reakce a sdílet informace o těchto mimořádných událostech a souvisejícím riziku (schopnost reakce na počítačové hrozby).

B.5. ***Zásada minimálnosti a zásada co nejomezenějších práv***

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

23. 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.

B.6. ***Povědomí o zabezpečení informací***

24. 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 nakládající s utajovanými informacemi;

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 jejich konkrétních úlohách v rámci daných systémů a procesů.

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

B.7. ***Hodnocení a schvalování bezpečnostních prostředků informačních technologií***

26. Komunikační a informační systémy nakládající s informacemi se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET či stupněm rovnocenným jsou chráněny takovým způsobem, aby informace nemohly být ohroženy kompromitujícím elektromagnetickým vyzařováním (bezpečnostní opatření TEMPEST).

27. Pokud je ochrana utajovaných informací zajišťována kryptografickými prostředky, jsou tyto prostředky schváleny orgánem pro bezpečnostní akreditaci jako součást kryptografických prostředků schválených EU.

28. Během elektronického přenosu utajovaných informací se použijí kryptografické prostředky schválené EU. Bez ohledu na tento požadavek se za mimořádných okolností nebo v případě zvláštních technických konfigurací mohou použít zvláštní postupy uvedené v bodech 41 až 44.

29. 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 pokyny.

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

31. Orgán pro bezpečnostní akreditaci schválí bezpečnostní pokyny pro způsobilost a schvalování nekryptografických bezpečnostních prostředků informačních technologií.

B.8. ***Přenos v zabezpečeném prostoru***

32. Je-li přenos utajovaných informací omezen na zabezpečený prostor, může být na základě výsledku procesu řízení rizik a se souhlasem orgánu pro bezpečnostní akreditaci použit přenos nešifrovaný nebo šifrovaný na nižší úrovni.

B.9. ***Bezpečné propojení komunikačních a informačních systémů***

33. Propojením se rozumí přímé spojení dvou nebo více informačních systémů za účelem jednosměrného či vícesměrného sdílení údajů a dalších informačních zdrojů.

34. Komunikační a informační systém považuje každý propojený informační systém za nedůvěryhodný a pro kontrolu výměny utajovaných informací s jakýmkoli jiným komunikačním a informačním systémem uplatní ochranná opatření.

35. 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) dotčené propojení je předmětem procesu řízení rizik a akreditačního řízení a je schváleno příslušným orgánem pro bezpečnostní akreditaci;

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

36. Certifikovaný komunikační a informační systém nesmí být propojen s nechráněnou nebo veřejnou sítí, s výjimkou případů, kdy má komunikační a informační systém schválené funkce PS 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.

37. Pokud je nechráněná nebo veřejná síť využívána výhradně k přenosu dat a informace jsou zašifrovány pomocí kryptografického prostředku EU schváleného v souladu s bodem 27, nepovažuje se takové spojení za propojení.

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

B.10. ***Počítačová paměťová média***

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

40. Počítačová paměťová média se znovu použijí nebo se u nich sníží či zruší stupeň utajení v souladu s pokyny pro nakládání s důvěrnými informacemi.

B.11. ***Mimořádné okolnosti***

41. Za mimořádných okolností, například během hrozící nebo probíhající krize, konfliktu, války nebo za výjimečných provozních okolností, mohou být použity níže popsané zvláštní postupy.

42. Utajované informace mohou být se souhlasem příslušného orgánu přenášeny za použití kryptografických prostředků schválených pro nižší stupeň utajení nebo v nešifrované podobě, 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 dostatečně včas předat jiným způsobem.

43. Za okolností uvedených v bodě 41 nenesou přenášené utajované informace žádná označení ani údaje, jež by je odlišovaly od informací, které nejsou utajované nebo které mohou být chráněny dostupným kryptografickým prostředkem. Příjemce informací je třeba neprodleně uvědomit o stupni utajení jiným způsobem.

44. Pokud se použije postup podle bodů 41 nebo 42, podá se následně zpráva příslušnému orgánu.

BEZPEČNOSTNÍ UPOZORNĚNÍ 4

FYZICKÁ BEZPEČNOST

A. **ÚVOD**

Toto bezpečnostní upozornění stanoví bezpečnostní zásady pro vytvoření zabezpečeného prostředí, které zajistí nakládání s důvěrnými informacemi v Evropském parlamentu. Tyto zásady, včetně zásad týkajících se technické bezpečnosti, budou doplněny pokyny pro nakládání s důvěrnými informacemi.

B. **ŘÍZENÍ BEZPEČNOSTNÍCH RIZIK**

1. Bezpečnostní rizika související s utajovanými informacemi 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 bezpečnostním upozorněním a na uplatňování těchto opatření v souladu s koncepcí hloubkové ochrany podle bezpečnostního upozornění 3. Účinnost těchto patření se průběžně vyhodnocuje.

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

3. V pohotovostních plánech se zohlední potřeba chránit utajované informace 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 a na uchovávání těchto informací.

C. **OBECNÉ ZÁSADY**

5. Stupeň utajení nebo označení informací je určující pro úroveň ochrany těchto informací v oblasti fyzické bezpečnosti.

6. Informace, které vyžadují utajení, musí být jako takové označeny a musí s nimi tak být nakládáno bez ohledu na jejich fyzickou podobu. Příjemci musí být jasně seznámeni s tím, že jde o utajované informace, buď tím, že jsou označeny stupněm utajení (mají-li písemnou formu, ať již jsou tištěné nebo v komunikačním a informačním systému), nebo formou sdělení (jsou-li podávány ústně, například během rozhovoru nebo prezentace). Utajované materiály musí být fyzicky označeny, aby bylo umožněno snadno rozpoznat stupeň jejich utajení.

7. Důvěrné informace nesmí být za žádných okolností čteny na veřejných místech, kde by je mohla spatřit osoba, která nemá potřebu vědět, např. ve vlacích či letadlech, kavárnách, barech atd. Nelze je zanechat v hotelových sejfech či pokojích nebo je ponechat bez dozoru na veřejných místech.

D. **ODPOVĚDNOSTI**

8. Oddělení CIU odpovídá za fyzickou bezpečnost při správě důvěrných informací uložených v jeho zabezpečených prostorech. CIU odpovídá i za správu svých zabezpečených prostor.

9. Za fyzickou bezpečnost při správě informací se stupněm utajení RESTREINT UE/EU RESTRICTED nebo stupněm rovnocenným a jiných důvěrných informací odpovídá příslušný orgán/funkcionář Parlamentu.

10. Ředitelství pro bezpečnost a posuzování rizika zajišťuje osobní bezpečnost a bezpečnostní prověrky potřebné k bezpečnému nakládání s důvěrnými informacemi v Evropském parlamentu.

11. DIT poskytuje poradenství a zajišťuje, aby byl jakýkoli vytvořený nebo používaný komunikační a informační systém v souladu s bezpečnostním upozorněním 3 a s příslušnými pokyny pro nakládání s důvěrnými informacemi.

E. **ZABEZPEČENÉ PROSTORY**

12. Odlišné zabezpečené prostory je možné instalovat v souladu s technickými bezpečnostními normami a se stupněm přiřazeným daným důvěrným informacím ve smyslu článku 7.

13. Zabezpečené prostory jsou schváleny orgánem pro bezpečnostní akreditaci a potvrzeny bezpečnostním orgánem.

F. **PROHLÍŽENÍ DŮVĚRNÝCH INFORMACÍ**

14. Pokud jsou informace se stupněm utajení RESTREINT UE/EU RESTRICTED nebo stupněm rovnocenným a jiné důvěrné informace uloženy na oddělení CIU a musí být prohlíženy mimo zabezpečený prostor, předá oddělení CIU kopii příslušnému oddělení, které k tomu má povolení, jež zajistí, aby prohlížení dotčených informací a nakládání s nimi bylo v souladu s čl. 8 odst. 2 a článkem 10 tohoto rozhodnutí a s příslušnými pokyny pro nakládání s důvěrnými informacemi.

15. Pokud jsou informace se stupněm utajení RESTREINT UE/EU RESTRICTED nebo stupněm rovnocenným a jiné důvěrné informace uloženy u jiného orgánu nebo funkcionáře Parlamentu, než je oddělení CIU, sekretariát tohoto oddělení nebo funkcionáře zajistí, aby prohlížení těchto informací a nakládání s nimi bylo v souladu s čl. 7 odst. 3, čl. 8 odst. 1, 2 a 4, čl. 9 odst. 3, 4 a 5, čl. 10 odst. 2 až 6 a článkem 11 tohoto rozhodnutí a s příslušnými pokyny pro nakládání s důvěrnými informacemi.

16. Pokud musí být informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET nebo stupněm rovnocenným prohlíženy v zabezpečeném prostoru, zajistí oddělení CIU, aby prohlížení těchto informací a nakládání s nimi bylo v souladu s články 9 a 10 tohoto rozhodnutí a s příslušnými pokyny pro nakládání s důvěrnými informacemi.

G. **TECHNICKÁ BEZPEČNOST**

17. Za technická bezpečnostní opatření odpovídá orgán pro bezpečnostní akreditaci, který v příslušných pokynech pro nakládání s důvěrnými informacemi určí specifická technická bezpečnostní opatření.

18. Zabezpečené čítárny určené k prohlížení informací se stupněm utajení RESTREINT UE/EU RESTRICTED nebo stupněm rovnocenným a jiných důvěrných informací podle čl. 7 odst. 3 tohoto rozhodnutí splňují specifická technická bezpečnostní opatření stanovená v pokynech pro nakládání s důvěrnými informacemi.

19. Součástí zabezpečeného prostoru podle čl. 7 odst. 2 tohoto rozhodnutí jsou tato zařízení:

a) místnost pro prověření zabezpečeného přístupu, instalovaná v souladu s technickými bezpečnostními opatřeními stanovenými v pokynech pro nakládání s důvěrnými informacemi. Přístup do tohoto zařízení se eviduje. Místnost pro prověření zabezpečeného přístupu odpovídá vysokým standardům, pokud jde o identifikaci osob s přístupem, záznam videa, zabezpečený prostor pro ukládání osobních věcí, které nejsou povoleny v zabezpečených místnostech (telefony, pera atd.);

b) komunikační místnost pro předávání a přijímání utajovaných informací, včetně zašifrovaných utajovaných informací, v souladu s bezpečnostním upozorněním 3 a příslušnými pokyny pro nakládání s důvěrnými informacemi;

c) zabezpečený archiv využívající schválené kontejnery s osvědčením, odděleně pro informace se stupněm utajení RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET EU/EU SECRET a stupněm rovnocenným. Informace se stupněm utajení TRES SECRETUE/EU TOP SECRET nebo stupněm rovnocenným jsou umístěny v oddělené místnosti ve zvláštním schváleném kontejneru. Jediným dalším zařízením v této místnosti je zařízení podpory pro nakládání s archivem poskytované oddělením CIU;

d) místnost s registrem vybavená nástroji potřebnými k tomu, aby mohla být registrace provedena na papíře nebo elektronicky, tedy vybavená zabezpečeným zařízením potřebným k instalaci příslušného komunikačního a informačního systému. Pouze v místnosti s registrem se mohou vyskytovat schválená a certifikovaná reprodukční zařízení (papírové či elektronické kopie). Pokyny pro nakládání s důvěrnými informacemi specifikují, která reprodukční zařízení jsou schválena a certifikována. Místnost s registrem musí mít rovněž kapacitu potřebnou pro uchovávání certifikovaného materiálu a nakládání s ním, je-li jej zapotřebí pro označení, kopírování a odeslání utajovaných informací ve fyzické podobě, podle stupně utajení. Veškerý certifikovaný materiál je na základě rady poskytnuté provozním orgánem pro zabezpečení informací definován oddělením CIU a certifikován orgánem pro bezpečnostní akreditaci. Tato místnost je dále vybavena certifikovaným destrukčním zařízením, schváleným pro nejvyšší stupeň utajení, jež je popsáno v pokynech pro nakládání s důvěrnými informacemi. Překlad informací se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET a stupněm rovnocenným se provádí v místnosti s registrem a v příslušném certifikovaném systému. Místnost s registrem obsahuje pracovní stanice umožňující práci na tomtéž dokumentu až dvěma překladatelům současně. Je přítomen jeden pracovník oddělení CIU.

e) čítárna sloužící k individuálnímu prohlížení utajovaných informací řádně oprávněnými osobami. Čítárna má dostatek prostoru pro dvě osoby, z nichž jednou je pracovník oddělení CIU, který je vždy přítomen po celou dobu prohlížení důvěrných informací. U této místnosti se počítá se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET. Čítárna může být vybavena zařízením TEMPEST umožňujícím v případě potřeby elektronické prohlížení informací, v souladu se stupněm utajení daných informací.

f) zasedací místnost, do níž se vejde až 25 osob, sloužící k diskusi o informacích se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET EU/EU SECRET a stupněm rovnocenným. Zasedací místnost je vybavena zabezpečeným a schváleným technickým zařízením s osvědčením, které je nezbytné pro tlumočení až ve dvou jazycích. Když není využívána ke schůzím, je možné zasedací místnost využívat jako další čítárnu pro individuální prohlížení informací. Ve výjimečných případech může oddělení CIU povolit prohlížení utajovaných informací více než jedné oprávněné osobě, pokud mají všechny oprávněné osoby v místnosti tentýž stupeň prověrky a stejnou potřebu vědět. Prohlížení utajovaných informací není možné povolit více než čtyřem osobám najednou. Přítomnost pracovníků oddělení CIU je posílena.

g) zabezpečené technické místnosti pro uložení veškerého technického zařízení souvisejícího s celým zabezpečeným prostorem a zabezpečené servery IT.

20. Zabezpečený prostor splňuje platné mezinárodní bezpečnostní normy a je schválen ředitelstvím pro bezpečnost a posuzování rizika. Zabezpečený obsahuje tyto minimální technické bezpečnostní požadavky:

a) poplašné a sledovací bezpečnostní systémy;

b) bezpečnostní vybavení a nouzový systém (systém dvousměrného varování);

c) systém CCTV;

d) systém pro odhalování vniknutí;

e) kontrola přístupu (včetně biometrického bezpečnostního systému);

f) kontejnery;

g) uzamykatelné skříňky;

h) protielektromagnetická ochrana.

21. Orgán pro bezpečnostní akreditaci může ve spolupráci s oddělením CIU a po schválení bezpečnostním orgánem přidat další technická bezpečnostní opatření, pokud je třeba.

22. Vybavení infrastruktury může být propojeno se systémy celkového řízení budov, v nichž se zabezpečený prostor nachází. Bezpečnostní vybavení vyhrazené pro kontrolu přístupu a pro komunikační a informační systémy je však na jakýchkoli takových stávajících systémech v Evropském parlamentu nezávislé.

H. **KONTROLY ZABEZPEČENÉHO PROSTORU**

23. Kontroly zabezpečeného prostoru provádí pravidelně a na žádost oddělení CIU orgán pro bezpečnostní akreditaci.

24. Orgán pro bezpečnostní akreditaci vypracuje a aktualizuje kontrolní seznam pro účely inspekcí obsahující položky, které je třeba během inspekce ověřit v souladu s pokyny pro nakládání s důvěrnými informacemi.

I. **PŘEPRAVA DŮVĚRNÝCH INFORMACÍ**

25. Důvěrné informace se přepravují v neprůhledném obalu bez jakéhokoli označení důvěrné povahy jejich obsahu v souladu s pokyny pro nakládání s důvěrnými informacemi.

26. Informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET nebo rovnocenným stupněm smějí přepravovat pouze kurýři nebo zaměstnanci s odpovídající úrovní bezpečnostního oprávnění.

27. Externí poštu nebo osobní přenos mimo budovu v případě utajovaných informací lze používat pouze v souladu s podmínkami uvedenými v pokynech pro nakládání s důvěrnými informacemi.

28. Informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET nebo rovnocenným nesmí být nikdy poslány elektronickou poštou nebo faxem, a to ani prostřednictvím bezpečného systému elektronické pošty nebo šifrovaného faxu. Informace se stupněm utajení RESTREINT UE/EU RESTRICTED nebo stupněm rovnocenným a jiné důvěrné informace je možné poslat elektronickou poštou, která používá certifikovaný šifrovací systém.

J. **UCHOVÁVÁNÍ DŮVĚRNÝCH INFORMACÍ**

29. Stupeň utajení nebo označení informací je určující pro úroveň ochrany těchto informací, pokud jde o jejich uchovávání, jež se provádí v zařízení schváleném pro tento účel v souladu s pokyny pro nakládání s důvěrnými informacemi.

30. Informace se stupněm utajení RESTREINT UE/EU RESTRICTED nebo se stupněm rovnocenným a jiné důvěrné informace:

a) se uchovávají v zamčené standardizované kovové skříňce, a to buď v kanceláři nebo v pracovních prostorách, nejsou-li v daném okamžiku používány;

b) nesmí být ponechány bez dozoru, pokud nejsou řádně uzamčeny a uskladněny;

c) nesmí být ponechány na pracovním či jiném stole, pokud by tam do nich mohly nahlédnout nebo je odstranit jakékoli neoprávněné osoby, např. návštěvníci, personál úklidu nebo údržby atd.;

d) nesmí se ukázat žádné neoprávněné osobě, ani se o nich nesmí s takovou osobou mluvit.

31. Informace se stupněm utajení RESTREINT UE / EU RESTRICTED nebo se stupněm rovnocenným a jiné důvěrné informace se uchovávají pouze v sekretariátech orgánů nebo funkcionářů Parlamentu nebo na oddělení CIU v souladu s pokyny pro nakládání s důvěrnými informacemi.

32. Informace se stupněm utajení CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET nebo TRÈS SECRET UE/EU TOP SECRET nebo stupněm rovnocenným:

a) se uchovávají v zabezpečeném prostoru, v bezpečnostním úschovném objektu nebo v trezorové místnosti. Ve výjimečných případech, např. je-li oddělení CIU zavřené, je lze uchovávat u bezpečnostních útvarů ve schválené bezpečnostní schránce s osvědčením;

b) nesmí být nikdy ponechány v zabezpečeném prostoru bez dozoru, pokud nebyly napřed uzamčeny ve schváleném sejfu (i v případě velmi krátké nepřítomnosti);

c) nesmí být ponechány na pracovním či jiném stole, pokud by tam do nich mohly nahlédnout nebo je odstranit jakékoli neoprávněné osoby, a to i když zůstává v místnosti odpovědný zaměstnanec oddělení CIU.

Pokud je dokument obsahující utajované informace produkován elektronicky v zabezpečeném prostoru, musí být v případě (i velmi krátké) nepřítomnosti autora dokumentu nebo odpovědného zaměstnance oddělení CIU dotyčný počítač uzamčen a obrazovka znepřístupněna. Za dostatečné opatření se nepovažuje bezpečnostní uzamčení spouštěné automaticky po několika minutách nečinnosti.

BEZPEČNOSTNÍ UPOZORNĚNÍ 5

PRŮMYSLOVÁ BEZPEČNOST

A. **ÚVOD**

1. Toto bezpečnostní upozornění se týká pouze utajovaných informací.

2. Obsahuje ustanovení pro uplatňování společných minimálních norem z části 1 přílohy I tohoto rozhodnutí.

3. Průmyslovou bezpečností se rozumí uplatňování opatření k zajištění ochrany utajovaných informací 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.

4. Evropský parlament 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.

B. **PRVKY UTAJOVANÉ SMLOUVY TÝKAJÍCÍ SE BEZPEČNOSTI**

B.1. ***Příručka pro stanovování stupňů utajení***

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

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

a) při přípravě příručky pro stanovování stupňů utajení bere Evropský parlament 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.

B.2. ***Seznam bezpečnostních požadavků***

7. 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.

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

B.3. ***Bezpečnostní pokyny k programu/projektu***

9. V závislosti na rozsahu programů nebo projektů, které zahrnují přístup k utajovaným informacím EU nebo nakládání s nimi či jejich uchovávání, může orgán zadávající zakázku a pověřený řízením programu nebo projektu připravit zvláštní bezpečnostní pokyny k dotčenému programu či projektu.

C. **OSVĚDČENÍ O BEZPEČNOSTNÍ PROVĚRCE ZAŘÍZENÍ**

10. Osvědčení o bezpečnostní prověrce zařízení vydává vnitrostátní 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 stupni utajení CONFIDENTIEL UE/EU CONFIDENTIAL nebo SECRET UE/EU SECRET nebo stupni rovnocenném. Důkaz o vydání osvědčení o bezpečnostní prověrce je třeba předložit Evropskému parlamentu 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.

11. Osvědčení o bezpečnostní prověrce zařízení:

a) posoudí integritu průmyslového nebo jiného subjektu;

b) posoudí vlastnické vztahy, kontrolu nebo jakýkoliv 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 tímto rozhodnutím; a

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.

12. Evropský parlament jakožto zadavatel oznámí, pokud to bude nutné, příslušnému vnitrostátnímu 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 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.

13. Zadavatel neuzavře utajovanou smlouvu s upřednostňovaným uchazečem, dokud neobdrží od vnitrostátního 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.

14. Kterýkoli příslušný bezpečnostní orgán, který vydal osvědčení o bezpečnostní prověrce zařízení, oznamuje Evropskému parlamentu jakožto zadavateli změny týkající se osvědčení o bezpečnostní prověrce zařízení. V případě subdodavatelské smlouvy je příslušný bezpečnostní orgán odpovídajícím způsobem informován.

15. Zrušení osvědčení o bezpečnostní prověrce zařízení příslušným vnitrostátním bezpečnostním orgánem nebo kterýmkoli jiným příslušným bezpečnostním orgánem je dostatečným důvodem k tomu, aby Evropský parlament jakožto zadavatel vypověděl utajovanou smlouvu nebo aby vyloučil určitého uchazeče z nabídkového řízení.

D. **UTAJOVANÉ SMLOUVY A UTAJOVANÉ SUBDODAVATELSKÉ SMLOUVY**

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

17. Jakmile je zadána zakázka na základě utajované smlouvy nebo utajované subdodavatelské smlouvy, Evropský parlament jakožto zadavatel informuje vnitrostátní bezpečnostní orgán příslušný pro daného dodavatele nebo subdodavatele nebo jakýkoli jiný příslušný bezpečnostní orgán o bezpečnostních ustanoveních utajované smlouvy.

18. V případě vypovězení této smlouvy Evropský parlament jakožto zadavatel (nebo v případě subdodavatelské smlouvy případně příslušný bezpečnostní orgán) uvědomí neprodleně vnitrostátní bezpečnostní orgán nebo kterýkoli jiný příslušný bezpečnostní orgán členského státu, v němž je dodavatel nebo subdodavatel registrován.

19. Obecně platí, že v případě vypovězení utajované smlouvy nebo utajované subdodavatelské smlouvy musí dodavatel nebo subdodavatel vrátit zadavateli veškeré utajované informace v jeho držení.

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

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

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

23. Předtím než dodavatel zadá jakékoli části utajované smlouvy subdodavateli, musí získat povolení od Evropského parlamentu jakožto zadavatele. Žádná subdodavatelská smlouva nesmí být uzavřena s průmyslovými nebo jinými subjekty registrovanými ve třetím státě, který s EU neuzavřel smlouvu o bezpečnosti informací.

24. 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.

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

E. **NÁVŠTĚVY SOUVISEJÍCÍ S UTAJOVANÝMI SMLOUVAMI**

26. Pokud Evropský parlament, 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 nebo s kterýmkoli jiným příslušným bezpečnostním orgánem. Vnitrostátní bezpečnostní orgány se však mohou v rámci konkrétních projektů dohodnout na postupu, kterým se mohou návštěvy sjednávat přímo.

27. Všechny navštěvující osoby musí být držiteli odpovídajícího osvědčení o bezpečnostní prověrce personálu a musí mít potřebu seznámit se s utajovanými informacemi souvisejícími se smlouvou uzavřenou Evropským parlamentem.

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

F. **PŘENOS A PŘEPRAVA UTAJOVANÝCH INFORMACÍ**

29. Pokud jde o elektronický přenos utajovaných informací, použijí se příslušná ustanovení bezpečnostního upozornění 3.

30. Pokud jde o přepravu utajovaných informací, použijí se příslušná ustanovení bezpečnostního upozornění 4 a příslušné pokyny pro nakládání s důvěrnými informacemi.

31. 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 nebo stupněm rovnocenným musí odesílatel vypracovat přepravní plán, který schválí generální tajemník;

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

f) přepravní trasy vždy, kdy je to možné, vedou přes území členských států.

G. **POSKYTOVÁNÍ UTAJOVANÝCH INFORMACÍ DODAVATELŮM SE SÍDLEM V TŘETÍCH STÁTECH**

32. Utajované informace jsou dodavatelům a subdodavatelům se sídlem v třetích státech poskytovány v souladu s bezpečnostními opatřeními dohodnutými mezi Evropským parlamentem jakožto zadavatelem a dotyčným třetím státem, v němž je dodavatel registrován.

H. **NAKLÁDÁNÍ S INFORMACEMI SE STUPNĚM UTAJENÍ REISTREINT UE/EU RESTRICTED A JEJICH UCHOVÁVÁNÍ**

33. Evropský parlament jakožto zadavatel je oprávněn případně ve spojení s vnitrostátním 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.

34. Evropský parlament jakožto zadavatel informuje vnitrostátní bezpečnostní orgány nebo kterýkoli jiný příslušný bezpečnostní orgán v rozsahu nezbytném podle vnitrostátních právních předpisů o smlouvách či subdodavatelských smlouvách obsahujících informace se stupněm utajení RESTREINT UE/EU RESTRICTED.

35. U smluv zadaných Evropským parlamentem 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.

36. Evropský parlament 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.

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

38. Pokud smlouva zahrnuje nakládání s informacemi se stupněm utajení RESTREINT UE/EU RESTRICTED v komunikačních a informačních systémech provozovaných dodavatelem, Evropský parlament jakožto zadavatel zajistí, aby ve smlouvě nebo subdodavatelské smlouvě byly uvedeny nezbytné technické a správní požadavky týkající se akreditace komunikačních a informačních systémů, které budou přiměřené posouzenému riziku a zohlední všechny příslušné faktory. Zadavatel a příslušný vnitrostátní bezpečnostní orgán / určený bezpečnostní orgán se dohodnou na rozsahu akreditace takových komunikačních a informačních systémů.

BEZPEČNOSTNÍ UPOZORNĚNÍ 6

NARUŠENÍ BEZPEČNOSTI, ZTRÁTA NEBO OHROŽENÍ DŮVĚRNÝCH INFORMACÍ

1. K narušení bezpečnosti dochází v důsledku jednání nebo opomenutí v rozporu s tímto rozhodnutím, které může vystavit nebezpečí nebo ohrozit důvěrné informace.

2. K vyzrazení důvěrných informací dojde, pokud se tyto informace dostanou zcela nebo zčásti do rukou neoprávněných osob, tj. osob, které neprošly příslušnou bezpečnostní prověrkou nebo nemají potřebu vědět, nebo je-li pravděpodobné, že k takové události došlo.

3. Důvěrné informace mohou být vyzrazeny následkem neopatrnosti, nedbalosti nebo nerozvážnosti anebo činností služeb, které se zaměřují na Unii, nebo činností podvratných organizací.

4. Pokud generální tajemník odhalí prokázané nebo domnělé narušení bezpečnosti, ztráty nebo ohrožení důvěrných informací nebo je o něm informován:

a) zjistí, k čemu došlo;

b) zhodnotí a sníží na minimum způsobenou škodu;

c) provede kroky s cílem zabránit opakování události;

d) informuje příslušný orgán třetí strany nebo členského státu, který byl původcem důvěrných informací nebo tyto informace předal.

Pokud se případ dotýká poslance Evropského parlamentu, jedná generální tajemník v součinnosti s předsedou Parlamentu.

Pokud jsou informace přijaty od jiných orgánů Unie, generální tajemník jedná v souladu s příslušnými bezpečnostními opatřeními týkajícími se utajovaných informací a zavedenými opatřeními, jež jsou stanoveny v rámcové dohodě s Komisí nebo v interinstitucionální dohodě s Radou.

5. Všechny osoby, které mají nakládat s důvěrnými informacemi, jsou důkladně poučeny o bezpečnostních postupech, o nebezpečí neuvážených rozhovorů a o vztazích s tiskem a v případě potřeby podepíší prohlášení, že nevyzradí obsah důvěrných informací třetí osobě, že budou dodržovat povinnost chránit utajované informace a že si uvědomují důsledky nesplnění této povinnosti. Přístup k utajovaným informacím nebo nakládání s nimi ze strany osoby, která nebyla poučena a nepodepsala příslušné prohlášení, se považuje za narušení bezpečnosti.

6. Každý poslanec Evropského parlamentu, úředník či jiný zaměstnanec Parlamentu pracující pro politické skupiny nebo smluvní dodavatel neprodleně ohlásí generálnímu tajemníkovi veškeré porušení bezpečnosti, ztrátu nebo ohrožení důvěrných informací, o kterém se dozví.

7. V souladu s příslušnými pravidly a předpisy jsou proti jakékoli osobě, která je odpovědná za vyzrazení utajovaných informací, přijata disciplinární opatření. Těmito opatřeními není dotčena možnost soudního postihu v souladu s platnými právními předpisy.

8. Aniž jsou dotčeny další právní kroky, v případě porušení, jichž se dopustí úředníci a jiní zaměstnanci Parlamentu pracující pro politické skupiny, se použijí postupy a sankce stanovené kapitole VI služebního řádu.

9. Aniž jsou dotčeny další právní kroky, v případě porušení, jichž se dopustí poslanci Evropského parlamentu, se postupuje v souladu s čl. 9 odst. 2 a články 152, 153 a 154 jednacího řádu Parlamentu.

ISSN 1977-0863 (elektronické vydání)
ISSN 1725-5163 (papírové vydání)



Úřad pro publikace Evropské unie
2985 Lucemburk
LUCEMBURSKO

CS