

Úradný vestník

Európskej únie

C 96



Slovenské vydanie

Informácie a oznámenia

Zväzok 57

1. apríla 2014

Obsah

II Oznámenia

OZNÁMENIA INŠTITÚCIÍ, ORGÁNOV, ÚRADOV A AGENTÚR EURÓPSKEJ ÚNIE

Európsky parlament

2014/C 96/01

Rozhodnutie predsedníctva Európskeho parlamentu z 15. apríla 2013 o pravidlách zaobchádzania s dôvernými informáciami zo strany Európskeho parlamentu 1

SK

II

(Oznámenia)

OZNÁMENIA INŠTITÚCIÍ, ORGÁNOV, ÚRADOV A AGENTÚR EURÓPSKEJ
ÚNIE

EURÓPSKY PARLAMENT

ROZHODNUTIE PREDSEDNÍCTVA EURÓPSKEHO PARLAMENTU

z 15. apríla 2013

o pravidlách zaobchádzania s dôvernými informáciami zo strany Európskeho parlamentu

(2014/C 96/01)

PREDSEDNÍCTVO EURÓPSKEHO PARLAMENTU,

so zreteľom na článok 23 ods. 12 Rokovacieho poriadku Európskeho parlamentu,

keďže:

- (1) Vzhľadom na Rámcovú dohodu o vzťahoch medzi Európskym parlamentom a Európskou komisiou ⁽¹⁾ podpísanú 20. októbra 2010 (ďalej len „rámcová dohoda“) a na Medziinštitucionálnu dohodu medzi Európskym parlamentom a Radou o postupovaní utajovaných skutočností, ktorých držiteľom je Rada a ktoré sa týkajú záležitostí mimo oblasti spoločnej zahraničnej a bezpečnostnej politiky, Európskemu parlamentu a o zaobchádzaní s takýmito skutočnosťami zo strany Parlamentu ⁽²⁾ podpísanú 12. marca 2014 (ďalej len „medziinštitucionálna dohoda“) je potrebné stanoviť osobitné pravidlá zaobchádzania s dôvernými informáciami zo strany Európskeho parlamentu.
- (2) Lisabonská zmluva ukladá Európskemu parlamentu nové úlohy a aby mohol Európsky parlament vykonávať činnosti v tých oblastiach, ktoré si vyžadujú určitý stupeň utajenia, je potrebné stanoviť základné zásady, minimálne bezpečnostné normy a vhodné postupy pre zaobchádzanie s dôvernými informáciami zo strany Európskeho parlamentu, a to vrátane utajovaných skutočností.
- (3) S cieľom uľahčiť hladké fungovanie rozhodovacieho procesu v Európskej únii majú pravidlá uvedené v tomto rozhodnutí zabezpečiť rovnakú úroveň ochrany ako zabezpečujú pravidlá prijaté ostatnými inštitúciami, orgánmi, úradmi a agentúrami zriadenými zmluvami alebo na základe zmlúv alebo členskými štátmi, ako aj ich zlučiteľnosť s týmito pravidlami.
- (4) Ustanoveniami tohto rozhodnutia nie sú dotknuté súčasné a budúce pravidlá prístupu k dokumentom prijatým v súlade s článkom 15 Zmluvy o fungovaní Európskej únie (ZFEÚ).

⁽¹⁾ Ú. v. EÚ L 304, 20.11.2010, s. 47.⁽²⁾ Ú. v. EÚ C 95, 1.4.2014, s. 1.

- (5) Ustanoveniami tohto rozhodnutia nie sú dotknuté súčasné ani budúce pravidlá ochrany osobných údajov prijaté v súlade s článkom 16 ZFEÚ,

PRIJALO TOTO ROZHODNUTIE:

Článok 1

Cieľ

Toto rozhodnutie upravuje správu dôverných informácií a zaobchádzanie s nimi v Európskom parlamente vrátane ich vzniku, prijímania, zasielania a ukladania s cieľom zabezpečiť zodpovedajúcu ochranu dôvernej povahy týchto informácií. Vykonáva sa ním medziinštitucionálna dohoda a rámcová dohoda a najmä jej príloha II.

Článok 2

Vymedzenie pojmov

Na účely tohto rozhodnutia:

- a) „informácie“ sú akékoľvek písomné alebo ústne informácie, bez ohľadu na nosič informácií a autora;
- b) „dôverné informácie“ sú „utajované skutočnosti“ a neutajované „ostatné dôverné informácie“;
- c) „utajované skutočnosti“ sú „utajované skutočnosti EÚ“ a „rovnocenné utajované skutočnosti“;
- d) „utajované skutočnosti EÚ“ (USEÚ) sú akékoľvek informácie a materiály s označením „TRÈS SECRET UE/EU TOP SECRET“, „SECRET UE/EU SECRET“, „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo „RESTREINT UE/EU RESTRICTED“, ktorých neoprávnené zverejnenie by mohlo spôsobiť rôzny stupeň poškodenia záujmov Únie alebo jedného alebo viacerých členských štátov bez ohľadu na to, či takéto informácie pochádzajú z inštitúcií, orgánov, úradov alebo agentúr zriadených zmluvami alebo na základe zmlúv. V tomto ohľade sú informácie a materiály utajované na úrovni:
 - „TRÈS SECRET UE/EU TOP SECRET“ informácie a materiály, ktorých neoprávnené zverejnenie by mohlo spôsobiť mimoriadne vážne poškodenie hlavných záujmov Únie alebo jedného či viacerých členských štátov,
 - „SECRET UE/EU SECRET“ informácie a materiály, ktorých neoprávnené zverejnenie by mohlo spôsobiť vážne poškodenie hlavných záujmov Únie alebo jedného či viacerých členských štátov,
 - „CONFIDENTIEL UE/EU CONFIDENTIAL“ informácie a materiály, ktorých neoprávnené zverejnenie by mohlo spôsobiť poškodenie hlavných záujmov Únie alebo jedného či viacerých členských štátov;
 - „RESTREINT UE/EU RESTRICTED“ informácie a materiály, ktorých neoprávnené zverejnenie by mohlo byť nevýhodné pre záujmy Únie alebo jedného či viacerých členských štátov;
- e) „rovnocenné utajované skutočnosti“ sú utajované informácie vydané členskými štátmi, tretími štátmi alebo medzinárodnými organizáciami, ktorých označenie stupňa utajenia je rovnocenné s niektorým z označení stupňa utajenia USEÚ a ktoré Európskemu parlamentu postúpila Rada alebo Komisia;

- f) „ostatné dôverné informácie“ sú akékoľvek iné dôverné informácie nepodliehajúce utajeniu vrátane informácií, na ktoré sa vzťahuje ochrana údajov alebo povinnosť služobného tajomstva, ktoré vzniknú v Európskom parlamente alebo ich Európskemu parlamentu poskytnú iné inštitúcie, orgány, úrady a agentúry zriadené zmluvami alebo na základe zmlúv alebo členské štáty;
- g) „dokument“ sú akékoľvek zaznamenané informácie bez ohľadu na ich fyzickú podobu alebo vlastnosti;
- h) „materiál“ je akýkoľvek dokument alebo časť zariadenia alebo vybavenia, či už vyrobeného alebo v procese výroby;
- i) „potreba vedieť“ je potreba určitej osoby mať prístup k dôverným informáciám, aby mohla vykonávať úradnú funkciu alebo splniť úlohu;
- j) „povolenie“ je rozhodnutie, ktoré prijíma v prípade poslancov Európskeho parlamentu jeho predseda alebo v prípade úradníkov Európskeho parlamentu a ostatných zamestnancov Európskeho parlamentu pracujúcich pre politické skupiny generálny tajomník, a na základe ktorého sa jednotlivcom povoľuje prístup k utajovaným skutočnostiam na určitej úrovni, a to na základe kladného výsledku bezpečnostnej previerky vykonanej vnútroštátnym orgánom podľa vnútroštátneho práva a v súlade s ustanoveniami prílohy I časti 2;
- k) „zaradenie do nižšieho stupňa“ je zníženie stupňa utajenia;
- l) „odtajnenie“ je zrušenie akéhokoľvek utajenia;
- m) „označenie“ je značka pripojená k „ostatným dôverným informáciám“, ktorá slúži na identifikáciu vopred stanovených konkrétnych pokynov týkajúcich sa zaobchádzania s nimi alebo oblasti, na ktorú sa vzťahuje daný dokument; môžu ňou byť opatrené aj „utajované skutočnosti“ s cieľom uložiť dodatočné požiadavky na zaobchádzanie s nimi;
- n) „zrušenie označenia“ je odstránenie akéhokoľvek označenia;
- o) „pôvodca“ je riadne splnomocnený autor dôverných informácií;
- p) „bezpečnostné upozornenia“ sú vykonávacie opatrenia stanovené v prílohe II;
- q) „pokyny pre zaobchádzanie s informáciami“ sú technické pokyny vydané pre útvary Európskeho parlamentu, ktoré sa týkajú správy dôverných informácií.

Článok 3

Základné zásady a minimálne normy

1. Zaobchádzanie s dôvernými informáciami zo strany Európskeho parlamentu sa riadi základnými zásadami a minimálnymi normami stanovenými v prílohe I časti 1.

2. Európsky parlament vytvorí v súlade s týmito základnými zásadami a minimálnymi normami systém pre riadenie bezpečnosti informácií (ISMS). ISMS tvoria bezpečnostné upozornenia, pokyny pre zaobchádzanie s informáciami a príslušné články rokovacieho poriadku. Cieľom ISMS je uľahčovať parlamentnú a administratívnu prácu a pritom zabezpečovať ochranu všetkých dôverných informácií, s ktorými Európsky parlament pracuje, pričom budú v plnom rozsahu dodržiavané pravidlá, ktoré pôvodca týchto informácií stanoví v bezpečnostnom upozornení.

Spracovanie dôverných informácií automatizovanými komunikačnými a informačnými systémami (CIS) Európskeho parlamentu sa uskutočňuje v súlade s koncepciou informačnej bezpečnosti, ako je stanovené v bezpečnostnom upozornení č. 3.

3. Poslancom Európskeho parlamentu sa môžu sprístupňovať utajované informácie až do a vrátane stupňa utajenia „RESTREINT UE/EU RESTRICTED“ bez toho, aby prešli bezpečnostnou previerkou.

4. Ak je predmetná informácia so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo s rovnocenným stupňom utajenia, prístup sa udelí tým poslancom Európskeho parlamentu, ktorým predseda udelil povolenie podľa odseku 5 alebo ktorí podpísali čestné vyhlásenie o tom, že obsah týchto informácií neposkytnú tretím osobám, že budú dodržiavať povinnosť chrániť informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ a že si uvedomujú dôsledky v prípade nesplnenia tejto povinnosti.

5. Ak je predmetná informácia so stupňom utajenia „SECRET UE/EU SECRET“ alebo „TRÈS SECRET/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia, prístup sa udelí tým poslancom Európskeho parlamentu, ktorým predseda udelil povolenie:

- a) po tom, ako prešli bezpečnostnou previerkou v súlade s prílohou I časťou 2 tohto rozhodnutia, alebo
- b) po tom, ako od príslušného vnútroštátneho orgánu dostane oznámenie o tom, že dotknutí poslanci sú náležite oprávnení na základe svojej funkcie v súlade s vnútroštátnym právom.

6. Poslanci Európskeho parlamentu sú pred udelením prístupu k utajovaným skutočnostiam poučení o svojich povinnostiach týkajúcich sa ochrany takýchto skutočností v súlade s prílohou I, pričom poslanci tieto povinnosti akceptujú. A sú tiež poučení o spôsoboch zabezpečenia takejto ochrany.

7. Úradníkom Európskeho parlamentu a ostatným zamestnancom Európskeho parlamentu pracujúcim pre politické skupiny sa môžu sprístupňovať dôverné informácie, ak majú preukázateľnú „potrebu vedieť“, pričom informácie so stupňom utajenia vyšším než „RESTREINT UE/EU RESTRICTED“ sa im môžu sprístupňovať, iba ak prešli bezpečnostnou previerkou na zodpovedajúcej úrovni. Prístup k utajovaným skutočnostiam sa im udelí iba vtedy, ak boli poučení a dostali písomné pokyny týkajúce sa ich povinností ohľadom ochrany takýchto skutočností, ako aj spôsobov zabezpečenia takejto ochrany, a podpísali vyhlásenie potvrdzujúce, že uvedené pokyny dostali a zaväzujú sa ich dodržiavať v súlade so súčasnými pravidlami.

Článok 4

Vznik dôverných informácií a ich administratívne spracovanie Európskym parlamentom

1. Predseda Európskeho parlamentu, predsedovia príslušných parlamentných výborov a generálny tajomník a/alebo akákoľvek osoba, ktorej bolo vydané riadne písomné povolenie, môže byť pôvodcom dôverných informácií a/alebo utajovaných skutočností, ako sa stanovuje v bezpečnostných upozorneniach.

2. Pôvodca pri vzniku utajovaných skutočností uplatní vhodný stupeň utajenia v súlade s medzinárodnými normami a vymedzeniami uvedenými v prílohe I. Pôvodca zároveň spravidla určí adresátov, ktorí sú oprávnení na sprístupnenie informácií vzhľadom na príslušný stupeň utajenia. Tieto informácie sa oznámia oddeleniu pre utajované skutočnosti (CIU) vo chvíli, keď sa dokument na tomto oddelení uschová.

3. S „ostatnými dôvernými informáciami“ na ktoré sa vzťahuje služobné tajomstvo, sa zaobchádza v súlade s prílohami I a II a pokynmi pre zaobchádzanie s informáciami.

Článok 5

Prijímanie dôverných informácií zo strany Európskeho parlamentu

1. Dôverné informácie, ktoré Európsky parlament dostane, sa oznamujú takto:

- a) informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatné dôverné informácie“: sekretariátu parlamentného orgánu/funkcionára, ktorí podali žiadosť, alebo priamo oddeleniu CIU;
- b) informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia: oddeleniu CIU.

2. Evidenciu, ukladanie a vyšetrovateľnosť dôverných informácií uskutočňuje buď, sekretariát parlamentného orgánu/funkcionára, ktorý tieto informácie dostal, alebo prípadne oddelenie CIU.
3. Dohodnuté opatrenia, ktoré sa zriadia spoločnou dohodou, na zachovanie dôvernosti informácií v prípade dôverných informácií, ktoré poskytuje Komisia podľa bodu 3.2 prílohy II k rámcovej dohode, alebo v prípade utajovaných skutočností, ktoré poskytla Rada podľa článku 5 ods. 4 medziinštitucionálnej dohody, sa ukladajú spoločne s dôvernými informáciami na sekretariáte parlamentného orgánu/funkcionára alebo prípadne na oddelení CIU.
4. Opatrenia uvedené v odseku 3 sa môžu obdobne uplatniť aj na poskytovanie dôverných informácií zo strany iných inštitúcií, orgánov, úradov a agentúr zriadených zmluvami alebo na základe zmlúv alebo členskými štátmi.
5. S cieľom zabezpečiť úroveň ochrany zodpovedajúcu stupňu utajenia „TRÈS SECRET UE/EU TOP SECRET“ alebo rovnocennému stupňu utajenia Konferencia predsedov zriadi výbor dohľadu. Informácie so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia sa Európskemu parlamentu poskytujú v súlade s ďalšími opatreniami, ktoré sa dohodnutú medzi Európskym parlamentom a inštitúciou Únie, od ktorej dostal informáciu.

Článok 6

Poskytovanie utajovaných skutočností Európskym parlamentom tretím stranám

Európsky parlament môže na základe predchádzajúceho písomného súhlasu pôvodcu alebo prípadne inštitúcie Únie, ktorá Európskemu parlamentu poskytla utajovanú skutočnosť, poskytnúť takúto utajovanú skutočnosť tretím stranám pod podmienkou, že pri nakladaní s takouto skutočnosťou v rámci ich oddelení a priestorov zabezpečia dodržiavanie pravidiel rovnocenných pravidiel stanoveným v tomto rozhodnutí.

Článok 7

Zabezpečené zariadenia

1. Na účely správy dôverných informácií Európsky parlament zriadi zabezpečený priestor a zabezpečené čítárne.
2. Zabezpečený priestor poskytuje zariadenia na evidenciu, sprístupňovanie, archiváciu, prenos utajovaných skutočností a zaobchádzanie s nimi. Zahŕňa okrem iného čítareň a zasadacia miestnosť na sprístupňovanie utajovaných skutočností a spravuje ho oddelenie CIU.
3. Mimo zabezpečeného priestoru je možné zriadiť zabezpečené čítárne s cieľom umožniť sprístupnenie informácií so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatných dôverných informácií“. Tieto zabezpečené čítárne spravujú príslušné útvary sekretariátu parlamentného orgánu/funkcionára alebo prípadne oddelenie CIU. Nie sú v nich kopírovacie stroje, telefóny, faxové zariadenia, skenery alebo iné technické zariadenie na reprodukciu alebo prenos dokumentov.

Článok 8

Evidencia dôverných informácií, ich ukladanie a zaobchádzanie s nimi

1. Informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatné dôverné informácie“ evidujú a ukladajú príslušné útvary sekretariátu parlamentného orgánu/funkcionára alebo oddelenie CIU v závislosti od toho, kto informácie dostal.

2. Tieto podmienky sa uplatňujú na zaobchádzanie s informáciami so stupňom utajenia „RESTREINT EU/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a na „ostatné dôverné informácie“:

- a) dokumenty sa osobne odovzdajú vedúcemu sekretariátu, ktorý ich zaeviduje a vydá potvrdenie o prijatí;
- b) tieto dokumenty v čase, keď sa práve nepoužívajú, uschová sekretariát na svoju zodpovednosť na uzamknutom mieste;
- c) v žiadnom prípade sa tieto informácie nemôžu uložiť na inom nosiči informácií alebo postúpiť tretej osobe; tieto dokumenty sa môžu kopírovať len prostredníctvom riadne schváleného zariadenia, ako je uvedené v bezpečnostných upozorneniach;
- d) prístup k takýmto informáciám sa obmedzí na osoby určené pôvodcom alebo inštitúciou Únie, ktorá poskytla informácie Európskemu parlamentu, v súlade s opatreniami uvedenými v článku 4 ods. 2 alebo článku 5 ods. 3, 4 a 5;
- e) sekretariát parlamentného orgánu/funkcionára vedie záznamy o osobách, ktorým sa sprístupnili informácie, a o dátumoch a časoch tohto sprístupnenia, a postúpi tento záznam oddeleniu CIU v čase uloženia informácií na oddelení CIU.

3. Informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia oddelenie CIU eviduje a ukladá a nakladá s nimi v zabezpečenom priestore v súlade s konkrétnym stupňom utajenia a ako je vymedzené v bezpečnostných upozorneniach.

4. V prípade porušenia pravidiel uvedených v odsekoch 1 až 3 zodpovedný úradník zo sekretariátu parlamentného orgánu/funkcionára alebo prípadne oddelenia CIS informuje generálneho tajomníka, ktorý vec postúpi predsedovi, ak ide o poslanca Európskeho parlamentu.

Článok 9

Prístup k zabezpečeným zariadeniam

1. Prístup do zabezpečeného priestoru majú iba tieto osoby:

- a) osoby, ktoré sú podľa článku 3 ods. 4 až 7 oprávnené na sprístupnenie informácií, ktoré sa tam nachádzajú, a ktoré predložili žiadosť podľa článku 10 ods. 1;
- b) osoby, ktoré sú podľa článku 4 ods. 1 oprávnené vytvárať utajované skutočnosti a ktoré predložili žiadosť podľa článku 10 ods. 1;
- c) úradníci Európskeho parlamentu pracujúci na oddelení CIU;
- d) úradníci Európskeho parlamentu zodpovední za riadenie CIS;
- e) v prípade potreby úradníci Európskeho parlamentu zodpovední za všeobecnú a požiaru bezpečnosť;
- f) upratovací personál, avšak len za prítomnosti a pod dohľadom úradníka z oddelenia CIU.

2. Oddelenie CIU môže zamietnuť prístup do zabezpečeného priestoru osobe, ktorá nie je oprávnená do neho vstúpiť. Akékoľvek námietky voči tomuto zamietnutiu prístupu sa v prípade žiadosti o prístup poslanca Európskeho parlamentu predložia predsedovi a v ostatných prípadoch generálnemu tajomníkovi.

3. Generálny tajomník môže povoliť stretnutie pre obmedzený počet osôb v zasadacej miestnosti nachádzajúcej sa vnútri zabezpečeného priestoru.

4. Prístup do zabezpečenej čítárne majú iba tieto osoby:
- a) poslanci Európskeho parlamentu, úradníci Európskeho parlamentu a ostatní zamestnanci Európskeho parlamentu pracujúci pre politické skupiny, ktorí sú riadne určení na účely sprístupnenia alebo vytvorenia dôverných informácií;
 - b) úradníci Európskeho parlamentu zodpovední za riadenie CIS, úradníci sekretariátu parlamentného orgánu/funkcionára, ktorý tieto informácie dostal, a úradníci oddelenia CIU;
 - c) v prípade potreby úradníci Európskeho parlamentu zodpovední za všeobecnú a požiarnu bezpečnosť;
 - d) upratovací personál, avšak len za prítomnosti a pod dohľadom úradníka pracujúceho na sekretariáte parlamentného orgánu/funkcionára alebo prípadne na oddelení CIU.
5. Príslušný sekretariát parlamentného orgánu/funkcionára alebo prípadne oddelenie CIU môžu zamietnuť prístup do zabezpečenej čítárne každej osobe, ktorá nie je oprávnená do nej vstúpiť. Akékoľvek námietky voči tomuto zamietnutiu prístupu sa v prípade žiadosti o prístup poslanca Európskeho parlamentu predložia predsedovi a v ostatných prípadoch generálnemu tajomníkovi.

Článok 10

Sprístupnenie alebo vytvorenie dôverných informácií v zabezpečených zariadeniach

1. Každá osoba, ktorá má záujem o sprístupnenie alebo vytvorenie dôverných informácií v zabezpečenom priestore, vopred oznámi svoje meno oddeleniu CIU. Oddelenie CIU skontroluje totožnosť tejto osoby, a overí, či je oprávnená v súlade s článkom 3 ods. 3 až 7, článkom 4 ods. 1 alebo článkom 5 ods. 3, 4 a 5 na sprístupnenie alebo vytvorenie dôverných informácií.
2. Každá osoba, ktorá má v súlade s článkom 3 ods. 3 a 7 záujem o sprístupnenie dôverných informácií so stupňom utajenia „RESTREINT EU/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatných dôverných informácií“ v zabezpečenej čítárni, vopred oznámi svoje meno príslušným útvarom sekretariátu parlamentného orgánu/funkcionára alebo oddeleniu CIU.
3. S výnimkou mimoriadnych okolností (napríklad v prípade početných žiadostí o sprístupnenie informácií podaných v krátkom čase) sa môžu dôverné informácie sprístupniť v zabezpečenom priestore naraz vždy len jednej osobe za prítomnosti úradníka sekretariátu parlamentného orgánu/funkcionára alebo oddelenia CIU.
4. Počas procesu sprístupnenia informácií je zakázaná komunikácia s vonkajším prostredím (vrátane používania telefónov alebo iných technologických zariadení), robenie si poznámok a kopírovanie či fotografovanie sprístupnených dôverných informácií.
5. Predtým ako osoba dostane povolenie opustiť zabezpečené zariadenie, úradník sekretariátu parlamentného orgánu/funkcionára alebo oddelenia CIU sa uistí o tom, či sú dôverné informácie, ktoré boli sprístupnené, na mieste, neporušené a úplné.
6. V prípade porušenia vyššie uvedených pravidiel úradník sekretariátu parlamentného orgánu/funkcionára alebo oddelenia CIU informuje generálneho tajomníka, ktorý vec postúpi predsedovi, ak ide o poslanca Európskeho parlamentu.

Článok 11

Minimálne normy pre sprístupnenie dôverných informácií na schôdzi za zatvorenými dverami mimo zabezpečených zariadení

1. Informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatné dôverné informácie“ sa môžu sprístupniť členom parlamentných výborov alebo iných politických alebo administratívnych orgánov Európskeho parlamentu na schôdzi za zatvorenými dverami mimo zabezpečených zariadení.

2. V prípade okolností stanovených v odseku 1 zabezpečí sekretariát parlamentného orgánu/funkcionára zodpovedného za schôdzu, aby boli dodržané tieto podmienky:

- a) len osoby, ktoré určí predseda príslušného výboru alebo orgánu, aby sa zúčastnili schôdze, môžu vstúpiť do zasadacej miestnosti;
- b) všetky dokumenty sú očíslované, rozdane na začiatku schôdze a zozbierané na jej konci, pričom sa z týchto dokumentov nerobia poznámky a dokumenty sa nekopírujú ani nefotografujú;
- c) zápisnica zo schôdze neobsahuje zmienku o obsahu diskusie k informáciám, o ktorých sa rokovalo; zaznamenať sa môže len príslušné rozhodnutie, ak bolo prijaté;
- d) dôverné informácie poskytované ústne príjemcom v Európskom parlamente podliehajú rovnakej úrovni ochrany ako písomné dôverné informácie;
- e) v zasadacej miestnosti sa uchováva žiaden dodatočný súbor dokumentov;
- f) kópie dokumentov sa poskytnú na začiatku schôdze len v potrebnom počte účastníkom a tlmočníkom;
- g) na začiatku schôdze predseda schôdze jasne stanoví, aký stupeň utajenia/aké označenie majú dokumenty;
- h) účastníci neodnášajú dokumenty zo zasadacej miestnosti;
- i) na konci schôdze sekretariát parlamentného orgánu/funkcionára zozbiera všetky kópie dokumentov a vedie o nich záznam; a
- j) do zasadacej miestnosti, kde sa sprístupňujú príslušné dôverné informáciami alebo sa o nich rokuje, sa neberú žiadne elektronické komunikačné zariadenia alebo iné elektronické zariadenia.

3. Ak sa v súlade s výnimkami uvedenými v bode 3.2.2. prílohy II rámcovej dohody a v článku 6 ods. 5 medziinstitucionálnej dohody na schôdzi konanej za zatvorenými dverami rokuje o informáciách so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo s rovnocenným stupňom utajenia, sekretariát parlamentného orgánu/funkcionára zodpovedný za konanie schôdze okrem zabezpečenia dodržania ustanovení uvedených v odseku 2 zabezpečí, aby určené osoby, ktoré sa môžu zúčastniť na schôdzi, dodržiavali požiadavky článku 3 ods. 4 a 7.

4. V prípade stanovenom v odseku 3 poskytuje oddelenie CIU sekretariátu parlamentného orgánu/funkcionára zodpovedného za schôdzu za zatvorenými dverami potrebný počet kópií dokumentov, o ktorých sa má rokovať, ktoré sa po schôdzi vrátia oddeleniu CIU.

Článok 12

Archivovanie dôverných informácií

1. V zabezpečenom priestore sa zaistí bezpečný systém archivovania. Oddelenie CIU je zodpovedné za spravovanie bezpečného archívu v súlade so štandardnými archivačnými kritériami.

2. Utajované skutočnosti definitívne uložené na oddelení CIU a informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia uložené na sekretariáte parlamentného orgánu/funkcionára sa presunú do bezpečného archívu v zabezpečenom priestore šesť mesiacov odo dňa, keď boli naposledy sprístupnené, a najneskôr jeden rok odo dňa, keď boli uložené. „Ostatné dôverné informácie“, okrem prípadov, keď sú uložené na oddelení CIU, archivuje dotknutý sekretariát parlamentného orgánu/funkcionára v súlade s všeobecnými pravidlami zaobchádzania s dokumentmi.

3. Sprístupnenie dôverných informácií archivovaných v bezpečnom archíve sa uskutočňuje za týchto podmienok:
 - a) oprávnenie na sprístupnenie týchto informácií majú len osoby identifikované podľa mena, funkcie alebo úradu v sprievodnom dokumente vyplnenom pri uložení dôverných informácií;
 - b) žiadosť o sprístupnenie dôverných informácií sa predkladá oddeleniu CIU, ktoré zabezpečí presun príslušného dokumentu do zabezpečenej čítárne; a
 - c) uplatňujú sa postupy a podmienky pre sprístupňovanie dôverných informácií uvedené v článku 10.

Článok 13

Zaradenie do nižšieho stupňa, odtajnenie a zrušenie označenia dôverných informácií

1. Dôverným informáciám môže byť znížený stupeň utajenia, môžu byť odtajnené alebo ich označenie môže byť zrušené len s vopred udeleným súhlasom pôvodcu a, ak je to potrebné, po prediskutovaní s ostatnými zainteresovanými stranami.
2. Zníženie stupňa utajenia alebo odtajnenie sa potvrdzuje písomne. Pôvodca je zodpovedný za informovanie adresátov o tejto zmene a títo adresáti sú zase povinní informovať o tejto zmene akýchkoľvek iných následných adresátov, ktorým dokument alebo jeho kópiu zaslali. Ak je to možné, pôvodcovia vyznačujú na utajovaných dokumentoch dátum, obdobie alebo udalosť, keď sa stupeň utajenia obsahu môže znížiť alebo sa obsah môže odtajniť. Inak dokumenty revidujú aspoň každých päť rokov, aby sa presvedčili, či je pôvodné utajenie potrebné.
3. Dôverné informácie archivované v bezpečných archívoch sa preskúmajú včas a najneskôr v 25. rok po dátume ich vytvorenia, aby sa určilo, či budú alebo nebudú odtajnené, či im bude alebo nebude znížený stupeň utajenia, alebo či bude alebo nebude ich označenie zrušené. Preskúmanie a uverejnenie takýchto informácií sa uskutočňuje v súlade s ustanoveniami nariadenia Rady (EHS, Euratom) č. 354/83 z 1. februára 1983 o otvorení historických archívov Európskeho hospodárskeho spoločenstva a Európskeho spoločenstva pre atómovú energiu pre verejnosť ⁽¹⁾. Odtajnenie uskutoční pôvodca dôverných informácií alebo útvar, ktorý je práve za ne zodpovedný, v súlade s prílohou I časťou 1 oddielom 10.
4. Po odtajnení sa bývalé utajované informácie archivované v bezpečnom archíve presunú do historických archívov Európskeho parlamentu na trvalé zachovanie a ďalšie spracovanie podľa platných pravidiel.
5. Po zrušení označenia podliehajú bývalé „ostatné dôverné informácie“ pravidlám Európskeho parlamentu o zaobchádzaní s dokumentmi.

Článok 14

Narušenia bezpečnosti, strata alebo vyzradenie dôverných informácií

1. Porušenie dôvernosti vo všeobecnosti a najmä porušenie tohto rozhodnutia v prípade poslancov Európskeho parlamentu znamená uplatnenie príslušných ustanovení týkajúcich sa sankcií stanovených v Rokovacom poriadku Európskeho parlamentu.
2. Porušenie zo strany zamestnanca Európskeho parlamentu vedie k uplatneniu postupov a sankcií stanovených v Služobnom poriadku úradníkov Európskej únie a v Podmienkach zamestnávania ostatných zamestnancov Európskej únie ustanovených nariadením (EHS, Euratom, ESUO) č. 259/68 ⁽²⁾ (ďalej len „služobný poriadok“).

⁽¹⁾ Ú. v. ES L 43, 15.2.1983, s. 1.

⁽²⁾ Ú. v. ES L 56, 4.3.1968, s. 1.

3. Predseda a/alebo generálny tajomník v prípade potreby nariadia potrebné vyšetrovanie v prípade porušenia v zmysle bezpečnostného upozornenia č. 6.
4. Ak boli dôverné informácie oznámené Európskemu parlamentu inštitúciou Únie alebo členským štátom, predseda a/alebo prípadne generálny tajomník informuje dotknutú inštitúciu Únie alebo členský štát o akejkoľvek preukázanej alebo domnanej strate alebo vyzrazení dôverných informácií, o výsledkoch vyšetrovania a opatreniach prijatých na zabránenie opakovaniu.

Článok 15

Úpravy tohto rozhodnutia a jeho vykonávacích predpisov a výročné správy o uplatňovaní tohto rozhodnutia

1. Generálny tajomník navrhne akúkoľvek potrebnú úpravu tohto rozhodnutia a jeho vykonávacích príloh a tieto návrhy postúpi Predsedníctvu, ktoré o nich rozhodne.
2. Generálny tajomník je zodpovedný za vykonávanie tohto rozhodnutia útvarmi Európskeho parlamentu a vydá pokyny pre zaobchádzanie s informáciami, na ktoré sa vzťahuje ISMS, v súlade so zásadami stanovenými v tomto rozhodnutí.
3. Generálny tajomník predkladá Predsedníctvu výročnú správu o uplatňovaní tohto rozhodnutia.

Článok 16

Prechodné a záverečné ustanovenia

1. Neutajované skutočnosti, ktoré sa nachádzajú na oddelení CIU alebo v ktoromkoľvek inom archíve Európskeho parlamentu, ktoré sa považujú za dôverné a ktoré vznikli pred 1. apríla 2014, sa na účely tohto rozhodnutia považujú za „ostatné dôverné informácie“. Ich pôvodca môže kedykoľvek prehodnotiť úroveň ich dôvernosti.
2. Odchylne od článku 5 ods. 1 písm. a) a článku 8 ods. 1 tohto rozhodnutia počas obdobia dvanástich mesiacov od 1. apríla 2014 informácie poskytnuté Radou podľa medziinštitucionálnej dohody so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia sa uložia, evidujú a uchovávajú na oddelení CIU. Tieto informácie môžu byť sprístupnené v súlade s článkom 4 ods. 2 písm. a) a c) a článkom 5 ods. 4 medziinštitucionálnej dohody.
3. Rozhodnutie Predsedníctva zo 6. júna 2011 o pravidlách zaobchádzania s dôvernými informáciami zo strany Európskeho parlamentu sa zrušuje.

Článok 17

Nadobudnutie účinnosti

Toto rozhodnutie nadobúda účinnosť dňom jeho uverejnenia v Úradnom vestníku Európskej únie.

PRÍLOHA I

Časť 1

ZÁKLADNÉ ZÁSADY A MINIMÁLNE BEZPEČNOSTNÉ NORMY PRE OCHRANU DÔVERNÝCH INFORMÁCIÍ**1. ÚVOD**

Tieto ustanovenia určujú základné zásady a minimálne bezpečnostné normy pre ochranu dôverných informácií, ktoré musí dodržiavať a/alebo spĺňať Európsky parlament na všetkých svojich pracoviskách, rovnako ako všetci príjemcovia utajovaných skutočností a „ostatných dôverných informácií“, aby sa zaručila bezpečnosť a všetky dotknuté osoby si mohli byť isté, že je zabezpečená spoločná úroveň ochrany. Tieto ustanovenia sú doplnené bezpečnostnými upozoreniami uvedenými v prílohe II a inými ustanoveniami týkajúcimi sa zaobchádzania s dôvernými informáciami zo strany parlamentných výborov a iných parlamentných orgánov/funkcionárov.

2. ZÁKLADNÉ ZÁSADY

Bezpečnostná politika Európskeho parlamentu tvorí neoddeliteľnú súčasť jeho všeobecnej politiky vnútorného riadenia a vychádza teda zo zásad upravujúcich jeho všeobecnú politiku. Medzi tieto zásady patrí zákonnosť, transparentnosť, zodpovednosť, subsidiarita a proporionalita.

Zákonnosť predstavuje potrebu ostať pri vykonávaní bezpečnostných funkcií prísne v právnom rámci a dodržiavať uplatniteľné právne požiadavky. Povinnosti v oblasti bezpečnosti musia navyše vychádzať z príslušných ustanovení právnych predpisov. V plnej miere sa uplatňujú ustanovenia služobného poriadku, najmä jeho článok 17 o povinnosti zamestnancov zdržať sa nepovoleného zverejnenia informácií získaných pri vykonávaní služby a jeho hlava IV o disciplinárnych opatreniach. Napokon, porušenie bezpečnosti v rámci zodpovednosti Európskeho parlamentu sa rieši spôsobom, ktorý je v súlade s jeho rokovacím poriadkom a jeho politikou o disciplinárnych opatreniach.

Transparentnosť znamená, že v súvislosti so všetkými pravidlami a ustanoveniami týkajúcimi sa bezpečnosti je potrebná jednoznačnosť, rovnováha medzi rôznymi útvarmi a rôznymi oblasťami (fyzická bezpečnosť v porovnaní s ochranou informácií atď.) a je nevyhnutná konzistentná a štruktúrovaná politika informovanosti o bezpečnosti. Na vykonávanie bezpečnostných opatrení sú navyše potrebné jasné písomné usmernenia.

Zodpovednosť znamená, že povinnosti v oblasti bezpečnosti musia byť jednoznačne vymedzené. Okrem toho to zahŕňa aj potrebu pravidelne monitorovať, či sa tieto povinnosti riadne plnia.

Subsidiarita znamená, že bezpečnosť sa musí organizovať na čo najnižšej úrovni a čo najbližšie ku generálnym riaditeľstvám a útvarom Európskeho parlamentu.

Proporionalita znamená, že bezpečnostné činnosti musia byť prísne obmedzené iba na to, čo je absolútne nevyhnutné, a že bezpečnostné opatrenia musia byť úmerné k záujmom, ktoré sa majú chrániť, a k skutočnej alebo potenciálnej hrozbe voči týmto záujmom, aby tieto záujmy boli chránené spôsobom, ktorý zabezpečí čo najmenšie narušenie.

3. ZÁKLADY BEZPEČNOSTI INFORMÁCIÍ

Základmi dobrej bezpečnosti informácií sú:

- a) riadne komunikačné a informačné systémy (CIS). Tieto patria do zodpovednosti bezpečnostného orgánu Európskeho parlamentu (ako je vymedzená v bezpečnostnom upozornení č. 1);
- b) v rámci Európskeho parlamentu orgán pre informačnú bezpečnosť (ako je vymedzená v bezpečnostnom upozornení č. 1) zodpovedný za spoluprácu s príslušným bezpečnostným orgánom s cieľom poskytovať informácie a poradenstvo v oblasti technických hrozieb voči CIS a prostriedkov ochrany pred týmito hrozbami;
- c) úzka spolupráca medzi zodpovednými útvarmi Európskeho parlamentu a bezpečnostnými službami ostatných inštitúcií Unie.

4. ZÁSADY BEZPEČNOSTI INFORMÁCIÍ

4.1. Ciele

Hlavné ciele bezpečnosti informácií sú:

- a) chrániť dôverné informácie pred špionážou, ohrozením alebo neoprávneným prezradením;
- b) chrániť utajované skutočnosti, s ktorými sa narába v komunikačných a informačných systémoch a sieťach, pred ohrozením ich dôvernosti, celistvosti a dostupnosti;
- c) chrániť priestory Európskeho parlamentu, v ktorých sa uchovávajú utajované skutočnosti, pred sabotážou a úmyselným poškodením;
- (d) v prípade zlyhania bezpečnosti posúdiť spôsobenú škodu, obmedziť jej dôsledky, uskutočniť bezpečnostné vyšetrovanie a prijať potrebné nápravné opatrenia.

4.2. Utajovanie

4.2.1. Ak ide o dôvernosť, potrebná je starostlivosť a skúsenosti s výberom informácií a materiálu, ktoré sa majú chrániť, ako aj pri posudzovaní stupňa ochrany, ktorú si vyžadujú. Podstatné je, aby stupeň ochrany zodpovedal bezpečnostnej citlivosti jednotlivej informácie alebo materiálu, ktoré treba zabezpečiť. Aby sa zabezpečil hladký tok informácií, je potrebné predchádzať nadmernému alebo nedostatočnému utajovaniu.

4.2.2. Systém utajenia je nástroj na realizovanie zásad ustanovených v tomto oddiele. Podobný systém utajovania sa dodržiava pri plánovaní a organizovaní spôsobov členenia špionáži, sabotáži, terorizmu a iným hrozbám tak, aby sa zabezpečila maximálna ochrana najdôležitejších priestorov, v ktorých sa uchovávajú utajované skutočnosti, a najdôležitejších bodov v rámci takýchto priestorov.

4.2.3. Zodpovednosť za utajovanie informácií spočíva výlučne na pôvodcovi danej informácie.

4.2.4. Stupeň utajenia môže závisieť výlučne na obsahu danej informácie.

4.2.5. Ak je viacero informácií zoskupených spolu, ich stupeň utajenia, musí byť aspoň taký vysoký, ako je najvyšší stupeň utajenia pridelený niektorej z týchto informácií. Súbor informácií však môže mať pridelený vyšší stupeň utajenia ako jeho jednotlivé časti.

4.2.6 Utajenie sa stanoví iba vtedy, ak je potrebné, a na dobu, na akú je potrebné.

4.3. Ciele bezpečnostných opatrení

Bezpečnostné opatrenia:

- a) sa vzťahujú na všetky osoby, ktoré majú prístup k utajovaným skutočnostiam, nosiče informácií uchovávajúce utajované skutočnosti a „ostatné dôverné informácie“, ako aj na všetky priestory, v ktorých sa nachádzajú takéto informácie, a dôležité zariadenia;
- b) sú navrhnuté tak, aby sa identifikovali osoby, ktorých postavenie (pokiaľ ide o prístup, vzťahy alebo iné) môže ohroziť bezpečnosť takýchto informácií a dôležitých zariadení, ktoré uchovávajú takéto informácie, a aby umožnili vylúčenie alebo odvolanie takýchto osôb;

- c) zabraňujú osobám bez povolenia v prístupe k takýmto informáciám alebo k zariadeniam, ktoré ich obsahujú;
- d) zabezpečujú, aby sa takéto informácie rozširovali výlučne na základe zásady "potreba vedieť", ktorá je zásadná pre všetky aspekty bezpečnosti;
- e) zabezpečujú celistvosť (prevenciou pred poškodením, neoprávneným pozmenením alebo neoprávneným vymazaním) a dostupnosť (tým, ktorí potrebujú a majú povolený prístup) dôverných informácií, najmä keď sa uchovávajú, spracúvajú alebo prenášajú v elektromagnetickej podobe.

5. SPOLOČNÉ MINIMÁLNE NORMY

Európsky parlament zabezpečuje, aby spoločné minimálne bezpečnostné normy dodržiavali všetci príjemcovia utajovaných skutočností v rámci inštitúcie a pod jej právomocou, najmä všetky jeho útvary a dodávatelia tak, aby tieto informácie bolo možné odovzdať s dôverou, že sa s nimi bude zaobchádzať s rovnakou starostlivosťou. Takéto minimálne normy obsahujú kritériá pre bezpečnostnú previerku úradníkov Európskeho parlamentu a ostatných zamestnancov Európskeho parlamentu pracujúcich pre politické skupiny a postupy na ochranu dôverných informácií.

Európsky parlament umožní prístup k týmto informáciám tretím stranám iba za podmienky, že tieto tretie strany zaručia, že sa s nimi bude nakladať v súlade s ustanoveniami, ktoré sú aspoň na striktné rovnocennej úrovni, ako sú tieto spoločné minimálne normy.

Takéto spoločné minimálne normy sa tiež uplatnia, keď Európsky parlament zmluvou alebo dohodou o grante zverí úlohy zahŕňajúce dôverné informácie priemyselným alebo iným subjektom.

6. BEZPEČNOSŤ, POKIAĽ IDE O ÚRADNÍKOV EURÓPSKEHO PARLAMENTU A OSTATNÝCH ZAMESTNANCOV EURÓPSKEHO PARLAMENTU PRACUJÚCICH PRE POLITICKÉ SKUPINY

6.1. *Bezpečnostné pokyny týkajúce sa úradníkov Európskeho parlamentu a ostatných zamestnancov Európskeho parlamentu pracujúcich pre politické skupiny*

Úradníci Európskeho parlamentu a ostatní zamestnanci Európskeho parlamentu pracujúci pre politické skupiny vo funkciách, kde by mohli mať prístup k utajovaným skutočnostiam, sú pri prevzatí svojich povinností a potom v pravidelných intervaloch dôkladne poučení o potrebe bezpečnosti a o príslušných postupoch. Takéto osoby musia písomne potvrdiť, že si uplatniteľné bezpečnostné ustanovenia prečítali a plne im porozumeli.

6.2. *Zodpovednosť vedúcich pracovníkov*

Súčasťou povinností vedúcich pracovníkov musí byť znalosť tých členov ich personálu, ktorí pri práci prichádzajú do styku s utajovanými skutočnosťami, alebo ktorí majú prístup k zabezpečeným komunikačným alebo informačným systémom, a zaznamenávanie a hlásenie akejkoľvek udalosti alebo zjavného citlivého miesta, u ktorých je pravdepodobné, že by mohli mať vplyv na bezpečnosť.

6.3. *Bezpečnostné postavenie úradníkov Európskeho parlamentu a ostatných zamestnancov Európskeho parlamentu pracujúcich pre politické skupiny*

Vypracujú sa postupy, ktoré zabezpečia, že v prípade zistenia nepriaznivej informácie o úradníkovi Európskeho parlamentu alebo inom zamestnancovi Európskeho parlamentu pracujúcom pre politickú skupinu sa podniknú kroky na určenie, či daný jednotlivec pracuje s utajovanými skutočnosťami alebo má prístup k zabezpečeným komunikačným alebo informačným systémom, a informuje sa o tom zodpovedný útvar Európskeho parlamentu. Ak príslušný vnútroštatný bezpečnostný orgán uvedie, že takýto jednotlivec predstavuje bezpečnostné riziko, je vylúčený alebo odvolaný z plnenia úloh, pri ktorých by mohol ohrozovať bezpečnosť.

7. FYZICKÁ BEZPEČNOSŤ

Fyzická bezpečnosť znamená uplatňovanie fyzických a technických ochranných opatrení na zamedzenie neoprávneného prístupu k utajovaným skutočnostiam.

7.1. **Potreba ochrany**

Stupeň opatrení fyzickej bezpečnosti, ktoré sa majú uplatňovať na zaistenie ochrany utajovaných skutočností, musí byť úmerný utajeniu a rozsahu a ohrozeniu uchovávaných informácií a materiálu. Všetci držitelia utajovaných skutočností musia dodržiavať jednotné postupy týkajúce sa utajovania týchto informácií a musia spĺňať spoločné normy ochrany týkajúce sa uchovávania, prenosu a likvidácie informácií a materiálu vyžadujúcich ochranu.

7.2. **Kontrola**

Pred zanechaním priestorov obsahujúcich utajované skutočnosti bez dozoru, osoby, ktoré ich spravujú, zabezpečia, aby takéto utajované skutočnosti boli bezpečne uschované a aby boli aktivované všetky bezpečnostné zariadenia (zámk, poplašné zariadenia atď.). Po pracovnom čase sa vykonávajú ďalšie nezávislé kontroly.

7.3. **Bezpečnosť budov**

Budovy, v ktorých sa uchováajú utajované skutočnosti alebo zabezpečené komunikačné a informačné systémy, sa chránia proti neoprávnenému prístupu.

Povaha ochrany, ktorá sa poskytuje utajovaným skutočnostiam, napríklad zamrežovanie okien, zámk na dverách, stráž pri vstupoch, automatizované systémy kontroly vstupu, bezpečnostné kontroly a hliadky, poplašné systémy, systémy na zisťovanie narušenia a strážne psy, závisí od:

- a) utajenia, množstva a umiestnenia informácií a materiálov, ktoré sa majú chrániť, v rámci budovy;
- b) kvality bezpečnostných schránok pre dotknuté informácie a materiály; a
- c) fyzickej povahy a umiestnenia budovy.

Povaha ochrany poskytovaná komunikačným a informačným systémom závisí od posúdenia hodnoty príslušného majetku a možnej škody, ak by bola ohrozená bezpečnosť, od fyzickej povahy a umiestnenia budovy, v ktorej sa nachádza systém, a od umiestnenia tohto systému v budove.

7.4. **Pohotovostné plány**

Vopred sa vypracujú podrobné plány na zabezpečenie ochrany utajovaných skutočností počas núdzovej situácie

8. **VYMEDZENIE ZABEZPEČENIA, OZNAČENIA, UVEDENIE A RIADENIE UTAJOVANIA**

8.1. **Vymedzenie zabezpečenia**

Nie sú povolené žiadne iné stupne utajenia ako stupne vymedzené v článku 2 písm. d) tohto rozhodnutia.

Na určenie obmedzenia platnosti utajenia (znamenajúce pre utajované skutočnosti automatické zníženie stupňa utajenia alebo odtajnenie) sa môže použiť dohodnuté vymedzenie zabezpečenia.

Vymedzenia zabezpečenia sa používajú iba v kombinácii s utajením.

Vymedzenia zabezpečenia sú ďalej upravené v bezpečnostnom upozornení č. 2 a vymedzené v pokynoch pre zaobchádzanie s informáciami.

8.2. Označenia

Označenie sa používa na špecifikovanie vopred stanovených konkrétnych pokynov týkajúcich sa zaobchádzania s dôvernými informáciami. Označením sa môže identifikovať aj oblasť, na ktorú sa vzťahuje daný dokument, konkrétna distribúcia na základe potreby vedieť alebo (pre neutajované skutočnosti) na označenie konca zákazu.

Označenie nie je utajenie a nepoužíva sa namiesto utajenia.

Označenia sú ďalej upravené v bezpečnostnom upozornení č. 2 a vymedzené v pokynoch pre zaobchádzanie s informáciami.

8.3. Uvedenie utajení a vymedzení zabezpečenia

Uvedenie utajení, vymedzení zabezpečenia a označení sa uskutočňuje v súlade s bezpečnostným upozornením č. 2 oddielom E a pokynmi pre zaobchádzanie s informáciami.

8.4. Riadenie utajovania

8.4.1 Všeobecne

Informácie sa utajujú iba vtedy, ak je to potrebné. Utajenie sa uvedie jasne a správne a zachováva sa iba dovtedy, pokiaľ si informácie vyžadujú ochranu.

Zodpovednosť za utajovanie informácií a za každé následné zníženie stupňa utajenia alebo odtajnenie spočíva výlučne na pôvodcovi.

Úradníci Európskeho parlamentu utajujú informácie, znižujú ich stupeň utajenia alebo ich odtajujú na základe pokynov generálneho tajomníka alebo na základe jeho poverenia.

Podrobné postupy na zaobchádzanie s utajovanými dokumentmi sa koncipujú tak, aby sa im zaistila ochrana primeraná informáciám, ktoré obsahujú.

Počet osôb oprávnených byť pôvodcom informácií so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“ je čo najmenší a ich mená sú uvedené na zozname vypracovanom oddelením CIU.

8.4.2 Uplatňovanie utajenia

Utajovanie dokumentu je určené úrovňou citlivosti jeho obsahu v súlade s vymedzeniami uvedenými v článku 2 písm. d). Je dôležité, aby sa utajovanie pridelovalo správne a používalo striedmo.

Stupeň utajenia listu alebo poznámky obsahujúcej prílohy je minimálne rovnako vysoký, ako najvyšší stupeň utajenia pridelený niektorej z príloh. Pôvodca jasne uvedie stupeň, v ktorom by mal byť utajený list alebo poznámka v prípade ich oddelenia od príloh.

Pôvodca dokumentu, ktorý sa má utajovať, musí dodržiavať pravidlá stanovené vyššie a predchádzať nadmernému alebo nedostatočnému utajovaniu.

Jednotlivé strany, odseky, oddiely, prílohy, dodatky, doplnky a vložky daného dokumentu môžu vyžadovať rozličné stupne utajenia a musia sa podľa toho utajiť. Stupeň utajenia dokumentu ako celku je rovnaký, ako má jeho časť s najvyšším stupňom utajenia.

9. KONTROLY

Pravidelné vnútorné kontroly bezpečnostných mechanizmov na ochranu utajovaných skutočností vykonáva Riaditeľstvo Európskeho parlamentu pre bezpečnosť a hodnotenie rizika, pričom môže požiadať o pomoc bezpečnostné orgány Rady alebo Komisie.

Bezpečnostné orgány a príslušné útvary inštitúcií Únie môžu vykonávať v rámci dohodnutého procesu iniciovaného jednou zo strán partnerské preskúmania bezpečnostných mechanizmov na ochranu utajovaných skutočností, ktorých výmena sa uskutočňuje na základe príslušných medziinštitucionálnych dohôd.

10. POSTUPY ODTAJNENIA A ZRUŠENIA OZNAČENIA

10.1. Oddelenie CIU preskúma dôverné informácie obsiahnuté v jeho evidencii a najneskôr v 25. roku od dátumu vytvorenia dokumentu bude žiadať pôvodcu o jeho súhlas s odtajnením alebo zrušením označenia dokumentu. Dokumenty, ktoré sa neodtajnia alebo v prípade ktorých sa nezruší označenie pri prvom preskúmaní, sa opätovne pravidelne preskúmajú, a to najmenej každých päť rokov. Okrem dokumentov, ktoré sa nachádzajú v bezpečných archívoch v zabezpečenom priestore a sú riadne utajené, sa môže postup zrušenia označenia vzťahovať aj na ostatné dôverné informácie uchovávané buď parlamentným orgánom/funkcionárom alebo v útvar, ktorý zodpovedá za historické archívy Európskeho parlamentu.

10.2. Rozhodnutie týkajúce sa odtajnenia dokumentu alebo zrušenia jeho označenia prijíma vo všeobecnosti výlučne pôvodca, alebo, vo výnimočných prípadoch, sa prijíma v spolupráci s parlamentným orgánom/funkcionárom, ktorý uchováva tieto informácie, a to predtým, ako sa informácie, ktoré obsahuje, postúpia útvaru, ktorý zodpovedá za historické archívy Európskeho parlamentu. K odtajneniu utajovaných skutočností alebo zrušeniu ich označenia môže dôjsť len po predchádzajúcom písomnom súhlase pôvodcu. V prípade „ostatných dôverných informácií“ sekretariát parlamentného orgánu/funkcionára, ktorý uchováva tieto informácie, rozhodne v spolupráci s pôvodcom o tom, či môže byť označenie tohto dokumentu zrušené.

10.3. Oddelenie CIU bude v mene pôvodcu zodpovedné za informovanie adresátov dokumentu o zmene utajenia alebo označenia a adresáti sú zase zodpovední za informovanie o tejto zmene akýchkoľvek následných adresátov, ktorým dokument alebo jeho kópiu zaslali.

10.4. Odtajnenie nemá vplyv na žiadne vymedzenie zabezpečenia ani na označenia, ktoré sa na dokumente môžu vyskytovať.

10.5. V prípade odtajnenia sa pôvodný stupeň utajenia v hornej a dolnej časti každej strany škrtne. Prvá (titulná) strana dokumentu sa opečiatkuje a doplní referenčným číslom oddelenia CIU. V prípade zrušenia označenia sa pôvodné označenie v hornej časti každej strany škrtne.

10.6. Text odtajneného dokumentu alebo dokumentu so zrušeným označením sa pripojí k elektronickej zložke alebo rovnocennému systému, v ktorom bol zaevidovaný.

10.7. V prípade dokumentov spadajúcich pod výnimku súvisiacu so súkromím a integritou jednotlivca alebo obchodnými záujmami fyzickej či právnickej osoby a v prípade citlivých dokumentov sa uplatní článok 2 nariadenia (EHS, Euratom) č. 354/83.

10.8. Okrem ustanovení v bodoch 10.1 až 10.7 sa uplatňujú tieto pravidlá:

- a) pokiaľ ide o dokumenty tretích strán, oddelenie CIU pred odtajnením alebo zrušením označenia konzultuje s dotknutou treťou stranou;
- b) pokiaľ ide o výnimku súvisiacu so súkromím a integritou jednotlivca, pri odtajnení alebo zrušení označenia sa zohľadní najmä súhlas dotknutej osoby, alebo prípadne nemožnosť identifikácie dotknutej osoby;
- c) pokiaľ ide o výnimku súvisiacu s obchodnými záujmami fyzickej alebo právnickej osoby, dotknutá osoba môže byť informovaná prostredníctvom uverejnenia v *Úradnom vestníku Európskej únie* a môže sa jej dať lehota štyroch týždňov od dátumu tohto uverejnenia na vznesenie pripomienok.

Časť 2

POSTUP BEZPEČNOSTNEJ PREVIERKY

11. POSTUP BEZPEČNOSTNEJ PREVIERKY POSLANCOV EURÓPSKEHO PARLAMENTU

11.1. V záujme získania prístupu k informáciám so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo s rovnocenným stupňom utajenia musia poslanci Európskeho parlamentu získať povolenie buď v súlade s postupom uvedeným v bodoch 11.3 a 11.4 tejto prílohy alebo na základe čestného vyhlásenia o neposkytnutí informácií podľa článku 3 ods. 4 tohto rozhodnutia.

11.2 Na prístup k informáciám so stupňom utajenia „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia musia poslanci Európskeho parlamentu získať povolenie v súlade s postupom uvedeným v bodoch 11.3 a 11.14.

11.3. Povolenie sa udelí iba poslancom Európskeho parlamentu, ktorí prešli bezpečnostnou previerkou príslušných vnútroštátnych orgánov členských štátov v súlade s postupom uvedeným v bodoch 11.9 až 11.14. Za udelenie povolenia poslancom zodpovedá predseda.

11.4 Predseda môže udeliť písomné povolenie po získaní stanoviska príslušných vnútroštátnych orgánov členských štátov na základe bezpečnostnej previerky, ktorá sa vykonala v súlade s bodmi 11.8 až 11.13.

11.5. Riaditeľstvo Európskeho parlamentu pre bezpečnosť a hodnotenie rizika vedie aktualizovaný zoznam všetkých poslancov Európskeho parlamentu, ktorým sa udelilo povolenie, vrátane dočasného povolenia v zmysle bodu 11.15.

11.6. Povolenie je platné počas obdobia piatich rokov alebo počas doby trvania úloh, v súvislosti s ktorými bolo udelené, podľa toho, ktoré z týchto období je kratšie. Môže sa obnoviť v súlade s postupom uvedeným v bode 11.4.

11.7. Predseda odobere povolenie, ak sa domnieva, že na toto odobratie existujú opodstatnené dôvody. Rozhodnutie odobrať povolenie sa oznámi dotknutému poslancovi Európskeho parlamentu, ktorý môže požiadať, aby ho vypočul predseda pred tým, ako odobratie nadobudne účinnosť, a príslušnému vnútroštátnemu orgánu.

11.8. Bezpečnostná previerka sa vykonáva za pomoci dotknutého poslanca Európskeho parlamentu a na žiadosť predsedu. Príslušným vnútroštátnym orgánom na vykonanie previerky je orgán členského štátu, ktorého je dotknutý poslanec štátnym príslušníkom.

11.9. Ako súčasť postupu previerky musí dotknutý poslanec Európskeho parlamentu vyplniť formulár s osobnými informáciami.

11.10. Predseda vo svojej žiadosti príslušnému vnútroštátnemu orgánu presne uvedie stupeň utajovaných skutočností, s ktorými príde dotknutý poslanec Európskeho parlamentu do styku, aby tento orgán mohol vykonať previerku.

11.11. Celý proces bezpečnostného preverovania vykonávaný príslušným vnútroštátnym orgánom spolu so získanými výsledkami musí byť v súlade s príslušnými pravidlami a predpismi platnými v danom členskom štáte, a to vrátane pravidiel, ktoré sa týkajú odvolaní.

11.12. Ak príslušný vnútroštátny orgán vydá kladné stanovisko, predseda môže dotknutému poslancovi Európskeho parlamentu udeliť povolenie.

11.13. Negatívne stanovisko príslušného vnútroštátneho orgánu sa oznámi dotknutému poslancovi Európskeho parlamentu, ktorý môže požiadať, aby ho vypočul predseda. Ak to predseda považuje za potrebné, môže požiadať príslušný vnútroštátny orgán o doplnujúce vysvetlenia. Ak sa potvrdí negatívne stanovisko, povolenie sa neudelí.

11.14. Všetci poslanci Európskeho parlamentu, ktorým je udelené povolenie v zmysle bodu 11.3, dostanú pri udelení povolenia a potom v pravidelných intervaloch potrebné usmernenia týkajúce sa ochrany utajovaných skutočností a prostriedkov na zabezpečenie tejto ochrany. Títo poslanci podpíšu vyhlásenie potvrdzujúce prijatie týchto usmernení.

11.15. Za výnimočných okolností môže predseda po zaslaní oznámenia príslušnému vnútroštátnemu orgánu a za predpokladu, že do jedného mesiaca tento orgán nereaguje, udeliť poslancovi Európskeho parlamentu dočasné povolenie na obdobie nepresahujúce šesť mesiacov pred obdržaním výsledku previerky uvedenej v bode 11.11. Takto udelené dočasné povolenie neoprávňuje na prístup k informáciám so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia.

12. POSTUP BEZPEČNOSTNEJ PREVIERKY PRE ÚRADNÍKOV EURÓPSKEHO PARLAMENTU A OSTATNÝCH ZAMESTNANCOV EURÓPSKEHO PARLAMENTU PRACUJÚCICH PRE POLITICKÉ SKUPINY

12.1. Iba úradníci Európskeho parlamentu a ostatní zamestnanci Európskeho parlamentu pracujúci pre politické skupiny, ktorí z dôvodu svojich povinností a požiadaviek služby musia mať vedomosť o utajovaných skutočnostiach alebo s nimi musia pracovať, môžu mať prístup k takýmto informáciám.

12.2. Na prístup k informáciám so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia musia úradníci Európskeho parlamentu a ostatní zamestnanci Európskeho parlamentu pracujúci pre politické skupiny získať povolenie v súlade s postupom uvedeným v bodoch 12.3 a 12.4.

12.3. Povolenie sa udelí iba osobám uvedeným v bode 12.1, ktoré prešli bezpečnostnou previerkou príslušných vnútroštátnych orgánov členských štátov v súlade s postupom uvedeným v bodoch 12.9 až 12.14. Za udelenie povolenia úradníkom Európskeho parlamentu a ostatným zamestnancom Európskeho parlamentu pracujúcim pre politické skupiny zodpovedá generálny tajomník.

12.4. Generálny tajomník môže udeliť písomné povolenie po získaní stanoviska príslušných vnútroštátnych orgánov členských štátov na základe bezpečnostnej previerky, ktorá sa vykonala v súlade s bodmi 12.8 až 12.13.

12.5. Riaditeľstvo Európskeho parlamentu pre bezpečnosť a hodnotenie rizika vedie aktualizovaný zoznam všetkých pracovných miest, ktoré si vyžadujú bezpečnostnú previerku a ktoré poskytujú príslušné útvary Európskeho parlamentu, a všetkých osôb, ktorým sa udelilo povolenie vrátane dočasného povolenia podľa bodu 12.15.

12.6. Povolenie je platné počas obdobia piatich rokov alebo počas doby trvania úloh, v súvislosti s ktorými bolo udelené, podľa toho, ktoré z týchto období je kratšie. Môže sa obnoviť v súlade s postupom uvedeným v bode 12.4.

12.7. Generálny tajomník odobere povolenie, ak sa domnieva, že na toto odobratie existujú opodstatnené dôvody. Rozhodnutie odobrať povolenie sa oznámi dotknutému úradníkovi Európskeho parlamentu alebo inému zamestnancovi Európskeho parlamentu pracujúcemu pre politickú skupinu, ktorý môže požiadať, aby ho vypočul generálny tajomník pred tým, ako odobratie nadobudne účinnosť, a príslušnému vnútroštátnemu orgánu.

12.8. Bezpečnostná previerka sa vykonáva za pomoci dotknutého úradníka Európskeho parlamentu alebo iného zamestnanca Európskeho parlamentu pracujúceho pre politickú skupinu a na žiadosť generálneho tajomníka. Príslušným vnútroštátnym orgánom na vykonanie previerky je orgán členského štátu, ktorého je dotknutá osoba štátnym príslušníkom. Ak to umožňujú vnútroštátne právne predpisy, príslušné vnútroštátne orgány môžu vykonať prešetrenie týkajúce sa osôb, ktoré nie sú štátnymi príslušníkmi, a ktoré žiadajú o prístup k informáciám so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“.

12.9. Ako súčasť postupu previerky musí dotknutý úradník Európskeho parlamentu alebo iný zamestnanec Európskeho parlamentu pracujúci pre politickú skupinu vyplniť formulár s osobnými informáciami.

12.10. Generálny tajomník vo svojej žiadosti príslušnému vnútroštátnemu orgánu presne uvedie stupeň utajovaných skutočností, ktoré majú byť sprístupnené dotknutému úradníkovi Európskeho parlamentu alebo inému zamestnancovi Európskeho parlamentu pracujúcemu pre politickú skupinu, aby mohol vykonať previerku a poskytnúť svoje stanovisko, pokiaľ ide o vhodnú úroveň povolenia, ktorá sa má udeliť tejto osobe.

12.11. Celý proces bezpečnostného preverovania vykonávaný príslušným vnútroštátnym orgánom spolu so získanými výsledkami musí byť v súlade s príslušnými pravidlami a predpismi platnými v danom členskom štáte, a to vrátane pravidiel, ktoré sa týkajú odvolaní.

12.12. Ak príslušný vnútroštátny orgán členského štátu vydá kladné stanovisko, generálny tajomník môže dotknutému úradníkovi Európskeho parlamentu alebo inému zamestnancovi Európskeho parlamentu pracujúcemu pre politickú skupinu udeliť povolenie.

12.13. Negatívne stanovisko príslušného vnútroštátneho orgánu sa oznámi dotknutému úradníkovi Európskeho parlamentu alebo inému zamestnancovi Európskeho parlamentu pracujúcemu pre politickú skupinu, ktorý môže požiadať, aby ho vypočul generálny tajomník. Ak to generálny tajomník považuje za potrebné, môže požiadať príslušný vnútroštátny orgán o doplnujúce vysvetlenia. Ak sa potvrdí negatívne stanovisko, povolenie sa neudelí.

12.14. Všetci úradníci Európskeho parlamentu a ostatní zamestnanci Európskeho parlamentu pracujúci pre politickú skupinu, ktorým sa udelilo povolenie v zmysle bodov 12.4 a 12.5, dostanú pri udelení povolenia a potom v pravidelných intervaloch potrebné pokyny týkajúce sa ochrany utajovaných skutočností a prostriedkov na zabezpečenie tejto ochrany. Títo úradníci a zamestnanci podpíšu vyhlásenie, ktorým potvrdia prijatie týchto pokynov a ktorým sa zaviažu ich dodržiavať.

12.15. Za výnimočných okolností môže generálny tajomník po zaslaní oznámenia príslušnému vnútroštátnemu orgánu a za predpokladu, že do jedného mesiaca tento orgán nereaguje, udeliť úradníkovi Európskeho parlamentu alebo inému zamestnancovi Európskeho parlamentu pracujúcemu pre politickú skupinu dočasné povolenie na obdobie nepresahujúce šesť mesiacov pred obdržaním výsledku previerky uvedenej v bode 12.11. Takto udelené dočasné povolenia neoprávňujú na prístup k informáciám so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia.

PRÍLOHA II

ÚVOD

Týmto ustanoveniami sa stanovujú bezpečnostné upozornenia, ktorými sa upravuje a zaisťuje bezpečné zaobchádzanie s dôvernými informáciami a ich správa v Európskom parlamente. Tieto bezpečnostné upozornenia spolu s pokynmi pre zaobchádzanie s informáciami tvoria systém pre riadenie bezpečnosti informácií (ISMS) Európskeho parlamentu uvedený v článku 3 ods. 2 tohto rozhodnutia;

BEZPEČNOSTNÉ UPOZORNENIE Č. 1

Organizácia bezpečnosti v Európskom parlamente v súvislosti s ochranou dôverných informácií

BEZPEČNOSTNÉ UPOZORNENIE Č. 2

Správa dôverných informácií

BEZPEČNOSTNÉ UPOZORNENIE Č. 3

Spracovanie dôverných informácií automatizovanými komunikačnými a informačnými systémami (CIS)

BEZPEČNOSTNÉ UPOZORNENIE Č. 4

Fyzická bezpečnosť

BEZPEČNOSTNÉ UPOZORNENIE Č. 5

Priemyselná bezpečnosť

BEZPEČNOSTNÉ UPOZORNENIE Č. 6

Narušenia bezpečnosti, strata alebo vyzradenie dôverných informácií

BEZPEČNOSTNÉ UPOZORNENIE Č. 1

ORGANIZÁCIA BEZPEČNOSTI V EURÓPSKOM PARLAMENTE V SÚVISLOSTI S OCHRANOU DÔVERNÝCH INFORMÁCIÍ

1. Za celkové a jednotné vykonávanie tohto rozhodnutia zodpovedá generálny tajomník.

Generálny tajomník prijme všetky potrebné opatrenia s cieľom zabezpečiť, aby sa toto rozhodnutie uplatňovalo v priestoroch Európskeho parlamentu, poslancami Európskeho parlamentu, úradníkmi Európskeho parlamentu, ostatnými zamestnancami Európskeho parlamentu pracujúcimi pre politické skupiny a zmluvnými dodávateľmi na účel zaobchádzania s dôvernými informáciami a ich uchovávania.

2. Generálny tajomník plní funkciu bezpečnostného orgánu. Generálny tajomník zodpovedá v tejto funkcii za:

- 2.1. koordinovanie všetkých záležitostí týkajúcich sa činností Európskeho parlamentu v súvislosti s ochranou dôverných informácií;

- 2.2. schvaľovanie zriadenia zabezpečeného priestoru, zabezpečených čítární a inštalácie zabezpečeného zariadenia;
- 2.3. vykonávanie rozhodnutí, ktorými sa podľa článku 6 tohto rozhodnutia povoľuje postúpenie utajovaných skutočností Európskym parlamentom tretím stranám;
- 2.4. vyšetrovanie alebo nariadenie vyšetrovania akéhokoľvek úniku dôverných informácií, ku ktorému prvoplánovo došlo v Európskeho parlamentu, a to v súčinnosti s predsedom Európskeho parlamentu, pokiaľ sa záležitosť týka poslanca Európskeho parlamentu;
- 2.5. udržiavanie úzkych kontaktov s bezpečnostnými orgánmi ostatných inštitúcií Únie a vnútroštátnymi bezpečnostnými orgánmi v členských štátoch s cieľom zabezpečiť optimálnu koordináciu bezpečnostnej politiky v súvislosti s utajovanými skutočnosťami;
- 2.6. neustále preskúvanie bezpečnostnej politiky a postupov Európskeho parlamentu a vydávaní z toho vyplývajúcich vhodných odporúčaní;
- 2.7. upovedomenie vnútroštátneho bezpečnostného orgánu, ktorý vykonal bezpečnostnú previerku, v súlade s prílohou I časťou 2 bodom 11.3 v prípadoch akýchkoľvek nepriaznivých informácií, ktoré sa môžu tohto orgánu týkať;
3. V prípade, že sa záležitosť týka poslanca Európskeho parlamentu, postupuje generálny tajomník v rámci svojich povinností v úzkej súčinnosti s predsedom Európskeho parlamentu.
4. Pri plnení jeho zodpovedností podľa bodov 2 a 3 sú generálnemu tajomníkovi nápomocní zástupca generálneho tajomníka, riaditeľstvo pre bezpečnosť a hodnotenie rizika, riaditeľstvo pre informačné technológie (DIT) a oddelenie pre utajované skutočnosti (CIU).
 - 4.1. Riaditeľstvo pre bezpečnosť a hodnotenie rizika zodpovedá za opatrenia osobnej ochrany, a najmä za postup bezpečnostnej previerky stanovený v prílohe I časti 2. Riaditeľstvo pre bezpečnosť a posudzovanie rizika taktiež:
 - a) funguje ako kontaktný bod pre bezpečnostné orgány ostatných inštitúcií Únie a pre vnútroštátne bezpečnostné orgány v záležitostiach týkajúcich sa postupov bezpečnostnej previerky poslancov Európskeho parlamentu, úradníkov Európskeho parlamentu a ostatných zamestnancov Európskeho parlamentu pracujúcich pre politické skupiny;
 - b) poskytuje potrebné všeobecné bezpečnostné poučenia o povinnosti chrániť utajované skutočnosti a o dôsledkoch jej neplnenia;
 - c) monitoruje fungovanie zabezpečeného priestoru a zabezpečených čítární v priestoroch Európskeho parlamentu, v prípade potreby v spolupráci s bezpečnostnými útvarmi iných inštitúcií Únie a vnútroštátnymi bezpečnostnými orgánmi;
 - d) v spolupráci s bezpečnostnými orgánmi iných inštitúcií Únie a vnútroštátnymi bezpečnostnými orgánmi vykonáva audit postupov správy a uchovávaní utajovaných skutočností, zabezpečeného priestoru a zabezpečených čítární v priestoroch Európskeho parlamentu, v ktorých sa zaobchádza s utajovanými skutočnosťami;
 - e) navrhuje generálnemu tajomníkovi vhodné pokyny pre zaobchádzanie s informáciami.

4.2. DIT zodpovedá za zaobchádzanie s dôvernými informáciami prostredníctvom bezpečných IT systémov v Európskom parlamente.

4.3. Oddelenie CIU zodpovedá za:

- a) identifikáciu potrieb v oblasti bezpečnosti v záujme účinnej ochrany dôverných informácií, a to v úzkej spolupráci s riaditeľstvom pre bezpečnosť a hodnotenie rizika a DIT a s bezpečnostnými orgánmi iných inštitúcií Únie;
- b) identifikáciu všetkých aspektov správy a uchovávanía dôverných informácií v Európskom parlamente, ako sú stanovené v pokynoch pre zaobchádzanie s informáciami;
- c) prevádzkovanie zabezpečeného priestoru;
- d) správu a oboznamovanie sa s dôvernými informáciami v zabezpečenom priestore alebo v zabezpečenej čítárni oddelenia CIU v súlade s článkom 7 ods. 2 a 3 tohto rozhodnutia;
- e) správu registra oddelenia CIU;
- f) predkladanie správy bezpečnostnému orgánu o akomkoľvek preukázanom alebo domnelom narušení bezpečnosti, strate alebo vyzrazení týkajúcich sa dôverných informácií uložených v rámci oddelenia CIU a uchovávaných v zabezpečenom priestore alebo v zabezpečenej čítárni oddelenia CIU.

5. Okrem toho generálny tajomník ako bezpečnostný orgán vymenúva tieto orgány:

- a) orgán pre bezpečnostnú akreditáciu (SAA);
- b) prevádzkový orgán pre informačnú bezpečnosť (IAOA);
- c) orgán pre distribúciu kryptografických materiálov (CDA);
- d) orgán TEMPEST (TA);
- e) orgán pre informačnú bezpečnosť (IAA).

Vykonávanie týchto funkcií nevyžaduje zriadenie samostatných organizačných zložiek. Musia mať samostatné mandáty. Tieto funkcie a súvisiace povinnosti môžu však byť kombinované alebo spojené v rovnakej organizačnej zložke alebo rozdelené do rôznych organizačných zložiek pod podmienkou, že nedochádza ku konfliktu záujmov a duplicite úloh.

6. Orgán pre bezpečnostnú akreditáciu poskytuje poradenstvo vo všetkých bezpečnostných otázkach v súvislosti s akreditáciou každého systému a siete informačných technológií v Európskom parlamente tak, že:

6.1. zabezpečuje, aby CIS bol v súlade s príslušnými bezpečnostnými politikami a bezpečnostnými pokynmi, vydáva rozhodnutie o schválení CIS pre nakladanie s utajovanými skutočnosťami do určitého stupňa utajenia v jeho prevádzkovom prostredí, v ktorom uvádza podmienky akreditácie a kritériá, na základe ktorých sa vyžaduje opakované schválenie;

6.2. stanovuje proces bezpečnostnej akreditácie v súlade s príslušnými politikami, pričom jasne stanovuje podmienky schválenia CIS pod jeho dohľadom;

6.3. vymedzuje stratégiu bezpečnostnej akreditácie stanovujúcu mieru podrobností vyžadovaných v akreditačnom konaní, ktorá je primeraná požadovanej úrovni zabezpečenia;

6.4. posudzuje a schvaľuje dokumentáciu týkajúcu sa bezpečnosti vrátane vyhlásenia o riadení rizika a zvyškovom riziku, dokumentáciu týkajúcu sa overenia vykonávania bezpečnostných opatrení a bezpečnostných prevádzkových postupov a zabezpečuje, aby táto dokumentácia bola v súlade s bezpečnostnými predpismi a politikou Európskeho parlamentu;

6.5. kontroluje vykonávanie bezpečnostných opatrení súvisiacich s CIS prostredníctvom uskutočňovania alebo zadávania bezpečnostných hodnotení, kontrol alebo revízií;

6.6. identifikuje bezpečnostné požiadavky (napríklad stupne utajenia pre personál) pre pracovné miesta citlivé z hľadiska bezpečnosti v súvislosti s CIS;

6.7. schvaľuje, prípadne sa zúčastňuje spoločného schvaľovania prepojenia určitého CIS s iným CIS;

6.8. schvaľuje bezpečnostné normy technického zariadenia plánovaného pre bezpečné nakladanie s utajovanými skutočnosťami a ich ochranu;

6.9. zaisťuje, aby kryptografické produkty používané v Európskom parlamente boli zaradené do zoznamu produktov schválených EÚ; a

6.10. konzultuje s poskytovateľom systému, s aktérmi v oblasti bezpečnosti a so zástupcami užívateľov otázky týkajúce sa riadenia bezpečnostných rizík, najmä zvyškového rizika, a podmienky vydávania rozhodnutia o schválení.

7. Prevádzkový orgán pre informačnú bezpečnosť zodpovedá za:

7.1. vypracovanie bezpečnostnej dokumentácie v súlade s bezpečnostnými politikami a pokynmi, najmä vrátane vyhlásenia o zostatkovom riziku, bezpečnostných prevádzkových postupov a plánu kryptografickej ochrany v rámci akreditačného konania pre CIS;

7.2. účasť pri výbere a testovaní technických bezpečnostných opatrení, zariadení a softvéru pre konkrétne systémy, dohľad nad ich používaním a zabezpečenie ich bezpečnej inštalácie, konfigurácie a údržby v súlade s príslušnou bezpečnostnou dokumentáciou;

7.3. monitorovanie zavádzania a uplatňovania bezpečnostných prevádzkových postupov, a prípadne delegovanie operačných bezpečnostných zodpovedností na vlastníka systému, konkrétne oddelenie CIU;

7.4. správu kryptografických produktov a zaobchádzanie s nimi, zabezpečenie ochrany kryptografických prvkov a kontrolovaných prvkov a v prípade potreby zabezpečenie vytvárania kryptografických premenných;

7.5. vykonávanie preskúmaní bezpečnostných analýz a testov, najmä na účel vypracovávania príslušných správ o riziku podľa požiadaviek orgánu pre bezpečnostnú akreditáciu;

7.6. zabezpečovanie odbornej prípravy v oblasti informačnej bezpečnosti konkrétnych CIS;

7.7. zavádzanie a vykonávanie bezpečnostných opatrení vzťahujúcich sa na konkrétne CIS.

8. Orgán pre distribúciu kryptografických materiálov (CDA) zodpovedá za:

8.1. správu a dokumentovanie kryptografických materiálov EÚ;

8.2. zabezpečenie v úzkej spolupráci s orgánom pre bezpečnostnú akreditáciu uplatňovania príslušných postupov a stanovenia plánov pre dokumentáciu všetkých kryptografických materiálov EÚ, bezpečného zaobchádzania s nimi a ich ukladanie a distribúciu; a

8.3. zabezpečenie distribúcie a spätného preberania kryptografických materiálov EÚ jednotlivcom alebo útvarom, ktorí ich využívajú.

9. Orgán TEMPEST zodpovedá za zabezpečenie toho, aby CIS dodržiavali politiky a pokyny TEMPEST pre zaobchádzanie s informáciami. Schvaľuje protiopatrenia pre inštalácie a produkty TEMPEST s cieľom chrániť utajované skutočnosti do určitého stupňa utajenia v ich prevádzkovom prostredí.

10. Orgán pre informačnú bezpečnosť zodpovedá za všetky hľadiská správy dôverných informácií a zaobchádzania s nimi v Európskom parlamente a osobitne za:

10.1 vypracovanie informačnej bezpečnosti a jeho bezpečnostných usmernení a sledovanie ich účinnosti a vhodnosti;

10.2. zabezpečenie a správu technických informácií týkajúcich sa kryptografických produktov;

10.3. zabezpečenie toho, aby opatrenia pre informačnú bezpečnosť zvolené na ochranu utajovaných skutočností boli v súlade s príslušnými politikami upravujúcimi ich spôsobilosť a výber;

10.4. zabezpečenie toho, aby boli kryptografické produkty zvolené v súlade s politikami upravujúcimi ich spôsobilosť a výber;

10.5. konzultácie s poskytovateľom systému, so subjektmi v oblasti bezpečnosti a zástupcami užívateľov, pokiaľ ide o informačnú bezpečnosť.

BEZPEČNOSTNÉ UPOZORNENIE Č. 2

SPRÁVA DÔVERNÝCH INFORMÁCIÍ

A. ÚVOD

1. Týmto bezpečnostným upozornením sa stanovujú ustanovenia pre správu dôverných informácií zo strany Európskeho parlamentu.

2. Pri vytváraní dôverných informácií pôvodca zváži mieru dôvernosti a prijme rozhodnutie na základe zásad stanovených v tomto bezpečnostnom upozornení pre stupeň utajenia alebo označenie daných informácií.

B. STUPEŇ UTAJENIA USEÚ

3. Rozhodnutie o tom, či sa dokumentu priradí stupeň utajenia, sa prijme pred jeho vytvorením. Na tento účel utajovanie informácií ako USEÚ zahrňuje predchádzajúce posúdenie miery ich dôvernosti a rozhodnutie pôvodcu o tom, že neoprávnené zverejnenie takýchto informácií by mohlo spôsobiť rôzny stupeň poškodenia záujmov Európskej únie alebo jedného či viacerých z jej členských štátov alebo jednotlivcov.

4. Hneď ako sa prijme rozhodnutie o utajení informácií, nasleduje druhé predchádzajúce posúdenie s cieľom stanoviť primeraný stupeň utajenia. Utajovanie dokumentov je určené úrovňou citlivosti ich obsahu.
5. Zodpovednosť za utajovanie informácií spočíva výlučne na pôvodcovi. Úradníci Európskeho parlamentu utajujú informácie na základe pokynov generálneho tajomníka alebo na základe jeho poverenia.
6. Utajenie sa používa správne a striedmo. Pôvodca dokumentu, ktorý sa má utajovať, obmedzuje tendenciu nadmerného alebo nedostatočného utajovania.
7. Stupeň utajenia priradený daným informáciám určuje stupeň ochrany týchto informácií v oblasti bezpečnosti zamestnancov, fyzickej bezpečnosti, procedurálnej bezpečnosti a informačnej bezpečnosti.
8. Informácie, ktoré si vyžadujú utajenie, sa ako také označia a musí sa s nimi tak zaobchádzať bez ohľadu na ich fyzickú podobu. Ich utajenie sa musí príjemcom jasne oznámiť, či už tým, že sú označené stupňom utajenia (ak sa poskytujú písomne, a to na papieri alebo v rámci CIS), alebo prostredníctvom oznámenia (ak sa poskytujú ústne, napríklad počas rozhovoru alebo na schôdzi konanej za zatvorenými dverami). Utajené materiály musia byť fyzicky označené, aby sa dal ľahko rozpoznať stupeň ich utajenia.
9. USEÚ v elektronickej forme možno vytvárať iba v rámci akreditovaného CIS. Samotné utajované skutočnosti, ako aj názov súboru a nosič dát (ak ide o externé zariadenie ako CD-ROM alebo USB kľúč) sú označené príslušným stupňom utajenia.
10. Informácie sa označia za utajené hneď po tom, ako nadobudnú určitú podobu. Napríklad osobné poznámky, návrhy alebo emailové správy obsahujúce informácie, ktoré si vyžadujú utajenie, sa musia od začiatku označiť ako USEÚ a musia sa vytvárať a musí sa s nimi zaobchádzať v súlade s týmto rozhodnutím a jeho pokynmi pre zaobchádzanie s informáciami vo fyzickom a technickom zmysle. Takáto informácia sa potom môže pretransformovať do oficiálneho dokumentu, ktorý bude následne primerane označený a s ktorým sa bude primerane zaobchádzať. V priebehu vypracúvania oficiálneho dokumentu môže byť potrebné vykonať prehodnotenie utajenia a prideliť vyšší alebo nižší stupeň utajenia podľa toho, ako sa mení dokument.
11. Pôvodca môže rozhodnúť o pridelení štandardného stupňa utajenia pre kategórie informácií, ktoré vytvára pravidelne. Pôvodca však zabezpečí, aby pri takomto postupe jednotlivým skutočnostiam neprideloval systematicky príliš vysoký alebo príliš nízky stupeň utajenia.
12. USEÚ sú vždy označené stupňom utajenia, ktorý zodpovedá ich stupňu utajenia.

B.1. *Stupne utajenia*

13. USEÚ sa utajujú na jednom z týchto stupňov:

— „TRÈS SECRET UE/EU TOP SECRET“, ako je vymedzené v článku 2 písm. d) tohto rozhodnutia, pričom ich ohrozenie by pravdepodobne:

- a) priamo ohrozilo vnútornú stabilitu Únie alebo jedného či viacerého z jej členských štátov alebo tretích krajín alebo medzinárodných organizácií;
- b) mimoriadne vážne poškodilo vzťahy s tretími krajinami alebo medzinárodnými organizáciami;
- c) priamo spôsobilo rozsiahle straty na životoch;

- d) mimoriadne vážne poškodilo operačnú účinnosť alebo bezpečnosť vyslaného personálu členských štátov alebo iných prispievajúcich síl alebo trvalú účinnosť mimoriadne cenných bezpečnostných alebo spravodajských operácií; alebo
 - e) mimoriadne vážne a dlhodobo poškodilo hospodárstvo Únie alebo členských štátov;
- „SECRET UE/EU SECRET“, ako je vymedzené v článku 2 písm. d) tohto rozhodnutia, pričom ich ohrozenie by pravdepodobne:
- a) významnou mierou zvýšilo medzinárodné napätie;
 - b) závažne poškodilo vzťahy s tretími krajinami a medzinárodnými organizáciami;
 - c) priamo ohrozilo životy alebo vážne narušilo verejný poriadok alebo bezpečnosť či slobodu jednotlivcov;
 - d) poškodilo zásadné obchodné alebo politické rokovania, čo by vyvolalo značné operačné problémy pre Úniu alebo členské štáty;
 - e) spôsobilo vážne poškodenie operačnej bezpečnosti členských štátov alebo efektívnosti mimoriadne cenných bezpečnostných alebo spravodajských operácií;
 - f) spôsobilo závažné materiálne škody Únii alebo členskému štátu v oblasti finančných, menových, hospodárskych a obchodných záujmov;
 - g) vážne zhoršilo finančnú situáciu významných organizácií alebo subjektov; alebo
 - h) vážne zabránilo rozvoju alebo uplatňovaniu politík Únie so závažnými hospodárskymi, obchodnými alebo finančnými dôsledkami;
- „CONFIDENTIEL UE/EU CONFIDENTIAL“, ako je vymedzené v článku 2 písm. d) tohto rozhodnutia, pričom ich ohrozenie by pravdepodobne:
- a) významne poškodilo diplomatické vzťahy, napríklad by to viedlo k oficiálnemu protestu alebo iným sankciám;
 - b) ohrozilo bezpečnosť alebo slobodu jednotlivcov;
 - c) vážne ohrozilo výsledok obchodných alebo politických rokovaní; spôsobilo operačné problémy pre Úniu alebo členské štáty;
 - d) spôsobovalo poškodenie operačnej bezpečnosti členských štátov alebo efektívnosti bezpečnostných alebo spravodajských operácií;
 - e) podstatne zhoršilo finančnú situáciu významných organizácií alebo subjektov;
 - f) bránilo vyšetrovaniu trestného činu alebo teroristickej činnosti alebo uľahčovalo páchanie trestného činu alebo teroristickej činnosti;
 - g) významne poškodzovalo finančné, menové, hospodárske a obchodné záujmy Únie alebo členských štátov;
 - h) vážne zabránilo rozvoju alebo uplatňovaniu politík Únie so závažnými hospodárskymi, obchodnými alebo finančnými dôsledkami;

- „RESTREINT UE/EU RESTRICTED“, ako je vymedzené v článku 2 písm. d) tohto rozhodnutia, pričom ich ohrozenie by pravdepodobne:
- a) bolo nevýhodné pre všeobecné záujmy Únie;
 - b) malo negatívny vplyv na diplomatické vzťahy;
 - c) spôsobilo závažné ťažkosti jednotlivcom alebo spoločnostiam;
 - d) uviedlo Úniu alebo členské štáty do nevýhodného postavenia pri obchodných alebo politických rokovaniach;
 - e) sťažilo zachovanie efektívnej bezpečnosti v Únii alebo členských štátoch;
 - f) bránilo efektívnemu rozvoju alebo uplatňovaniu politík Únie;
 - g) narušilo náležité riadenie Únie a jej činnosti;
 - h) znamenalo porušenie záväzkov Európskeho parlamentu zachovávať utajovanú povahu informácií poskytnutých tretími stranami;
 - i) spôsobilo porušenie zákonných obmedzení zverejňovania informácií;
 - j) spôsobilo finančné straty alebo jednotlivcom či spoločnostiam uľahčilo neoprávnené obohatenie sa alebo získanie neoprávnenej výhody;
 - k) bránilo vyšetrovaniu trestného činu alebo uľahčovalo jeho spáchanie.

B.2. Utajovanie kompilácií, titulných strán a výňatkov

14. Stupeň utajenia listu alebo poznámky obsahujúcej prílohy je rovnaký, ako najvyšší stupeň utajenia pridelený niektorej z príloh. Pôvodca jasne uvedie stupeň utajenia listu alebo poznámky v prípade ich oddelenia od príloh. Ak sprievodná poznámka/list nemusí byť utajené, je na nich uvedená táto záverečná formulácia: „Samostatne bez svojich príloh nie je táto poznámka/tento list utajovaná/utajovaný“.

15. Dokumenty alebo súbory obsahujúce časti s rôznym stupňom utajenia sú podľa možnosti štruktúrované tak, aby časti s rôznym stupňom utajenia bolo možné v prípade potreby jednoducho identifikovať a oddeliť. Celkový stupeň utajenia dokumentu alebo súboru musí byť aspoň taký vysoký ako v prípade jeho časti s najvyšším stupňom utajenia.

16. Jednotlivé strany, odseky, oddiely, prílohy, dodatky, doplnky a vložky daného dokumentu môžu vyžadovať rozličné stupne utajenia a musia sa podľa toho utajiť. Na označenie stupňa utajenia oddielov alebo častí textu, ktoré sú kratšie ako jedna strana, možno v dokumentoch obsahujúcich USEÚ používať štandardné skratky.

17. Keď sa spájajú informácie z rôznych zdrojov, konečný produkt sa preskúma s cieľom určiť celkový stupeň utajenia, pretože si môže vyžadovať vyšší stupeň utajenia ako jeho jednotlivé časti.

C. OSTATNÉ DÔVERNÉ INFORMÁCIE

18. „Ostatné dôverné informácie“ sa označia v súlade s bodom E tohto bezpečnostného upozornenia a pokynmi pre zaobchádzanie s informáciami.

D. VYTVÁRANIE DÔVERNÝCH INFORMÁCIÍ

19. Dôverné informácie môžu vytvárať iba osoby, ktoré sú na to oprávnené na základe tohto nariadenia alebo ktorým bezpečnostný orgán udelil povolenie.

20. Dôverné informácie sa nepridávajú do systémov pre správu dokumentov na internete alebo intranete.

D.1. Vytváranie USEÚ

21. Na vytvorenie USEÚ so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ musí mať príslušná osoba oprávnenie na základe tohto rozhodnutia alebo musí mať najprv povolenie udelené podľa článku 4 ods. 1 tohto rozhodnutia.

22. USEÚ so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ sa vytvárajú iba v zabezpečenom priestore.

23. Pri vytváraní USEÚ sa uplatňujú tieto pravidlá:

- a) na každej strane sa jasne vyznačí príslušný stupeň utajenia;
- b) každá strana je očíslovaná a uvedie sa celkový počet strán;
- c) na dokumente je uvedené referenčné číslo na prvej strane a predmet jeho obsahu, čo samo o sebe nie je utajovanou skutočnosťou, pokiaľ to za takúto informáciu nie je označené;
- d) na dokumente je uvedený dátum na prvej strane;
- e) na prvej strane akéhokoľvek dokumentu so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ sa uvádza zoznam všetkých príloh a vložiek;
- f) v dokumentoch so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“, ak sa majú distribuovať v niekoľkých kópiách, je na každej strane uvedené číslo kópie; v prípade každej kópie je tiež na prvej strane uvedený celkový počet kópií a strán; a
- g) ak dokument odkazuje na iné dokumenty obsahujúce utajované skutočnosti získané od iných inštitúcií Únie, alebo ak obsahuje utajované skutočnosti vyplývajúce z týchto dokumentov, je označený rovnakým stupňom utajenia ako tieto dokumenty a nesmie byť bez predchádzajúceho písomného súhlasu jeho pôvodcu distribuovaný osobám iným, než sú uvedené na distribučnom zozname k pôvodnému dokumentu alebo dokumentom obsahujúcim utajované skutočnosti.

24. Pôvodca si zachováva kontrolu nad USEÚ, ktoré vytvoril. Jeho predchádzajúci písomný súhlas sa vyžaduje pred tým, ako sa USEÚ:

- a) zníži stupeň utajenia alebo sa odtajnia;
- b) použijú na účely iné ako na tie, ktoré uviedol pôvodca,
- c) sprístupnia akejkolvek tretej krajine alebo medzinárodnej organizácii;
- d) sprístupnia akejkolvek osobe, inštitúcii, krajine alebo medzinárodnej organizácii inej, než adresátom, ktorých pôvodne oprávnil pôvodca na oboznámenie sa s predmetnými informáciami;

- e) sprístupnia dodávateľovi alebo budúcemu dodávateľovi, ktorý sa nachádza v tretej krajine;
- f) rozmnožujú alebo prekladajú, ak sú informácie klasifikované ako „TRÈS SECRET UE/EU TOP SECRET“;
- g) zničia.

D.2. *Vznik ostatných dôverných informácií*

25. Generálny tajomník konajúc ako bezpečnostný orgán môže rozhodnúť, či povolí vznik „ostatných dôverných informácií“ dotknutou funkciou, útvaram a/alebo osobou.

26. „Ostatné dôverné informácie“ majú jedno z označení uvedených v pokynoch pre zaobchádzanie s informáciami.

27. Pri vzniku „ostatných dôverných informácií“ sa uplatňujú tieto pravidlá:

- a) ich označenie je uvedené v hornej časti prvej strany dokumentu;
- b) každá strana je očíslovaná s celkovým počtom strán;
- c) na dokumente je uvedené referenčné číslo na prvej strane a predmet jeho obsahu;
- d) na dokumente je uvedený dátum na prvej strane; a
- e) na poslednej strane dokumentu sa uvádza zoznam všetkých príloh a vložiek.

28. Vznik „ostatných dôverných informácií“ podlieha osobitným pravidlám a postupom stanoveným v pokynoch pre zaobchádzanie s informáciami.

E. **VYMEDZENIA ZABEZPEČENIA A OZNAČENIA**

29. Účelom vymedzení zabezpečia a označení na dokumentoch je kontrola toku informácií a obmedzenie prístupu k dôverným informáciám na základe zásady „potreby vedieť“.

30. Ak sa používajú a alebo pripájajú vymedzenia zabezpečenia a/alebo označenia, dbá sa na to, aby sa zabránilo zámene so stupňami utajenia USEÚ: „RESTREINT UE/EU RESTRICTED“, „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“, „TRÈS SECRET UE/EU TOP SECRET“.

31. V pokynoch pre zaobchádzanie s informáciami sú stanovené osobitné pravidlá použitia vymedzení zabezpečenia a označení spolu so zoznamom schválených označení zabezpečenia Európskeho parlamentu.

E.1. *Vymedzenia zabezpečenia*

32. Vymedzenia zabezpečenia sa používajú iba v spojení so stupňom utajenia a neuplatňujú sa samostatne na dokumenty. Vymedzenie zabezpečenia sa môže uplatňovať na USEÚ s cieľom:

- a) stanoviť obmedzenia platnosti utajenia (pre utajované skutočnosti označujúce automatické zníženie stupňa utajenia alebo odtajnenie);
- b) obmedziť distribúciu predmetných USEÚ;
- c) stanoviť osobitné pravidlá zaobchádzania okrem tých, ktoré zodpovedajú stupňu utajenia.

33. Dodatočné kontroly uplatniteľné na zaobchádzanie a ukladanie dokumentov obsahujúcich USEÚ prinášajú všetkým zúčastneným stranám dodatočnú záťaž. Na minimalizáciu práce potrebnej v tejto súvislosti je osvedčeným postupom, že pri vytváraní takéhoto dokumentu sa stanoví lehota alebo udalosť, po ktorej utajenie automaticky uplynie a informáciám obsiahnutým v tomto dokumente sa zníži stupeň utajenia alebo sa odtajnia.

34. Ak sa dokument zaoberá konkrétnou oblasťou práce a jeho distribúcia musí byť obmedzená a/alebo predmetom osobitných pravidiel zaobchádzania, môže byť k jeho utajeniu doplnené oznámenie v tomto zmysle s cieľom pomôcť pri určovaní jeho cieľovej skupiny.

E.2. Označenia

35. Označenia nepredstavujú stupeň utajenia. Ich účelom je len poskytnúť konkrétne pokyny týkajúce sa spracovania dokumentu, a nepoužívajú sa na opis obsahu takéhoto dokumentu.

36. Označenia sa môžu použiť samostatne na dokumenty alebo spolu so stupňom utajenia.

37. Vo všeobecnosti platí, že označenia sa uplatňujú na informácie na ktoré sa vzťahuje služobné tajomstvo uvedené v článku 339 ZFEÚ a článku 17 služobného poriadku, alebo ktoré musia byť chránené Európskym parlamentom z právnych dôvodov, ale nemusia alebo nemôžu byť utajované.

E.3. Použitie označení v CIS

38. Pravidlá používania označovania platia aj v rámci akreditovaného CIS.

39. Orgán pre bezpečnostnú akreditáciu stanoví osobitné pravidlá používania označení v akreditovanom CIS.

F. PRÍJEM INFORMÁCIÍ

40. Len oddelenie CIU smie v rámci Európskeho parlamentu prijímať informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia od tretích strán.

41. Pokiaľ ide o informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a o „ostatné dôverné informácie“, za ich príjem od tretích strán a za uplatňovanie zásad stanovených v tomto bezpečnostnom upozornení môže byť zodpovedné oddelenie CIU alebo príslušný parlamentný orgán/funkcionár.

G. EVIDENCIA

42. Evidencia je uplatňovanie postupov, ktorými sa zaznamenáva životný cyklus utajovaných skutočností vrátane ich šírenia, sprístupnenia a zničenia.

43. Na účely tohto bezpečnostného upozornenia je „denník“ súpis, v ktorom sa zaznamenávajú najmä dátumy a časy, kedy dôverné informácie:

- a) vstúpili do príslušného sekretariátu parlamentného orgánu/funkcionára, alebo prípadne oddelenia CIU alebo z neho odišli;
- b) k nim pristupovala bezpečnostne preverená osoba, alebo boli postúpené takejto osobe; a
- c) boli zničené.

44. Pôvodca utajovaných skutočností je zodpovedný za označenie počiatočného vyhlásenia pri vytvorení dokumentu obsahujúceho takéto informácie. Takéto vyhlásenie sa oznámi oddeleniu CIU pri vytvorení dokumentu.

45. Informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia môže evidovať len oddelenie CIU na bezpečnostné účely. Informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatné dôverné informácie“ prijaté od tretích strán eviduje útvar zodpovedný za oficiálne prijatie dokumentu, t. j. buď oddelenie CIU alebo sekretariát parlamentného orgánu/funkcionára, na administratívne účely. „Ostatné dôverné informácie“ vypracované v rámci Európskeho parlamentu eviduje pôvodca na administratívne účely.

46. Informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia sa evidujú najmä keď:

- a) sú vypracúvané;
- b) sa doručia do oddelenia CIU alebo keď ho opustia; a
- c) sa doručia do CIS alebo keď ho opustia.

47. Informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia sa evidujú najmä keď:

- a) sú vypracúvané;
- b) sa doručia do alebo opustia príslušný sekretariát parlamentného orgánu/funkcionára, alebo oddelenie CIU; a
- c) sa doručia do CIS alebo keď ho opustia.

48. Evidencia dôverných informácií sa môže vykonávať v papierových alebo elektronických denníkoch/CIS.

49. Pokiaľ ide o informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a o „ostatné dôverné informácie“, zaznamenáva sa aspoň:

- a) dátum a čas, kedy boli doručené do alebo odišli z príslušného sekretariátu parlamentného orgánu/funkcionára, alebo prípadne oddelenia CIU;
- b) názov dokumentu, stupeň utajenia alebo označenie, dátum uplynutia utajenia/označenia a každé referenčné číslo priradené dokumentu.

50. Pokiaľ ide o informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia zaznamenáva sa aspoň:

- a) dátum a čas, keď sa doručia do oddelenia CIU alebo keď ho opustia;
- b) názov dokumentu, stupeň utajenia alebo označenie, každé referenčné číslo priradené dokumentu a dátum uplynutia utajenia/označenia;
- c) informácie o pôvodcovi;

- d) záznam totožnosti každej osoby, ktorej sa poskytol prístup k dokumentu, a dátum, kedy sa prístup tejto osoby uskutočnil;
- e) záznam o všetkých vyhotovených kópiách alebo prekladoch dokumentu;
- f) dátum a čas, keď akékoľvek kópie alebo preklady dokumentu odišli z alebo sa vrátili do oddelenia CIU, a podrobnosti o tom, kam boli zaslané a kto ich vrátil;
- g) dátum a čas, keď bol dokument zničený, a kým, v súlade s bezpečnostnými predpismi Európskeho parlamentu o skartácii; a
- h) odtajnenie alebo zníženie stupňa utajenia dokumentu.

51. Denníky sa podľa potreby utajujú alebo označujú. Denníky pre informácie so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia sa evidujú na rovnakej úrovni.

52. Utajované skutočnosti možno evidovať:

- a) v jedinom denníku; alebo
- b) v samostatných denníkoch podľa stupňa ich utajenia, skutočnosti, či ide o vstupujúce alebo vystupujúce informácie, alebo podľa ich pôvodu alebo určenia.

53. V prípade elektronického zaobchádzania v rámci CIS sa môžu evidenčné postupy vykonávať prostredníctvom takých procesov v samotnom CIS, ktoré spĺňajú požiadavky rovnocenné požiadavkám uvedeným vyššie. Kedykoľvek opustí USEÚ systém CIS, uplatňuje sa vyššie opísaný postup evidencie.

54. Oddelenie CIU vedie záznam o všetkých utajovaných skutočnostiach poskytnutých Európskym parlamentom tretím stranám a o utajovaných skutočnostiach, ktoré Európsky parlament prijal od tretích strán.

55. Po dokončení evidencie informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia oddelenie CIU skontroluje, či má adresát platné bezpečnostné povolenie. V takomto prípade oddelenie CIU adresáta informuje. Sprístupnenie utajovaných skutočností sa môže uskutočniť až po evidovaní dokumentu, ktorý ich obsahuje.

H. DISTRIBÚCIA

56. Pôvodca vypracuje prvý distribučný zoznam pre USEÚ, ktoré vytvoril.

57. Informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ a „ostatné dôverné informácie“ vytvorené Európskym parlamentom distribuuje v Európskom parlamente pôvodca v súlade s príslušnými pokynmi pre zaobchádzanie s informáciami na základe zásady „potreby vedieť“. Pre informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ vytvorené Európskym parlamentom v zabezpečenom priestore sa distribučný zoznam (a všetky ďalšie pokyny týkajúce sa distribúcie) poskytne oddeleniu CIU, ktoré je zodpovedné za jeho správu.

58. USEÚ vypracované Európskym parlamentom môže distribuovať tretím stranám len oddelenie CIU na základe zásady „potreby vedieť“.

59. Dôverné informácie, ktoré prijalo oddelenie CIU alebo akýkoľvek parlamentný orgán/funkcionár, ktorý podal príslušnú žiadosť, sú distribuované v súlade s pokynmi prijatými od pôvodcu.

I. ZAOBCHÁDZANIE, USKLADŇOVANIE A SPRÍSTUPNENIE

60. Zaobchádzanie, uskladňovanie a sprístupnenie dôverných informácií sa vykonáva v súlade s bezpečnostným upozornením č. 4 a pokynmi pre zaobchádzanie s informáciami.

J. ROZMNOŽOVANIE/PREKLAD/TLMOČENIE UTAJOVANÝCH SKUTOČNOSTÍ

61. Dokumenty obsahujúce informácie so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia sa nesmú rozmnožovať alebo prekladať bez predchádzajúceho písomného súhlasu pôvodcu. Dokumenty obsahujúce informácie so stupňom utajenia „SECRET UE/EU SECRET“ alebo s rovnocenným stupňom utajenia alebo so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo s rovnocenným stupňom utajenia sa môžu rozmnožovať alebo prekladať na základe pokynov držiteľa za predpokladu, že pôvodca to nezakázal.

62. Každá kópia dokumentu obsahujúceho informácie so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“, „SECRET UE/EU SECRET EU“ alebo „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo s rovnocenným stupňom utajenia sa eviduje z bezpečnostných dôvodov.

63. Bezpečnostné opatrenia uplatniteľné na pôvodný dokument obsahujúci utajované skutočnosti sa uplatňujú aj na jeho kópie a preklady.

64. Dokumenty prijímané od Rady by sa mali prijať vo všetkých úradných jazykoch.

65. Kópie a/alebo preklady dokumentov obsahujúcich utajované skutočnosti môže vyžiadať pôvodca alebo držiteľ kópie. Kópie dokumentov obsahujúcich informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET EU“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia sa môžu vytvárať len v zabezpečenom priestore a na kopírovacích zariadeniach, ktoré sú súčasťou akreditovaného CIS. Kópie dokumentov obsahujúcich informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatné dôverné informácie“ sa vytvárajú na akreditovanom kopírovacom zariadení v priestoroch Európskeho parlamentu.

66. Všetky kópie a preklady akýchkoľvek dokumentov alebo častí kópií dokumentov obsahujúcich utajované skutočnosti sú náležite označené, očíslované a zaevidované.

67. Nevytvárajú sa žiadne ďalšie kópie než tie, ktoré sú nevyhnutne potrebné. Všetky kópie sa zničia v súlade s pokynmi pre zaobchádzanie s informáciami na konci obdobia sprístupnenia.

68. Len tlmočníkom a prekladateľom, ktorí sú úradníkmi Európskeho parlamentu, sa udelí prístup k utajovaným skutočnostiam.

69. Tlmočníci a prekladatelia s prístupom k dokumentom obsahujúcim informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET EU“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia musia mať bezpečnostnú previerku na zodpovedajúcej úrovni.

70. Pri práci s dokumentmi obsahujúcimi informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET EU“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia tlmočníci a prekladatelia pracujú v zabezpečenom priestore.

K. ZARADENIE DO NIŽŠIEHO STUPŇA, ODTAJNENIE A ZRUŠENIE OZNAČENIA DÔVERNÝCH INFORMÁCIÍ**K.1. Všeobecné zásady**

71. Dôverné informácie sa odtajnia, zníži sa ich stupeň utajenia alebo sa zruší ich označenie, ak ich ochrana už nie je nutná alebo nie je potrebná na pôvodnej úrovni.

72. Rozhodnutia o znížení stupňa utajenia informácií obsiahnutých v dokumentoch vypracovaných v Európskom parlamente, o ich odtajnení alebo o zrušení ich označenia sa tiež môžu musieť prijať *ad hoc*, napríklad v reakcii na žiadosť o prístup verejnosti alebo inej inštitúcie Únie, alebo na podnet oddelenia CIU alebo parlamentného orgánu/funkcionára.

73. V čase jej vytvorenia pôvodca USEÚ podľa možnosti uvedie, či je možné znížiť stupeň utajenia USEÚ alebo ju odtajniť k určitému dátumu alebo po istej udalosti. Ak to nemožno uviesť, pôvodca, oddelenie CIU alebo parlamentný orgán/funkcionár, ktorý drží informácie, posúdi stupeň utajenia USEÚ najmenej raz za päť rokov. V každom prípade USEÚ sa môže zaradiť do nižšieho stupňa utajenia alebo odtajniť len po predchádzajúcom písomnom súhlase pôvodcu.

74. V prípade, ak pôvodcu USEÚ nie je možné určiť alebo vysledovať v prípade dokumentov vypracovaných v Európskom parlamente, bezpečnostný orgán prehodnotí stupeň utajenia predmetnej USEÚ na základe návrhu parlamentného orgánu/funkcionára, ktorý drží informácie, ktorý môže v tejto súvislosti konzultovať oddelenie CIU.

75. Oddelenie CIU alebo parlamentný orgán/funkcionár, ktorý drží informáciu, je zodpovedný za informovanie adresátov o odtajnení informácie alebo jej zaradení do nižšieho stupňa utajenia a títo adresáti sú zase zodpovední za informovanie o tejto zmene akýchkoľvek následných adresátov, ktorým dokument alebo jeho kópiu zaslali.

76. Odtajnenie dokumentu, zníženie stupňa utajenia alebo zrušenie označenia informácií obsiahnutých v dokumente sa zaznamenáva.

K.2. Odtajnenie

77. USEÚ môžu byť odtajnené v celku alebo čiastočne. Môžu byť odtajnené čiastočne, ak sa ochrana už nepovažuje za potrebnú pri konkrétnej časti dokumentu, ktorá ich obsahuje, ale pri zvyšku dokumentu je naďalej oprávnená.

78. Ak je výsledkom posúdenia USEÚ obsiahnutých v dokumente vytvorenom v Európskom parlamente rozhodnutie o jeho odtajnení, zväži sa otázka, či sa dokument uverejní alebo či bude mať distribučné označenie (t. j. nebude uverejnený).

79. Zrušenie utajenia USEÚ sa musí zaznamenať v denníku spolu s týmito údajmi: dátum odtajnenia, mená osôb, ktoré on požiadali a ktoré ho povolili, referenčné číslo odtajneného dokumentu a jeho konečné určenie.

80. Staré označenia utajenia sa v odtajnenom dokumente a vo všetkých jeho kópiách musia prečiarknuť. Dokumenty a všetky ich kópie sa uložia zodpovedajúcim spôsobom.

81. Po čiastočnom odtajnení utajovanej skutočnosti sa časť, ktorá sa odtajnila, vypracuje vo forme výpisu, a náležite sa uloží. Príslušný útvar zaeviduje:

- a) dátum čiastočného odtajnenia;
- b) mená osôb, ktoré žiadali o odtajnenie a ktoré ho povolili; a
- c) referenčné číslo odtajneného výpisu.

K.3. Zníženie stupňa utajenia

82. Po znížení stupňa utajenia utajovanej skutočnosti sa dokument obsahujúci tieto informácie zaeviduje v denníkoch, ktoré zodpovedajú starému i novému stupňu utajenia. Zaznamená sa dátum zníženia stupňa utajenia, ako aj meno osoby, ktorá to povolila.

83. Dokument obsahujúci informácie so zníženým stupňom utajenia a všetky jeho kópie sa klasifikuje novým stupňom utajenia a náležite sa uloží.

L. ZNIČENIE DÔVERNÝCH INFORMÁCIÍ

84. Dôverné informácie (v tlačenej alebo elektronickej podobe), ktoré už nie sú potrebné, sa zničia alebo vymažú v súlade s pokynmi pre zaobchádzanie s informáciami a platnými pravidlami archivácie.

85. Ničenie informácií so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“, alebo „SECRET UE/EU SECRET“, alebo s rovnocenným stupňom utajenia vykonáva oddelenie CIU. Toto ničenie sa vykoná za prítomnosti osoby, ktorý má bezpečnostnú previerku so stupňom utajenia zodpovedajúcim minimálne stupňu utajenia zničených informácií.

86. Informácie so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia sa zničia len s predchádzajúcim písomným súhlasom pôvodcu.

87. Informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia zničí a odstraňuje oddelenie CIU na pokyn pôvodcu alebo príslušného orgánu. Denníky a ostatné evidencie sa aktualizujú zodpovedajúcim spôsobom. Informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia zničí a odstraňuje buď oddelenie CIU alebo príslušný parlamentný orgán/funkcionár.

88. Úradník zodpovedný za zničenie a osoba prítomná pri ničení informácií podpíšu potvrdenie o zničení, ktoré sa vyplní a archivuje v oddelení CIU. Oddelenie CIU uchováva spolu s formulármi pre distribúciu dokumentov potvrdenia o zničení informácií so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia po dobu najmenej desiatich rokov, a informácií so stupňom utajenia „SECRET UE/EU SECRET“ alebo s rovnocenným stupňom utajenia a so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo s rovnocenným stupňom utajenia po dobu najmenej piatich rokov.

89. Dokumenty obsahujúce utajované skutočnosti sa zničia spôsobom, ktorý spĺňa príslušné normy Únie alebo rovnocenné normy tak, aby nebolo možné znovu zostaviť celý dokument alebo jeho časť.

90. Zničenie počítačových zálohovacích médií použitých na uloženie utajovaných skutočností sa vykonáva v súlade s príslušnými pokynmi pre zaobchádzanie s informáciami.

91. Zničenie utajovanej skutočnosti sa musí zaznamenať v príslušnom denníku spolu s týmito údajmi:

- a) dátum a čas zničenia;
- b) meno úradníka zodpovedného za zničenie;
- c) označenie zničeného dokumentu alebo jeho kópií;
- d) pôvodná fyzická forma zničených USEÚ;

- e) spôsob zničenia; a
- f) miesto zničenia.

M. ARCHIVÁCIA

92. Utajované skutočnosti vrátane všetkých sprievodných poznámok/listu, príloh, potvrdenia o odovzdaní a/alebo iných častí spisu sa premiestnia do bezpečného archívu v zabezpečenom priestore šesť mesiacov po ich poslednom prístupnutí, najneskôr však jeden rok po ich uložení. Podrobné pravidlá archivácie utajovaných skutočností sú ustanovené v pokynoch pre zaobchádzanie s informáciami.

93. V prípade „ostatných dôverných informácií“ sa uplatňujú všeobecné pravidlá o správe dokumentov bez toho, aby tým boli dotknuté ďalšie osobitné ustanovenia o zaobchádzaní s informáciami.

BEZPEČNOSTNÉ UPOZORNENIE Č. 3

SPRACOVANIE DÔVERNÝCH INFORMÁCIÍ AUTOMATIZOVANÝMI KOMUNIKAČNÝMI A INFORMAČNÝMI SYSTÉMAMI (CIS)

A. INFORMAČNÁ BEZPEČNOSŤ UTAJOVANÝCH SKUTOČNOSTÍ, S KTORÝMI SA ZAOBCHÁDZA V INFORMAČNÝCH SYSTÉMOCH

1. Informačná bezpečnosť v oblasti informačných systémov je istota, že takéto systémy ochránia utajované skutočnosti, s ktorými zaobchádzajú, a že budú fungovať tak, ako majú, a keď je to potrebné, pod dohľadom oprávnených užívateľov. Účinná informačná bezpečnosť zaisťuje náležité miery dôvernosti, celistvosti, dostupnosti, nespochybniteľnosti a autenticity. Informačná bezpečnosť je založená na procese riadenia rizika.

2. „Komunikačný a informačný systém“ (CIS) pre zaobchádzanie s utajovanými skutočnosťami znamená systém, ktorý umožňuje zaobchádzanie s informáciami v elektronickej podobe. Takýto informačný systém zahŕňa všetky zložky potrebné na jeho fungovanie vrátane infraštruktúry, organizácie, zamestnancov a informačných zdrojov.

3. V CIS sa nakladá s utajovanými skutočnosťami v súlade s koncepciou informačnej bezpečnosti.

4. CIS podlieha akreditačnému procesu. Cieľom akreditácie je získať istotu, že boli vykonané všetky primerané bezpečnostné opatrenia a že bola dosiahnutá dostatočná úroveň ochrany utajovaných skutočností a CIS v súlade s týmto bezpečnostným upozornením. Rozhodnutie o akreditácii stanovuje najvyšší stupeň utajenia informácií, s ktorými je možné v CIS zaobchádzať, a príslušné podmienky.

5. Pre bezpečné a správne fungovanie operácií CIS sú zásadné tieto vlastnosti a koncepcie informačnej bezpečnosti:

- a) autenticita: záruka, že informácie sú autentické a pochádzajú z dôveryhodných zdrojov;
- b) dostupnosť: prístupnosť a použiteľnosť informácií na žiadosť oprávneného subjektu;
- c) dôvernosť: skutočnosť, že informácie sa nespístupnia neoprávneným jednotlivcom, subjektom alebo procesom;

- d) integrita: zabezpečenie presnosti a úplnosti informácií a aktív;
- e) nespochybniteľnosť: schopnosť preukázať uskutočnenie akcie alebo udalosti tak, aby sa zamedzilo možnosti túto udalosť alebo akciu kedykoľvek následne spochybniť.

B. ZÁSADY INFORMAČNEJ BEZPEČNOSTI

6. Ustanovenia uvedené nižšie predstavujú základ bezpečnosti každého CIS, v ktorom sa manipuluje s utajovanými skutočnosťami. Podrobné požiadavky, ktorými sa vykonávajú tieto ustanovenia, sa vymedzia v bezpečnostných politikách a bezpečnostných usmerneniach pre informačnú bezpečnosť.

B.1. Riadenie bezpečnostných rizík

7. Riadenie bezpečnostných rizík tvorí neoddeliteľnú súčasť činností pri definovaní, rozvíjaní, prevádzke a údržbe CIS. Riadenie rizík (hodnotenie, zabezpečenie, akceptácia a oznamovanie) spoločne vykonávajú ako nepretržitý proces zástupcovia vlastníkov systému, projektových orgánov, operačných orgánov a orgánov schvaľujúcich bezpečnosť, ako je stanovené v bezpečnostnom upozornení č. 1, uplatňujúc overený, transparentný a plne pochopiteľný proces hodnotenia rizík. Na začiatku procesu riadenia rizík sa jednoznačne vymedzí rozsah CIS a jeho majetku.

8. Príslušné orgány stanovené v bezpečnostnom upozornení č. 1 preskúmajú potenciálne hrozby pre CIS a zabezpečujú aktualizované a presné posúdenie hrozieb, ktoré zohľadňuje aktuálne operačné prostredie. Nepretržite aktualizujú svoje poznatky o citlivých miestach a pravidelne preverujú posúdenie citlivých miest s cieľom reagovať na meniace sa prostredie v oblasti informačných technológií (IT).

9. Cieľom zabezpečenia sa proti bezpečnostným rizikám je uplatňovať súbor bezpečnostných opatrení, čím sa zabezpečí uspokojivá rovnováha medzi požiadavkami používateľov, nákladmi a zvyškovým bezpečnostným rizikom.

10. Akreditácia CIS zahŕňa formálne vyhlásenie o zvyškovom riziku a akceptáciu zvyškového rizika zo strany zodpovedného orgánu. Špecifické požiadavky, rozsah a miera podrobnosti stanovená príslušným orgánom pre bezpečnostnú akreditáciu na certifikáciu CIS zodpovedajú posúdenému riziku, pričom sa zohľadňujú všetky relevantné faktory vrátane stupňa utajenia utajovaných skutočností, s ktorými sa zaobchádza v CIS.

B.2. Bezpečnosť počas celého životného cyklu CIS

11. Zariadenie bezpečnosti predstavuje požiadavku, ktorá musí byť splnená počas celého životného cyklu CIS od jeho spustenia do prevádzky po vyradenie z prevádzky.

12. Pre každú fázu životného cyklu sa stanoví úloha a interakcia každého účastníka podieľajúceho sa na činnosti CIS, pokiaľ ide o jeho bezpečnosť.

13. CIS vrátane svojich technických a netechnických bezpečnostných opatrení podlieha počas procesu certifikácie bezpečnostnému testovaniu, ktorého cieľom je zaručiť, že sa dosiahla náležitá úroveň bezpečnosti, a overiť, že je CIS spolu so svojimi technickými a netechnickými bezpečnostnými opatreniami správne implementovaný, integrovaný a konfigurovaný.

14. Počas prevádzky a údržby CIS, ako aj v prípade vzniku výnimočných okolností sa pravidelne vykonávajú bezpečnostné hodnotenia, kontroly a previerky.

15. Vývoj bezpečnostnej dokumentácie pre CIS počas jeho životného cyklu je neoddeliteľnou súčasťou procesu riadenia zmien.

16. Postupy na účely evidencie, ktoré vykonáva CIS, sa v prípade potreby preveria v rámci postupu akreditácie.

B.3. *Najlepšie postupy*

17. Orgán pre informačnú bezpečnosť vypracúva najlepšie postupy na ochranu utajovaných skutočností, s ktorými sa zaobchádza v CIS. Pokyny týkajúce sa najlepších postupov stanovujú technické, fyzické, organizačné a procedurálne bezpečnostné opatrenia pre CIS, ktoré sa ukázali ako účinné v boji proti daným hrozbám a citlivým miestam.

18. Pri ochrane utajovaných skutočností, s ktorými sa zaobchádza v CIS, sa využívajú skúsenosti, ktoré získali subjekty zabezpečujúce informačnú bezpečnosť.

19. Šírenie a následné zavedenie najlepších postupov pomáhajú dosiahnuť rovnocennú úroveň bezpečnosti CIS, ktorý prevádzkuje sekretariát Európskeho parlamentu a v ktorom sa zaobchádza s utajovanými skutočnosťami.

B.4. *Hĺbková ochrana*

20. Na zníženie rizika pre CIS sa zavádza škála technických a netechnických bezpečnostných opatrení, ktoré sa organizujú do viacerých vrstiev ochrany. Tieto vrstvy zahŕňajú:

- a) odradenie: bezpečnostné opatrenia zamerané na odradenie protivníka od plánovania útoku na CIS;
- b) predchádzanie: bezpečnostné opatrenia zamerané na zabránenie alebo zastavenie útoku na CIS;
- c) detekciu: bezpečnostné opatrenia zamerané na zistenie výskytu útoku na CIS;
- d) odolnosť: bezpečnostné opatrenia zamerané na obmedzenie následkov útoku na minimálny súbor informácií alebo majetku CIS a zabránenie ďalším škodám; a
- e) obnovu: bezpečnostné opatrenia zamerané na znovunastolenie bezpečnej situácie CIS.

Stupeň prísnosti takýchto bezpečnostných opatrení sa stanovuje na základe posúdenia rizika.

21. Príslušné orgány stanovené v bezpečnostnom upozornení č. 1 zabezpečujú svoju spôsobilosť reagovať na incidenty, ktoré môžu prekročiť organizačné hranice, a to tak že koordinujú svoju reakciu a vymieňajú si informácie o týchto incidentoch a súvisiacich rizikách (spôsobilosť núdzovej reakcie v súvislosti s počítačmi).

B.5. *Zásada minimálnych a najnižších práv*

22. S cieľom vyhnúť sa zbytočnému riziku sa uplatňujú len základné funkcie, zariadenia a služby potrebné na splnenie operačných požiadaviek.

23. Aby sa obmedzili všetky škody vyplývajúce z porúch, omylov alebo neoprávneného využívania zdrojov CIS, majú používatelia CIS a automatizovaných procesov len taký prístup, práva alebo oprávnenia, ktoré potrebujú na plnenie svojich úloh.

B.6. Informovanosť o informačnej bezpečnosti

24. Prvou obrannou líniou bezpečnosti CIS je informovanosť o rizikách a dostupných bezpečnostných opatreniach. Najmä všetci členovia personálu, ktorí prichádzajú do kontaktu s CIS počas jeho životného cyklu, vrátane užívateľov, majú byť poučení:

- a) že bezpečnostné zlyhanie môže závažne poškodiť CIS, v ktorom sa zaobchádza s utajovanými skutočnosťami;
- b) o potenciálnych škodách pre tretie strany, ktoré môžu vyplynúť zo vzájomného prepojenia a vzájomnej závislosti, a
- c) o svojej osobnej zodpovednosti za bezpečnosť CIS, ktorá sa odvíja od ich úloh v rámci systémov a procesov.

25. Na zabezpečenie pochopenia bezpečnostných povinností sa povinne vykonáva informačno-bezpečnostné vzdelávanie a odborná príprava pre príslušný personál, ako aj vyšších riadiacich pracovníkov, poslancov Európskeho parlamentu a používateľov CIS.

B.7. Hodnotenie a schvaľovanie bezpečnostných produktov IT

26. CIS, v ktorom sa zaobchádza s utajovanými skutočnosťami so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia, musí byť chránený tak, aby nemohlo dôjsť k neúmyselnému vyzradeniu informácií prostredníctvom elektromagnetického vyžarovania (ďalej len „bezpečnostné opatrenia TEMPEST“).

27. Ak ochranu utajovaných skutočností zabezpečujú kryptografické produkty, tieto produkty dostávajú certifikát od orgánu pre bezpečnostnú akreditáciu ako kryptografické produkty schválené EÚ.

28. Počas prenosu utajovaných skutočností elektronickými prostriedkami sa použijú kryptografické produkty schválené EÚ. Bez ohľadu na túto požiadavku možno v núdzových situáciách uvedených v bodoch 41 až 44 použiť špecifické postupy alebo špecifické technické konfigurácie.

29. Požadovaná úroveň spoľahlivosti bezpečnostných opatrení, vymedzená ako stupeň bezpečnosti, sa stanovuje na základe výsledku procesu riadenia rizík a v súlade s príslušnými bezpečnostnými politikami a usmerneniami.

30. Tento stupeň bezpečnosti sa preverí pomocou medzinárodne uznávaných alebo vnútroštátne schválených postupov a metodík. Tie predovšetkým zahŕňajú hodnotenie, kontroly a audit.

31. Orgán pre bezpečnostnú akreditáciu schvaľuje bezpečnostné usmernenia pre oblasť kvalifikovania a schvaľovania nekryptografických bezpečnostných produktov IT.

B.8. Prenos v zabezpečenom priestore

32. Keď sa prenos utajovaných skutočností uskutočňuje len v rámci zabezpečeného priestoru, môže sa používať nešifrovaná distribúcia alebo šifrovanie na nižšej úrovni, ak to umožňuje výsledok procesu riadenia rizík a ak to schválil orgán pre bezpečnostnú akreditáciu.

B.9. Bezpečné prepojenie CIS

33. Prepojenie znamená priame spojenie dvoch alebo viacerých systémov IT na účely spoločného využívania údajov a iných informačných zdrojov, ktoré môže byť jednosmerné alebo viacsmerné.

34. CIS pristupuje ku každému pripojenému systému IT ako nedôveryhodnému a na kontrolu výmeny utajovaných skutočností s inými CIS uplatňuje ochranné opatrenia.

35. Všetky prepojenia CIS s iným systémom IT spĺňajú tieto základné požiadavky:

- a) funkčné alebo prevádzkové požiadavky takýchto prepojení stanovujú a schvaľujú príslušné orgány;
- b) predmetné prepojenie podlieha procesu riadenia rizík a akreditácii a musí byť schválené príslušným orgánom pre bezpečnostnú akreditáciu;
- c) na perimetri CIS sa zavedie ochrana (ďalej len PS – Protection Services).

36. CIS s akreditáciou nesmie mať nijaké prepojenie s nechránenou alebo verejnou sieťou okrem prípadu, ak má CIS schválenú ochranu PS nainštalovanú na tento účel na rozhraní medzi týmto CIS a nechránenou alebo verejnou sieťou. Bezpečnostné opatrenia týkajúce sa takéhoto prepojenia prehodnocuje príslušný orgán pre informačnú bezpečnosť a schvaľuje príslušný orgán pre bezpečnostnú akreditáciu.

37. Keď sa nechránená alebo verejná sieť používa výhradne ako nosič dát, ktoré sú šifrované kryptografickým produktom EÚ certifikovaným v súlade s bodom 27, toto spojenie sa nepovažuje za prepojenie.

38. Priame alebo kaskádové prepojenie nechránenej alebo verejnej siete a CIS s akreditáciou na zaobchádzanie s utajovanými skutočnosťami so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“ alebo rovnocenným stupňom utajenia alebo „SECRET UE/EU SECRET“ alebo s rovnocenným stupňom utajenia je zakázané.

B.10. Elektronické médiá na uchovávanie

39. Elektronické médiá na uchovávanie sa zničia v súlade s postupom schváleným príslušným bezpečnostným orgánom.

40. Elektronické médiá na uchovávanie sa znovu použijú, zníži sa ich stupeň utajenia alebo odtajnia v súlade s pokynmi pre zaobchádzanie s informáciami.

B.11. Núdzové situácie

41. V núdzových situáciách, ako napríklad v situáciách bezprostredne hroziacej krízy alebo počas krízy, alebo vojnového stavu alebo pri výnimočných operačných okolnostiach, sa môžu uplatňovať osobitné postupy uvedené nižšie.

42. Utajované skutočnosti sa môžu so súhlasom príslušného orgánu prenášať s použitím kryptografických produktov, ktoré boli schválené pre nižší stupeň utajenia, alebo bez šifrovania, ak by akékoľvek zdržanie spôsobilo škody, ktoré jednoznačne prevyšujú škodu spôsobenú zverejnením utajovaného materiálu, a ak:

- a) odosielateľ a príjemca nemajú požadované šifrovacie zariadenie alebo nemajú nijaké šifrovacie zariadenie; a
- b) utajovaný materiál nemožno dostatočne včas doručiť inými prostriedkami.

43. Utajované skutočnosti prenášané za okolností uvedených v bode 41 nesmú mať žiadne označenia alebo odkazy, ktorými by sa odlišovali od neutajovanej skutočnosti alebo skutočnosti, ktorá sa môže chrániť dostupným kryptografickým produktom. Prijemcovia sa o stupni utajenia bezodkladne informujú iným spôsobom.

44. V prípade uplatnenia ustanovení bodu 41 alebo 42 sa následne zasiela správa príslušnému orgánu.

BEZPEČNOSTNÉ UPOZORNENIE Č. 4

FYZICKÁ BEZPEČNOSŤ

A. ÚVOD

V tomto bezpečnostnom upozornení sa stanovujú bezpečnostné zásady na vytvorenie bezpečného prostredia na zaistenie správneho zaobchádzania s dôvernými informáciami v Európskom parlamente. Tieto zásady spolu s tými, ktoré sa týkajú technickej bezpečnosti sa doplnia o pokyny pre zaobchádzanie s informáciami.

B. RIADENIE BEZPEČNOSTNÝCH RIZÍK

1. Riadenie rizík týkajúcich sa utajovaných skutočností sa uskutočňuje ako proces. Tento proces sa zameriava na určenie známych bezpečnostných rizík, stanovenie bezpečnostných opatrení na zníženie týchto rizík na prijateľnú úroveň v súlade s hlavnými zásadami a minimálnymi normami stanovenými v tomto bezpečnostnom upozornení a na uplatňovanie týchto opatrení v súlade s koncepciou hĺbkovej ochrany definovanej v bezpečnostnom upozornení č. 3. Účinnosť týchto opatrení sa neustále vyhodnocuje.

2. Bezpečnostné opatrenia na ochranu utajovaných skutočností počas celého ich životného cyklu zodpovedajú najmä ich stupňu utajenia, podobe a množstvu predmetných informácií alebo materiálov, miestu, kde sa nachádzajú objekty, v ktorých sa utajované skutočnosti uchovávajú, a ich konštrukcii, a stanovenej lokálnej úrovni ohrozenia zákernými a/alebo trestnými činnosťami vrátane špionáže, sabotáže a terorizmu.

3. V núdzových plánoch sa prihliada na potrebu chrániť utajované skutočnosti počas núdzových situácií s cieľom predísť neoprávnenému prístupu k nim, ich zverejneniu alebo strate ich integrity alebo dostupnosti.

4. Preventívne a nápravné opatrenia zamerané na minimalizáciu dôsledkov významného zlyhania alebo významných incidentov pri zaobchádzaní s utajovanými skutočnosťami a ich uchovávaní sú uvedené v plánoch na zabezpečenie kontinuity činností.

C. VŠEOBECNÉ ZÁSADY

5. Stupeň utajenia či označenia pridelený informáciám určuje úroveň im poskytovanej ochrany v oblastiach fyzickej bezpečnosti.

6. Informácie, ktoré si vyžadujú utajenie, sa označujú ako také a zaobchádza sa s nimi ako s takými bez ohľadu na ich fyzickú formu. Stupeň ich utajenia sa jasne oznamuje ich príjemcovi, či už označením stupňa utajenia (ak sa doručuje písomnou formou, či už na papieri, alebo v CIS), alebo oznámením (ak sa doručuje ústnou formou, napríklad počas rozhovoru alebo prezentácie). Utajovaný materiál sa fyzicky označuje ako utajený, aby bola možná jednoduchá identifikácia stupňa jeho utajenia.

7. Dôverné informácie sa za nijakých okolností nesmú čítať na verejných miestach, kde by ich mohol vidieť jednotlivec, ktorý nemá „potrebu vedieť“, napríklad vo vlakoch, v lietadlách, v kaviarňach, baroch atď. Neponechávajú sa v hotelových trezoroch ani na izbách, ani sa neponechávajú bez dozoru na verejných miestach.

D. ZODPOVEDNOSŤ

8. Oddelenie CIU zodpovedá za zaistenie fyzickej bezpečnosti v správe dôverných informácií uložených v jeho zabezpečených zariadeniach. Oddelenie CIU zodpovedá aj za správu svojich zabezpečených zariadení.

9. Za fyzickú bezpečnosť v správe informácií so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatných dôverných informácií“ zodpovedá príslušný parlamentný orgán/funkcionár.

10. Riaditeľstvo pre bezpečnosť a hodnotenie rizika zaisťuje osobnú bezpečnosť a bezpečnostnú previerku potrebnú na zaistenie bezpečného zaobchádzania s dôvernými informáciami v Európskom parlamente.

11. Riaditeľstvo pre informačné technológie poskytuje poradenstvo a zaisťuje, aby každý vytvorený alebo používaný CIS bol plne v súlade s bezpečnostným upozornením č. 3 a príslušnými pokynmi pre zaobchádzanie s informáciami.

E. ZABEZPEČENÉ ZARIADENIA

12. Zabezpečené zariadenia možno inštalovať podľa noriem technickej bezpečnosti a v súlade s úrovňou priradenou dôverným informáciám, ako sa uvádza v článku 7.

13. Osvedčenia pre zabezpečené zariadenia vydáva orgán pre bezpečnostnú akreditáciu a potvrdzuje ich bezpečnostný orgán.

F. KONZULTÁCIE O DÔVERNÝCH INFORMÁCIÁCH

14. Keď skutočnosť so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatné dôverné informácie“ sú uložené na oddelení CIU a majú sa sprístupniť mimo zabezpečeného priestoru, oddelenie CIU zasiela kópiu príslušnému autorizovanému útvaru, ktorý zabezpečí, aby sprístupnenie a zaobchádzanie s týmito informáciami boli v súlade s článkom 8 ods. 2 a článkom 10 tohto rozhodnutia a príslušnými pokynmi pre zaobchádzanie s informáciami.

15. Keď informácia so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatné dôverné informácie“ sú uložené v parlamentnom orgáne/u funkcionára, ktorý nie je oddelením CIU, sekretariát tohto parlamentného orgánu/funkcionára, zabezpečuje, aby sprístupnenie a zaobchádzanie s týmito informáciami boli v súlade s článkom 7 ods. 3, článkom 8 ods. 1, 2 a 4, článkom 9 ods. 3, 4 a 5, článkom 10 ods. 2 až 6 a článkom 11 tohto rozhodnutia a príslušnými pokynmi pre zaobchádzanie s informáciami.

16. Keď sa majú informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRET UE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia sprístupniť v zabezpečenom priestore, oddelenie CIU zaisťuje, aby sprístupnenie a zaobchádzanie s týmito informáciami boli v súlade s článkami 9 a 10 tohto rozhodnutia a príslušnými pokynmi pre zaobchádzanie s informáciami.

G. TECHNICKÁ BEZPEČNOSŤ

17. Za opatrenia technickej bezpečnosti zodpovedá orgán pre bezpečnostnú akreditáciu, ktorý určuje v pokynoch pre zaobchádzanie s informáciami, aké konkrétne opatrenia technickej bezpečnosti sa majú uplatniť.

18. Zabezpečené čítarne na sprístupnenie informácií so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatných dôverných informácií“ musia spĺňať konkrétne opatrenia technickej bezpečnosti, ako sa uvádza v pokynoch pre zaobchádzanie s informáciami.

19. Zabezpečený priestor zahŕňa tieto zariadenia:

- a) previerkovú miestnosť so zabezpečeným prístupom (Security Access Screening Room – SAS), ktorá sa má zriadiť podľa opatrení technickej bezpečnosti, ako sa uvádza v pokynoch pre zaobchádzanie s informáciami. Prístup k tomuto zariadeniu sa zaznamenáva. SAS musí spĺňať prísne normy z hľadiska identifikácie osôb s prístupom, videozáznamov a zabezpečeného priestoru na odkladanie osobných prvkov, ktoré nie sú dovolené v zabezpečených miestnostiach (telefóny, perá atď.);
- b) komunikačnú miestnosť na vysielanie a prijímanie utajovaných skutočností vrátane šifrovaných utajených skutočností v súlade s bezpečnostným upozornením č. 3 a pokynmi pre zaobchádzanie s informáciami;
- c) bezpečný archív, kde sa schválené a certifikované schránky používajú oddelene pre informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“, „CONFIDENTIEL UE/EU CONFIDENTIAL“ a/alebo „SECRET EU/EU SECRET“ alebo s rovnocenným stupňom utajenia. Informácie so stupňom utajenia „TRÈS SECRETUE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia sa umiestňujú v oddelenej miestnosti v osobitnej certifikovanej schránke. Jediná dodatočná vec, ktorá sa v tejto oddelenej miestnosti nachádza, je pracovný stôl, na ktorom oddelenie CIU spracúva archív;
- d) evidenčnú miestnosť, ktorá poskytuje nástroje potrebné na zabezpečenie toho, aby sa evidencia vykonávala na papieri alebo elektronicky, a preto sa v nej nachádzajú zabezpečené zariadenia potrebné na inštalovanie vhodných CIS. Iba evidenčná miestnosť môže obsahovať schválené a akreditované rozmnožovacie prístroje (pre rozmnožovanie v papierovej alebo v elektronickej forme). V pokynoch pre zaobchádzanie s informáciami sa konkretizuje, ktoré rozmnožovacie zariadenia sú schválené a akreditované. Evidenčná miestnosť poskytuje aj priestor potrebný na skladovanie a spracovanie akreditovaného materiálu, aby sa mohli označiť, rozmnožovať a rozosielať utajované skutočnosti vo fyzickej forme, a to podľa stupňa utajenia. Oddelenie CIU určí všetok akreditovaný materiál, na ktorý vydáva akreditáciu orgán pre bezpečnostnú akreditáciu v súlade s odporúčaním prevádzkového orgánu pre informačnú bezpečnosť (IAOA). V evidenčnej miestnosti sa nachádza aj akreditovaný prístroj na ničenie informácií schválený pre najvyšší stupeň utajenia, ako sa uvádza v pokynoch pre zaobchádzanie s informáciami. Preklad informácií so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL EU“, „SECRET EU/EU SECRET“ alebo „TRÈS SECRETUE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia sa vypracúva v evidenčnej miestnosti, vo vhodnom a akreditovanom systéme. V evidenčnej miestnosti sa vytvoria pracovné miesta najviac pre dvoch prekladateľov, ktorí môžu pracovať v tom istom čase na tom istom dokumente. Prítomný musí byť jeden zamestnanec oddelenia CIU;
- e) čítať, určenú na individuálne sprístupnenie utajovaných skutočností riadne oprávneným osobám. Čítať musí mať dost miesta pre dve osoby vrátane zamestnanca oddelenia CIU, ktorý je prítomný po celý čas každého tohto sprístupnenia informácií. Úroveň zabezpečenia tejto miestnosti musí zodpovedať sprístupňovaniu informácií so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET EU/EU SECRET“ alebo „TRÈS SECRETUE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia. V čitárni možno umiestniť zariadenie TEMPEST na umožnenie prípadných elektronických sprístupnení informácií v súlade so stupňom utajenia predmetnej informácie;
- f) zasadaciu miestnosť, do ktorej sa musí zmestiť až 25 osôb na účely rokovania o informáciách so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET EU/EU SECRET“ alebo s rovnocenným stupňom utajenia. Zasadacia miestnosť poskytuje potrebné technické zabezpečenie a certifikované zariadenia na tlmočenie najviac do dvoch jazykov alebo z dvoch jazykov. Zasadacia miestnosť sa môže využívať aj ako doplnková čítať na individuálne sprístupnenie informácií, keď sa nevyužíva na zasadnutia. Oddelenie CIU môže vo výnimočných prípadoch povoliť viac než jednej oprávnenej osobe, aby sa im sprístupnili utajované skutočnosti, ak všetky osoby v miestnosti majú rovnakú úroveň bezpečnostnej previerky a ich „potreba vedieť“ je rovnaká. Najviac štyri osoby súčasne môžu mať sprístupnené utajované skutočnosti. Prítomnosť zamestnancov oddelenia CIU sa posilní;
- g) technicky zabezpečené miestnosti na umiestnenie všetkého technického zariadenia, súvisiaceho s bezpečnosťou celého zabezpečeného priestoru, a zabezpečených serverov IT.

20. Zabezpečený priestor spĺňa platné medzinárodné bezpečnostné normy a certifikát preň vydáva Riaditeľstvo pre bezpečnosť a hodnotenie rizika. V zabezpečenom priestore sa nachádza toto minimálne bezpečnostné technické zariadenie:

- a) poplašné a monitorovacie bezpečnostné systémy;
- b) bezpečnostné zariadenie a núdzové systémy (dvojsmerný výstražný systém);

- c) systém priemyselnej televízie;
- d) detekčný systém proti narušeniu;
- e) ovládanie prístupu (vrátane biometrického bezpečnostného systému);
- f) schránky;
- g) skrinky;
- h) protielektromagnetická ochrana.

21. Orgán pre bezpečnostnú akreditáciu môže doplniť potrebné dodatočné opatrenia technickej bezpečnosti v spolupráci s oddelením CIU a na základe súhlasu bezpečnostného orgánu.

22. Zariadenie infraštruktúry sa môže pripojiť k systémom všeobecného riadenia budovy, v ktorej sa zabezpečený priestor nachádza. Bezpečnostné zariadenie určené na ovládanie prístupu a CIS sú však nezávislé od všetkých iných takýchto systémov existujúcich v Európskom parlamente.

H. INŠPEKCIE ZABEZPEČENÉHO PRIESTORU

23. Orgán pre bezpečnostnú akreditáciu na požiadanie oddelenia CIU vykonáva pravidelné inšpekcie zabezpečeného priestoru.

24. Orgán pre bezpečnostnú akreditáciu vypracuje a priebežne aktualizuje inšpekčný kontrolný zoznam bodov, ktoré treba kontrolovať počas inšpekcie v súlade s pokynmi pre zaobchádzanie s informáciami.

I. PREPRAVA DÔVERNÝCH INFORMÁCIÍ

25. Dôverné informácie sa prepravujú chránené pred pohľadom a bez označenia dôvernej povahy svojho obsahu v súlade s pokynmi pre zaobchádzanie s informáciami.

26. Iba kuriéri alebo zamestnanci s primeranou úrovňou bezpečnostného povolenia môžu prenášať informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET EU/EU SECRET“ alebo „TRÈS SECRETUE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia.

27. Dôverné informácie sa môžu odoslať prostredníctvom vonkajšej poštovej služby alebo odnesením v ruke mimo budovy iba v súlade s podmienkami stanovenými v pokynoch pre zaobchádzanie s informáciami.

28. Informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET EU/EU SECRET“ alebo „TRÈS SECRETUE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia sa nikdy neposielajú elektronickou poštou ani faxom, dokonca ani prostredníctvom „bezpečného“ systému elektronickej pošty alebo faxu so šifrovaním. Informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatné dôverné informácie“ sa môžu posielat elektronickou poštou za použitia akreditovaného šifrovacieho systému.

J. UCHOVÁVANIE DÔVERNÝCH INFORMÁCIÍ

29. Stupeň utajenia alebo označenia pridelený dôverným informáciám určuje úroveň poskytovanej ochrany v súvislosti s ich uchovávaním. Uchovávať sa v zariadení certifikovanom na tento účel v súlade s pokynmi pre zaobchádzanie s informáciami.

30. Informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatné dôverné informácie“:

- a) sa uchovávajú v štandardnom formáte, v ocelevej zamknutej skrinke, buď v kancelárii, alebo na pracovisku, ak sa momentálne nepoužívajú;
- b) nesmú zostať bez dozoru, ak nie sú riadne uzamknuté a uložené;
- c) nemožno nechať ležať na stole apod. tak, žeby ich mohla čítať alebo odnieť nejaká osoba, ktorá nemá povolenie, napríklad návštevníci, upratovacia služba, údržbári a pod.;
- d) sa nesmú ukazovať osobe, ktorá nemá povolenie, ani sa nesmie o nich diskutovať s touto osobou.

31. Informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ alebo s rovnocenným stupňom utajenia a „ostatné dôverné informácie“ sa uchovávajú len na sekretariáte parlamentného orgánu/funkcionára alebo na oddelení CIU v súlade s pokynmi pre zaobchádzanie s informáciami.

32. Informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ alebo „TRÈS SECRETUE/EU TOP SECRET“ alebo s rovnocenným stupňom utajenia:

- a) sa uchovávajú v zabezpečenom priestore v bezpečnostnej schránke alebo v komorovom trezore. Výnimočne, napríklad, keď je oddelenie CIU zatvorené, môžu sa uchovávať v schválenej a certifikovanej bezpečnostnej schránke v priestoroch bezpečnostných služieb;
- b) nesmú nikdy zostať bez dozoru v zabezpečenom priestore bez toho, aby sa najprv neuzamkli v schválenej schránke (dokonca ani počas mimoriadne krátkej neprítomnosti);
- c) nesmú zostať ležať na stole apod. tak, žeby ich nejaká osoba, ktorá nemá povolenie, mohla čítať alebo odnieť, dokonca ani vtedy, keď zodpovedný zamestnanec oddelenia CIU je prítomný v miestnosti.

Ak sa dokument obsahujúci dôverné informácie vypracuje v elektronickej forme v zabezpečenom priestore, počítač sa uzamkne a obrazovka sa stane neprístupnou, keď pôvodca alebo zodpovedný zamestnanec oddelenia CIU opustí miestnosť (dokonca aj počas mimoriadne krátkej neprítomnosti). Automatická bezpečnostná zámka, ktorá sa zapne po niekoľkých minútach, sa nepovažuje za dostatočné opatrenie.

BEZPEČNOSTNÉ UPOZORNENIE Č. 5

PRIEMYSELNÁ BEZPEČNOSŤ

A. ÚVOD

1. Toto bezpečnostné upozornenie sa týka iba utajovaných skutočností.
2. Ustanovuje ustanovenia na vykonávanie spoločných minimálnych noriem časti 1 prílohy I tohto rozhodnutia.
3. „Priemyselná bezpečnosť“ je uplatňovanie opatrení na zabezpečenie ochrany utajovaných skutočností zo strany dodávateľov a subdodávateľov počas rokovaní pred uzavretím zmluvy a počas celého životného cyklu utajovaných zmlúv. Tieto zmluvy nezahŕňujú prístup k informáciám so stupňom utajenia „TRÈS SECRET UE/EU TOP SECRET“.
4. Európsky parlament ako verejný obstarávateľ zabezpečuje, že pri uzatváraní utajovaných zmlúv s priemyselným alebo iným subjektom sú splnené minimálne normy priemyselnej bezpečnosti stanovené v tomto rozhodnutí, a že sú uvedené v zmluve.

B. BEZPEČNOSTNÉ PRVKY V UTAJOVANEJ ZMLUVE**B.1. Návod na určovanie stupňa utajenia (Security Classification Guide – SCG)**

5. Európsky parlament ako verejný obstarávateľ pred začatím výberového konania alebo uzavretím utajovanej zmluvy určí stupeň utajenia všetkých informácií, ktoré sa majú poskytnúť predkladateľom ponuky a dodávateľom, ako aj stupeň utajenia všetkých informácií, ktoré dodávateľ vytvorí. Európsky parlament na tento účel pripraví Návod na určovanie stupňa utajenia (SGC), ktorý sa bude uplatňovať pri plnení zmluvy.

6. Pri určovaní stupňa utajenia rôznych prvkov utajovanej zmluvy sa uplatňujú tieto zásady:

a) Európsky parlament pri príprave SCG zohľadňuje všetky príslušné bezpečnostné hľadiská vrátane stupňa utajenia prideleného informácii, ktorý určil a schválil pôvodca informácie na použitie v súvislosti so zmluvou;

b) celkový stupeň utajenia zmluvy nesmie byť nižší ako najvyšší stupeň utajenia každého z jej prvkov.

B.2. Bezpečnostná doložka (Security aspects letter – SAL)

7. Bezpečnostné požiadavky špecifické pre zmluvu sa opíšu v bezpečnostnej doložke (SAL). SAL podľa potreby obsahuje SCG a tvorí neoddeliteľnú súčasť utajovanej zmluvy alebo utajovanej subdodávateľskej zmluvy.

8. SAL obsahuje ustanovenia, podľa ktorých musí dodávateľ a/alebo subdodávateľ dodržiavať minimálne normy stanovené v tomto rozhodnutí. Nedodržanie týchto minimálnych noriem sa môže považovať za dôvod na vypovedanie zmluvy.

B.3. Bezpečnostné pokyny pre program/projekt (Programme/Project Security Instructions – PSI)

9. V závislosti od rozsahu programov alebo projektov, ktorých súčasťou je prístup k USEÚ alebo zaobchádzanie s nimi alebo ich uchovávanie, verejný obstarávateľ určený na riadenie dotknutého programu alebo projektu môže pripraviť špecifické bezpečnostné pokyny pre program/projekt (PSI).

C. BEZPEČNOSTNÁ PREVIERKA ZARIADENIA (FACILITY SECURITY CLEARANCE – FSC)

10. Národný bezpečnostný orgán (NSA) alebo iný príslušný bezpečnostný orgán členského štátu udelí FSC, aby v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi preukázal, že priemyselný alebo iný subjekt je schopný vo svojich zariadeniach chrániť USEÚ so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo „SECRET UE/EU SECRET“ alebo s rovnocenným stupňom utajenia. Európsky parlament ako verejný obstarávateľ dostane doklad o udelení FSC skôr, ako sa dodávateľovi alebo subdodávateľovi, alebo potenciálnemu dodávateľovi či subdodávateľovi poskytne alebo udelí prístup k USEÚ.

11. FSC:

a) zhodnotí integritu priemyselného alebo iného subjektu;

b) zhodnotí vlastníctvo, kontrolu a/alebo možný nevhodný vplyv, ktorý možno považovať za bezpečnostné riziko;

- c) overí, že priemyselný alebo iný subjekt vo svojom zariadení zaviedol bezpečnostný systém, ktorý zahrnuje všetky príslušné bezpečnostné opatrenia potrebné na ochranu informácií či materiálu so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo „SECRET UE/EU SECRET“ v súlade s požiadavkami ustanovenými v tomto rozhodnutí;
- d) overí, či sa status personálnej bezpečnosti vedenia, majiteľov a zamestnancov, ktorí potrebujú prístup k informáciám so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo „SECRET UE/EU SECRET“, stanovil v súlade s požiadavkami ustanovenými v tomto rozhodnutí; a
- e) overí, či priemyselný alebo iný subjekt vymenoval úradníka pre bezpečnosť zariadenia, ktorý zodpovedá vedeniu za dodržiavanie bezpečnostných povinností v rámci tohto subjektu.

12. Európsky parlament ako verejný obstarávateľ v prípade potreby oznámi príslušnému NSA alebo inému príslušnému bezpečnostnému orgánu, že FSC je sa vyžaduje vo fáze pred uzavretím zmluvy alebo na účely plnenia zmluvy. FSC alebo osobná bezpečnostná previerka (Personal Security Clearance – PSC) sa vyžaduje vo fáze pred uzavretím zmluvy, ak sa počas predkladania ponúk musia poskytnúť informácie so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo „SECRET UE/EU SECRET“.

13. Verejný obstarávateľ neuzavrie utajovanú zmluvu s predkladateľom ponuky, ktorého uprednostňuje, kým mu NSA alebo iný príslušný bezpečnostný orgán členského štátu, v ktorom má príslušný dodávateľ alebo subdodávateľ sídlo, nepotvrdí, že sa v potrebných prípadoch vydala príslušná FSC.

14. Každý príslušný bezpečnostný orgán, ktorý vydal FSC, oznamuje Európskemu parlamentu ako verejnému obstarávateľovi všetky zmeny, ktoré majú vplyv na toto FSC. V prípade subdodávateľskej zmluvy príslušný bezpečnostný orgán dostáva potrebné informácie.

15. Odňatie FSC príslušným NSA alebo iným príslušným bezpečnostným orgánom predstavuje pre Európsky parlament ako verejný obstarávateľ dostatočný dôvod na vypovedanie utajovanej zmluvy alebo na vylúčenie predkladateľa ponuky zo súťaže.

D. UTAJOVANÉ ZMLUVY A UTAJOVANÉ SUBDODÁVATELSKÉ ZMLUVY

16. V prípade, keď sa utajované skutočnosti potencionálnym predkladateľom ponuky poskytujú vo fáze pred uzavretím zmluvy, výzva na predkladanie ponúk obsahuje ustanovenie, ktoré potencionálnych predkladateľov ponuky zaväzuje, že ak nepredložia ponuku alebo nie sú vybratí, sú povinní v stanovenej lehote vrátiť všetky utajované dokumenty.

17. Európsky parlament ako verejný obstarávateľ po uzavretí utajovanej zmluvy alebo utajovanej subdodávateľskej zmluvy oznámi NSA daného dodávateľa alebo subdodávateľa a/alebo inému príslušnému bezpečnostnému orgánu bezpečnostné ustanovenia utajovanej zmluvy.

18. Keď sa takéto zmluvy vypovedajú, Európsky parlament ako verejný obstarávateľ (a/alebo príslušný bezpečnostný orgán v prípade subdodávateľskej zmluvy) to bezodkladne oznámi NSA alebo inému príslušnému bezpečnostnému orgánu členského štátu, v ktorom má dodávateľ alebo subdodávateľ sídlo.

19. Od dodávateľov alebo subdodávateľov sa spravidla požaduje, aby po ukončení utajovanej zmluvy alebo subdodávateľskej zmluvy vrátili verejnému obstarávateľovi všetky utajované skutočnosti, ktorých sú držiteľmi.

20. V SAL sa stanovujú konkrétne ustanovenia týkajúce sa manipulácie s utajovanými skutočnosťami počas plnenia zmluvy alebo po jej ukončení.

21. Ak sa dodávateľovi alebo subdodávateľovi povolí, aby si ponechal utajované skutočnosti po ukončení zmluvy, dodávateľ alebo subdodávateľ musí naďalej spĺňať minimálne normy uvedené v tomto rozhodnutí a chrániť dôvernosť USEÚ.

22. Podmienky, za ktorých môže dodávateľ uzatvárať subdodávateľské zmluvy, sa musia vymedziť vo výzve na predkladanie ponúk a v zmluve.

23. Dodávateľ musí získať povolenie od Európskeho parlamentu ako verejného obstarávateľa skôr, ako zadá niektorú z častí utajovanej zmluvy subdodávateľom. S priemyselnými alebo inými subjektmi so sídlom v tretej krajine, ktorá neuzavrela s Úniou dohodu o bezpečnosti informácií, sa subdodávateľská zmluva nesmie uzavrieť.

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

25. Čo sa týka utajovaných skutočností, ktoré vytvoril alebo s ktorými zaobchádza dodávateľ alebo subdodávateľ, práva pôvodcu vykonáva verejný obstarávateľ.

E. NÁVŠTEVY VYKONÁVANÉ V SÚVISLOSTI S UTAJOVANÝMI ZMLUVAMI

26. Ak Európsky parlament, dodávatelia a subdodávatelia potrebujú na účely plnenia utajovanej zmluvy prístup k informáciám so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo „SECRET UE/EU SECRET“ v objektoch druhej strany, v súčinnosti s NSA alebo iným dotknutým príslušným bezpečnostným orgánom zorganizujú návštevy. V súvislosti so špecifickými projektmi však NSA môžu súhlasiť aj s postupom, pri ktorom sa tieto návštevy môžu organizovať priamo.

27. Všetci návštevníci musia byť držiteľmi príslušných PSC a musia mať „potrebu vedieť“ na účely prístupu k utajovaným skutočnostiam, ktoré sa týkajú zmluvy s Európskym parlamentom.

28. Návštevníkom sa udelí prístup len k utajovaným skutočnostiam, ktoré sa týkajú účelu návštevy.

F. PRENOS A PREPRAVA UTAJOVANÝCH SKUTOČNOSTÍ

29. Čo sa týka prenosu utajovaných skutočností elektronickými prostriedkami, uplatňujú sa príslušné ustanovenia bezpečnostného upozornenia č. 3.

30. Čo sa týka prepravy utajovaných skutočností, uplatňujú sa príslušné ustanovenia bezpečnostného upozornenia č. 4 a príslušné pokyny pre zaobchádzanie s informáciami.

31. Pri určovaní bezpečnostných opatrení na prepravu utajovaných materiálov ako nákladu sa uplatňujú tieto zásady:

- a) bezpečnosť sa zaisťuje vo všetkých etapách prepravy z miesta pôvodu do miesta konečného určenia;
- b) úroveň ochrany zásielky sa určuje podľa stupňa utajenia materiálu s najvyšším stupňom utajenia, ktorý sa v nej nachádza;
- c) pre spoločnosti poskytujúce prepravu sa musí zabezpečiť FSC príslušného stupňa. V týchto prípadoch je personál, ktorý so zásielkou manipuluje, bezpečnostne preverený v súlade s prílohou I;

- d) pred každou cezhraničnou prepravou materiálu so stupňom utajenia „CONFIDENTIEL UE/EU CONFIDENTIAL“ alebo „SECRET UE/EU SECRET“ alebo s rovnocenným stupňom utajenia vypracuje odosielateľ plán prepravy, ktorý schváli generálny tajomník;
- e) cesty sa vykonávajú, pokiaľ je to možné, z miesta pôvodu do miesta určenia a uskutočňujú sa v čo najkratšom čase podľa aktuálnych okolností;
- f) trasy ciest tam, kde je to možné, prechádzajú cez územia členských štátov.

G. POSTÚPENIE UTAJOVANÝCH SKUTOČNOSTÍ DODÁVATEĽOM, KTORÍ SA NACHÁDZAJÚ V TRETÍCH KRAJINÁCH

32. Postúpenie utajovaných skutočností dodávateľom a subdodávateľom, ktorí sa nachádzajú v tretích krajinách, sa uskutočňuje v súlade s bezpečnostnými opatreniami dohodnutými medzi Európskym parlamentom ako verejným obstarávateľom a príslušnou treťou krajinou, kde má dodávateľ sídlo.

H. ZAOBCHÁDZANIE S INFORMÁCIAMI SO STUPŇOM UTAJENIA „RESTREINT UE/EU RESTRICTED“ A ICH UCHOVÁVANIE

33. Európsky parlament ako verejný obstarávateľ môže podľa potreby v súčinnosti s NSA príslušného členského štátu a na základe zmluvných ustanovení vykonávať návštevy zariadení dodávateľa/subdodávateľa s cieľom overiť, či sa uplatňujú príslušné bezpečnostné opatrenia potrebné na ochranu USEÚ so stupňom utajenia „RESTREINT UE/EU RESTRICTED“, ako sa to požaduje v zmluve.

34. Európsky parlament ako verejný obstarávateľ informuje NSA alebo iné príslušné bezpečnostné orgány o zmluvách alebo subdodávateľských zmluvách, ktoré obsahujú informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“, v takom rozsahu, ako to ukladajú vnútroštátne zákony a iné právne predpisy.

35. FSC ani PSC pre dodávateľov alebo subdodávateľov a ich zamestnancov sa nevyžaduje v prípade zmlúv uzavretých s Európskym parlamentom, ktoré obsahujú informácie so stupňom utajenia „RESTREINT UE/EU RESTRICTED“.

36. Bez ohľadu na požiadavky ustanovené vo vnútroštátnych zákonoch a iných právnych predpisoch, ktoré sa týkajú FSC alebo PSC, Európsky parlament ako verejný obstarávateľ preskúma odpovede na výzvy na predloženie ponuky v prípade zmlúv, v rámci ktorých je potrebný prístup k informáciám so stupňom utajenia „RESTREINT UE/EU RESTRICTED“.

37. Podmienky, za ktorých môže dodávateľ uzatvárať subdodávateľské zmluvy, sa vymedzia vo výzve na predkladanie ponúk a v zmluve.

38. Ak sa v rámci zmluvy zaobchádza s informáciami so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ v komunikačných a informačných systémoch, ktoré prevádzkuje dodávateľ, Európsky parlament ako verejný obstarávateľ zabezpečuje, aby sa v zmluve alebo subdodávateľských zmluvách uviedli potrebné technické a administratívne požiadavky týkajúce sa akreditácie komunikačných a informačných systémov zodpovedajúce vyhodnotenému riziku, pričom sa zohľadnia všetky relevantné faktory. Rozsah akreditácie týchto komunikačných a informačných systémov sa dohodne medzi verejným obstarávateľom a príslušným NSA.

BEZPEČNOSTNÉ UPOZORNENIE Č. 6

NARUŠENIE BEZPEČNOSTI, STRATA ALEBO VYZRADENIE DÔVERNÝCH INFORMÁCIÍ

1. K narušeniu bezpečnosti dochádza v dôsledku konania alebo opomenutia v rozpore s týmto rozhodnutím, čo môže ohroziť dôvernú informáciu.

2. K ohrozeniu dôverných informácií dochádza vtedy, keď sa všetky informácie alebo ich časť dostanú do rúk osôb bez povolenia, t. j. osôb, ktoré nemajú ani príslušnú bezpečnostnú previerku ani nespĺňajú zásadu „potreba vedieť“, alebo ak existuje pravdepodobnosť, že k takejto udalosti došlo.

3. Dôvernosť informácií možno ohroziť v dôsledku neopatrnosti, nedbanlivosti alebo indiskrétnosti, ako aj činnosti služieb, ktoré si berú Úniu za cieľ, alebo rozvratných organizácií.

4. Keď generálny tajomník odhalí alebo je informovaný o dokázanom či údajnom porušení bezpečnosti, o strate alebo vyzrazení dôverných informácií:

- a) zistí skutočnosť;
- b) zhodnotí a minimalizuje spôsobenú škodu;
- c) prijme opatrenia na zabránení opakovania situácie;
- d) upozorní príslušný orgán tretej strany alebo členský štát, ktorý vypracoval alebo postúpil dôverné informácie.

Ak sa vec týka poslanca Európskeho parlamentu, generálny tajomník koná spolu s predsedom Európskeho parlamentu.

Keď generálny tajomník získa informácie od inej inštitúcie Únie, koná v súlade s príslušnými bezpečnostnými opatreniami pre utajované skutočnosti a bežnými opatreniami stanovenými na základe rámcovej dohody s Komisiou alebo medziinštitucionálnej dohody s Radou.

5. Všetky osoby, ktoré musia zaobchádzať s dôvernými informáciami, sú dôkladne poučené o bezpečnostných postupoch, nebezpečenstvách indiskrétného rozhovoru a ich vzťahu s médiami a podľa potreby podpisujú vyhlásenie, že nezverejnia obsah dôverných informácií tretím osobám, že budú dodržiavať povinnosť ochrany utajovaných skutočností a že berú na vedomie následky, ak tak nebudú postupovať. Prístup k utajovaným skutočnostiam alebo ich využívanie zo strany osoby, ktorá nebola poučená a nepodpísala zodpovedajúce vyhlásenie, sa považuje za porušenie bezpečnosti.

6. Poslanci Európskeho parlamentu, parlamentní úradníci a ostatní zamestnanci Európskeho parlamentu pracujúci pre politické skupiny alebo dodávateľov bezodkladne oznamujú generálnemu tajomníkovi každé porušenie bezpečnosti, stratu alebo vyzrazenie dôverných informácií, o ktorých sa dozvedia.

7. Každá osoba zodpovedná za vyzrazenie dôverných informácií bude disciplinárne stíhaná podľa príslušných pravidiel a predpisov. Tento postup sa uplatní bez toho, aby boli dotknuté právne kroky, ktoré sa môžu prijať v súlade s uplatniteľným právom.

8. Bez toho, aby boli dotknuté iné právne kroky, porušenia, ktorých sa dopustia úradníci Európskeho parlamentu a ostatní zamestnanci Európskeho parlamentu pracujúci pre politické skupiny, majú za následok uplatňovanie postupov a sankcií, ktoré sa uvádzajú v hlave VI služobného poriadku.

9. Bez toho, aby boli dotknuté iné právne kroky, porušenia, ktorých sa dopustia poslanci Európskeho parlamentu, podliehajú postupu podľa článku 9 ods. 2 a článkov 152, 153 a 154 Rokovacieho poriadku Európskeho parlamentu.

ISSN 1977-1037 (elektronické vydanie)
ISSN 1725-5236 (papierové vydanie)



Úrad pre vydávanie publikácií Európskej únie
2985 Luxemburg
LUXEMBURSKO

SK