

## II

*(Akty, ktorých uverejnenie nie je povinné)*

## KOMISIA

## ROZHODNUTIE KOMISIE

z 29. novembra 2001,

ktorým sa mení a dopĺňa jej Rokovací poriadok

*(oznámené pod dokumentačným číslom C(2001) 3031)*

(2001/844/ES, ESUO, Euratom)

## KOMISIA EURÓPSKÝCH SPOLOČENSTIEV

so zreteľom na Zmluvu o založení Európskeho spoločenstva, najmä na jej článok 218(2),

so zreteľom na Zmluvu o založení Európskeho spoločenstva uhlia a ocele, najmä na jej článok 16,

so zreteľom na Zmluvu o založení Európskeho spoločenstva pre atómovú energiu, najmä na jej článok 131,

so zreteľom na Zmluvu o Európskej únii, najmä na jej článok 28(1) a článok 41(1),

## ROZHODLA TAKTO:

*Článok 1*

Ustanovenia Komisie týkajúce sa bezpečnosti, ktorých znenie je priložené k tomuto rozhodnutiu, sa týmto pripájajú k Rokovaciemu poriadku Komisie vo forme prílohy.

*Článok 2*

Toto rozhodnutie nadobúda účinnosť v deň jeho uverejnenia v *Úradnom vestníku Európskych spoločenstiev*.

Uplatňuje sa od 1. decembra 2001.

V Bruseli 29. novembra 2001

*Za Komisiu*  
*predseda*  
Romano Prodi

*PRÍLOHA*

## USTANOVENIA KOMISIE TÝKAJÚCE SA BEZPEČNOSTI

Keďže:

- (1) Aby sa rozvíjali činnosti spoločenstva v oblastiach, ktoré vyžadujú určitý stupeň utajenia, je vhodné, aby sa zaviedol komplexný bezpečnostný systém platný pre Komisiu, ostatné inštitúcie, orgány, úrady a agentúry založené podľa alebo na základe zmluvy o založení ES alebo Zmluvy o Európskej únii, členské štáty rovnako ako akéhokoľvek iného príjemcu utajovaných informácií Európskej únie, ďalej uvádzaných ako „utajované informácie EÚ“.
- (2) Aby sa zabezpečila účinnosť takto vytvoreného bezpečnostného systému, Komisia sprístupní utajované informácie EÚ iba tým cudzím orgánom, ktoré ponúknu záruky, že prijali všetky opatrenia potrebné na uplatnenie pravidiel, ktoré sú prísne rovnocenné s týmito ustanoveniami.
- (3) Tieto ustanovenia sa prijímajú bez toho, aby bolo dotknuté Nariadenie č. 3 z 31. júla 1995, ktoré vykonáva článok 24 zmluvy o založení Európskeho spoločenstva pre atómovú energiu<sup>1</sup>, Nariadenie rady (ES) č. 1588(90) z 11. júna 1990 o prenose údajov, ktoré podliehajú štatistickému utajeniu, do Štatistického úradu Európskych spoločenstiev<sup>2</sup>, a Rozhodnutie Komisie C(95) 1510 konečné z 23. novembra 1995 o ochrane informačných systémov.
- (4) Bezpečnostný systém Komisie je založený na zásadách uvedených v Rozhodnutí rady 2001/264/ES z 19. marca 2001, ktorým sa prijímajú Bezpečnostné pravidlá rady<sup>3</sup> s cieľom zabezpečiť hladké fungovanie procesov rozhodovania únie.
- (5) Komisia podčiarkuje dôležitosť prípadného stotožnenia sa ostatných inštitúcií s pravidlami a normami dôvernosti, ktoré sú potrebné, aby sa zabezpečila ochrana záujmov únie a jej členských štátov.
- (6) Komisia uznáva potrebu vytvoriť vlastnú koncepciu bezpečnosti, pričom zohľadňuje všetky prvky bezpečnosti a osobitný charakter Komisie ako inštitúcie.

<sup>1</sup> Ú. v. ES L 17/58, 6. 10. 1958, str. 406/58.

<sup>2</sup> Ú. v. ES L 151, 15. 6. 1990, str. 1.

<sup>3</sup> Ú. v. ES L 101, 11. 4. 2001, str. 1.

- (7) Tieto ustanovenia sa prijímajú bez toho, aby bol dotknutý článok 255 zmluvy a Nariadenie (ES) č. 1049/2001 Európskeho parlamentu a rady z 30. mája 2001 o verejnom prístupe k dokumentom Európskeho parlamentu, Rady a Komisie<sup>4</sup>;

### Článok 1

Pravidlá Komisie týkajúce sa bezpečnosti sú uvedené v prílohe.

### Článok 2

1. Člen Komisie zodpovedný za bezpečnostné záležitosti prijme primerané opatrenia, aby zabezpečil, aby úradníci a ostatní zamestnanci Komisie a pomocný personál Komisie pri narábaní s utajovanými informáciami v rámci Komisie ako aj v rámci všetkých priestorov Komisie, vrátane jej zastúpení a úradov v únii a jej delegácií v tretích krajinách a externí dodávatelia Komisie dodržiavali pravidlá uvedené v článku 1.
  
2. Členské štáty, ostatné inštitúcie, orgány, úrady a agentúry založené podľa zmlúv alebo na základe zmlúv môžu obdržať utajované informácie pod podmienkou, že zabezpečia, aby sa pri narábaní s utajovanými informáciami v rámci ich služieb a priestorov dodržiavali pravidlá prísne rovnocenné s pravidlami uvedenými v článku 1, najmä, aby ich dodržiavali:
  - (a) členovia stálych zastúpení členských štátov v Európskej únii rovnako ak členovia ich národných delegácií, ktorí sa zúčastňujú zasadnutí Komisie alebo jej orgánov, alebo ktorí sa zúčastňujú iných činností Komisie,
  
  - (b) ostatní členovia národných administratív členských štátov, ktoré narábajú s utajovanými informáciami, bez ohľadu na to, či pôsobia na území členského štátu alebo v zahraničí,
  
  - (c) externí dodávatelia a pomocný personál, ktorí narábajú s utajovanými informáciami EÚ.

### Článok 3

Tretie štáty, organizácie a iné orgány môžu obdržať utajované informácie pod podmienkou, že zabezpečia, aby sa pri narábaní s takýmito informáciami dodržiavali pravidlá, ktoré sú prísne rovnocenné s pravidlami, ktoré sú uvedené v článku 1.

---

<sup>4</sup> Ú. v. ES L 145, 31. 5. 2001, str. 43.

#### Článok 4

Pri dodržaní základných zásad a minimálnych noriem bezpečnosti uvedených v časti I tejto prílohy môže člen Komisie zodpovedný za bezpečnostné záležitosti prijať opatrenia v súlade s časťou II tejto prílohy.

#### Článok 5

Tieto ustanovenie nahradia ku dňu svojho uplatnenia:

- (a) Rozhodnutie Komisie C(94) 3282 z 30 novembra 1994 o bezpečnostných opatreniach uplatniteľných na utajované informácie, ktoré vzniknú alebo sa prenášajú v súvislosti s činnosťami Európskej únie;
- (b) Rozhodnutie Komisie C(99) 423 z 25. februára 1999, ktoré sa týka postupov, ktorými úradníci a iní zamestnanci Európskej komisie môžu povoliť prístup k utajovaným informáciám, ktoré vlastní Komisia.

#### Článok 6

K dátumu uplatnenia týchto ustanovení všetky utajované informácie vo vlastníctve Komisie do tohto dátumu s výnimkou utajovaných informácií Euratom:

- (a) ak ich vytvorila Komisia, sa automaticky považujú za prekvalifikované na VYHRADENÉ INFORMÁCIE EÚ, pokiaľ ich autor do 31. januára 2002 nerozhodne, že sa im prideli iné utajenie. V takomto prípade autor musí informovať všetkých adresátov príslušného dokumentu;
- (b) ak ich vytvorili autori mimo Komisie, ponechajú si svoje pôvodné utajenie, a preto sa budú považovať za utajované informácie EÚ rovnocennej úrovne, pokiaľ autor nebude súhlasiť s ich odtajnením alebo pridelením nižšej úrovne.

*PRÍLOHA*  
BEZPEČNOSTNÉ PRAVIDLÁ

Obsah

ČASŤ I: ZÁKLADNÉ ZÁSADY A MINIMÁLNE BEZPEČNOSTNÉ NORMY

1. ÚVOD

2. VŠEOBECNÉ ZÁSADY

3. ZÁKLADY BEZPEČNOSTI

4. ZÁSADY INFORMAČNEJ BEZPEČNOSTI

4.1. Ciele

4.2. Definície

4.3. Utajenie

4.4. Ciele bezpečnostných opatrení

5. ORGANIZÁCIA BEZPEČNOSTI

5.1. Všeobecné minimálne normy

5.2. Organizácia

6. PERSONÁLNA BEZPEČNOSŤ

6.1. Personálne previerky

6.2. Záznamy o personálnych previerkach

6.3. Bezpečnostné pokyny pre personál

6.4. Zodpovednosti riadenia

6.5. Bezpečnostný štatút personálu

7. FYZICKÁ BEZPEČNOSŤ

7.1. Potreba ochrany

7.2. Kontrola

7.3. Bezpečnosť budov

7.4. Havarijné plány

8. INFORMAČNÁ BEZPEČNOSŤ

9. BOJ PROTI SABOTÁŽI A KONTROLA INÝCH FORIEM ZLOVOENÝCH  
ÚMYSELNÝCH ŠKÔD

10. UVOLENENIE UTAJOVANÝCH INFORMÁCIÍ TRETÍM ŠTÁTOM ALEBO  
MEDZINÁRODNÝM ORGANIZÁCIÁM

ČASŤ II: ORGANIZÁCIA BEZPEČNOSTI V KOMISII

11. ČLEN KOMISIE ZODPOVEDNÝ ZA BEZPEČNOSTNÉ ZÁLEŽITOSTI

12. PORADNÁ SKUPINA KOMISIE PRE BEZPEČNOSTNÚ POLITIKU

13. BEZPEČNOSTNÁ RADA KOMISIE

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

14. BEZPEČNOSTNÝ ÚRAD KOMISIE

15. BEZPEČNOSTNÉ INŠPEKCIE

16. UTAJENIE, VYMEDZENIE UTAJENIA A OZNAČOVANIE

16.1. Úrovne utajenia

16.2. Vymedzenie utajenia

16.3. Označovania

16.4. Uvádzanie utajovania

16.5. Uvedenie vymedzenia utajenia

17. RIADENIE UTAJOVANIA

17.1. Všeobecne

17.2. Uplatňovanie utajovania

17.3. Zníženie úrovne utajenia a odtajnenie

18. FYZICKÁ BEZPEČNOSŤ

18.1. Všeobecne

18.2. Bezpečnostné požiadavky

18.3. Fyzické bezpečnostné opatrenia

*18.3.1. Bezpečnostné oblasti*

*18.3.2. Administratívny priestor*

18.3.3. *Vstupné a výstupné kontroly*

18.3.4. *Strážne obhliadky*

18.3.5. *Bezpečnostné schránky a zabezpečené miestnosti*

18.3.6. *Zámky*

18.3.7. *Kontrola kľúčov a kombinácií*

18.3.8. *Poplašné detekčné zariadenia*

18.3.9. *Schválené zariadenie*

18.3.10. *Fyzická ochrana kopírovacích a faxových prístrojov*

18.4. Ochrana proti neoprávnenému nazeraniu a odpočúvaniu

18.4.1. *Neoprávnené nazeranie*

18.4.2. *Odpočúvanie*

18.4.3. *Zavedenie elektronického a záznamového zariadenia*

18.5. Technicky bezpečné oblasti

19. VŠEOBECNÉ PRAVIDLÁ O ZÁSADĚ POTREBY OBOZNÁMENIA SA  
A BEZPEČNOSTNÉ PREVIERKY PERSONÁLU EÚ

19.1. Všeobecne

19.2. Osobitné pravidlá o prístupe k INFORMÁCIÁM EÚ PRÍSNE TAJNÉ

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

- 19.3. Osobitné pravidlá o prístupe k TAJNÝM INFORMÁCIÁM EÚ  
a DÔVERNÝM INFORMÁCIÁM EÚ
- 19.4. Osobitné pravidlá o prístupe k VYHRADENÝM INFORMÁCIÁM EÚ
- 19.5. Presuny
- 19.6. Zvláštne pokyny
20. POSTUP BEZPEČNOSTNÝCH PREVIEROK PRE ÚRADNÍKOV KOMISIE  
A OSTATNÝCH ZAMESTNANCOV
21. PRÍPRAVA, DISTRIBÚCIA, ROZŠIROVANIE, BEZPEČNOSŤ KURIÉRSKEHO  
PERSONÁLU A ZVLÁŠTNE KÓPIE ALEBO PREKLADY A VÝPISY Z  
UTAJOVANÝCH INFORMÁCIÍ EÚ
- 21.1. Príprava
- 21.2. Distribúcia
- 21.3. Prenos utajovaných dokumentov EÚ
- 21.3.1. *Balenie, príjem*
- 21.3.2. *Prenos v rámci budovy alebo skupiny budov*
- 21.3.3. *Prenos v rámci krajiny*
- 21.3.4. *Prenos zo štátu do štátu*
- 21.3.5. *Prenos dokumentov EÚ vyhradené*
- 21.4. Bezpečnosť kuriérskeho personálu
- 21.5. Elektronické a iné prostriedky technického prenosu
- 21.6. Zvláštne kópie a preklady výpisov a výpisy z utajovaných dokumentov EÚ
22. REGISTRE UTAJOVANÝCH INFORMÁCIÍ EÚ, PREHLIADKY, KONTROLY,  
ARCHÍVNE SKLADOVANIE A LIKVIDÁCIA UTAJOVANÝCH INFORMÁCIÍ  
EÚ
- 22.1. Miestne registre utajovaných informácií EÚ
- 22.2. Register INFORMÁCIÍ EÚ PRÍSNE TAJNÉ
- 22.2.1. *Všeobecne*
- 22.2.2. *Centrálny register INFORMÁCIÍ EÚ PRÍSNE TAJNÉ*
- 22.2.3. *Vedľajšie registre INFORMÁCIÍ EÚ PRÍSNE TAJNÉ*
- 22.3. Súpis, prehliadky a kontroly utajovaných dokumentov EÚ
- 22.4. Archívne skladovanie utajovaných dokumentov EÚ
- 22.5. Likvidácia utajovaných dokumentov EÚ
- 22.6. Likvidácia v núdzových situáciách
23. BEZPEČNOSTNÉ OPATRENIA PRE KONKRÉTNE STRETNUTIA, KTORÉ SA  
KONAJÚ MIMO PRIESTOROV KOMISIE A ZAHŔŇAJÚ UTAJOVANÉ  
INFORMÁCIE EÚ
- 23.1. Všeobecne

← Naformátovano: Odrážky a  
číslování

← Naformátovano: Odrážky a  
číslování

← Naformátovano: Odrážky a  
číslování

← Naformátovano: Odrážky a  
číslování

← Naformátovano: Odrážky a  
číslování

← Naformátovano: Odrážky a  
číslování

← Naformátovano: Odrážky a  
číslování

23.2. Zodpovednosti23.2.1. *Bezpečnostný úrad komisie*23.2.2. *Bezpečnostný referent zasadnutia (MSO)*

23.3. Bezpečnostné opatrenia

23.3.1. *Bezpečnostné oblasti*23.3.2. *Priepustky*23.3.3. *Kontrola fotografických a audio zariadení*23.3.4. *Kontrola aktoviek, prenosných počítačov a balíkov*23.3.5. *Technická bezpečnosť*23.3.6. *Dokumenty delegácií*23.3.7. *Bezpečná úschova dokumentov*23.3.8. *Inšpekcia kancelárií*23.3.9. *Likvidácia odpadu utajovaných informácií EÚ*

## 24. PORUŠENIE BEZPEČNOSTI A OHROZENIE UTAJOVANÝCH INFORMÁCIÍ EÚ

24.1. Definície

24.2. Hlásenie porušenia bezpečnosti24.3. Právne opatrenia

## 25. OCHRANA UTAJOVANÝCH INFORMÁCIÍ EÚ, S KTORÝMI SA NARÁBA V INFORMAČNEJ TECHNOLOGII A KOMUNIKAČNÝCH SYSTÉMOCH

25.1. Úvod

25.1.1. *Všeobecne*25.1.2. *Hrozby a zraniteľnosť systémov*25.1.3. *Hlavný účel bezpečnostných opatrení*25.1.4. *Vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke (SSRS)*25.1.5. *Bezpečnostné režimy prevádzky*

25.2. Definície

25.3. Bezpečnostné zodpovednosti25.3.1. *Všeobecne*25.3.2. *Bezpečnostný akreditačný úrad(SAA)*25.3.3. *Úrad INFOSEC(IA)*25.3.4. *Majiteľ technických systémov(TSO)*25.3.5. *Majiteľ informácií (IO)*25.3.6. *Užívatelia*25.3.7. *Školenie INFOSEC*

25.4. Netechnické bezpečnostné opatrenia

← **Naformátovano:** Odrážky a číslavání← **Naformátovano:** Odrážky a číslavání← **Naformátovano:** Odrážky a číslavání← **Naformátovano:** Odrážky a číslavání← **Naformátovano:** Odrážky a číslavání← **Naformátovano:** Odrážky a číslavání← **Naformátovano:** Odrážky a číslavání← **Naformátovano:** Odrážky a číslavání← **Naformátovano:** Odrážky a číslavání

25.4.1. *Personálna bezpečnosť*

25.4.2. Fyzická bezpečnosť

25.4.3. Kontrola prístupu k systému

25.5. Technické bezpečnostné opatrenia

25.5.1. *Bezpečnosť informácií*

25.5.2. Kontrola a zodpovednosť za informácie

25.5.3. Manipulácia a kontrola odstrániteľných počítačových pamäťových médií

25.5.4. Odtajnenie a likvidácia počítačových pamäťových médií

25.5.5. Komunikačná bezpečnosť

25.5.6. Inštalačná a radiačná bezpečnosť

25.6. Bezpečnosť počas manipulácie

25.6.1. *Bezpečnostné prevádzkové postupy*

25.6.2. *Riadenie softwarovej ochrany/konfigurácie*

25.6.3. *Kontrola prítomnosti zlovolného softwaru/počítačových vírusov*

25.6.4. *Údržba*

25.7. Obstarávanie

25.7.1. *Všeobecne*

25.7.2. Akreditácia

25.7.3. Vyhodnotenie a certifikácia

25.7.4. Bežné kontroly bezpečnostných funkcií pre neustálu akreditáciu

25.8. Dočasné alebo príležitostné použitie

25.8.1. *Bezpečnosť mikropočítačov/osobných počítačov*

25.8.2. *Použitie informačnej technológie v súkromnom vlastníctve pre oficiálnu prácu komisie*

25.8.3. Použitie informačnej technológie vo vlastníctve dodávateľov alebo technológie národne dodávanej pre oficiálnu prácu komisie

26. UVOLENENIE UTAJOVANÝCH INFORMÁCIÍ EÚ TRETÍM ŠTÁTOM ALEBO MEDZINÁRODNÝM ORGANIZÁCIÁM

26.1.1. *Zásady upravujúce uvoľnenie utajovaných informácií EÚ*

26.1.2. Úrovne

26.1.3. Dohody o bezpečnosti

DODATOK 1: Porovnanie národných úrovní bezpečnostného utajovania

DODATOK 2: Praktický návod pre utajovanie

DODATOK 3: Usmernenia o uvoľnení utajovaných informácií EÚ tretím štátom alebo medzinárodným organizáciám: Úroveň spolupráce 1

DODATOK 4: Usmernenia o uvoľnení utajovaných informácií EÚ tretím štátom alebo medzinárodným organizáciám: Úroveň spolupráce 2

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

DODATOK 5: Usmernenia o uvoľnení utajovaných informácií EÚ tretím štátom alebo medzinárodným organizáciám: Úroveň spolupráce 3

DODATOK 6: Zoznam skratiek

## ČASŤ I: ZÁKLADNÉ ZÁSADY A MINIMÁLNE NORMY BEZPEČNOSTI

### 1. ÚVOD

Tieto ustanovenia určujú základné zásady a minimálne normy bezpečnosti, ktoré komisia musí primeraným spôsobom rešpektovať na všetkých úrovniach zamestnania, rovnako ako všetci príjemcovia utajovaných informácií EÚ (EUCI) tak, aby sa zabezpečila bezpečnosť a všetci zainteresovaní mohli byť uistení, že je zabezpečená všeobecná norma ochrany.

### 2. VŠEOBECNÉ ZÁSADY

Bezpečnostná politika komisie tvorí jednotnú časť jej všeobecnej vnútornej politiky riadenia, a preto vychádza zo zásad určujúcich jej všeobecnú politiku.

Tieto zásady zahŕňajú legálnosť, prehľadnosť, zodpovednosť a podriadenosť (úmernosť).

Legálnosť predstavuje potrebu zostať prísne v právnom rámci pri vykonávaní bezpečnostných funkcií a potrebu byť v súlade s právnymi požiadavkami. Znamená to tiež, že zodpovednosť v oblasti bezpečnosti musia vychádzať z náležitých právnych ustanovení. Ustanovenia v personálnom poriadku sa plne uplatňujú, najmä jeho článok 17 o povinnosti personálu uplatňovať rozvážnosť vzhľadom na informácie komisie a jeho hlavu VI o disciplinárnych opatreniach. Napokon, legálnosť znamená, že porušenia bezpečnosti v rámci zodpovednosti komisie sa musia riešiť spôsobom, ktorý je zhodný s politikou komisie o disciplinárnych opatreniach a politikou o spolupráci s členskými štátmi v oblasti trestného právneho systému.

Prehľadnosť predstavuje potrebu jasnosti v súvislosti so všetkými bezpečnostnými pravidlami, rovnováhy medzi rozličnými službami a rozličnými oblasťami (fyzická bezpečnosť verzus ochrana informácií atď.) a potrebu dôslednej a štruktúrovanej politiky týkajúcej sa bezpečnostného povedomia. Určuje tiež potrebu jasných písomných usmernení na zavedenie bezpečnostných opatrení.

Zodpovednosť znamená, že zodpovednosť v oblasti bezpečnosti musia byť jasne definované. Okrem toho predstavuje potrebu pravidelne overovať, či sa tieto zodpovednosti vykonávajú správne.

Podriadenosť alebo úmernosť znamená, že bezpečnosť sa musí organizovať na najnižšej možnej úrovni a čo najbližšie ku generálnym riaditeľstvám a službám komisie. Tiež predstavuje to, že bezpečnostné činnosti sa musia obmedziť iba na tie prvky, ktoré ju naozaj vyžadujú. A napokon to znamená, že bezpečnostné opatrenia musia byť úmerné k záujmom, ktoré sa majú chrániť a skutočnej alebo potenciálnej hrozbe pre tieto záujmy, pričom sa zohľadňuje obrana, ktorá spôsobuje čo najmenšie narušenie.

### 3. ZÁKLADY BEZPEČNOSTI

Základmi bezpečnosti sú:

- (a) V rámci každého členského štátu národná bezpečnostná organizácia zodpovedná za:
1. zber a registrovanie tajných informácií o špionáži, sabotáži, terorizme a iných podvratných činnosti, a
  2. poskytovanie informácií a rád vláde a prostredníctvom tohto komisii o povahe bezpečnostných hrozieb a o prostriedkoch proti ich ochrane.
- (b) V rámci každého členského štátu a v rámci komisii technický úrad INFOSEC (IA) zodpovedný za spoluprácu s daným bezpečnostným orgánom s cieľom získať informácie a rady o technických bezpečnostných hrozbách a o prostriedkoch ochrany proti nim;
- (c) Pravidelná spolupráca medzi vládnymi oddeleniami a primerané služby európskych inštitúcií, aby sa stanovilo resp. odporúčalo:
1. ktoré osoby, informácie a zdroje sa musia chrániť a
  2. všeobecné normy ochrany.
- (d) Úzka spolupráca medzi bezpečnostným úradom komisii a bezpečnostnými službami ostatných európskych inštitúcií a s Bezpečnostným úradom NATO.

← Naformátovano: Odrážky a číslovaní

#### 4. ZÁSADY INFORMAČNEJ BEZPEČNOSTI

##### 4.1. Ciele

Informačná bezpečnosť má nasledujúce hlavné ciele:

- (a) chrániť utajované informácie EÚ (EUCI) pred špionážou, ohrozením alebo neoprávneným uverejnením;
- (b) chrániť informácie EÚ, s ktorými sa narába v komunikačných a informačných systémoch a sieťach, pred ohrozením ich dôvernosti, celistvosti a dostupnosti;
- (c) chrániť priestory komisii, v ktorých sa uchováajú informácie EÚ, pred sabotážou a zlovoľným poškodením;
- (d) v prípade zlyhania posúdiť spôsobenú škodu, obmedziť jej dôsledky a prijať potrebné nápravné opatrenia.

##### 4.2. Definície

Vo všetkých týchto pravidlách:

- (a) Výraz „utajované informácie EÚ“ (EUCI) znamená ľubovoľné informácie a materiál, ktorých neoprávnené zverejnenie by mohlo spôsobiť rozličné stupne poškodenia záujmov EÚ alebo jednému alebo viacerým jej členským štátom, tiež keď takáto

informácia pochádza z EÚ alebo sa prijme z členských štátov, tretích štátov alebo medzinárodných organizácií.

- (b) Výraz „dokument“ znamená ľubovoľný list, poznámka, zápisnica, správa, memorandum, signál/odkaz, náčrt, fotografia, diapozitív, film, mapa, tabuľka, plán, zápisník, šablóna, prepisovací papier, písací stroj alebo páska do písacieho stroja, magnetofónová páska, kazeta, počítačový disk, CD-ROM alebo iné fyzické médium, na ktorom sa zaznamenala informácia.
- (c) Výraz „materiál“ znamená „dokument“ ako je definovaný v b) a tiež ľubovoľná položka zariadenia, už vyrobeného alebo v procese zhotovovania.
- (d) Výraz „potreba oboznámenia sa“ znamená potrebu jednotlivého zamestnanca mať prístup k utajovaným informáciám EÚ, aby mohol vykonávať funkciu alebo úlohu.
- (e) „Oprávnenie“ znamená rozhodnutie predsedu komisie udeliť jednotlivcovi prístup k EUCI až do špecifikovanej úrovni na základe pozitívneho preverenia bezpečnostného overenia (lustrovania), ktoré vykoná Národný bezpečnostný úrad podľa národného práva.
- (f) Výraz „utajovanie“ znamená pridelenie primeranej úrovne bezpečnosti pre dané informácie, ktorých neoprávnené zverejnenie môže spôsobiť určitý stupeň škody pre komisiu alebo záujmy členských štátov.
- (g) Výraz „zníženie“ (déclassement) znamená zníženie úrovne utajenia.
- (h) Výraz „odtajnenie“ (déclassification) znamená odstránenie akéhokoľvek stupňa utajenia.
- (i) Výraz „pôvodca“ znamená príslušne oprávnený autor utajených dokumentov. V rámci komisie môžu vedúci oddelení opraviť svojich zamestnancov, aby vytvorili EUCI.
- (j) Výraz „oddelenia komisie“ znamená oddelenia a služby komisie, vrátane kabinetov, na všetkých miestach zamestnanosti, vrátane spoločného výskumného centra, reprezentácií a úradov v únií a delegácií v tretích krajinách.

#### 4.3. Utajovanie

- (a) V prípade dôvernosti je nutná starostlivosť a skúsenosť pri výbere informácií a materiálu, ktorý sa má chrániť, a posúdení stupňa ochrany, ktorá je potrebná. Podstatné je, aby stupeň ochrany zodpovedal bezpečnostnej nutnosti jednotlivých

informácií a materiálu, ktorý treba chrániť. Aby sa zabezpečil hladký tok informácií, prijímajú sa kroky, aby sa vyhol nadmernému utajovaniu a nedostatočnému utajovaniu

- (b) Systém utajovania je nástroj na uskutočnenie týchto zásad; podobný systém utajovania sa dodržiava pri plánovaní a organizovaní spôsobov zameraných proti špionáži, sabotáži, terorizmu a iným hrozbám tak, aby sa zabezpečila najväčšia možná ochrana najdôležitejších priestorov, v ktorých sa uchovávajú utajované informácie, a najdôležitejšie body v rámci takýchto priestorov.
- (c) Zodpovednosť za utajovanie informácií spočíva výlučne na pôvodcovi danej informácie.
- (d) Úroveň utajovania môže závisieť výlučne na obsahu danej informácie.
- (e) Ak je viacero informácií spolu zoskupených, úroveň utajovania, ktorá sa vzťahuje na celok, musí byť aspoň taká vysoká, ako je najvyššia úroveň utajovania. Súbor informácií však môže mať pridelenú vyššiu úroveň utajovania, ako jeho jednotlivé časti.
- (f) Utajovanie sa prideluje iba vtedy, ak je potrebné a na nevyhnutne dlhú dobu.

#### 4.4. Cieľ bezpečnostných opatrení

Bezpečnostné opatrenia:

- (a) sa vzťahujú na všetky osoby, ktoré majú prístup k utajovaným informáciám, médiám pre prenos utajovaných informácií, všetkým priestorom obsahujúcim takéto informácie a dôležitým inštaláciám.
- (b) sú navrhnuté tak, aby sa stanovili osoby, ktorých postavenie môže ohroziť bezpečnosť utajovaných informácií a dôležitých inštalácií, ktoré uschovávajú utajované informácie, a umožnili vylúčenie alebo odstránenie takýchto osôb.
- (c) zabráňujú neoprávnenej osobe v prístupe k utajovaným informáciám alebo inštaláciám, ktoré ich obsahujú.
- (d) zabezpečujú, aby utajované informácie sa rozširovali výlučne na základe zásady potreby oboznámenia sa s nimi, ktorý je podstatný pre všetky aspekty bezpečnosti.
- (e) zabezpečujú celistvosť (prevencia pre zneužitím alebo neoprávnenou zmenou alebo neoprávneným vymazaním) a dostupnosť (t.j. prístup nie je zamietnutý tým, ktorí majú prístup) všetkých informácií, utajovaných aj neutajovaných a najmä takých informácií, ktoré sa uschovávajú, spracovávajú alebo prenášajú v elektromagnetickej forme.

## 5. ORGANIZÁCIA BEZPEČNOSTI

### 5.1. Všeobecné minimálne normy

Komisia zabezpečuje, aby všeobecné minimálne normy bezpečnosti dodržiavali všetci príjemcovia EUCI vo vnútri inštitúcií a podľa svojich právomocí, napríklad všetky oddelenia a dodávatelia tak, aby utajované informácie EÚ bolo možné odovzdať v dôvernosti, s ktorou sa bude narábať s rovnakou starostlivosťou. Takéto minimálne normy zahŕňajú kritériá udeľovania oprávnení pre personál a postupy na ochranu utajovaných informácií EÚ.

Komisia umožní prístup k EUCI vonkajším orgánom iba pod podmienkou, že zabezpečia, aby pri narábaní s EUCI sa dodržiavali ustanovenia aspoň prísne rovnocenné opatreniam týchto minimálnych noriem.

### 5.2. Organizácia

V rámci komisie sa bezpečnosť organizuje na dvoch úrovniach:

- (a) Na úrovni komisie ako celku existuje bezpečnostný úrad komisie s bezpečnostným akreditačným úradom, ktorý pôsobí tiež ako úrad pre kódovanie a ako úrad TEMPEST, a s úradom INFOSEC a jeden alebo viacero centrálnych registrov EUCI, pričom každý z nich má jedného alebo viacerých registračných kontrolných referentov.
- (b) Na úrovni oddelení komisie zodpovednosť za bezpečnosť spočíva na jednom alebo viacerých miestnych bezpečnostných referentoch, jednom alebo viacerých centrálnych informačných bezpečnostných referentoch, miestnych informačných bezpečnostných referentoch a miestnych registroch utajovaných informácií EÚ s jedným alebo viacerými registračnými kontrolnými referentmi.
- (c) Centrálné bezpečnostné orgány zabezpečia pre miestne bezpečnostné orgány prevádzkové usmernenia.

## 6. PERSONÁLNA BEZPEČNOSŤ

### 6.1. Preverenia pre personál

Všetky osoby, ktoré žiadajú prístup k utajovaným informáciám EÚ DÔVERNÉ alebo vyššie, musia byť primerane preverené skôr, ako sa im takýto prístup udelí. Podobné preverenie sa vyžaduje v prípade osôb, ktorých povinnosti zahŕňajú technickú prevádzku alebo údržbu komunikačných a informačných systémov obsahujúcich utajované informácie. Toto preverenie sa vykonáva tak, aby sa určilo, či takíto jednotlivci:

- (a) majú nespochybnú lojalitu;
- (b) sú takej povahy a rozvážnosti, že niet pochýb o ich bezúhonnosti pri narábaní s utajovanými informáciami, alebo
- (c) môžu podľahnúť tlaku zahraničných alebo iných zdrojov.

Zvlášť starostlivé skúmanie pri previerkových postupoch sa musí uplatniť v prípade osôb:

- (d) ktorým sa má udeliť prístup k informáciám EÚ NAJVYŠŠIEHO UTAJENIA;
- (e) ktoré sú na pozíciách, ktoré zahŕňajú pravidelný prístup k značnému objemu informácií EÚ TAJNÉ;
- (f) ktorých povinnosti im dávajú zvláštny prístup k bezpečnostným komunikačným alebo informačným systémom, a tak majú možnosť získať neoprávnený prístup k veľkému množstvu utajovaných informácií EÚ alebo spôsobiť vážnu škodu pri vykonávaní svojej úlohy tým, že vykonali kroky technickej sabotáže.

Za okolností uvedených vyššie v pododsekoch (d), (e) a (f) sa čo najviac využíva technika vyšetrovania pozadia.

Ak osoby, u ktorých sa nekonštatuje „potreba oboznámenia sa“, sú zamestnané za okolností, pri ktorých môžu mať prístup k utajovaným informáciám EÚ (napríklad kuriéri, bezpečnostní agenti, údržbársky personál, upratovačský personál atď.), musia sa takéto osoby najprv primerane bezpečnostne preveriť.

#### 6.2. Záznamy o personálnych previerkach

Všetky oddelenia komisie, ktoré narábajú s utajovanými informáciami EÚ, alebo uchovávajú bezpečnostné komunikačné alebo informačné systémy, musia viesť záznam o previerkach, ktorými prešiel personál pridelený do daného oddelenia. Všetky previerky sa musia byť overené podľa potreby, aby sa zabezpečilo, že sú primerané pre aktuálne pridelenie danej osoby; opätovne sa revidujú podľa potrebnej priority vždy, keď sa prijme nová informácia naznačujúca, že pokračujúce pridelenie na práce súvisiace s utajením už nie je viac v súlade so záujmami bezpečnosti. Miestny bezpečnostný referent oddelenia komisie musí viesť záznam o previerkach v rámci jeho oblasti.

#### 6.3. Bezpečnostné pokyny pre personál

Všetci členovia personálu, ktorí sú zamestnaní na pozíciách, kde by mohli mať prístup k utajovaným informáciám, musia pri prevzatí úlohy obdržať vyčerpávajúce pokyny a v pravidelných intervaloch pokiaľ ide o potrebu bezpečnosti a postupy jej dosahovania. Takíto členovia personálu musia písomne potvrdiť, že predložené bezpečnostné opatrenia si prečítali a plne im porozumeli.

#### 6.4. Zodpovednosti riadenia

Vedúci pracovníci majú povinnosť poznať tých členov svojho personálu, ktorí sa zúčastňujú dôverných prác, alebo ktorí majú prístup k bezpečnostným komunikačným alebo informačným systémom, a hlásiť akékoľvek prípady alebo zjavné náchylnosti, o ktorých je pravdepodobné, že majú dopad na bezpečnosť.

### 6.5. Bezpečnostný štatút personálu

Vypracujú sa postupy, ktoré zabezpečia, že v prípade objavenia sa nepriaznivej informácie o jednotlivcovi, sa určí, či jednotlivец pracuje s utajovanými informáciami alebo má prístup k bezpečnostným komunikačným alebo informačným systémom, a bezpečnostný referent komisie sa o tomto informuje. Ak sa stanoví, že takýto jednotlivец predstavuje bezpečnostné riziko, zakáže sa mu pokračovať na zadaní alebo je zadanía zbavený, ak by mohol ohroziť bezpečnosť.

## 7. FYZICKÁ BEZPEČNOSŤ

### 7.1. Potreba ochrany

Stupeň opatrení fyzickej ochrany, ktoré sa majú uplatňovať, aby sa zabezpečila ochrana utajovaných informácií EÚ, musí byť primeraný k utajovaniu, objemu a ohrozeniu vlastných informácií a materiálu. Všetci držiteľia utajovaných informácií EÚ musia dodržiavať jednotné postupy ohľadne utajovania informácií a spĺňať všeobecné normy ochrany ohľadne spravovania, prenosu a likvidovania informácií a materiálov vyžadujúcich si ochranu.

### 7.2. Kontrola

Pred zanechaním priestorov obsahujúcich utajované informácie EÚ bez dozoru, osoby, ktoré ich spravujú, musia zabezpečiť, aby takéto informácie boli bezpečne uschované a aby sa aktivovali všetky bezpečnostné zariadenia (zámky, poplašné zariadenia atď.). Po skončení pracovných hodín sa vykonáva ďalšia nezávislá kontrola.

### 7.3 Bezpečnosť budov

Budovy, v ktorých sa uchovávajú utajované informácie EÚ alebo bezpečnostné komunikačné alebo informačné systémy, sa chránia proti neoprávnenému prístupu. Povaha ochrany udelennej utajovaným informáciám EÚ, napríklad zamrežovanie okien, zámky na dverách, stráž pri vstupoch, automatizované kontrolné vstupné systémy, bezpečnostné kontroly a pochôdzky, poplašné systémy, detekčné systémy proti vlámaniu a strážne psy, závisia od:

- (a) utajenia, objemu a umiestnenia v rámci budovy informácií a materiálov, ktoré sa majú chrániť;
- (b) kvality bezpečnostných schránok na tieto informácie a materiály a
- (c) fyzickej povahy a umiestnenia budovy.

Povaha ochrany pridelennej komunikačným a informačným systémom podobne závisí od posúdenia hodnoty majetku, o ktorý ide, a potenciálnej škody, ak by došlo k poľaveniu bezpečnosti, od fyzickej povahy a umiestnenia budovy, v ktorej sa systém nachádza, a od umiestnenia systému v rámci budovy.

### 7.4. Havarijné plány

Vopred sa musia vypracovať podrobné havarijné plány na ochranu utajovaných informácií počas miestnej alebo národnej havarijnej situácie.

## 8. BEZPEČNOSŤ INFORMÁCIÍ

Informačná bezpečnosť (INFOSEC) sa týka identifikovania a uplatnenia bezpečnostných opatrení na ochranu utajovaných informácií EÚ, ktoré sa spracovávajú, skladujú alebo prenášajú komunikačnými, informačnými alebo inými elektronickými systémami, proti stroje dôvernosti, celistvosti alebo dostupnosti, náhodnej alebo úmyselnej. Musia sa prijať primerané protiopatrenia, aby sa zabránil prístup k utajovaným informáciám EÚ neoprávneným užívateľom, zabránilo odmietnutie prístupu k utajovaným informáciám EÚ oprávneným užívateľom, a zabránilo zneužitie alebo neoprávnené upravenie alebo vymazanie utajovaných informácií EÚ.

## 9. BOJ PROTI SABOTÁŽI A KONTROLA INÝCH FORIEM ZLOVOĽNÝCH ÚMYSELNÝCH ŠKÔD

Fyzické opatrenia na ochranu dôležitých inštalácií uchovávajúcich utajované informácie sú najlepšie ochranné bezpečnostné opatrenia proti sabotáži a zlovoľnému úmyselnému poškodeniu, a samotné previerky personálu nie sú účinnou náhradou. Príslušný národný orgán sa požiada, aby zabezpečil tajné služby ohľadne špionáže, sabotáže, terorizmu a iných podvratných činností.

## 10. UVOĽNENIE UTAJOVANÝCH INFORMÁCIÍ TRETÍM ŠTÁTOM ALEBO MEDZINÁRODNÝM ORGANIZÁCIÁM

Rozhodnutie uvoľniť utajované informácie EÚ pochádzajúce od komisie tretiemu štátu alebo medzinárodnej organizácii prijíma komisia ako kolégium. Ak pôvodcom informácie, pre ktorú sa žiada uvoľnenie, nie je komisia, komisia najprv získa súhlas pôvodcu na uvoľnenie. Ak nie je možné určiť pôvodcu, zodpovednosť pôvodcu prevezme komisia.

Ak komisia obdrží utajované informácie od tretích štátov, od medzinárodných organizácií alebo od iných tretích strán, týmto informáciám sa prideli ochrana primeraná ich utajeniu a rovnocenná normám stanoveným v týchto ustanoveniach pre utajované informácie EÚ alebo také vyššie normy, ako prípadne žiada tretia strana uvoľňujúca tieto informácie. Je možné dojednať vzájomné kontroly.

Vyššie uvedené zásady sa uplatňujú v súlade s podrobnými ustanoveniami uvedenými v časti II, oddiel 26 a dodatkoch 3, 4 a 5.

## ČASŤ II: ORGANIZÁCIA BEZPEČNOSTI V KOMISII

### 11. ČLEN KOMISIE ZODPOVEDNÝ ZA BEZPEČNOSTNÉ ZÁLEŽITOSTI

Člen komisie zodpovedný za bezpečnostné záležitosti:

- (a) vykonáva bezpečnostnú politiku komisie;
- (b) zaoberá sa bezpečnostnými problémami, ktoré mu prideli komisia alebo jej príslušný orgán;

- (c) skúma otázky zahŕňajúce zmeny v bezpečnostnej politike komisie v úzkej spolupráci s národnými bezpečnostnými (alebo inými vhodnými) úradmi členských štátov (ďalej ako NBU).

Člen komisie zodpovedný za bezpečnostné záležitosti je zodpovedný najmä za:

- (a) koordinovanie všetkých bezpečnostných záležitostí týkajúcich sa činností komisie;
- (b) postúpenie určeným úradom členských štátov žiadostí, aby NBÚ zabezpečili bezpečnostné preverky personálu zamestnaného v komisii v súlade s oddielom 20;
- (c) vyšetrowanie alebo nariadenia vyšetrowania ľubovoľného prieniku utajovaných informácií EÚ, ku ktorému v komisii podľa jasného dôkazu došlo;
- (d) požadovanie, aby príslušné bezpečnostné úrady začali vyšetrowanie, ak podľa všetkého došlo k úniku utajovaných informácií EÚ mimo komisie, a koordinovanie vyšetrowania, ak sa týka viacerých bezpečnostných úradov;
- (e) vykonávanie periodických vyšetrowaní bezpečnostných zabezpečení na ochranu utajovaných informácií EÚ;
- (f) zachovanie úzkej spolupráce so všetkými danými bezpečnostnými orgánmi, aby sa dosiahla celková koordinácia bezpečnosti;
- (g) sústavne skúmanie bezpečnostnej politiky komisie a postupov a prípadne vypracovanie primeraných odporúčaní. V tejto súvislosti člen komisie zodpovedný za bezpečnostné záležitosti komisii predkladá ročný plán inšpekcií, ktorý vypracovala bezpečnostná služba komisie.

← Naformátovano: Odrážky a číslování

← Naformátovano: Odrážky a číslování

## 12. PORADNÁ SKUPINA KOMISIE PRE BEZPEČNOSTNÚ POLITIKU

Ustanovuje sa poradná skupina komisie pre bezpečnostnú politiku. Skladá sa z člena komisie zodpovedného za bezpečnostné záležitosti alebo jeho zástupcu, ktorý a jej predsedá, a zo zástupcu NBÚ každého členského štátu. Zástupcovia ostatných európskych inštitúcií môžu sa tiež prizvať. Zástupcovia príslušných decentralizovaných agentúr EC a EÚ sa môžu tiež prizvať na zasadnutie, na ktorom sa rokuje o otázkach, ktoré sa ich týkajú.

Poradná skupina komisie pre bezpečnostnú politiku sa schádza na žiadosť jej predsedu alebo ľubovoľného jej člena. Skupina má za úlohu preskúmať a posúdiť všetky príslušné bezpečnostné otázky a komisii podľa potreby predložiť odporúčania.

## 13. BEZPEČNOSTNÁ RADA KOMISIE

Ustanovuje sa bezpečnostná rada komisie. Skladá sa z generálneho tajomníka, ktorý jej predsedá a z generálnych riaditeľov právnej služby, administratívy a personálu, vonkajších vzťahov, spravodlivosti a vnútorných záležitostí a spoločného výskumného centra a vedúceho služby vnútorného auditu a vedúceho bezpečnostného úradu komisie. Môžu sa prizvať ostatní úradníci komisie. V jej právomoci je posúdiť bezpečnostné opatrenia v rámci komisie a členovi komisie zodpovednému za bezpečnostné záležitosti predložiť odporúčania v tejto oblasti.

#### 14. BEZPEČNOSTNÝ ÚRAD KOMISIE

Aby sa splnili zodpovednosti uvedené v oddieli 11, člen komisie zodpovedný za bezpečnostné záležitosti má k dispozícii na koordinovanie, dohliadanie a zavádzanie bezpečnostných opatrení bezpečnostný úrad komisie.

Vedúci bezpečnostného úradu komisie je hlavným poradcom pre člena komisie zodpovedného za bezpečnostné záležitosti o bezpečnostných záležitostiach a pôsobí ako tajomník poradnej skupiny pre bezpečnostnú politiku. Z tohto hľadiska riadi aktualizáciu bezpečnostných pravidiel a koordinuje bezpečnostné opatrenia s príslušnými orgánmi členských štátov a podľa potreba s medzinárodnými organizáciami spojenými s komisiou podľa bezpečnostných dohôd. V tomto zmysle pôsobí ako prostredník.

Vedúci bezpečnostného úradu komisie je zodpovedný za akreditáciu systémov a sietí informačnej technológie v rámci komisie. Vedúci bezpečnostného úradu komisie rozhoduje po dohode s príslušným NBÚ o akreditácii systémov a sietí informačnej technológie, ktoré sa týkajú komisie na jednej strane a ľubovoľného príjemcu utajovaných informácií EÚ na strane druhej.

#### 15. BEZPEČNOSTNÉ INŠPEKCIE

Bezpečnostný úrad komisie vykonáva periodické inšpekcie bezpečnostných zariadení na ochranu utajovaných informácií EÚ.

Bezpečnostnému úradu komisie môžu pri tejto úlohe pomáhať bezpečnostné služby ostatných inštitúcií EÚ, ktoré vlastnia EUCI, alebo národné bezpečnostné úrady členských štátov<sup>5</sup>.

Na žiadosť ľubovoľného členského štátu môže jeho NBÚ vykonať inšpekciu EUCI v rámci komisie spoločne s bezpečnostnou službou komisie a po vzájomnej dohode.

#### 16. UTAJOVANIE, VYMEDZENIE UTAJENIA A OZNAČOVANIE

##### 16.1. Úrovne utajovania<sup>6</sup>

Informácie sú utajované na nasledujúcich úrovniach (pozri tiež dodatok2):

**PRÍSNE TAJNÉ INFORMÁCIE EÚ:** Toto utajovanie sa uplatňuje iba na informácie a materiál, ktorých neoprávnené zverejnenie by mohlo zapríčiniť mimoriadne závažné dopady na podstatné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov.

<sup>5</sup> Bez dopadu na Viedenský dohovor z roku 1961 o diplomatických vzťahoch a Protokol o výsadách a imunitách Európskych spoločenstiev z 8. apríla 1965.

<sup>6</sup> Pozri komparatívnu tabuľku bezpečnostných klasifikácií EÚ, NATO, ZEÚ a členských štátov v prílohe I.

**TAJNÉ INFORMÁCIE EÚ:** Toto utajovanie sa uplatňuje iba na informácie a materiály, ktorých neoprávnené zverejnenie by mohlo vážne poškodiť podstatné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov.

**DÔVERNÉ INFORMÁCIE EÚ:** Toto utajovanie sa uplatňuje na informácie a materiály, ktorých neoprávnené zverejnenie by mohlo poškodiť podstatné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov.

**VYHRADENÉ INFORMÁCIE EÚ:** Toto utajovanie sa uplatňuje na informácie a materiály, ktorých neoprávnené zverejnenie by bolo nevýhodným pre záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov.

Žiadne iné utajovanie nie je povolené.

#### 16.2. Vymedzenie utajenia

Na určenie limitov platnosti utajovania (pre utajované informácie predstavujúce automatické zníženie alebo odtajnenie) sa môže využiť dohodnuté vymedzenie utajenia. Takéto vymedzenie je buď „AŽ DO ... (čas/dátum)“ alebo „AŽ DO ... (udalosť)“.

Dodatočné vymedzenie utajenia ako KÓDOVANIE alebo ľubovoľné iné bezpečnostné utajenie uznané v EÚ sa uplatňuje, ak existuje potreba obmedzenej distribúcie a zvláštneho narábania s informáciou v porovnaní s tým, čo určuje bezpečnostná klasifikácia.

Bezpečnostné vymedzenia sa používajú iba v kombinácii s utajovaním.

#### 16.3. Označovania

Označovanie sa môže používať iba na špecifikovanie oblasti, na ktorú sa vzťahuje dokument alebo konkrétne distribuovanie na základe zásady potreby oboznámenia sa alebo (pre neutajované informácie) na označenie konca embarga.

Označovanie sa nerovná utajovaniu a nesmie sa používať namiesto utajovania.

Označenie ESDP (Európska politika bezpečnosti a obrany) sa uplatňuje na dokumenty a ich kópie, ktoré sa týkajú bezpečnosti a obrany únie alebo jedného alebo viacerých jej členských štátov, alebo ktoré sa týkajú vojenského alebo nevojenského krízového riadenia.

#### 16.4. Uvádzanie utajovania

Utajovanie sa uvádza takto:

- (a) Na dokumenty VYHRADENÉ INFORMÁCIE EÚ mechanickými alebo elektronickými prostriedkami;

- (b) Na dokumenty DÔVERNÉ INFORMÁCIE EÚ mechanickými prostriedkami alebo ručne alebo tlačou na vopred opečiatkovaný zaevidovaný papier;
- (c) Na dokumenty PRÍSNE TAJNÉ ALEBO TAJNÉ INFORMÁCIE EÚ mechanickými prostriedkami alebo ručne.

#### 16.5. Uvádzanie obmedzenia utajenia

Bezpečnostné vymedzenia utajenia sa uvádzajú priamo pod klasifikáciou utajenia rovnakými prostriedkami ako uvádzanie utajenia.

### 17. RIADENIE UTAJOVANIA

#### 17.1. Všeobecne

Informácie sa utajujú iba vtedy, ak je to potrebné. Utajovanie musí byť jasne a správne naznačené a musí sa zachovávať tak dlho, ako to vyžaduje ochrana informácií.

Zodpovednosť za utajovanie informácií a za následné zníženie úrovne utajenia alebo odtajnenie spočíva výlučne na pôvodcovi informácie.

Úradníci a ostatní zamestnanci komisie utajujú, znižujú úroveň utajenia alebo odtajňujú informácie podľa pokynov alebo po dohode s vedúcim svojho oddelenia.

Podrobné postupy na narábanie s utajovanými dokumentmi sú tak koncipované, aby sa zabezpečilo, že podliehajú ochrane, ktorá zodpovedá informácii, ktorú obsahujú.

Počet osôb oprávnených vypracovať dokumenty s PRÍSNE TAJNÝMI INFORMÁCIAMI EÚ sa udržiava na minime a ich mená sú uvedené na zozname, ktorý vypracoval bezpečnostný úrad komisie.

#### 17.2. Uplatňovanie utajovania

Utajovanie dokumentov je určené úrovňou citlivosti ich obsahu v súlade s definíciou v oddieli 16. Je dôležité, aby sa utajovanie používalo správne a striedmo. Toto sa uplatňuje najmä na utajovanie PRÍSNE TAJNÉ INFORMÁCIE EÚ.

Pôvodca dokumentu, ktorý sa má utajovať, musí mať na pamäti pravidlá uvedené vyššie a obmedziť ľubovoľnú tendenciu nadmerného alebo nedostatočného utajovania.

Praktické usmernenie pre utajovanie je obsiahnuté v dodatku 2.

Jednotlivé strany, odseky, oddiely, prílohy, dodatky a doplnky daného dokumentu môžu vyžadovať rozličné utajovania a musia byť podľa toho utajené. Utajovanie dokumentu ako celku sa musí rovnať najprísnejšiemu utajeniu jeho časti.

Utajovanie listu alebo poznámok, ktoré dopĺňajú prílohy, musí byť takej úrovne, na akej je najvyššie utajenie príloh. Pôvodca by mal jasne uviesť, na akej úrovni by sa list alebo poznámka mala utajovať, ak sa oddelí od príloh.

Verejný prístup riadi nariadenie (ES) č. 1049/2001.

### 17.3. Zníženie úrovne utajenia a odtajnenie

Utajovaným dokumentom EÚ sa môžu znížiť úrovne utajenia, alebo sa môžu odtajniť iba so súhlasom pôvodcu a prípadne po diskusii s ostatnými zainteresovanými stranami. Zníženie úrovne utajenia alebo odtajnenie sa písomne potvrdzuje. Pôvodca je zodpovedný za informovanie adresátov o tejto zmene a adresáti sú zase zodpovední za informovanie o tejto zmene akýchkoľvek iných následných adresátov, ktorým prípadne dokument alebo jeho kópiu zaslali.

Ak je to možné, pôvodcovia určujú na utajovaných dokument dátum, obdobie alebo udalosť, keď sa utajenie obsahu môže utajiť nižšou úrovňou, alebo sa obsah môže odtajniť. V opačnom prípade uchovávajú dokumenty pod revíziou aspoň raz za päť rokov, aby sa presvedčili, že pôvodné utajovanie je potrebné.

## 18. FYZICKÁ BEZPEČNOSŤ

### 18.1. Všeobecne

Hlavným cieľom fyzických bezpečnostných opatrení je zabrániť neoprávnenej osobe, aby získala prístup k utajovaným informáciám a/alebo materiálom EÚ, zabrániť krádeži a znehodnoteniu zariadenia a iného majetku a zabrániť vyhrážaniu alebo ľubovoľnému inému druhu agresie personálu, ostatných zamestnancov a návštevníkov.

### 18.2. Bezpečnostné požiadavky

Všetky priestory, plochy, budovy, miestnosti, komunikačné a informačné systémy atď., v ktorých sa uchovávajú utajované informácie a materiály a/alebo v ktorých sa narába s utajovanými informáciami a/alebo dokumentmi, musia byť chránené primeranými fyzickými bezpečnostnými opatreniami.

Pri rozhodovaní, aký je potrebný stupeň fyzickej bezpečnostnej ochrany, sa musia zohľadniť všetky príslušné faktory, napríklad:

- (a) úroveň utajovania informácií a/alebo materiálu;
- (b) množstvo a forma (napríklad tvrdá väzby, počítačové pamäťové médium) uchovávaných informácií;

- (c) miestne posúdená hrozba zo strany tajných služieb, ktorých cieľom je EÚ, členské štáty a/alebo iné inštitúcie alebo tretie strany, ktoré majú utajované informácie EÚ, teda hrozba sabotáže, terorizmu a iných podvratných a/alebo zločinných činností.

Uplatňované fyzické bezpečnostné opatrenia musia byť navrhnuté tak, aby:

- (a) odmietli tajný alebo násilný vstup nepovolanej osoby;
- (b) odradili, zabránili a identifikovali kroky nelojálnych členov personálu;
- (c) tím, ktorí nemajú nutnosť oboznámenia sa, zabránili prístup k utajovaným informáciám EÚ.

← Naformátováno: Odrážky a číslování

### 18.3. Fyzické bezpečnostné opatrenia

#### 18.3.1. Bezpečnostné oblasti

Oblasti, kde sa utajované informácie EÚ klasifikované ako DÔVERNÉ alebo vyššieho utajovania skladujú alebo kde sa s nimi narába, musia byť organizované a štruktúrované tak, aby zodpovedali niektorej z nasledujúcich tried:

- (a) Bezpečnostná oblasť triedy I: oblasť, kde sa utajované informácie EÚ klasifikované ako DÔVERNÉ alebo vyššieho utajovania skladujú alebo kde sa s nimi narába tak, že vstup do tejto oblasti predstavuje pre všetky praktické účely prístup k utajovaným informáciám. Takáto oblasť vyžaduje:
- (i) jasne definovanú a chránenú hranicu, cez ktorú sa všetky vstupy a výstupy kontrolujú;
  - (ii) vstupný kontrolný systém, ktorý pripustí iba tých, ktorí sú príslušne preverení a majú zvláštne oprávnenie na vstup do danej oblasti;
  - (iii) špecifikáciu utajenia informácie, ktorá sa zvyčajne v danej oblasti uchováva, t.j. informácia, ku ktorej vstup do oblasti vedie k jej prístupu.
- (b) Bezpečnostná oblasť triedy II: oblasť, kde sa utajované informácie EÚ klasifikované ako DÔVERNÉ alebo vyššieho utajovania skladujú alebo kde sa s nimi narába tak, že ich možno chrániť pred prístupom neoprávnených osôb prostredníctvom vnútorne zavedených kontrol, napríklad priestory, kde sa nachádzajú služby, kde sa pravidelne uchovávajú utajované informácie EÚ klasifikované ako DÔVERNÉ alebo vyššieho utajovania, alebo kde sa s takýmito informáciami pravidelne narába. Takáto oblasť vyžaduje:
- (i) jasne definovanú a chránenú hranicu, cez ktorú sa všetky vstupy a výstupy kontrolujú;
  - (ii) vstupný kontrolný systém, ktorý pripustí osoby bez sprievodu iba vtedy, ak sú takéto osoby príslušne preverené a majú zvláštne oprávnenie na vstup do danej oblasti. Pre všetky ostatné osoby sa musí zabezpečiť sprievod alebo ekvivalentné kontroly, aby sa zabránilo neoprávnenému vstupu k utajovaným informáciám EÚ a nekontrolovanému vstupu do oblastí, ktoré podliehajú technickým bezpečnostným inšpekciám.

Tie oblasti, kde sa nenachádza služobný personál 24 hodín denne, sa musia podrobiť prehliadke okamžite po zvyčajných pracovných hodinách, aby sa zabezpečilo, že utajované informácie EÚ sú príslušne zabezpečené.

### 18.3.2. *Administratívny priestor*

Okolo bezpečnostných oblastí triedy I alebo triedy II alebo smerom k bezpečnostným oblastiam týchto tried sa môže ustanoviť administratívny priestor menšieho stupňa bezpečnosti. Takýto priestor vyžaduje viditeľne definovanú hranicu, ktorá umožňuje, aby sa personál a vozidlá podrobili kontrolám. V takýchto oblastiach sa môžu skladovať a narábať iba s informáciami EÚ VYHRADENÉ a neutajovanými informáciami.

### 18.3.3. *Vstupné a výstupné kontroly*

Vstup a výstup do bezpečnostných oblastí triedy I a triedy II a z bezpečnostných oblastí triedy I a triedy II sa kontroluje rozlišovacím systémom založeným na priepustkách alebo osobným rozlišovacím systémom, ktorý sa uplatňuje na všetkých členov personálu zvyčajne pracujúcich v týchto oblastiach. Musí sa tiež zaviesť systém kontrol návštevníkov navrhnutý tak, aby sa odoprel neoprávnený prístup k utajovaným informáciám EÚ. Systémy priepustiek môžu byť podporené automatizovanou identifikáciou, ktoré sa považuje za doplnok, ale nie úplnú náhradu strážnikov. Zmena v posúdení hrozby môže viesť k posilneniu vstupných a výstupných opatrení, napríklad počas návštevy prominentných osôb.

### 18.3.4 *Strážne obhliadky*

Obhliadky bezpečnostných oblastí triedy I a triedy II sa uskutočňujú mimo zvyčajných pracovných hodín s cieľom chrániť majetok EÚ proti ohrozeniu, škode alebo strate. Frekvencia obhliadok sa určuje podľa miestnych okolností, ale, ako pomôcka, vykonávajú sa raz za dve hodiny.

### 18.3.5 *Bezpečnostné schránky a zabezpečené miestnosti*

Na uskladnenie utajovaných informácií EÚ sa používajú tri triedy schránok:

- trieda A: schránky národne schválené na uskladňovanie informácií EÚ PRÍSNE TAJNÉ v rámci bezpečnostných oblastí triedy I a triedy II;
- trieda B: schránky národne schválené na uskladňovanie informácií EÚ TAJNÉ a DÔVERNÉ v rámci bezpečnostných oblastí triedy I alebo triedy II;
- trieda C: služobný nábytok vhodný iba na uskladňovanie informácií EÚ VYHRADENÉ.

V zabezpečených miestnostiach vybudovaných v rámci bezpečnostnej oblasti triedy I alebo triedy II a pre všetky bezpečnostné oblasti triedy I, kde sa utajované informácie EÚ DÔVERNÉ a vyššieho utajenia uskladňujú na otvorených policiach alebo sú zobrazené na náčrtoch, mapách atď., musia byť steny, podlahy, stropy a dvere so zámkami certifikované podľa bezpečnostného akreditačného úradu ako možnosti ponúkajúce ekvivalentnú ochranu triedy bezpečnostnej schránky schválenej na uchovávanie informácií rovnakého utajenia.

### 18.3.6. *Zámky*

Zámky, ktoré sa používajú s bezpečnostnými schránkami a zabezpečenými miestnosťami, kde sa uchovávajú utajované informácie EÚ, musia spĺňať nasledujúce normy:

- skupina A: národne schválené pre schránky triedy A;
- skupina B: národne schválené pre schránky triedy B;
- skupina C: vhodné iba pre služobný nábytok triedy C.

#### 18.3.7. *Kontrola kľúčov a kombinácií*

Kľúče bezpečnostných schránok sa nesmú brať mimo budov komisie. Nastavenia kombinácií bezpečnostných schránok si osoby, ktoré ich potrebujú vedieť, musia zapamätať. Na použitie v núdzovom prípade je miestny bezpečnostný referent daného oddelenia komisie zodpovedný za uchovávanie náhradných kľúčov a vedenie písomného záznamu o všetkých nastavených kombináciách; nastavené kombinácie sa uchovávajú v oddelených nepriehľadných obálkach. Pracovné kľúče, náhradné bezpečnostné kľúče a nastavené kombinácie sa uchovávajú v oddelených bezpečnostných schránkach. Tieto kľúče a nastavené kombinácie by mali mať pridelenú bezpečnostnú ochranu nie menej prísnu ako ochrana materiálu, ku ktorému dávajú prístup.

Oboznámenie sa s nastavenými kombináciami bezpečnostných schránok sa obmedzuje na čo najmenej osôb. Kombinácie sa znovu nastavujú:

- (a) po prijatí novej schránky;
- (b) pri každej personálnej zmene;
- (c) ak došlo k odcudzeniu alebo existuje podozrenie z odcudzenia;
- (d) podľa možností v šesťmesačných intervaloch, ale aspoň raz za dvanásť mesiacov.

← Naformátovano: Odrážky a číslovaní

#### 18.3.8. *Poplašné detekčné zariadenia*

Ak sa na ochranu utajovaných informácií EÚ používajú poplašné systémy, bezpečnostné kamery a iné elektrické zariadenia, musí byť k dispozícii núdzový zdroj napätia, aby sa zabezpečila kontinuálna prevádzka systému, ak sa hlavný zdroj napätia preruší. Ďalšou základnou požiadavkou je, že zlyhanie takýchto systémov alebo svojvoľná manipulácia s takýmito systémami vedie k poplachu alebo inému spoľahlivému varovaniu pre dozorný personál.

#### 18.3.9. *Schválené zariadenie*

Bezpečnostný úrad komisie uchováva aktualizované zoznamy podľa typu a modelu bezpečnostných zariadení, ktoré schválil na ochranu utajovaných informácií za rozličných špecifikovaných okolností a podmienok. Bezpečnostný úrad komisie vychádza pri týchto zoznamoch *inter alia* z informácií od národných bezpečnostných úradov.

#### 18.3.10. *Fyzická ochrana kopírovacích a faxových prístrojov*

Kopírovacie a faxové prístroje musia byť fyzicky chránené do rozsahu potrebného, aby sa zabezpečilo, že iba oprávnené osoby ich môžu používať na spracovávanie utajovaných informácií a že všetky utajované produkty podliehajú príslušným kontrolám.

#### 18.4. Ochrana proti neoprávnenému nazeraniu a odpočúvaniu

##### 18.4.1. *Neoprávnené nazeranie*

Vo dne aj v noci sa musia dodržiavať všetky primerané opatrenia, aby sa zabezpečilo, že neoprávnené osoby nemajú možnosť zazrieť utajované informácie EÚ ani náhodne.

##### 18.4.2. *Odpočúvanie*

Služby alebo oblasti, kde sa o utajovaných informáciách EÚ TAJNÉ a vyššieho utajenia pravidelne diskutuje, musia byť chránené proti útokom pasívneho a aktívneho odpočúvania, ak to tak riziká vyžadujú. Posúdenie rizika takýchto útokov je zodpovednosťou bezpečnostného úradu komisie po prípadných konzultáciách s národnými bezpečnostnými úradmi.

##### 18.4.3. *Zavedenie elektronického a záznamového zariadenia*

Bez predchádzajúceho oprávnenia od vedúceho bezpečnostného úradu komisie nie je povolené zavádzať mobilné telefóny, súkromné počítače, záznamové zariadenia, kamery a iné elektronické alebo záznamové zariadenia do bezpečnostných oblastí alebo technicky bezpečnostných oblastí.

Aby sa určili ochranné opatrenia, ktoré sa musia prijať v priestoroch citlivých na pasívne odpočúvanie (izolácia stien, dverí, podláh a stropov, meranie ohrozujúceho vyžarovania) a aktívne odpočúvanie (napríklad pátranie po mikrofónoch), komisia môže požadovať pomoc od odborníkov národných bezpečnostných úradov.

Podobne, ak tak okolnosti vyžadujú, telekomunikačné zariadenia a elektrické alebo elektronické kancelárske zariadenia ľubovoľného druhu, ktoré sa používajú počas stretnutí na úrovni EÚ TAJNÉ a vyššej, sa môžu podrobiť kontrole technických bezpečnostných špecialistov národných bezpečnostných úradov na žiadosť vedúceho bezpečnostného úradu komisie.

#### 18.5 Technicky bezpečné oblasti

Určité oblasti možno vyčleniť ako technické bezpečné oblasti. Vykonáva sa zvláštna vstupná kontrola. Takéto oblasti sa schváleným spôsobom uzamykajú, ak nie sú obsadené, a so všetkými kľúčmi sa narába ako s bezpečnostnými kľúčmi. Takéto oblasti sú predmetom pravidelných fyzických inšpekcí, ktoré sa tiež vykonávajú po neoprávnenom vstupe alebo pri podozrení z takéhoto vstupu.

Vedie sa podrobný súpis zariadenia a nábytku, aby bolo možné sledovať ich pohyb. Žiadna položka nábytku ani zariadenia sa do takejto oblasti nesmie pridať, pokiaľ nepodstúpila starostlivú inšpekciu zvláštne školeného bezpečnostného personálu, ktorá má odhaliť

akékoľvek načúvacie zariadenia. Vo všeobecnosti, inštalácia komunikačných liniek v technicky bezpečných oblastiach nie je povolená bez predchádzajúceho oprávnenia od príslušného úradu.

## 19. VŠEOBECNÉ PRAVIDLÁ O ZÁSADĚ POTREBY OBOZNÁMENIA SA A BEZPEČNOSTNÉ PREVIERKY PERSONÁLU EÚ

### 19.1. Všeobecne

Prístup k utajovaným informáciám EÚ sa udeľuje iba osobám, ktoré majú „potrebu oboznámenia sa“, aby mohli vykonávať svoje povinnosti alebo poslania. Prístup k informáciám EÚ PRÍSNE TAJNÉ, TAJNÉ a DÔVERNÉ sa udeľuje iba osobám, ktoré úspešne prešli príslušnou bezpečnostnou previerkou.

Zodpovednosť za určenie „potreby oboznámenia sa“ spočíva na oddelení, kde daná osoba pracuje.

Žiadanie o preverenie personálu je zodpovednosťou jednotlivých oddelení.

Toto vedie k vydaniu „osobného bezpečnostného certifikátu EÚ“, ktorý uvádza úroveň utajovaných informácií, ku ktorým môže mať preverená osoba prístup, a dátum skončenia platnosti.

Osobný bezpečnostný certifikát EÚ pre dané utajenie môže udeliť držiteľovi prístup k informáciám nižšieho utajenia.

Osoby iné ako úradníci alebo ostatní zamestnanci, napríklad externí dodávatelia, odborníci alebo konzultanti, s ktorými je prípadne nutné diskutovať, alebo ktorým je potrebné utajované informácie EÚ zverejniť, musia sa podrobiť osobnej bezpečnostnej previerke EÚ, pokiaľ ide o utajované informácie EÚ, a musia byť oboznámení o ich zodpovednosti za bezpečnosť.

Verejný prístup naďalej určuje nariadenie (ES) č. 1049/2001.

### 19.2. Osobitné pravidlá o prístupe k informáciám EÚ PRÍSNE TAJNÉ

Všetky osoby, ktoré majú prístup k informáciám EÚ PRÍSNE TAJNÉ, menuje člen komisie zodpovedným za bezpečnostné záležitosti a ich mená sú uvedené v príslušnom registri informácií EÚ PRÍSNE TAJNÉ. Tento register vytvorí a vedie bezpečnostný úrad komisie.

Všetky osoby pred tým, ako získajú prístup k informáciám EÚ PRÍSNE TAJNÉ, musia podpísať vyhlásenie v tom zmysle, že boli oboznámené o bezpečnostných postupoch komisie a že plne chápu svoju zvláštnu zodpovednosť za ochraňovanie informácií EÚ PRÍSNE TAJNÉ a dôsledky, ktoré stanovujú pravidlá EÚ a národného práva alebo administratívne pravidlá, ak sa utajované informácie dostanú do neoprávnených rúk zámerne alebo v dôsledku nedbanlivosti.

V prípade osôb, ktoré majú prístup k informáciám EÚ PRÍSNE TAJNÉ na zasadnutiach atď., príslušný kontrolný referent danej služby alebo orgánu, kde daná osoba pracuje, upovedomí orgán, ktorý organizuje zasadnutie, že príslušné osoby majú takéto oprávnenie.

Mená všetkých osôb, ktoré už viac nepracujú na povinnostiach vyžadujúcich prístup k informáciám EÚ PRÍSNE TAJNÉ, sa odstránia zo zoznamu EÚ PRÍSNE TAJNÉ. Okrem toho, všetky takéto osoby sa znova upozornia na ich zvláštnu zodpovednosť za ochraňovanie informácií EÚ PRÍSNE TAJNÉ. Podpíšu tiež vyhlásenie, ktoré uvedie, že nepoužijú ani neposkytnú informácie EÚ PRÍSNE TAJNÉ, ktoré majú k dispozícii.

### 19.3. Osobitné pravidlá o prístupe k informáciám EÚ TAJNÉ alebo EÚ DÔVERNÉ

Všetky osoby, ktoré majú prístup k informáciám EÚ TAJNÉ alebo EÚ DÔVERNÉ, musia najprv prejsť previerkou pre daný stupeň.

Všetky osoby, ktoré majú prístup k informáciám EÚ TAJNÉ alebo EÚ DÔVERNÉ, musia byť oboznámené s bezpečnostnými ustanoveniami a musia si byť vedomé dôsledkov zanedbania.

V prípade osôb, ktoré majú prístup k informáciám EÚ TAJNÉ alebo EÚ DÔVERNÉ na zasadnutiach atď., príslušný bezpečnostný úrad orgánu, kde daná osoba pracuje, upovedomí orgán, ktorý organizuje zasadnutie, že príslušné osoby majú takéto oprávnenie.

### 19.4. Osobitné pravidlá o prístupe k informáciám EÚ VYHRADENÉ

Osoby s prístupom k informáciám EÚ VYHRADENÉ sa oboznámia o týchto bezpečnostných pravidlách a o dôsledkoch zanedbania.

### 19.5. Presuny

Ak je člen personálu presunutý z miesta, ktoré zahŕňa narábanie s utajovaným materiálom EÚ, register dozrie na náležitý presun tohto materiálu od odchádzajúceho úradníka k prichádzajúcemu úradníkovi.

Ak člen personálu je presunutý na iné miesto, ktoré zahŕňa narábanie s utajovaným materiálom EÚ, miestny bezpečnostný referent ho s tým príslušne oboznámi.

### 19.6. Zvláštne pokyny

Osoby, ktoré musia narábať s utajovanými informáciami EÚ, by mali byť oboznámené najprv pri prevzatí svojich povinností a potom pravidelne, o:

- (a) nebezpečenstvách pre bezpečnosť, ktoré vyplývajú z indiskrétnych rozhovorov;
- (b) opatreniach, ktoré musia prijať v súvislosti so vzťahom s tlačou a predstaviteľmi zvláštnych záujmových skupín;
- (c) nebezpečenstve, ktoré predstavujú činnosti tajných služieb, ktoré sa zameriavajú na EÚ a členské štáty, pokiaľ ide o utajované informácie a činnosti EÚ;

Naformátovano: Odrážky a číslování

- (d) povinnosti okamžite nahlásiť príslušným bezpečnostným úradom akékoľvek oslovenie alebo manéver, ktorý vedie k podozreniu o špiónážnej činnosti, alebo akékoľvek nezvyčajné okolnosti týkajúce sa bezpečnosti.

Všetky osoby, ktoré sú zvyčajne vystavené častým kontaktom so zástupcami krajín, ktorých tajné služby sa zameriavajú na utajované informácie a činnosti EÚ, sa oboznamujú o technikách, o ktorých je známe, že ich používajú rozličné tajné služby.

Neexistujú žiadne bezpečnostné ustanovenia komisie týkajúce sa súkromných ciest do akýchkoľvek cieľových miest personálu, ktorý prešiel previerkami pre prístup k utajovaným informáciám EÚ. Bezpečnostný úrad komisie však oboznámi úradníkov a ostatných zamestnancov, ktorí spadajú pod jeho zodpovednosť, s cestovnými nariadeniami, ktorým prípadne podliehajú.

## 20. POSTUP BEZPEČNOSTNÝCH PREVIEROK PRE ÚRADNÍKOV KOMISIE A OSTATNÝCH ZAMESTNANCOV

- (a) Iba úradníci a ostatní zamestnanci komisie alebo osoby pracujúce v rámci komisie, ktoré z dôvodu svojich povinností a požiadaviek služby potrebujú vedomosť alebo musia používať utajované informácie, ktoré vlastní komisia, majú prístup k takýmto informáciám.
- (b) Na získanie prístupu k informáciám klasifikovaným ako „EÚ PRÍSNE TAJNÉ“, „EÚ TAJNÉ“ a „EÚ DÔVERNÉ“, osoby uvedené v odseku (a) vyššie musia byť oprávnené v súlade s postupom uvedeným v odsekoch (c) a (d) tohto oddielu.
- (c) Oprávnenie sa udeľuje iba osobám, ktoré prešli bezpečnostnými previerkami príslušných národných bezpečnostných úradov členských štátov (NBÚ) v súlade s postupom uvedeným v odsekoch (i) až (n).
- (d) Vedúci bezpečnostného úradu komisie je zodpovedný za udeľovanie oprávnení uvedených v odsekoch (a), (b) a (c).
- (e) Vedúci bezpečnostného úradu komisie udelí oprávnenie po získaní stanoviska príslušných národných úradov členských štátov na základe bezpečnostných previerok, ktoré sa vykonali v súlade s odsekmi (i) až (n).
- (f) Bezpečnostný úrad komisie vedie aktualizovaný zoznam všetkých citlivých pozícií, ktoré poskytujú príslušné oddelenia komisie, a všetkých osôb, ktorým sa udelilo (dočasné) oprávnenie.
- (g) Oprávnenie, ktoré je platné na obdobie piatich rokov, nesmie prekročiť dĺžku úloh na základe ktorých bolo udelené. Môže sa obnoviť v súlade s postupom uvedeným v odseku (e).

- (h) Vedúci bezpečnostného úradu komisie odoberie oprávnenie, ak usúdi, že existujú pre to opodstatnené dôvody. Rozhodnutie odobrať oprávnenie sa oznámi danej osobe a príslušnému národnému úradu. Osoba, ktorej sa oprávnenie odobralo, môže požiadať vedúceho bezpečnostného úradu komisie o vypočutie.
- (i) Bezpečnostné preverovanie sa vykonáva za asistencie danej osoby a na žiadosť vedúceho bezpečnostného úradu komisie. Príslušný národný úrad na preverovanie je úradom členského štátu, ktorého je osoba podliehajúca oprávneniu štátnym príslušníkom. Ak daná osoba nie je štátnym príslušníkom členského štátu EÚ, vedúci bezpečnostného úradu komisie požiada o bezpečnostné preverenie členský štát EÚ, kde má daná osoba trvalé bydlisko alebo kde sa zvyčajne zdržiava.
- (j) Ako súčasť previerkového postupu sa daná osoba požiada, aby vyplnila osobné informačné tlačivo.
- (k) Vedúci bezpečnostného úradu komisie vo svojej žiadosti špecifikuje typ a úroveň utajovaných informácií, ktoré sa majú sprístupniť danej osobe, tak, aby príslušné národné úrady mohli vykonať previerku a poskytnúť svoje stanovisko ohľadne úrovne oprávnenia, ktorá by bola primeraná, aby sa danej osobe udelila.
- (l) Celý bezpečnostný preverovací proces spolu so získanými výsledkami podliehajú príslušným pravidlám a nariadeniam účinným v danom členskom štáte vrátane tých, ktoré sa týkajú odvolania.
- (m) Ak príslušné národné úrady členského štátu dajú pozitívne stanovisko, môže vedúci bezpečnostného úradu komisie danej osobe oprávnenie udeliť.
- (n) Negatívne stanovisko príslušných národných úradov sa oznámi danej osobe, ktoré môže vedúceho bezpečnostného úradu komisie požiadať o vypočutie. Ak vedúci bezpečnostného úradu komisie usúdi, že je potrebné, aby príslušné národné úrady poskytli ďalšie vysvetlenie, môže ich požiadať, aby poskytli akékoľvek iné vysvetlenia, ktoré môžu predložiť. Ak sa negatívne stanovisko potvrdí, oprávnenie sa neudelí.
- (o) Všetky osoby, ktorým sa udelilo oprávnenie v zmysle odsekov (d) a (e), obdržia v čase udelenia oprávnenia a potom v pravidelných intervaloch ľubovoľné potrebné pokyny ohľadne utajovaných informácií a prostriedkoch zabezpečenia takejto ochrany. Takéto osoby podpíšu vyhlásenie, ktorým potvrdia, že obdržali takéto pokyny, a zaviazu sa, že ich budú dodržiavať.

- (p) Vedúci bezpečnostného úradu komisie prijme všetky potrebné opatrenia, aby vykonal tento oddiel, najmä pokiaľ ide o pravidlá riadiace prístup k zoznamu oprávnených osôb.
- (q) Vedúci bezpečnostného úradu komisie môže výnimočne, ak tak vyžaduje služba, udeliť po predložení oznámenia príslušných národných úradov a ak príslušné národné úrady nereagujú do jedného mesiaca, dočasné oprávnenie na obdobie nepresahujúce šesť mesiacov, očakávajúci výsledok preverky uvedenej v odseku (i).
- (r) Dočasné a predbežné oprávnenia takto udelené nedávajú prístup k informáciám EÚ PRÍSNE TAJNÉ; takýto prístup sa obmedzuje na úradníkov, ktorí sa už skutočne podrobili preverke s pozitívnymi výsledkami v súlade s odsekom (i). Úradníci, ktorí požiadali, aby boli preverení na úrovni informácií EÚ PRÍSNE TAJNÉ a ešte stále očakávajú výsledok preverky, môžu dočasne a predbežne získať oprávnenie na prístup k informáciám utajeným až po úroveň EÚ DÔVERNÉ vrátane.

## 21. PRÍPRAVA, DISTRIBÚCIA, ROZŠIROVANIE, BEZPEČNOSŤ KURIÉRSKEHO PERSONÁLU A ZVLÁŠTNE KÓPIE ALEBO PREKLADY A VÝPISY Z UTAJOVANÝCH INFORMÁCIÍ EÚ

### 21.1. Príprava

1. Utajovanie informácií EÚ sa uplatňuje, ako je stanovené v oddieli 16, a pre informácie EÚ DÔVERNÉ a vyššej úrovne sa uvádza na hornej a dolnej časti v strede na každej strane, pričom každá strana je očíslovaná. Všetky utajované dokumenty EÚ sú opatrené referenčným číslom a dátumom. V prípade dokumentov EÚ PRÍSNE TAJNÉ a EÚ TAJNÉ sa toto referenčné číslo uvádza na každej strane. Ak sa dokumenty majú distribuovať v niekoľkých kópiách, každá kópia musí mať číslo kópie, ktoré sa uvádza na prvej strane, spolu s celkovým počtom strán. Všetky prílohy a dodatky sa uvádzajú v zozname na prvej strane dokumentu klasifikovaného ako EÚ DÔVERNÉ a vyššej úrovne utajovania.
2. Dokumenty klasifikované ako EÚ DÔVERNÉ a vyššej úrovne utajovania, môžu písať, prekladať, uschovávať, fotokopírovať a reprodukovat' magneticky alebo mikrofilmami iba osoby, ktoré boli preverené na prístup k utajovaným informáciám EÚ aspoň do bezpečnostnej úrovne utajovania daného dokumentu.
3. Ustanovenia, ktoré riadia počítačové vyhotovovanie utajovaných dokumentov, sú uvedené v oddieli 25.

### 21.2. Distribúcia

1. Utajované informácie EÚ sa distribuujú iba osobám, ktoré ich potrebujú poznať a majú príslušné bezpečnostné preverenie. Pôvodca informácií označuje počiatočnú distribúciu.

2. Dokumenty EÚ PRÍSNE TAJNÉ sa ostávajú do obehu prostredníctvom registrov EÚ PRÍSNE TAJNÉ (pozri oddiel 22.2). V prípade odkazov EÚ PRÍSNE TAJNÉ môže príslušný register oprávniť vedúceho komunikačného centra, aby vyhotovil určitý počet kópií uvedený v zozname adresátov.
3. Dokument klasifikovaný ako EÚ TAJNÉ a nižšej úrovne utajenia môže pôvodný adresát ďalej distribuovať ďalším adresátom podľa zásady potreby oboznámenia sa. Úrady, ktoré sú pôvodcami takýchto dokumentov, však jasne určia akékoľvek upozornenia, ktoré si želajú zaviesť v súvislosti s týmito dokumentmi. Ak sú takéto upozornenia zavedené, adresáti môžu dokumenty ďalej distribuovať iba s oprávnením úradov, ktoré sú pôvodcami dokumentov.
4. Všetky dokumenty, ktoré sú klasifikované EÚ DÔVERNÉ a vyššej úrovne utajenia musí pri príchode alebo pri opúšťaní generálneho riaditeľstva alebo služby zaznamenať miestny register utajovaných informácií EÚ daného oddelenia. Konkrétne údaje, ktoré sa zaznamenávajú (odkazy, dátum a prípadne číslo kópie), musia byť také, aby bolo podľa nich možné dokumenty identifikovať, a zapisujú sa do knihy alebo sa uchovávajú na zvlášť chránenom počítačovom médiu (pozri oddiel 22.1).

### 21.3. Prenos utajovaných dokumentov EÚ

#### 21.3.1. *Balenie, príjem*

1. Dokumenty klasifikované ako EÚ DÔVERNÉ a vyššej úrovne utajenia sa prenášajú v odolných, nepriesvitných dvojitéch obálkach. Vnútoraná obálka sa označí príslušným bezpečnostným utajením EÚ a, ak je možné, tiež úplnými údajmi o názve funkcie príjemcu a adrese.
2. Iba kontrolný referent registra (pozri oddiel 22.1) alebo jeho zástupca môže otvoriť vnútornú obálku a potvrdiť príjem priložených dokumentov, pokiaľ obálka nie je adresovaná jednotlivcovi. V takomto prípade príslušný register (pozri oddiel 22.1) zapíše príchod obálky a iba jednotlivec, ktorému je obálka adresovaná, smie otvoriť vnútornú obálku a potvrdiť príjem dokumentu, ktorý obálka obsahuje.
3. Tlačivo o príjme sa umiestňuje do vnútornej obálky. Príjmové tlačivo, ktoré sa neutajuje, by malo uvádzať referenčné číslo, dátum a číslo kópie dokumentu, ale nie predmet dokumentu.
4. Vnútoraná obálka sa vkladá do vonkajšej obálky, na ktorej je číslo balíka pre účely príjmu. Za žiadnych okolností sa na vonkajšej obálke nesmie uvádzať bezpečnostné utajenie.

5. V prípade dokumentov klasifikovaných ako EÚ DÔVERNÉ a vyššej úrovne utajenia, kuriéri a poslovia obdržia príjmové tlačivo proti číslam balíkov.

### 21.3.2. Prenos v rámci budovy alebo skupiny budov

V rámci danej budovy alebo skupiny budov sa utajované dokumenty môžu prenášať v zapečatenej obálke, na ktorej je uvedené iba meno adresáta, pokiaľ obálku prenáša osoba, ktorá je preverená pre úroveň utajenia prenášaných dokumentov.

### 21.3.3. Prenos v rámci krajiny

1. V rámci krajiny by sa dokumenty EÚ PRÍSNE TAJNÉ mali zasielať iba prostredníctvom oficiálnej kuriérskej služby alebo prostredníctvom osôb oprávnených na prístup k informáciám EÚ PRÍSNE TAJNÉ.
2. Ak sa na prenos dokumentu EÚ PRÍSNE TAJNÉ mimo budovy alebo skupiny budov používa kuriérska služba, musí sa dodržiavať balenie a ustanovenia o príjme uvedené v tejto kapitole. Kuriérske služby musia mať také personálne obsadenie, aby sa zabezpečilo, že balíky obsahujúce dokumenty EÚ PRÍSNE TAJNÉ zostanú po celý čas pod priamym dozorom zodpovedného referenta.
3. Výnimočne môžu aj referenti iní ako kuriéri prenášať dokumenty EÚ PRÍSNE TAJNÉ mimo budovy alebo skupiny budov pre miestne použitie na zasadnutiach a rokovaniach, ak:
  - (a) daný posol má oprávnenie na prístup k takýmto dokumentom EÚ PRÍSNE TAJNÉ;
  - (b) spôsob dopravy je v súlade s pravidlami uplatňovanými pre prenos dokumentov EÚ PRÍSNE TAJNÉ;
  - (c) za žiadnych okolností nenechá daný posol dokumenty EÚ PRÍSNE TAJNÉ bez dozoru;
  - (d) je zabezpečené, že zoznam dokumentov takto prenášaných je uvedený v registri dokumentov EÚ PRÍSNE TAJNÉ a je zaznamenaný v knihe, pričom sa zoznam skontroluje oproti tomuto zápisu v čase návratu dokumentov.
4. V rámci danej krajiny sa dokumenty EÚ TAJNÉ a EÚ DÔVERNÉ môžu zasielať poštou, ak je takýto prenos povolený národnými nariadeniami a je v súlade s ustanoveniami týchto nariadení, alebo kuriérskou službou alebo osobami, ktoré sú preverené na prístup k utajovaným informáciám EÚ.
5. Bezpečnostný úrad komisie pripraví pokyny o osobnej preprave utajovaných dokumentov EÚ na základe týchto pravidiel. Doručiteľ je povinný si tieto pokyny prečítať a podpísať. Tieto pokyny musia najmä jasne uvádzať, že dokumenty v žiadnom prípade nesmú:

← Naformátovano: Odrážky a číslovaní

- (a) zostať mimo doručiteľa, pokiaľ nie sú v bezpečnej úschove v súlade s ustanoveniami uvedenými v oddieli 18;
- (b) zostať bez dozoru v prostriedkoch verejnej alebo súkromnej dopravy, alebo na miestach ako napríklad hotely alebo reštaurácie. Nesmú sa uschovávať v hotelových trezoroch ani nechať bez dohľadu v hotelových izbách;
- (c) sa čítať na verejných miestach, ako napríklad lietadlá alebo vlaky.

#### 21.3.4. Prenos zo štátu do štátu

1. Materiál klasifikovaný ako EÚ DÔVERNÉ a vyššej úrovne utajenia sa prenáša diplomatickými službami EÚ alebo vojenskými kuriérskymi službami EÚ.
2. Je však možné povoliť osobný prenos materiálu klasifikovaného ako EÚ TAJNÉ a EÚ DÔVERNÉ, ak sú opatrenia pre prenos také, že zabezpečia, že sa dané dokumenty nedostanú do rúk neoprávnených osôb.
3. Člen komisie zodpovedný za bezpečnostné záležitosti môže oprávniť osobný prenos, ak nie sú k dispozícii diplomatickí ani vojenský kuriéri, alebo ak by použitie takýchto kuriérov viedlo k zdržaniu, ktoré by bolo na škodu pre činnosť EÚ a materiál je s úrne potrebný pre určeného príjemcu. Bezpečnostný úrad komisie pripraví pokyny, ktoré sa vzťahujú na osobný prenos zo štátu do štátu utajovaného materiálu až do úrovne EÚ TAJNÉ vrátane osobami inými, ako sú diplomatickí a vojenský kuriéri. Pokyny musia požadovať, aby:
  - (a) doručiteľ mal príslušné bezpečnostné preverenie;
  - (b) sa viedol záznam v príslušnom oddelení alebo registri o všetkých materiáloch takto prenášaných;
  - (c) na balíkoch alebo vreciach obsahujúcich materiál EÚ bola úradná pečať, ktorá by zabránila alebo znemožnila colnú kontrolu, a nálepky s identifikáciou a s pokynmi pre nálezcu;
  - (d) doručiteľ mal kuriérsky certifikát a/alebo príkaz na úlohu, ako ich uznávajú všetky členské štáty EÚ a ktoré ho oprávňujú, aby prenášal daný balík, ako je stanovené;
  - (e) sa neprechádzalo cez žiaden nečlenský štát EÚ ani cez jeho pohraničné územie, ak sa cestuje po súši, pokiaľ zasielajúci štát nemá konkrétnu záruku od takéhoto štátu;
  - (f) cestovné zabezpečenia doručiteľa týkajúce sa cieľových miest, trás, po ktorých sa má cestovať, a cestovných prostriedkov, ktoré sa majú použiť, boli v súlade s pravidlami EÚ alebo – ak sú národné pravidlá pre takéto činnosti prísnejšie - v súlade s takýmito nariadeniami;

Naformátovano: Odrážky a číslovaní

- (g) materiál sa nesmie dostať mimo opatrovania doručiteľa, pokiaľ nie je uschovaný v súlade s ustanoveniami o bezpečnej úschove uvedenými v oddieli 18;
  - (h) materiál sa nesmie nechať bez dozoru vo verejných alebo súkromných dopravných prostriedkoch ani na miestach ako napríklad reštaurácie alebo hotely. Nesmie sa uchovávať v hotelových trezoroch ani zanechať bez dozoru v hotelových izbách;
  - (i) ak prenášaný materiál obsahuje dokumenty, takéto dokumenty sa nesmú čítať na verejných miestach (napríklad v lietadlách, vlakoch atď.).
4. Osoba určená na prenos utajovaného materiálu si musí prečítať a podpísať bezpečnostný pokyn, ktoré uvádza minimálne pokyny uvedené vyššie a postupy, ktoré sa musia dodržiavať v núdzovom prípade alebo ak balík obsahujúci utajovaný materiál spochybnia colní alebo letiskoví bezpečnostní úradníci.

#### 21.3.5 Prenos dokumentov EÚ VYHRADENÉ

Pre prenos dokumentov EÚ VYHRADENÉ nie sú stanovené žiadne zvláštne ustanovenia s výhradou, že by mali byť také, aby sa zabezpečilo, že sa nedostanú do rúk neoprávnených osôb.

#### 21.4. Bezpečnosť kuriérskeho personálu

Všetci kuriéri a poslovia, ktorí sú zamestnaní na prenos dokumentov EÚ TAJNÉ a EÚ DÔVERNÉ, musia byť príslušne preverení.

#### 21.5. Elektronické a iné prostriedky technického prenosu

1. Komunikačné bezpečnostné opatrenia sú navrhnuté tak, aby zabezpečili bezpečný prenos utajovaných informácií EÚ. Podrobné pravidlá uplatňované pre prenos takýchto utajovaných informácií EÚ sú uvedené v oddieli 25.
2. Iba akreditované komunikačné centrá a siete a/alebo terminály a systémy môžu prenášať informácie EÚ DÔVERNÉ a EÚ TAJNÉ.

#### 21.6. Zvláštne kópie a preklady a výpisy z utajovaných dokumentov EÚ

1. Iba pôvodca môže oprávniť kópiu alebo preklad dokumentov EÚ PRÍSNE TAJNÉ.
2. Ak osoby bez preverenia pre úroveň EÚ PRÍSNE TAJNÉ žiadajú informácie, ktoré, aj keď sú uvedené v dokumente EÚ PRÍSNE TAJNÉ, nemajú tento stupeň utajenia, vedúci registra dokumentov EÚ PRÍSNE TAJNÉ (pozri oddiel 22.2) môže oprávniť vyhotovenie potrebného počtu výpisov z týchto dokumentov. Súčasne prijme potrebné kroky, aby zabezpečil, že sa týmto výpisom pridelí príslušná klasifikácia utajenie.

3. Dokumenty klasifikované ako EÚ TAJNÉ a nižšej úrovne utajenia môže adresát reprodukovať a prekladať v rámci týchto bezpečnostných ustanovení a pod podmienkou, že sa dodržiava zásada potreby oboznámenia sa. Bezpečnostné opatrenia uplatňované pre originálny dokument sú tiež uplatňované pre jeho reprodukcie a/alebo preklady.

## 22. REGISTRE UTAJOVANÝCH INFORMÁCIÍ EÚ, PREHLIADKY, KONTROLY, ARCHÍVNE SKLADOVANIA A LIKVIDÁCIA EUCI

### 22.1. Miestne registre utajovaných informácií EÚ

1. V rámci komisie v každom oddelení je jeden prípadne viacero miestnych registrov EUCI zodpovedných za registráciu, reprodukciu, rozosielanie, archivovanie a likvidáciu dokumentov klasifikovaných ako EÚ TAJNÉ a EÚ DÔVERNÉ.
2. Ak oddelenie nemá miestny register EUCI, jeho funkciu vykonáva miestny register EUCI generálneho sekretariátu.
3. Miestne registre EUCI podliehajú vedúcemu oddelenia, od ktorého dostávajú pokyny. Vedúci takýchto registrov sú registračnými kontrolnými referentmi.
4. Miestne registre EUCI podliehajú dohľadu miestneho bezpečnostného referenta, pokiaľ ide o uplatňovanie ustanovení týkajúcich sa narábania s dokumentmi EUCI a súlad s príslušnými bezpečnostnými opatreniami.
5. Úradníci pridelení do miestnych registrov EUCI musia mať oprávnenie na prístup k EUCI v súlade s oddielom 20.
6. Pod dozorom príslušného vedúceho oddelenia miestne registre EUCI:
  - (a) riadia operácie týkajúce sa registrácie, reprodukcie, prekladu, prenosu, rozosielania a likvidácie takýchto dokumentov;
  - (b) aktualizujú zoznam údajov o utajovaných informáciách;
  - (c) pravidelne overujú potrebu zachovávať utajovanie informácií.
7. Miestne registre EUCI vedú evidenciu nasledujúcich údajov:
  - (a) dátum vypracovania utajovaných informácií;
  - (b) úroveň utajenia;
  - (c) dátum ukončenie platnosti utajenia;
  - (d) meno a oddelenie vydavateľa;
  - (e) príjemca alebo príjemcovia spolu so sériovým číslom;

← Naformátovano: Odrážky a číslování

- (f) predmet;
- (g) počet;
- (h) počet kópií v obehu;
- (i) príprava súpisu utajovaných informácií predložených oddeleniu;
- (j) evidencia odtajnenia a zníženia stupňa utajenia informácií.

8. Všeobecné pravidlá určené v oddieli 21 sa uplatňujú na miestne registre EUCI komisie, pokiaľ nie sú upravené osobitnými pravidlami uvedenými v tomto oddieli.

## 22.2. Register informácií EÚ PRÍSNE TAJNÉ

### 22.2.1. Všeobecne

1. Centrálny register informácií EÚ PRÍSNE TAJNÉ zabezpečuje zaznamenávanie, manipuláciu a distribúciu dokumentov EÚ PRÍSNE TAJNÉ v súlade s týmito bezpečnostnými ustanoveniami. Vedúci registra EÚ PRÍSNE TAJNÉ je kontrolným referentom registra EÚ PRÍSNE TAJNÉ.
2. Centrálny register informácií EÚ PRÍSNE TAJNÉ pôsobí ako hlavný prijímajúci a odosielač úrad v komisii voči ostatným inštitúciám EÚ, členským štátom, medzinárodným organizáciám a tretím štátom, s ktorými má komisia dohody o bezpečnostných postupoch pre výmenu utajovaných informácií.
3. V prípade potreby sa zakladajú vedľajšie registre, ktoré sú zodpovedné za vnútorné riadenie dokumentov EÚ PRÍSNE TAJNÉ; vedú aktualizované záznamy o obehu všetkých dokumentov, za ktoré je takýto vedľajší register zodpovedný.
4. Vedľajšie registre EÚ PRÍSNE TAJNÉ sa zakladajú podľa uvedeného v časti 22.2.3. ako odpoveď na dlhodobé potreby a sú priradené k centrálnemu registru EÚ PRÍSNE TAJNÉ. Ak je potrebné nahliadnuť do dokumentov EÚ PRÍSNE TAJNÉ iba dočasne a príležitostne, je možné tieto dokumenty uvoľniť bez založenia vedľajšieho registra EÚ PRÍSNE TAJNÉ, ak sú stanovené pravidlá na zabezpečenie, aby dokumenty zostali pod kontrolou príslušného registra EÚ PRÍSNE TAJNÉ a aby sa dodržiavali všetky fyzické a osobné bezpečnostné opatrenia.
5. Vedľajšie registre nesmú dokumenty EÚ PRÍSNE TAJNÉ prenášať priamo ostatným vedľajším registrom toho istého centrálného registra EÚ PRÍSNE TAJNÉ bez výslovného súhlasu centrálného registra EÚ PRÍSNE TAJNÉ.
6. Všetky výmeny dokumentov EÚ PRÍSNE TAJNÉ medzi vedľajšími registrami, ktoré nie sú priradené tomu istému centrálnemu registru, sa vykonávajú cez centrálny register EÚ PRÍSNE TAJNÉ.

### 22.2.2. *Centrálny register EÚ PRÍSNE TAJNÉ*

Vedúci centrálneho registra EÚ PRÍSNE TAJNÉ je ako kontrolný referent zodpovedný za:

- (a) rozširovanie dokumentov EÚ PRÍSNE TAJNÉ v súlade s ustanoveniami definovanými v oddieli 21.3;
- (b) vedenie zoznamu všetkých podriadených vedľajších registrov EÚ PRÍSNE TAJNÉ spolu menami a podpismi menovaných kontrolných referentov a ich oprávnených zástupcov;
- (c) uchovávanie potvrdení o príjmoch z registrov pre všetky dokumenty EÚ PRÍSNE TAJNÉ, ktoré distribuuje centrálny register;
- (d) vedenie záznamu o dokumentoch EÚ PRÍSNE TAJNÉ, ktoré uchováva a distribuuje;
- (e) vedenie aktualizovaného zoznamu všetkých centrálnych registrov EÚ PRÍSNE TAJNÉ, s ktorými zvyčajne korešponduje, spolu s menami a podpismi ich menovaných kontrolných referentov a ich oprávnených zástupcov;
- (f) fyzické ochraňovanie všetkých dokumentov EÚ PRÍSNE TAJNÉ, ktoré sa uchovávajú v registri, v súlade s pravidlami uvedenými v oddieli 18.

### 22.2.3. *Vedľajšie registre EÚ PRÍSNE TAJNÉ*

Vedúci vedľajšieho registra EÚ PRÍSNE TAJNÉ je ako kontrolný referent zodpovedný za:

- (a) rozširovanie dokumentov EÚ PRÍSNE TAJNÉ v súlade s ustanoveniami definovanými v oddieli 21.3;
- (b) vedenie aktualizovaného zoznamu všetkých osôb, ktoré majú prístup k informáciám EÚ PRÍSNE TAJNÉ za jeho kontroly;
- (c) distribuovanie dokumentov EÚ PRÍSNE TAJNÉ v súlade s pokynmi pôvodcu alebo podľa zásady potreby oboznámenia sa, pričom najprv skontroluje, či adresát má potrebné bezpečnostné preverenie;
- (d) vedenie aktualizovaného záznamu všetkých dokumentov EÚ PRÍSNE TAJNÉ, ktoré sa uchovávajú alebo ktoré sú v obehu pod jeho kontrolou, alebo ktoré boli postúpené iným registrom EÚ PRÍSNE TAJNÉ, a za uchovávanie príslušných príjmových tlačív;
- (e) vedenie aktualizovaného zoznamu registrov informácií EÚ PRÍSNE TAJNÉ, s ktorými má oprávnenie vymieňať si dokumenty úradu PRÍSNE TAJNÉ, spolu s menami a podpismi ich kontrolných referentov a ich oprávnených zástupcov;

- (f) fyzickú ochranu všetkých dokumentov EÚ PRÍSNE TAJNÉ, ktoré sa uchovávajú v rámci vedľajšieho registra v súlade s pravidlami uvedenými v oddieli 18.

### 22.3. Súpisy, prehliadky a kontroly utajovaných dokumentov EÚ

1. Všetky registre informácií EÚ PRÍSNE TAJNÉ, ako sú uvedené v tomto oddieli, každoročne vykonávajú súpis dokumentov EÚ PRÍSNE TAJNÉ podľa položiek. Dokument sa považuje za počítať, ak register dokument fyzicky obhliadne alebo má doklad o prijíme od registra EÚ PRÍSNE TAJNÉ, do ktorého bol dokument prevedený, potvrdenie o likvidácii dokumentu alebo o znížení stupňa utajenia, alebo príkaz na odtajnenie dokumentu. Zistenia ročných súpisov sa predkladajú členovi komisie zodpovednému za bezpečnostné záležitosti najneskôr do 1. apríla každého roka.
2. Vedľajšie registre EÚ PRÍSNE TAJNÉ predkladajú zistenia ročných inventúr centrálnemu registru, ktorému podliehajú, ku dňu, ktorý takýto centrálny register určí.
3. Utajované informácie EÚ pod úrovňou utajenia EÚ PRÍSNE TAJNÉ sú predmetom interných kontrol podľa príkazov od člena komisie zodpovedného za bezpečnostné záležitosti.
4. Tieto opatrenia majú umožniť, aby držiteľia predložili svoje stanoviská ohľadne:
  - (a) možnosti znížiť úroveň utajenia alebo odtajniť určité dokumenty;
  - (b) dokumentov, ktoré sa majú zlikvidovať.

← Naformátovano: Odrážky a číslování

### 22.4. Archivné skladovanie utajovaných informácií EÚ

1. EUCI sa musia skladovať za podmienok, ktoré sú v súlade s príslušnými požiadavkami uvedenými v oddieli 118.
2. Aby sa minimalizovali skladovacie problémy, kontrolní referenti všetkých registrov musia mať oprávnenie, aby mohli dať zhotoviť z dokumentov EÚ PRÍSNE TAJNÉ, EÚ TAJNÉ a EÚ DÔVERNÉ mikrofilmy alebo iné formy uschovania na magnetických alebo optických médiách pre účely archivovania, s podmienkou že:
  - (a) proces zhotovovania mikrofilmov/skladovania vykonáva personál s aktuálny preverením pre zodpovedajúcu úroveň utajenia;
  - (b) mikrofilm/skladovacie médium má priradenú tú istú bezpečnosť ako pôvodné dokumenty;

← Naformátovano: Odrážky a číslování

- (c) zhotovovanie mikrofilmu/skladovanie ľubovoľného dokumentu EÚ PRÍSNE TAJNÉ sa nahlási pôvodcovi;
  - (d) zvitky filmu alebo iný typ podpory obsahujú iba dokumenty rovnakej úrovne utajovania EÚ PRÍSNE TAJNÉ, EÚ TAJNÉ alebo EÚ DÔVERNÉ;
  - (e) zhotovovanie mikrofilmov/skladovanie ľubovoľného dokumentu EÚ PRÍSNE TAJNÉ alebo EÚ TAJNÉ je jasne naznačené v zázname používanom pre ročný súpis;
  - (f) pôvodné dokumenty, z ktorých boli vyhotovené mikrofilmy, alebo ktoré boli inak uskladnené, sa zničia v súlade s pravidlami uvedenými v oddieli 22.5.
3. Tieto pravidlá sa uplatňujú pre akúkoľvek formu oprávneného skladovania, ako napríklad elektromagnetické médiá a optický disk.

Naformátovano: Odrážky a číslovaní

### 22.5. Likvidácia utajovaných dokumentov EÚ

1. Aby sa zabránilo zbytočnému zhromažďovaniu utajovaných dokumentov EÚ, tie dokumenty, o ktorých vedúci jednotky usúdi, že sú neaktuálne a v nadbytočnom počte, sa zlikvidujú, len čo je to možné, nasledujúcim spôsobom:
  - (a) Dokumenty EÚ PRÍSNE TAJNÉ likviduje iba centrálny register, ktorý je za ne zodpovedný. Všetky dokumenty, ktoré boli zlikvidované, sa uvedú na zozname potvrdenia o likvidácii, ktoré podpíše kontrolný referent dokumentov EÚ PRÍSNE TAJNÉ a referent, ktorý bol svedkom likvidácie, pričom obidvaja musia mať preverenie pre úroveň EÚ PRÍSNE TAJNÉ. V knihe sa v tomto zmysle urobí záznam;
  - (b) Register vedie potvrdenie o likvidácii spolu s rozdeľovníkmi počas obdobia desiatich rokov. Kópie sa predložia pôvodcovi alebo príslušnému centrálnemu registru iba vtedy, ak sa o to výslovne požiada;
  - (c) Dokumenty EÚ PRÍSNE TAJNÉ vrátane celého utajeného odpadu vzniknutého z prípravy dokumentov EÚ PRÍSNE TAJNÉ, ako napríklad pokazené kópie, pracovné náčrty, rukou písané poznámky alebo diskety, sa musia zničiť pod dohľadom kontrolného referenta registra pre informácie EÚ PRÍSNE TAJNÉ spálením, rozdrvením, skartovaním alebo iným ničením na nespoznateľnú a neobnoviteľnú formu.
2. Dokumenty EÚ TAJNÉ likviduje register, ktorý je za dokumenty zodpovedný, pod dohľadom bezpečnostne preverenej osoby, pričom sa použije niektorý z procesov uvedených v odseku 1(c). Dokumenty EÚ TAJNÉ, ktoré sa zničili, sú uvedené na zozname podpísaných potvrdení o likvidácii, ktoré uchováva register spolu s rozdeľovníkmi počas doby minimálne troch rokov.

3. Dokumenty EÚ DÔVERNÉ likviduje register, ktorý je za dokumenty zodpovedný, pod dohľadom bezpečnostne preverenej osoby, pričom sa použije niektorý z procesov uvedených v odseku 1(c). Ich likvidácia sa zaznamenáva podľa príkazov od člena komisie zodpovedného za bezpečnostné záležitosti.
4. Dokumenty EÚ VYHRADENÉ likviduje register, ktorý je za dokumenty zodpovedný, alebo ich užívateľ v súlade s pokynmi od člena komisie zodpovedného za bezpečnostné záležitosti.

#### 22.6. Likvidácia v núdzových situáciách

1. Oddelenia komisie pripravujú plány vychádzajúce z miestnych podmienok, ktoré sú zamerané na ochranu utajovaného materiálu EÚ v krízovej situácii, vrátane prípadnej likvidácie, a evakuačné plány. Komisia vyhlási príkazy považované za potrebné, aby sa zabránilo tomu, že utajované informácie EÚ sa dostanú do nepovolaných rúk.
2. Zabezpečenia pre ochranu a/alebo likvidáciu dokumentov EÚ TAJNÉ a EÚ DÔVERNÉ v krízovej situácii nesmú v žiadnom prípade nepriaznivo ovplyvniť ochranu alebo likvidáciu dokumentov EÚ PRÍSNE TAJNÉ, vrátane kódovacieho zariadenia, s ktorými sa narába s najvyššou prioritou pred všetkými úlohami.
3. Opatrenia, ktoré sa musia prijať na ochranu a likvidáciu kódovacieho zariadenia v stave núdze, musia byť stanovené v osobitných pokynoch.
4. Takéto pokyny musia byť k dispozícii priamo na mieste v zapečatenej obálke. K dispozícii musia byť prostriedky/nástroje na likvidáciu.

### 23. BEZPEČNOSTNÉ OPATRENIA PRE KONKRÉTNE STRETNUTIA, KTORÉ SA KONAJÚ MIMO PRIESTOROV KOMISIE A ZAHŔŇAJÚ UTAJOVANÉ INFORMÁCIE EÚ

#### 23.1. Všeobecne

Ak sa zasadnutia komisie alebo iné dôležité zasadnutia konajú mimo priestorov komisie a ak to opodstatňujú konkrétne bezpečnostné požiadavky týkajúce sa vysokej citlivosti diskutovaných záležitostí alebo informácií, musia sa prijať bezpečnostné opatrenia opísané nižšie. Tieto opatrenia sa týkajú iba ochrany utajovaných informácií EÚ; ostatné bezpečnostné opatrenia bude prípadne nutné plánovať.

#### 23.2. Zodpovednosti

##### 23.2.1. Bezpečnostný úrad komisie

Bezpečnostný úrad komisie spolupracuje s príslušnými úradmi členského štátu, na území ktorého sa zasadnutie koná (hostiteľský členský štát), aby sa zabezpečila bezpečnosť zasadnutia komisie alebo iných dôležitých zasadnutí a bezpečnosť delegátov a ich personálu. Pokiaľ ide o ochranu bezpečnosti, mala by konkrétne zabezpečiť, aby:

- (a) sa vyhotovili plány, podľa ktorých sa postupuje v čase bezpečnostného ohrozenia a iných situáciách týkajúcich sa bezpečnosti, pričom dané opatrenia sa vzťahujú najmä na bezpečné uchovávanie utajovaných dokumentov EÚ v kanceláriách;
- (b) sa prijali opatrenia na zabezpečenie prístupu ku komunikačnému systému komisie na príjem a odosielanie utajovaných správ EÚ. Hostiteľský členský štát sa požiada, aby prípadne poskytol prístup k bezpečnostným telefonickým systémom.

Bezpečnostný úrad komisie koná ako poradca pre bezpečnosť pri príprave zasadnutia; pri príprave by mal byť zastúpený, aby podľa potreby pomohol a poradil bezpečnostnému referentovi zasadnutia a delegáciám.

Každá jednotlivá delegácia na zasadnutí sa požiada, aby menovala bezpečnostného referenta, ktorý bude zodpovedný za vybavovanie bezpečnostných záležitostí v rámci jeho delegácie a za vykonávanie funkcie prostredníka s bezpečnostným referentom zasadnutia rovnako ako prípadne so zástupcom bezpečnostného úradu komisie.

#### 23.2.2. Bezpečnostný referent zasadnutia (MSO)

Bezpečnostný referent zasadnutia je menovaný a je zodpovedný za všeobecnú prípravu a kontrolu vnútorných bezpečnostných opatrení a za koordináciu s ostatnými príslušnými bezpečnostnými úradmi. Opatrenia, ktoré prijíma bezpečnostný referent zasadnutia sa vo všeobecnosti týkajú:

- (a) ochranných opatrení na mieste zasadnutia, ktoré zabezpečujú, že zasadnutie sa uskutoční bez incidentu, ktorý by mohol ohroziť bezpečnosť akýchkoľvek utajovaných informácií EÚ, ktoré sa na zasadnutí prípadne používajú;
- (b) ochrany personálu, ktorého prístup na miesto zasadnutia, do priestorov delegácií a do konferenčných miestností je povolený, a kontroly ľubovoľného zariadenia;
- (c) sústavnej koordinácie s príslušnými úradmi hostiteľského členského štátu a s bezpečnostným úradom komisie;
- (d) zaradenie bezpečnostných pokynov do spisov zasadnutia s príslušným upozornením na požiadavky uvedené v týchto bezpečnostných pravidlách a ľubovoľné iné bezpečnostné pokyny, ktoré sa považujú za potrebné.

← Naformátovano: Odrážky a číslování

### 23.3. Bezpečnostné opatrenia

#### 23.3.1. Bezpečnostné oblasti

Určujú sa nasledujúce bezpečnostné oblasti:

- (a) bezpečnostná oblasť triedy II, ktorá pozostáva z pracovnej miestnosti, kancelárií komisie a reprografického zariadenia rovnako ako prípade z kancelárií delegácií;
- (b) bezpečnostná oblasť triedy I, ktorá pozostáva z konferenčnej miestnosti a kabínok tlmočníkov a zvukových technikov;
- (c) administratívne priestory pozostávajúce z priestoru pre tlač a tých častí zasadacej miestnosti, ktoré sa používajú pre administratívu, stravovanie a ubytovanie rovnako ako priestor bezprostredne susediaci s tlačovým centrom a zasadacou miestnosťou.

### 23.3.2. *Priepustky*

Bezpečnostný referent zasadnutia vydá primerané označenia, ako ich vyžadujú delegácie podľa svojich potrieb. Ak sa tak požaduje, je možné rozlišovať prístupy do rozličných bezpečnostných oblastí.

Bezpečnostné pokyny pre zasadnutie musia vyžadovať, aby všetky príslušné osoby jasne a viditeľne nosili svoje identifikačné označenie po celý čas v rámci miesta zasadnutia tak, aby ich bolo možné v prípade potreby overiť bezpečnostným personálom.

Okrem účastníkov, ktorí majú identifikačné označenie, sa na miesto zasadnutia pripustí čo najmenej ľudí. Bezpečnostný referent zasadnutia povolí národným delegáciám iba na ich žiadosť, aby počas zasadnutia mohli prijať návštevníkov. Návštevy dostanú návštevnícke označenia. Musí sa vyplniť tlačivo pre návštevnícku priepustku, ktoré uvádza meno návštevníka a meno osoby, ktorá návštevu prijme. Návštevníci musia byť po celý čas sprevádzaní členom ochrany alebo navštívenou osobou. Tlačivo návštevníckej priepustky má pri sebe po celý čas sprevádzajúca osoba, ktorá ho vráti spolu s návštevníckym označením bezpečnostnému personálu, keď návšteva opúšťa miesto zasadnutia.

### 23.3.3. *Kontrola fotografického a audio zariadenia*

Do bezpečnostnej oblasti triedy I nie je možné priniesť žiadne fotoaparáty, kamery ani záznamové zariadenia s výnimkou zariadenia, ktoré so sebou doniesli fotografovia a zvukoví technici príslušne oprávnení bezpečnostným referentom zasadnutia.

### 23.3.4 *Kontrola aktoviek, prenosných počítačov a balíkov*

Držitelia priepustky, ktorí majú povolený prístup do bezpečnostnej oblasti, si môžu zvyčajne ponechať aktovky a prenosné počítače (len s vlastným zdrojom napätia) bez vykonania kontroly. V prípade balíkov pre delegácie, delegácia môže prevziať doručený balík, ktorý sa podrobí inšpekcii bezpečnostného referenta delegácie, preverí zvláštnym zariadením alebo ho otvorí bezpečnostný personál na inšpekciu. Ak to bezpečnostný referent zasadnutia považuje za potrebné, môžu sa stanoviť prísnejšie opatrenia na inšpekciu aktoviek a balíkov.

### 23.3.5 *Technická bezpečnosť*

Zasadacia miestnosť sa môže technicky zabezpečiť technickým bezpečnostným tímom, ktorý môže tiež vykonávať elektronický dohľad počas zasadnutia.

### 23.3.6. Dokumenty delegácií

Delegácie sú zodpovedné za prinesenie dokumentov na zasadnutie a odnesenie dokumentov zo zasadnutia. Sú tiež zodpovedné za overenie a bezpečnosť dokumentov počas ich používania v priestoroch, ktoré im boli pridelené. Hostiteľský členský štát môže byť požiadaný o pomoc pri preprave utajovaných dokumentov na miesto zasadnutia a z miesta zasadnutia.

### 23.3.7. *Bezpečná úschova dokumentov*

Ak komisia alebo delegácie nie sú schopné svoje utajované dokumenty uskladniť v súlade so schválenými normami, môžu takéto dokumenty uložiť v zapečatenej obálke u bezpečnostného referenta zasadnutia proti potvrdeniu o prijíme, a bezpečnostný referent zasadnutia bude príslušné dokumenty uschovávať v súlade so schválenými normami.

### 23.3.8. *Inšpekcia kancelárií*

Bezpečnostný referent zasadnutia zariadi, aby sa kancelárie komisie a delegácií podrobili inšpekcii na konci každého pracovného dňa, aby sa zabezpečilo, že všetky utajované dokumenty EÚ sa uchovávajú na bezpečnom mieste. Ak tomu tak nie je, bezpečnostný referent zasadnutia prijme príslušné opatrenia.

### 23.3.9 *Likvidácia odpadu utajovaných informácií EÚ*

Celý odpad sa považuje za utajovaný materiál EÚ a komisia a delegácie by mali dostať odpadové koše alebo vrecia na papier na jeho likvidáciu. Pred opustením priestorov, ktoré boli komisii a delegácii pridelené, komisia a delegácie odovzdajú celý svoj odpad bezpečnostnému referentovi zasadnutia, ktorý zabezpečí jeho likvidáciu v súlade s týmito pravidlami.

Na konci zasadnutia sa všetky držané dokumenty, ktoré už ani komisia ani delegácie nepotrebujú, považujú za odpad. Pred tým, ako sa zrušia bezpečnostné opatrenia prijaté pre zasadnutie, sa vykoná dôkladná prehliadka priestorov komisie a delegácií. Dokumenty, pre ktoré sa podpísalo potvrdenie o prijíme, sa podľa možnosti čo najviac zlikvidujú, ako je uvedené v oddieli 22.5.

## 24. PORUŠENIE BEZPEČNOSTI A OHROZENIE UTAJOVANÝCH INFORMÁCIÍ EÚ

### 24.1. Definície

K porušeniu bezpečnosti dochádza v dôsledku konania alebo opomenutia v rozpore s bezpečnostnými ustanoveniami komisie, ktoré by mohlo ohroziť alebo spôsobiť ohrozenie utajovaných informácií EÚ.

K ohrozeniu utajovaných informácií EÚ dochádza, keď sa celé alebo ich časť dostanú do rúk neoprávnených osôb, t.j. osôb, ktoré nemajú príslušné bezpečnostné preverenie ani nespĺňajú zásadu potreby oboznámenia sa, alebo ak existuje pravdepodobnosť, že k takejto udalosti došlo.

Utajované informácie EÚ môžu byť ohrozené dôsledkom nedbanlivosti, ľahostajnosti alebo neuváženosti rovnako ako činnosťami služieb, ktorých cieľom je EÚ alebo jej členské štáty, pokiaľ ide o utajované informácie EÚ a jej činnosti, alebo podvratnými organizáciami.

#### 24.2. Hlásenie porušenia bezpečnosti

Všetky osoby, ktoré musia narábať s utajovanými informáciami EÚ, sú dôsledne poučené o svojich zodpovednostiach v tejto oblasti. Okamžite musia hlásiť ľubovoľné porušenie bezpečnosti, o ktorom sa dozvedeli.

Ak miestny bezpečnostný referent alebo bezpečnostný referent zasadnutia objaví alebo je informovaný o porušení bezpečnosti týkajúcej sa utajovaných informácií EÚ, alebo o strate alebo zmiznutí utajovaných materiálov EÚ, okamžite podnikne kroky na:

- (a) ochranu dôkazov;
- (b) konštatovanie faktov;
- (c) posúdenie a minimalizovanie vzniknutej škody;
- (d) zabránenie opakovaniu;
- (e) oznámenie príslušným úradom o účinkoch porušenia bezpečnosti.

← Naformátovano: Odrážky a číslovaní

← Naformátovano: Odrážky a číslovaní

V tomto kontexte sa musia zabezpečiť nasledujúce informácie:

- (i) opis danej informácie, vrátane stupňa jej utajovania, referenčného čísla a čísla kópie, dátumu, pôvodcu, predmetu a rozsahu;
- (ii) krátky opis okolností, za ktorých došlo k porušeniu bezpečnosti, vrátane dátumu a obdobia, počas ktorého bola informácia vystavená odcudzeniu;
- (iii) vyhlásenie, či pôvodca bol o tejto skutočnosti informovaný.

Je povinnosťou každého bezpečnostného úradu, aby okamžite po informovaní o tom, že mohlo dôjsť k porušeniu bezpečnosti, túto skutočnosť okamžite nahlásil bezpečnostnému úradu komisie.

Prípady, ktoré zahŕňajú informácie EÚ VYHRADENÉ, sa musia hlásiť iba vtedy, ak predstavujú nezvyčajné okolnosti.

Člen komisie zodpovedný za bezpečnostné záležitosti musí po informovaní, že došlo k porušeniu bezpečnosti:

- (a) upovedomiť úrad, ktorý je pôvodcom príslušnej utajovanej informácie;
- (b) požiadať príslušné bezpečnostné úrady, aby začali vyšetrovanie;

← Naformátovano: Odrážky a číslovaní

- (c) koordinovať skúmanie, či sa prípad týka viacerých ako jedného bezpečnostného úradu;
- (d) získať správu o okolnostiach porušenia, dátume a období, počas ktorého k porušeniu mohlo dôjsť a kedy bolo zistené, s podrobným opisom obsahu a utajenia príslušného materiálu. Tiež sa musí ohlásiť škoda, ktorá vznikla záujmom EÚ alebo jednému alebo viacerým jej členským štátom a opatrenia, ktoré sa prijali na zabránenie opakovania.

Úrad, ktorý je pôvodcom danej informácie, informuje o udalosti adresátov a dá im vhodné pokyny.

### 24.3. Právne opatrenia

Každý jedinec, ktorý je zodpovedný za ohrozenie utajovaných informácií EÚ, podlieha disciplinárnym opatreniam podľa príslušných pravidiel a nariadení, najmä hlavy VI personálneho poriadku. Takéto opatrenie je bez dopadu na akékoľvek iné právne opatrenie.

V primeraných prípadoch na základe správy uvedenej v oddieli 24.2 člen komisie zodpovedný za bezpečnostné záležitosti prijme všetky potrebné kroky, aby príslušným národným úradom umožnil začať trestno-právne konanie.

## 25. OCHRANA UTAJOVANÝCH INFORMÁCIÍ EÚ, S KTORÝMI SA NARÁBA V INFORMAČNEJ TECHNOLOGII A KOMUNIKAČNÝCH SYSTÉMOCH

### 25.1. Úvod

#### 25.1.1. *Všeobecne*

Bezpečnostná politika a požiadavky sa vzťahujú na všetky komunikačné a informačné systémy a siete (ďalej ako systémy), ktoré narábajú s utajovanými informáciami EÚ DÔVERNÉ a vyššieho stupňa utajenia. Uplatňujú sa ako dodatok k rozhodnutiu komisie C(95) 1510 konečné z 23. novembra 1995 o ochrane informačných systémoch.

Systémy, ktoré narábajú s utajovanými informáciami EÚ VYHRADENÉ tiež vyžadujú bezpečnostné opatrenia na ochranu dôvernosti týchto informácií. Všetky systémy vyžadujú bezpečnostné opatrenia na ochranu celistvosti a dostupnosti týchto systémov a informácií, ktoré obsahujú.

Bezpečnostná politika pre informačné technológie, ktorú uplatňuje komisia, má nasledujúce prvky:

- tvorí jednotnú časť bezpečnosti vo všeobecnosti a dopĺňa všetky prvky informačnej bezpečnosti, personálnej bezpečnosti a fyzickej bezpečnosti;

- rozdelenie zodpovedností medzi majiteľmi technických systémov, majiteľmi utajovaných informácií EÚ, ktoré sú uložené alebo s ktorými sa narába v technických systémoch, bezpečnostnými špecialistami na informačné technológie a užívateľmi;
- opis bezpečnostných zásad a požiadaviek pre každý systém informačnej technológie;
- schválenie týchto zásad a požiadaviek určeným úradom;
- zohľadnenie osobitných hrozieb a zraniteľnosti v oblasti informačnej technológie.

#### 25.1.2. *Hrozby a zraniteľnosť systémov*

Hrozbu možno definovať ako potenciál náhodného alebo úmyselného ohrozenia bezpečnosti. V prípade systémov takéto ohrozenie zahŕňa stratu jednej alebo viacerých z vlastností dôvernosti, celistvosti a dostupnosti. Zraniteľnosť možno definovať ako slabinu alebo nedostatok kontroly, ktorý by umožnil alebo povolil vyvolanie hrozby voči určitému majetku alebo cieľu.

Utajované a neutajované informácie EÚ, s ktorými sa narába v systémoch v koncentrovanej forme navrhnutej na rýchle vyhľadanie, komunikáciu a použitie, sú zraniteľné mnohými hrozbami. Tieto hrozby zahŕňajú prístup k informáciám neoprávnenými užívateľmi, alebo naopak odoprenie prístupu oprávneným osobám. Zahŕňajú tiež riziká neoprávneného zverejnenia, zneužitia, úpravy alebo vymazania informácií. Okrem toho, zložitá a niekedy krehké zariadenia sú drahé a často náročné na rýchlu opravu alebo nahradenie.

#### 25.1.3. *Hlavný cieľ bezpečnostných opatrení*

Hlavným cieľom bezpečnostných opatrení uvedených v tomto oddieli je poskytnúť ochranu proti neoprávnenému zverejneniu utajovaných informácií EÚ (strata dôvernosti) a proti strate celistvosti a dostupnosti takýchto informácií. Aby sa dosiahla primeraná bezpečnostná ochrana systému, ktorý narába s utajovanými informáciami EÚ, bezpečnostný úrad komisie určí primerané normy všeobecnej bezpečnosti spolu s primeranými zvláštnymi bezpečnostnými postupmi a technikami navrhnutými konkrétne pre každý systém.

#### 25.1.4. *Vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke (SSRS)*

Pre všetky systémy, ktoré narábajú s utajovanými informáciami EÚ DÔVERNÉ a vyššieho stupňa utajovania, musí jeho majiteľ technického systému (pozri oddiel 25.3.4) a informačný majiteľ (pozri oddiel 25.3.5) predložiť vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke, v spolupráci so vstupom a pomocou podľa žiadosti projektového personálu a bezpečnostného úradu komisie (ako úrad INFOSEC – IA, pozri oddiel 25.3.3.) a ako ho schválil Bezpečnostný akreditačný úrad (pozri oddiel 25.3.2).

Vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke sa tiež požaduje, keď Bezpečnostný akreditačný úrad považuje dostupnosť a celistvosť informácií EÚ VYHRADENÉ alebo neutajovaných informácií za kritickú.

Vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke sa formuluje v čo najskoršej fáze vzniku projektu a vyvíja sa a zlepšuje sa súčasne, ako sa vyvíja projekt, pričom v rozličných fázach projektového cyklu a životného cyklu systému plní rozličné úlohy.

#### 25.1.5 Bezpečnostné režimy prevádzky

Všetky systémy, ktoré narábajú s utajovanými informáciami EÚ DÔVERNÉ a vyššieho stupňa utajovania, musia mať akreditáciu na operovanie v jednom alebo, ak je oprávnené požiadavkami počas rozličných časových období, viacerých z nasledujúcich bezpečnostných režimov prevádzky alebo ich národných ekvivalentov:

- (a) Jednoúčelový.
- (b) Systém vysoký a
- (c) Viacúrovňový.

← Naformátovano: Odrážky a číslování

#### 25.2. Definície

„Akreditácia“ znamená: oprávnenie a schválenie udelené systému na spracovanie utajovaných informácií EÚ v ich operačnom prostredí.

#### Poznámka:

Takáto akreditácia by sa mala priznať, keď sa zaviedli všetky primerané bezpečnostné postupy a dosiahla sa dostatočná úroveň ochrany systémových zdrojov. Akreditácia sa zvyčajne udeľuje na základe vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke:

- (a) vyhlásenie cieľa akreditácie pre systém; najmä, s akou úrovňou (úrovňami) utajovania informácií sa môže narábať a aký systém alebo sieťový bezpečnostný režim (režimy) sa navrhujú;
- (b) vypracovanie prehľadu riadenia rizík, aby sa identifikovali hrozby a zraniteľnosti a opatrenia na ich zamedzenie;
- (c) bezpečnostné prevádzkové postupy s podrobným opisom navrhovanej prevádzky (napríklad režimy, služby, ktoré sa majú poskytovať) a vrátane opisu systémových bezpečnostných funkcií, ktoré tvoria základ akreditácie;
- (d) plán na zavedenie a údržbu bezpečnostných funkcií;
- (e) plán pre počiatočný a následný systémový bezpečnostný alebo sieťový bezpečnostný test, vyhodnotenie a certifikáciu, a
- (f) certifikácia, ak sa požaduje, spolu s ostatnými prvkami akreditácie.

„Centrálny informačný bezpečnostný referent“ znamená úradník v centrálnej službe informačných technológií, ktorý koordinuje a dohliada na bezpečnostné opatrenia pre centrálné organizované systémy.

„Certifikácia“ znamená: vydanie formálneho vyhlásenia, ktoré vychádza z nezávislého preskúmania správania a výsledkov vyhodnotenia, rozsahu, do ktorého systém spĺňa bezpečnostné požiadavky alebo do ktorého počítačový bezpečnostný produkt spĺňa vopred definované bezpečnostné nároky.

„Komunikačná bezpečnosť“ znamená: uplatňovanie bezpečnostných opatrení na telekomunikácie, aby sa neoprávneným osobám odopreli informácie hodnoty, ktorá by sa mohla získať vlastnením a analýzou takýchto telekomunikácií, alebo sa zabezpečila autenticita takýchto telekomunikácií.

„Počítačový bezpečnostný produkt“ znamená: generická počítačová bezpečnostná položka, ktorá je určená na začlenenie do systému informačnej technológie na používanie pri zlepšovaní alebo zabezpečovaní dôvernosti, celistvosti alebo dostupnosti informácií, s ktorými sa narába.

„Jednouúčelový bezpečnostný režim prevádzky“ znamená: režim prevádzky, v ktorom sú VŠETCI jednotlivci s prístupom do systému preverení pre najvyššiu úroveň utajovania informácií v rámci systému a so všeobecnou potrebou oboznámenia sa pre všetky informácie, s ktorými sa narába v rámci systému.

**Poznámky:**

- (1) Všeobecná potreba oboznámenia sa naznačuje, že neexistuje žiadna povinná požiadavka, aby počítačové bezpečnostné funkcie zabezpečovali oddeľovanie informácií v rámci systému.
- (2) Ostatné bezpečnostné funkcie (napríklad fyzické, personálne a procesné) musia zodpovedať požiadavkám na najvyššiu úroveň utajovania a pre všetky označenia kategórií informácií, s ktorými sa narába v rámci systému.

„Vyhodnotenie“ znamená: podrobné technické preskúmanie príslušným úradom bezpečnostných aspektov systému alebo kódovacieho alebo počítačového bezpečnostného produktu.

**Poznámky:**

- (1) Vyhodnotenie skúma prítomnosť požadovanej bezpečnostnej funkčnosti a neprítomnosť ohrozujúcich vedľajších účinkov takejto funkčnosti a posudzuje nezneužitelnosť takejto funkčnosti.
- (2) Vyhodnotenie určuje rozsah, do ktorého sú splnené bezpečnostné požiadavky systému alebo bezpečnostné nároky na počítačový bezpečnostný produkt, a stanovuje úroveň zabezpečenia

spoľahlivej funkcie systému alebo kódovacieho alebo počítačového bezpečnostného produktu.

„Majiteľ informácií“ znamená úrad (vedúci oddelenia), ktorý je zodpovedný za vytvorenie, spracovanie a použitie informácií, vrátane rozhodovania, komu bude umožnený prístup k týmto informáciám.

„Informačná bezpečnosť“ (INFOSEC) znamená: uplatnenie bezpečnostných opatrení na ochranu informácií, ktoré sa spracovávajú, ukladajú alebo prenášajú v komunikačných, informačných a ostatných elektronických systémoch, proti strate dôvernosti, celistvosti alebo dostupnosti, náhodnej alebo zámernej, a na zabránenie proti strate celistvosti a dostupnosti systémov samotných.

„Opatrenia INFOSEC“ zahŕňajú opatrenia počítačovej, prenosovej, vysielacej a kódovacej bezpečnosti, detekciu a dokumentáciu hrozieb a čelenie hrozbám pre informácie a systémy.

„Oblasť informačnej technológie“ znamená: oblasť, ktorá obsahuje jeden alebo viacej počítačov, ich miestne periférne a pamäťové jednotky, kontrolné jednotky a jednoúčelové sieťové a komunikačné zariadenia.

Poznámka:

Toto nezahŕňa oddelenú oblasť, kde sú umiestnené vzdialené periférne zariadenia alebo terminály/pracovné stanice, aj keď tieto zariadenia sú napojené na zariadenia v oblasti informačných technológií.

„Sieť informačných technológií“ znamená: organizácia, geograficky rozptýlená, systémov informačných technológií prepojených na výmenu údajov, a pozostávajúca z komponentov prepojených systémov informačnej technológie a ich rozhraní s podpornými dátovými alebo komunikačnými sieťami.

Poznámky:

(1) Sieť informačnej technológie môže používať služby jednej alebo viacerých komunikačných sietí prepojených na výmenu dát; viacero sietí informačných technológií môže používať služby spoločnej komunikačnej siete.

(2) Sieť informačnej technológie sa nazýva miestna, ak spája spolu viacero počítačov na tom istom mieste.

„Sieťové bezpečnostné funkcie informačnej technológie“ zahŕňajú systémové bezpečnostné funkcie informačnej technológie jednotlivých systémov informačnej technológie tvoriacich sieť spolu s dodatočnými komponentmi a funkciami súvisiacimi so sieťou ako takou (napríklad sieťová komunikácia, bezpečnostná identifikácia a označovacie mechanizmy a postupy, prístupové kontroly, programy a dôsledky auditov) potrebné na zabezpečenie prijateľnej úrovne ochrany utajovaných informácií.

„Systém informačnej technológie“ znamená: súbor zariadení, metód a postupov a prípade personál tak organizovaný, aby mohol vykonávať funkcie spracovávania informácií.

Poznámky:

- (1) Treba to chápať ako súbor zariadení, ktoré sú konfigurované tak, aby mohli v rámci systému narábať s informáciami.
- (2) Takéto systémy môžu predstavovať podporu pre konzultačné, príkazové, kontrolné, komunikačné, vedecké alebo administratívne uplatnenia vrátane prác s textom.
- (3) Hranice systému sa vo všeobecnosti určujú ako prvky, ktoré sú pod kontrolou jediného majiteľa technických systémov.
- (4) Systém informačnej technológie môže obsahovať podsystémy, z ktorých niektoré samotné sú systémami informačnej technológie.

„Bezpečnostné funkcie systému informačných technológií“ sa skladajú zo všetkých hardwarových/firmwarových/softwareových funkcií, charakteristík a vlastností; operačných postupov, postupov zodpovednosti a kontroly prístupu, oblasti informačných technológií, oblasti vzdialeného terminálu/pracovnej stanice a stálych riadiacich obmedzení, fyzickej štruktúry a zariadení, personálnej a komunikačnej kontroly potrebnej na zabezpečenie prijateľnej úrovne ochrany utajovaných informácií, s ktorými sa má narábať v systéme informačnej technológie.

„Miestny referent informačnej bezpečnosti“ znamená: úradník v oddelení komisie, ktorý je zodpovedný za koordináciu a dohľad nad bezpečnostnými opatreniami v rámci jeho oblasti.

„Viacúrovňový bezpečnostný režim prevádzky“ znamená: režim prevádzky, v ktorom NIE VŠETCI jednotlivci s prístupom do systému sú preverení na najvyššiu úroveň utajovania informácií, s ktorými sa narába v rámci systému, a NIE VŠETCI jednotlivci s prístupom do systému majú všeobecnú potrebu oboznámenia sa pre informácie, s ktorými sa narába v rámci systému.

Poznámky:

- (1) Tento režim prevádzky povoľuje súčasne narábať s informáciami rozličného utajovania a s informáciami rozličného označenia kategórií.
- (2) Skutočnosť, že nie všetci jednotlivci sú preverení na najvyššie úrovne, v spojení s nedostatkom všeobecnej potreby oboznámenia sa naznačuje, že existuje požiadavka, aby

počítačové bezpečnostné funkcie zabezpečovali selektívny prístup k informáciám v rámci systému a oddeľovanie informácií v rámci systému.

„Oblasť vzdialeného terminálu/pracovnej stanice“ znamená: oblasť obsahujúca niektoré počítačové zariadenia, ich miestne periférne zariadenia alebo terminály/pracovné stanice a ľubovoľné pridružené komunikačné zariadenie, oddelená od oblasti informačnej technológie.

„Bezpečnostné prevádzkové postupy“ znamená: postupy, ktoré vypracoval majiteľ technických systémov a ktoré definujú zásady, ktoré sa majú prijať pre bezpečnostné záležitosti, prevádzkové postupy, ktoré treba dodržiavať, a personálne zodpovednosti.

„Bezpečnostný prevádzkový režim SYSTÉM VYSOKÝ“ znamená: režim prevádzky, v ktorom VŠETCI jednotlivci s prístupom do systému sú preverení pre najvyššiu úroveň utajovania informácií, s ktorými sa narába v rámci systému, ale NIE VŠETCI jednotlivci s prístupom do systému majú všeobecnú potrebu oboznámenia sa pre informácie, s ktorými sa narába v rámci systému.

Poznámky:

(1) Nedostatok všeobecnej potreby oboznámenia sa naznačuje, že existuje požiadavka, aby počítačové bezpečnostné funkcie zabezpečovali selektívny prístup k informáciám v rámci systému a oddeľovanie týchto informácií.

(2) Ostatné bezpečnostné funkcie (napríklad fyzické, personálne a procesné) musia zodpovedať požiadavkám na najvyššiu úroveň utajovania a všetky označenia kategórií informácií, s ktorými sa narába v systéme.

(3) Všetky informácie, s ktorými sa narába v systéme alebo sú systému dostupné podľa tohto režimu prevádzky, spolu s generovaným výstupom musia byť chránené ako potenciálne informácie kategorizácie a najvyššieho utajenia, s ktorými sa narába, až kým sa nerozhodne inak, pokiaľ neexistuje prijateľná úroveň dôvery, ktorú možno zaviesť do ľubovoľnej prítomnej funkcie označovania.

„Vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke“ je úplné a výslovné vyhlásenie o bezpečnostných zásadách, ktoré treba dodržiavať a o podrobných bezpečnostných požiadavkách, ktoré treba splniť. Vychádza z bezpečnostnej politiky komisie a rizikového posúdenia, alebo je dané parametrami, ktoré sa vzťahujú na prevádzkové prostredie, najnižšou úrovňou personálneho bezpečnostného preverenia, najvyššou úrovňou utajenia informácií, s ktorými sa narába, bezpečnostným režimom prevádzky alebo užívateľskými požiadavkami. Vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke je jednotnou časťou projektovej dokumentácie, ktorá sa predkladá príslušným úradom z technických, rozpočtových a bezpečnostných schvaľovacích dôvodov. Vo svojej konečnej forme vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke predstavuje úplné vyhlásenie o tom, čo to znamená, že systém je bezpečný.

„Majiteľ technických systémov“ znamená úrad, ktorý je zodpovedný za tvorbu, údržbu, prevádzku a uzatvorenie systému.

„Búrkové“ protiopatrenia: bezpečnostné opatrenia určené na ochranu zariadenia a komunikačnej infraštruktúry proti ohrozeniu utajovaných informácií v dôsledku neúmyselného elektromagnetického žiarenia a v dôsledku vodivosti.

### 25.3. Bezpečnostné zodpovednosti

#### 25.3.1. *Všeobecne*

Poradné zodpovednosti poradnej skupiny komisie pre bezpečnostnú politiku, definovanej v oddieli 12, zahŕňajú záležitosti INFOSEC. Táto skupina organizuje svoje činnosti tak, aby mohla poskytovať odborné rady o vyššie uvedených záležitostiach.

Bezpečnostný úrad komisie je zodpovedný za vydávanie podrobných ustanovení INFOSEC podľa ustanovení v tejto kapitole.

V prípade problémov ohľadne bezpečnosti (nehody, porušenia atď.) bezpečnostný úrad komisie okamžite prijme opatrenia.

Bezpečnostný úrad komisie má jednotku INFOSEC.

#### 25.3.2. *Bezpečnostný akreditačný úrad (SAA)*

Vedúci bezpečnostného úradu predstavuje Bezpečnostný akreditačný úrad pre komisiu. Bezpečnostný akreditačný úrad má zodpovednosti vo všeobecnej oblasti bezpečnosti a v špecializovaných oblastiach INFOSEC, komunikačnej bezpečnosti, bezpečnosti kódovania a bezpečnosti rušivých vplyvov.

Bezpečnostný akreditačný úrad je zodpovedný za zabezpečenie súladu systémov s bezpečnostnou politikou komisie. Jedna z jeho úloh je udeľovať schválenia systému na prácu s utajovanými informáciami EÚ po stanovení úroveň utajovania v jeho operačnom prostredí.

Právomoc bezpečnostného akreditačného úradu komisie sa vzťahuje na všetky systémy v prevádzke v rámci priestorov komisie. Ak sa pod právomoc bezpečnostného akreditačného úradu komisie a ostatných akreditačných úradov dostanú rozličné súčasti systému, všetky zúčastnené strany môžu vymenovať spoločnú akreditačnú radu pod koordinovaním bezpečnostného akreditačného úradu komisie.

#### 25.3.3. *Úrad INFOSEC (IA)*

Vedúci jednotku INFOSEC bezpečnostného úradu komisie predstavuje úrad INFOSEC pre komisiu. Úrad INFOSEC je zodpovedný za:

- poskytovanie technickej rady a pomoci bezpečnostnému akreditačnému úradu,
- pomáhanie pri vypracovávaní vyhlásenia o osobitnej systémovej bezpečnostnej požiadavke
- skúmanie vyhlásenia o osobitnej systémovej bezpečnostnej požiadavke, aby sa zabezpečila zhoda s týmito bezpečnostnými pravidlami a zásadami INFOSEC a staviteľskými dokumentmi;
- zúčastňovanie sa v akreditačných porotách/radách, ako je nutné a za poskytovanie odporúčaní INFOSEC o akreditácii bezpečnostnému akreditačnému úradu;
- poskytovanie podpory školeniam INFOSEC a vzdelávacím akciám;
- poskytovanie technickej rady pri skúmaní prípadov súvisiacich s INFOSEC;
- zavedenie usmernení o technickej politike, aby sa zabezpečilo, že sa používa iba jeden autorizovaný software.

#### 25.3.4. *Majiteľ technických systémov (TSO)*

Zodpovednosť za zavedenie a vykonávanie kontroly a zvláštnych bezpečnostných funkcií systému spočíva na majiteľovi tohto systému, majiteľovi technických systémov. V prípade centrálne vlastnených systémov sa menuje referent pre centrálnu informačnú bezpečnosť. Každé oddelenie menuje podľa potreby miestneho referenta pre informačnú bezpečnosť. Zodpovednosť majiteľa technických systémov zahŕňa tvorbu bezpečnostných prevádzkových postupov a vzťahuje sa na celý životný cyklus systému od projekčného konceptu až po konečnú likvidáciu.

Majiteľ technických systémov určuje bezpečnostné normy a zvyklosti, ktoré musí dodávateľ systému splniť.

Majiteľ technických systémov môže prípadne delegovať časť svojich zodpovedností na miestneho referenta pre informačnú bezpečnosť. Jedna osoba môže vykonávať rozličné funkcie INFOSEC.

#### 25.3.5. *Majiteľ informácií (IO)*

Majiteľ informácií je zodpovedný za utajované informácie EÚ (a ostatné informácie), ktoré sa musia zaviesť, spracovať a vyrobiť v technických systémoch. Definuje požiadavky na prístup k týmto informáciám v systémoch. Túto zodpovednosť môže delegovať na informačného správcu alebo databázového správcu v rámci svojej oblasti.

#### 25.3.6. *Užívatelia*

Všetci užívatelia sú zodpovední za zabezpečenie toho, aby ich činnosti neovplyvňovali nepriaznivo bezpečnosť systému, ktorý užívajú.

#### 25.3.7. Školenie INFOSEC

Školenie a vzdelávanie v oblasti INFOSEC musí byť dostupné pre všetkých členov personálu, ktorí ho potrebujú.

### 25.4. Netechnické bezpečnostné opatrenia

#### 25.4.1. *Personálna bezpečnosť*

Užívatelia systému musia byť preverení a musia mať potrebu oboznámenia sa, ako to vyžaduje utajenie a obsah informácií, s ktorými sa narába v rámci určitého systému. Prístup k určitému zariadeniu alebo informáciám osobitným pre bezpečnosť systémov vyžaduje zvláštne preverenie, ktoré sa prideluje podľa postupov komisie.

Bezpečnostný akreditačný úrad menuje všetky citlivé pozície a špecifikuje úroveň preverenia a dohľadu, ktorá sa vyžaduje od všetkých členov personálu, ktorí sú na týchto pozíciách.

Systémy sa špecifikujú a navrhujú tak, aby sa umožnilo pridelovanie povinností a zodpovedností členom personálu, a tak sa zabránilo tomu, aby jedna osoba mala úplnú vedomosť alebo kontrolu nad kľúčovými bodmi systémovej bezpečnosti.

Oblasti informačnej technológie a vzdialených terminálov/pracovných staníc, kde je možné modifikovať bezpečnosť systému, nesmie zastávať iba jeden oprávnený úradník alebo iný zamestnanec.

Na zmenu bezpečnostného nastavenia systému sú potrební aspoň dvaja oprávnení členovia personálu, ktorí pracujú spoločne.

#### 25.4.2. *Fyzická bezpečnosť*

Oblasti informačnej technológie a vzdialených terminálov/pracovných staníc (ako sú definované v oddieli 25.2), v ktorých sa narába s utajovanými informáciami EÚ DÔVERNÉ a vyššej úrovne utajovania s prostriedkami informačných technológií, alebo kde je možný potenciálny prístup k takýmto informáciám, sa musia stanoviť ako bezpečnostné oblasti utajovaných informácií EÚ triedy I prípadne triedy II.

#### 25.4.3. *Kontrola prístupu k systému*

Všetky informácie a materiál, ktorá umožňuje kontrolovať prístup k systému, musia byť chránené opatreniami rovnocennými opatreniam najvyššieho utajovania a určením kategórie informácií, ku ktorým môžu mať prístup.

Ak sa už prístupové kontrolné informácie a materiál viac nepoužívajú, zničia sa podľa ustanovení uvedených v oddieli 25.5.4.

## 25.5. Technické bezpečnostné opatrenia

### 25.5.1. *Bezpečnosť informácií*

Je povinnosťou pôvodcu informácií, aby identifikoval a klasifikoval všetky dokumenty, ktoré obsahujú informácie, bez ohľadu na to, či sú výstupy v tlačenej forme alebo uložené na počítačových médiách. Každá strana tlačenej formy musí byť označená úrovňou utajenia na hornej a dolnej časti. Výstup v tlačenej forme alebo uložený na počítačovom médiu musí mať také isté utajenie ako informácia, ktorá sa použila na jeho tvorbu. Spôsob operácie systému tiež môže mať dopad na utajenie výstupov z tohto systému.

Je povinnosťou oddelení komisie a ich držiteľov informácií, aby zohľadnili problémy hromadenia jednotlivých prvkov informácií a interferencií, ktoré možno získať z príbuzných prvkov, a stanovili, či nie je pre výsledný súhrn informácií primeraná vyššia úroveň utajenia.

Skutočnosť, že informácia môže byť v skrátenom kóde, prenosovom kóde alebo ľubovoľnej inej forme binárneho vyjadrenia, nepredstavuje žiadnu bezpečnostnú ochranu, a preto by nemala mať vplyv na utajovanie informácií.

Ak sa informácie prenášajú z jedného systému do iného, informácia musí byť chránená počas prenosu a v prijímajúcom systéme spôsobom, ktorý je rovnocenný pôvodnému utajeniu a kategórii informácií.

So všetkými pamäťovými počítačovými médiami sa musí narábať spôsobom, ktorý je rovnocenný najvyššiemu utajeniu uložených informácií alebo označeniu média, a musia byť sústavne primerane chránené.

Opakovane použiteľné počítačové pamäťové médiá používané na záznam utajovaných informácií EÚ si musia zachovať najvyššie utajenie, pre ktoré boli použité, až kým príslušná informácia nemá znížený stupeň utajenia alebo nie je odtajnená, a príslušne médiá preklasifikované alebo odtajnené alebo zničené v súlade s postupom schváleným bezpečnostným akreditačným úradom (pozri 25.5.4).

### 25.5.2. *Kontrola a zodpovednosť za informácie*

Ako záznamy o prístupe k informáciám utajených na úrovni EÚ TAJNÉ a vyššie sa vedú automatizované (auditorské reťazce) alebo ručné záznamové knihy. Tieto záznamy sa uchovávajú v súlade s týmito bezpečnostnými pravidlami.

S výstupmi utajovaných informácií EÚ, ktoré sa uchovávajú v oblasti informačných technológií, sa môže narábať ako s utajenou položkou a nemusia sa registrovať, ak je materiál identifikovaný, označený úrovňou utajenia a príslušne riadený.

Ak systém narábajúci s utajovanými informáciami EÚ generuje výstup, ktorý sa z oblasti informačnej technológie prenáša do oblasti vzdialeného terminálu/pracovnej stanice, musia sa stanoviť postupy odsúhlasené bezpečnostným akreditačným úradom, na riadenie a zapisovanie výstupu do záznamovej knihy. V prípade informácií EÚ TAJNÉ a vyššieho stupňa utajenia takéto postupy zahŕňajú osobitné pokyny ohľadne zodpovednosti za informácie.

#### *25.5.3. Manipulácia a kontrola odstrániteľných počítačových pamäťových médií*

Všetky odstrániteľné počítačové pamäťové médiá klasifikované ako informácie EÚ DÔVERNÉ a vyššieho stupňa utajovania sa musia považovať za materiál, pre ktorý sa uplatňujú všeobecné pravidlá. Konkrétne fyzické vzhlady médií sa upravujú príslušnou identifikáciou a úrovňou utajenia tak, aby sa umožnilo ich jednoduché rozlíšenie.

Užívatelia preberajú zodpovednosť za zabezpečenie, že všetky utajované informácie EÚ sa ukladajú na médiách s príslušným označením a ochranou utajenia. Stanovujú sa postupy, aby sa zabezpečilo, že pre všetky úrovne utajovaných informácií EÚ sa ukladanie informácií na počítačových pamäťových médiách vykonáva v súlade s týmito bezpečnostnými pravidlami.

#### *25.5.4 Odtajnenie a likvidácia počítačových pamäťových médií*

Počítačové pamäťové médiá používané na záznam utajovaných informácií EÚ sa môžu znížiť v stupni utajenia alebo odtajniť v súlade s postupom, ktorý schválil Bezpečnostný akreditačný úrad.

Počítačové pamäťové médiá, na ktorých boli uložené informácie EÚ PRÍSNE TAJNÉ alebo inej zvláštnej kategórie, sa nesmú odtajniť ani opakovane používať.

Ak počítačové pamäťové médiá nie je možné odtajniť alebo nie sú na opakované použitie, musia sa zlikvidovať v súlade s vyššie uvedeným postupom.

#### *25.5.5. Počítačová bezpečnosť*

Vedúci bezpečnostného úradu komisie predstavuje šifrovací úrad.

Ak sa utajované informácie EÚ prenášajú elektromagneticky, musia sa zaviesť zvláštne opatrenia na ochranu dôvernosti, celistvosti a dostupnosti takýchto prenosov. Bezpečnostný akreditačný úrad určí požiadavky na ochranu prenosov pred odhalením a zachytením. Informácie, ktoré sa prenášajú v komunikačnom systéme, sa musia chrániť podľa požiadaviek na dôvernosť, celistvosť a dostupnosť.

Ak sa vyžadujú šifrovacie metódy na zabezpečenie dôvernosti, celistvosti a dostupnosti, takéto metódy a súvisiace produkty musia byť osobitny schválené pre daný účel bezpečnostným akreditačným úradom ako šifrovacím úradom.

Počas prenosu sa dôvernosť utajovaných informácií EÚ TAJNÉ a vyššej úrovne utajenia chráni šifrovacími metódami alebo produktmi schválenými členom komisie zodpovedným za bezpečnostné záležitosti po konzultáciách s poradnou skupinou komisie pre bezpečnostnú politiku. Počas prenosu sa dôvernosť informácií EÚ DÔVERNÉ alebo EÚ VYHRADENÉ chráni šifrovacími metódami alebo produktmi schválenými šifrovacím úradom komisie po konzultáciách s poradnou skupinou komisie pre bezpečnostnú politiku.

Podrobné pravidlá uplatňované na prenos utajovaných informácií EÚ sa uvádzajú vo zvláštnych bezpečnostných pokynoch, ktoré schválil bezpečnostný úrad komisie po konzultáciách s poradnou skupinou komisie pre bezpečnostnú politiku.

Za výnimočných okolností je možné informácie EÚ VYHRADENÉ, EÚ DÔVERNÉ a EÚ TAJNÉ prenášať v jasnom texte, ak je každý takýto konkrétny prenos výslovne schválený a primerane registrovaný majiteľom informácií. Takýmito výnimočnými okolnosťami sú:

- (a) počas hroziacej alebo aktuálnej krízy, konfliktu alebo vojnovnej situácie a
- (b) ak rýchlosť doručenia je mimoriadneho významu a šifrovacie prostriedky nie sú k dispozícii a posúdi sa, že prenos informácií nemôže byť zneužitý tak rýchlo, aby nepriaznivo ovplyvnil operácie.

Systém musí mať schopnosť pozitívneho odmietnutia prístupu k utajovaným informáciám EÚ na ktorejkoľvek na všetkých pracovných staniciach alebo vzdialených termináloch, ak sa požaduje fyzickým odpojením alebo zvláštnym softwarovými funkciami schválenými bezpečnostným akreditačným úradom.

#### 25.5.6 *Inštalácia a radiačná bezpečnosť*

Počítačová inštalácia systémov a ľubovoľné väčšie zmeny inštalácie musia byť tak špecifikované, že inštaláciu vykonávajú inštalatéri s bezpečnostnými previerkami za sústavného dozoru technicky kvalifikovaného personálu, ktorý je preverený pre prístup k utajovaným informáciám EÚ až po úroveň rovnú najvyššiemu utajeniu, s ktorým má systém narábať a uchovávať.

Systémy narábajúce s informáciami EÚ DÔVERNÉ a vyššieho stupňa utajovania musia byť chránené tak, aby ich bezpečnosť nebolo možné ohroziť nebezpečným žiarením a/alebo vodivosťou, o čom štúdia a kontrola sa označuje ako „búrková“.

Búrkové protiopatrenia skúma a schvaľuje úrad pre rušivé vplyvy (pozri 25.3.2).

#### 25.6. Bezpečnosť počas manipulácie

##### 25.6.1. *Bezpečnostné prevádzkové postupy*

Bezpečnostné prevádzkové postupy definujú zásady, ktoré sa prijímajú pre bezpečnostné záležitosti, prevádzkové postupy, ktoré sa musia dodržiavať, a personálne zodpovednosti.

Bezpečnostné prevádzkové postupy sa pripravujú za zodpovednosti majiteľa technických systémov.

#### 25.6.2. Riadenie softwarovej ochrany/konfigurácie

Bezpečnostná ochrana aplikačných programov sa určuje na základe posúdenia bezpečnostného utajenia samotného programu, a nie utajenia informácií, ktoré sa majú spracovať. Softwarové verzie, ktoré sa používajú, sa overujú v pravidelných intervaloch, aby sa zabezpečila ich celistvosť a správne fungovanie.

Nové ani modifikované verzie softwaru sa na prácu s utajovanými informáciami EÚ nesmú používať, pokiaľ nie sú overené majiteľom technických systémov.

#### 25.6.3. Kontrola prítomnosti zlovoľného softwaru/počítačových vírusov

Kontrola zameraná na zisťovanie, či nie je prítomný zlovoľný software/počítačové vírusy, sa vykonáva pravidelne v súlade s požiadavkami bezpečnostného akreditačného úradu.

Všetky počítačové pamäťové médiá prichádzajúce do komisie sa pred tým, ako sa zavedú do ľubovoľného systému, musia overiť, či neobsahujú zlovoľný software alebo počítačové vírusy.

#### 25.6.4. Údržba

Zmluvy a postupy pre plánovanú a pohotovostnú údržbu systémov, pre ktoré boli vytvorené vyhlásenia o osobitnej systémovej bezpečnostnej požiadavke, musia špecifikovať požiadavky a opatrenia pre údržbársky personál a ich súvisiace zariadenie, ktoré vstupuje do oblasti počítačových technológií.

Požiadavky musia byť vo vyhláseniach o osobitnej systémovej bezpečnostnej požiadavke jasne uvedené. Dodávateľská údržba, ktorá vyžaduje postupy pre vzdialený diagnostický prístup, je povolená iba vo výnimočných prípadoch za prísnej bezpečnostnej kontroly a iba so súhlasom bezpečnostného akreditačného úradu.

### 25.7. Obstarávanie

#### 25.7.1. Všeobecne

Ľubovoľný bezpečnostný produkt na používanie so systémom, ktorý sa má obstaráť, musí byť vyhodnotený a certifikovaný, alebo práve v procese vyhodnocovania a certifikovania príslušným vyhodnocovacím alebo certifikačným orgánom niektorého z členských štátov podľa medzinárodne uznaných kritérií (ako napríklad Spoločné kritériá pre bezpečnostné vyhodnotenie informačnej technológie, ISO 15 408). Aby sa získal súhlas poradného výboru pre obstarávanie a zmluvy, sú potrebné konkrétne postupy.

Pri rozhodovaní, či by sa zariadenie, najmä počítačové pamäťové médiá, mali prenajať, a nie zakúpiť, sa musí pamätať na to, že takéto zariadenie, keď sa už používalo na prácu

s utajovanými informáciami EÚ, nie je možné uvoľniť mimo primerane bezpečnostného prostredia bez toho, aby sa najprv neodtajnilo sú súhlasom bezpečnostného akreditačného úradu a že takýto súhlas nie je vždy možný.

#### 25.7.2. Akreditácia

Všetky systémy, pre ktoré je nutné vypracovať vyhlásenia o osobitnej systémovej bezpečnostnej požiadavke, musia byť pred prácou s utajovanými informáciami EÚ akreditované bezpečnostným akreditačným úradom podľa informácií uvedených vo vyhláseniach o osobitnej systémovej bezpečnostnej požiadavke, bezpečnostných prevádzkových postupoch a iných príslušných dokumentoch. Vedľajšie systémy a vzdialené terminály/pracovné stanice musia byť akreditované ako časť všetkých systémov, na ktoré sú pripojené. Ak systém podporuje komisiu aj iné organizácie, komisia a príslušné bezpečnostné úrady sa spoločne dohodnú na akreditácii.

Proces akreditácie sa môže vykonať v súlade s akreditačnou stratégiou primeranou pre daný systém a definovanou bezpečnostným akreditačným úradom.

#### 25.7.3. Vyhodnotenie a certifikácia

Pred akreditáciou sa v niektorých prípadoch musí vyhodnotiť systémove bezpečnostné funkcie softwaru, firmwaru a hardwaru a certifikovať ako schopné chrániť informácie na určenej úrovni utajenia.

Požiadavky na vyhodnotenie a certifikáciu sa musia zahrnúť do systémoveho plánovania a jasne uviesť vo vyhláseniach o osobitnej systémovej bezpečnostnej požiadavke.

Procesy vyhodnotenia a certifikácie sa musia vykonávať v súlade so schválenými usmerneniami a technicky kvalifikovanými a príslušne prevereným personálom, ktorý koná v mene majiteľa technických systémov.

Tímy môže poskytnúť menovaný hodnotiaci alebo certifikačný úrad členského štátu alebo jeho menovaní zástupcovia, napríklad kvalifikovaný a preverený dodávateľ.

Stupeň procesov vyhodnotenia a certifikovania môže byť znížený (napríklad zahŕňajúci iba integračné aspekty), ak sú systémy založené na existujúcich národne vyhodnotených a certifikovaných počítačových bezpečnostných produktoch.

#### 25.7.4. Bežná kontrola bezpečnostných funkcií pre stálu akreditáciu

Majiteľ technických systémov vypracuje bežné kontrolné postupy, ktoré zabezpečia, aby boli všetky bezpečnostné funkcie stále platné.

Typy zmien, ktoré by viedli k novej akreditácii, alebo vyžadujú predchádzajúce schválenie bezpečnostného akreditačného úradu, musia byť jasne určené a uvedené vo vyhláseniach

o osobitnej systémovej bezpečnostnej požiadavke. Po ľubovoľnej modifikácii, oprave alebo zlyhaní, ktoré by mohli ovplyvniť bezpečnostné funkcie systému, musí majiteľ technických systémov zabezpečiť, aby sa skontrolovala správna operácia bezpečnostných funkcií. Stála akreditácia systému zvyčajne závisí od uspokojivého ukončenia kontrol

Všetky systémy, kde sa zaviedli bezpečnostné funkcie, musí Bezpečnostný akreditačný úrad pravidelne preverovať a skúmať. V prípade systémov, ktoré pracujú s informáciami EÚ PRÍSNE TAJNÉ, inšpekcie sa musia vykonávať aspoň raz ročne.

## 25.8 Dočasné alebo príležitostné používanie

### 25.8.1. *Bezpečnosť mikropočítačov/osobných počítačov*

Mikropočítače/osobné počítače s pevnými diskmi (alebo inými pamäťovými médiami udržiavajúcimi dáta aj pri výpadku prúdu), ktoré sú operačné v samostatnom režime alebo v sieťovej konfigurácii, a prenosné počítačové zariadenia (napríklad prenosné osobné počítače a elektronické notebooky) s pevnými diskmi sa považujú za informačné pamäťové médiá v rovnakom zmysle ako diskety alebo iné odstrániteľné počítačové pamäťové médiá.

Zariadeniu sa priraduje úroveň ochrany z hľadiska prístupu, manipulácie, ukladania a prepravy, ktorá je rovnocenná s najvyššou úrovňou utajovania informácií, ktoré kedy boli ukladané alebo spracovávané (až do času zníženia úrovne utajenia alebo odtajnenia v súlade so schválenými postupmi).

### 25.8.2. *Použitie súkromne vlastneného zariadenia informačnej technológie pre oficiálnu prácu komisie*

Zakázané je použitie súkromne vlastnených prenosných počítačových pamäťových médií, softwaru a hardwaru (napríklad osobné počítače a prenosné počítačové zariadenia) s pamäťovými kapacitami na manipuláciu s utajovanými informáciami EÚ.

Súkromne vlastnený software, hardware a médiá sa nesmú prinášať do oblasti triedy I alebo triedy II, kde sa narába s utajovanými informáciami EÚ, bez písomného oprávnenia vedúceho bezpečnostného úradu komisie. Toto oprávnenie je možné poskytnúť iba vo výnimočných prípadoch z technických dôvodov.

### 25.8.3. *Použitie informačnej technológie vo vlastníctve dodávateľov alebo technológie národne dodávanej pre oficiálnu prácu komisie*

Použitie informačnej technológie a softwaru vo vlastníctve dodávateľov v organizáciách na podporu oficiálnej práce komisie môže povoliť iba vedúci bezpečnostného úradu komisie. Použitie národne poskytovaného zariadenia informačnej technológie a softwaru sa môže tiež povoliť. V takomto prípade sa zariadenie informačnej technológie musí zahrnúť pod kontrolu príslušného inventárneho spísania komisie. V hocijakom prípade, ak sa zariadenie

informačnej technológie má používať na manipuláciu s utajovanými informáciami EÚ, musí sa konzultovať s bezpečnostným akreditačným úradom, aby sa primerane zohľadnili a zaviedli prvky INFOSEC, ktoré sú uplatňované pre použitie daného zariadenia.

## 26. UVOĽNENIE UTAJOVANÝCH INFORMÁCIÍ TRETÍM ŠTÁTOM ALEBO MEDZINÁRODNÝM ORGANIZÁCIÁM

### 26.1.1. *Zásady upravujúce uvoľnenie utajovaných informácií EÚ*

Komisia ako kolektívny orgán rozhoduje o uvoľnení utajovaných informácií EÚ tretím štátom alebo medzinárodným organizáciám na základe:

- povahy a obsahu takýchto informácií;
- potreby oboznámenia sa prijímateľov;
- miery výhod pre EÚ.

Pôvodca utajovaných informácií EÚ, ktoré sa majú uvoľniť, sa musí požiadať o súhlas.

Tieto rozhodnutia sa prijímajú podľa jednotlivých prípadov a v závislosti od:

- želaného stupňa spolupráce s danými tretími štátmi alebo medzinárodnými organizáciami;
- dôvery, ktorú im možno prejavíť – čo vyplýva z úrovne bezpečnosti, ktorá by sa uplatnila na utajované informácie EÚ zverené týmto štátom alebo organizáciám a zo súladu medzi bezpečnostnými pravidlami uplatňovanými v daných tretích štátoch alebo medzinárodných organizáciách a v EÚ. Poradná skupina komisie pre bezpečnostnú politiku predloží komisii ohľadne tohto bodu svoje technické stanovisko.

Prijatie utajovaných informácií EÚ tretími štátmi alebo medzinárodnými organizáciami implikuje uistenie, že sa informácie nebudú používať pre účely iné, ako sú účely, pre ktoré sa dané informácie uvoľnili alebo vymenili, a že sa týmto informáciám prideli ochrana, ktorú vyžaduje komisia.

### 26.1.2. *Úrovne*

Komisia po svojom rozhodnutí, že utajované informácie EÚ možno uvoľniť alebo si vymeniť s daným štátom alebo medzinárodnou organizáciou, rozhodne o úrovni spolupráce, ktorá je možná. Toto závisí najmä od bezpečnostnej politiky a pravidiel, ktoré uplatňuje daný štát alebo organizácia.

Existujú tri úrovne spolupráce:

#### Úroveň 1

Spolupráca s tretími štátmi alebo s medzinárodnými organizáciami, ktorých bezpečnostná politika a nariadenia sú veľmi blízke bezpečnostnej politike a nariadeniam EÚ.

## Úroveň 2

Spolupráca s tretími štátmi alebo s medzinárodnými organizáciami, ktorých bezpečnostná politika a nariadenia sú značne rozdielne od bezpečnostnej politiky a nariadení EÚ.

## Úroveň 3

Občasná spolupráca s tretími štátmi alebo medzinárodnými organizáciami, ktorých bezpečnostnú politiku a nariadenia nie je možné posúdiť.

Každá úroveň spolupráce určuje postupy a bezpečnostné ustanovenia podrobne uvedené v dodatkoch 3, 4 a 5.

### 26.1.3. *Bezpečnostné dohody*

Komisia po svojom rozhodnutí, že existuje stála alebo dlhodobá potreba výmeny utajovaných informácií medzi komisiou a tretími štátmi alebo inými medzinárodnými organizáciami, vypracuje s nimi „dohody o bezpečnostných postupoch pre výmenu utajovaných informácií“, ktoré definujú účel spolupráce a recipročné pravidlá o ochrane vymenených informácií.

V prípade úrovne 3, občasná spolupráca, ktorá je svojou definíciou obmedzená časom a účelom, môže jednorázové memorandum o porozumení, definujúce povahu utajovaných informácií, ktoré sa majú vymieňať a recipročné povinnosti ohľadne týchto informácií, nahradiť „dohodu o postupoch pre výmenu utajovaných informácií“ za podmienky, že utajované informácie nie sú vyššej úrovne utajenia ako EÚ VYHRADENÉ.

Predtým, ako sa návrhy dohôd o bezpečnostných postupoch alebo memoránd o porozumení predložia komisii na rozhodnutie, musí ich prerokovať poradná skupina komisie pre bezpečnostnú politiku.

Člen komisie zodpovedný za bezpečnostné záležitosti požiada o akúkoľvek pomoc od národného bezpečnostného úradu členského štátu potrebnú na zabezpečenie toho, aby informácie, ktoré sa majú uvoľniť, sa používali a chránili v súlade s ustanoveniami dohôd o bezpečnostných postupoch alebo v súlade s memorandom o porozumení.

## DODATOK I

## POROVNANIE NÁRODNÝCH ÚROVNÍ BEZPEČNOSTNÉHO UTAJOVANIA

Utajovanie EÚ	EÚ PRÍSNE TAJNÉ	EÚ TAJNÉ	EÚ DÔVERNÉ	EÚ VYHRADENÉ
Utajovanie NATO <sup>1</sup>				
Utajovanie ZEÚ				
Utajovanie EURATOM <sup>2</sup>	Focal Top Secret	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Belgicko	Très Secret Zeet Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Bepaalde Verspreiding
Dánsko	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Nemecko	STRENG GEHEIM	GEHEIM	VS <sup>3</sup> - VERTRAULICH	VS – NUR FÜR DIENSTGEBRAUCH
Grécko	Ακρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Španielsko	Secreto	Reservado	Confidencial	Difusión limitada
Francúzsko	Très Secret Défense <sup>4</sup>	Secret Défense	Confidentiel Défense	Diffusion restreinte
Írsko	Top Secret	Secret	Confidential	Restricted
Taliansko	Segretissimo	Segreto	Riservatissimo	Riservato
Luxembursko	Très Secret	Secret	Confidentiel	Diffusion restreinte
Holandsko	Stg. Zeet Geheim	Stg. Geheim	Stg. Confidenciel	
Rakúsko	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugalsko	Muito Secreto	Secreto	Confidencial	Reservado
Fínsko	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Švédsko	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Spojené kráľovstvo	Top Secret	Secret	Confidential	Restricted

<sup>1</sup> NATO – zhoda s úrovňami utajovania NATO sa stanoví, keď sa rokovaniami dosiahne bezpečnostná dohoda medzi komisiou a NATO

<sup>2</sup>Nariadenie Euratom č. 3 z 31. júla 1958 o ochrane utajovaných informácií Euratom

<sup>3</sup> Nemecko: VS = Verschlussache

<sup>4</sup> Francúzsko: utajovanie „Très Secret Défense“, ktoré riadi vládne prioritné záležitosti, je možné zmeniť iba s oprávnením ministerského predsedu.

**DODATOK 2**  
**PRAKTICKÝ NÁVOD PRE UTAJOVANIE**

Tento návod je iba orientačný a nie je ho možné chápať ako bližšie určenie ustanovení uvedených v oddieloch 16, 17, 20 a 21.

Utajenie	Kedy	Kto	Označenie	Zníženie utajenia/ odtajnenie/likvidácia	
				Kto	Kedy
EÚ PRÍSNE TAJNÉ: Toto utajenie sa vzťahuje iba na informácie a materiály, ktorých neoprávnené zverejnenie by mohlo spôsobiť mimoriadne vážne poškodenie najdôležitejších záujmov Európskej únie alebo jedného alebo viacerých jej členských štátov. [16.1]	Odcudzenie položiek klasifikovaných ako EÚ PRÍSNE TAJNÉ by mohlo: - ohroziť priamo vnútornú stabilitu EÚ alebo jedného alebo viacerých jej členských štátov alebo spriateľených štátov - mimoriadne vážne poškodiť vzťahy so spriateľenými vládami - viesť priamo k rozsiahlym stratám na životoch - mimoriadne poškodiť operačnú účinnosť alebo bezpečnosť členských štátov alebo iných podporných síl, alebo trvalú účinnosť mimoriadne dôležitých bezpečnostných alebo tajných operácií - vážne dlhodobo poškodiť hospodárstvo EÚ alebo členských štátov	Príslušne oprávnené osoby (pôvodcovia), generálni riaditelia, vedúci služieb. [17.1]  Pôvodcovia určujú dátum, obdobie alebo udalosť, kedy je možné obsah utajiť na nižšej úrovni alebo odtajniť. [16.2]  Inak dokumenty revidujú aspoň raz za päť rokov, aby sa zabezpečilo, že je stále potrebná pôvodná úroveň utajenia. [17.3]	EÚ PRÍSNE TAJNÉ a prípadne bezpečnostný ukazovateľ a/alebo bezpečnostné značenie Európskej bezpečnostnej a obrannej politiky sa priraduje dokumentom, ktoré sú EÚ PRÍSNE TAJNÉ, strojovo a ručne. [16.4, 16.5, 16.3]  Utajenie EÚ a bezpečnostný menovateľ sa uvádza na vrchnej a spodnej časti strany v strede, pričom každá strana je očíslovaná. Všetky dokumenty musia mať referenčné číslo a dátum. Toto referenčné číslo sa uvádza na všetkých stranách.  Ak sa dokumenty majú distribúvať vo viacerých kópiách, každá musí mať číslo kópie, ktoré sa uvádza na prvej strane, spolu s celkovým počtom strán. Na prvej strane musí	Zníženie úrovne utajenia alebo odtajnenie spočíva výlučne na pôvodcovi, ktorý o zmenách informuje akýchkoľvek následných adresátov, ktorým zaslal alebo kopíroval dokument. [17.3]  Dokumenty EÚ PRÍSNE TAJNÉ likviduje centrálny register alebo vedľajší register, ktorý je za nich zodpovedný. Všetky zlikvidované dokumenty musia byť uvedené v potvrdení o likvidácii podpísanom kontrolným referentom EÚ PRÍSNE TAJNÉ a referentom, ktorý bol svedkom likvidácie. V knihe sa urobí zápis o likvidácii. Register uchováva potvrdenia o likvidácii spolu s rozdeľovníkmi desať rokov. [22.5]	Prebytočné kópie a dokumenty, ktoré nie sú viac potrebné, sa musia zlikvidovať. [22.5]  Dokumenty EÚ PRÍSNE TAJNÉ vrátane utajeného odpadu z prípravy dokumentov EÚ PRÍSNE TAJNÉ, napríklad pokazené kópie, písané poznámky a prepisovací papier, sa musia zlikvidovať za dozoru kontrolného referenta EÚ PRÍSNE TAJNÉ spálením, rozdručením, skartovaním alebo inou destrukciou na formu, ktorá nie je spoznatelná a obnoviteľná. [22.5]

Utajenie	Kedy	Kto	Označenie	Zníženie utajenia/ odtajnenie/likvidácia	
				Kto	Kedy
			byť zoznam všetkých príloh a dodatkov. [21.1]		

Utajenie	Kedy	Kto	Označenie	Zníženie utajenia/ odtajnenie/likvidácia	
				Kto	Kedy
EÚ TAJNÉ: Toto utajenie sa vzťahuje iba na informácie a materiály, ktorých neoprávnené zverejnenie by mohlo spôsobiť vážne poškodenie najdôležitejších záujmov Európskej únie alebo jedného alebo viacerých jej členských štátov. [16.1]	Odcudzenie položiek klasifikovaných ako EÚ TAJNÉ by mohlo: - zvýšiť medzinárodné napätie - vážne poškodiť vzťahy so spriatelými vládami - ohroziť životy priamo alebo vážne ohroziť verejný poriadok alebo bezpečnosť alebo slobodu jednotlivcov - vážne poškodiť operačnú účinnosť alebo bezpečnosť členských štátov alebo iných podporných síl, alebo trvalú účinnosť mimoriadne dôležitých bezpečnostných alebo tajných operácií - spôsobiť vážne materiálne škody na finančných, peňažných, ekonomických a obchodných záujmoch EÚ alebo niektorého z jej členských štátov	Oprávnené osoby (pôvodcovia), generálni riaditelia, vedúci služieb. [17.1]  Pôvodcovia určujú obdobie kedy je možné obsah utajiť na nižšej úrovni alebo odtajniť. [16.2]  Inak dokumenty revidujú aspoň raz za päť rokov, aby sa zabezpečilo, že je stále potrebná pôvodná úroveň utajenia. [17.3]	EÚ TAJNÉ a prípadne bezpečnostný ukazovateľ a/alebo bezpečnostné značenie Európskej bezpečnostnej obrannej politiky sa priraduje dokumentom, ktoré sú EÚ TAJNÉ, strojovo a ručne. [16.4, 16.5, 16.3]  Utajenie EÚ a bezpečnostný menovateľ sa uvádza na vrchnej a spodnej časti strany v strede, pričom každá strana je očíslovaná. Všetky dokumenty musia mať referenčné číslo a dátum. Toto referenčné číslo sa uvádza na všetkých stranách.  Ak sa dokumenty majú distribuovať vo viacerých kópiách, každá musí mať číslo kópie, ktoré sa uvádza na prvej strane, spolu s celkovým počtom strán. Na prvej strane musí byť zoznam všetkých príloh a dodatkov. [21.1]	Zníženie úrovne utajenia alebo odtajnenie spočíva výlučne na pôvodcovi, ktorý o zmenách informuje akýchkoľvek následných adresátov, ktorým zaslal alebo kopíroval dokument. [17.3]  Dokumenty EÚ TAJNÉ likviduje register alebo vedľajší register, ktorý je za nich zodpovedný, za dozoru bezpečnostne preverenej osoby. Všetky zlikvidované dokumenty EÚ TAJNÉ musia byť uvedené v potvrdení o likvidácii. Register uchováva potvrdenia o likvidácii spolu s rozdeľovníkmi tri roky. [22.5]	Prebytočné kópie a dokumenty, ktoré nie sú viac potrebné, sa musia zlikvidovať. [22.5]  Dokumenty EÚ TAJNÉ vrátane utajeného odpadu z prípravy dokumentov EÚ TAJNÉ, napríklad pokazené kópie, pracovné návrhy, písané poznámky a prepisovací papier, sa musia zlikvidovať spálením, rozdrvením, skartovaním alebo inou deštrukciou na formu, ktorá nie je spoznatel'ná a obnoviteľ'ná. [22.5]

Utajenie	Kedy	Kto	Označenie	Zníženie utajenia/ odtajnenie/likvidácia	
				Kto	Kedy
EÚ DÔVERNÉ: Toto utajenie sa vzťahuje na informácie a materiály, ktorých neoprávnené zverejnenie by mohlo spôsobiť poškodenie dôležitých záujmov Európskej únie alebo jedného alebo viacerých jej členských štátov. [16.1]	Odcudzenie položiek klasifikovaných ako EÚ DÔVERNÉ by mohlo: - vážne poškodiť diplomatické vzťahy, t.j. viesť k formálnym protestom alebo iným sankciám - ohroziť bezpečnosť alebo slobodu jednotlivcov; - vážne poškodiť operačnú účinnosť alebo bezpečnosť členských štátov alebo iných podporných síl, alebo účinnosť dôležitých bezpečnostných alebo tajných operácií; - podstatne poškodiť finančnú existenciu významných organizácií - znemožniť vyšetrenie alebo umožniť spáchanie vážnych zločinov; - pracovať významne proti finančným, peňažným, ekonomickým a obchodným záujmom EÚ alebo jej členských štátov; - vážne ohroziť rozvoj alebo realizovanie významných politík EÚ; - ukončiť alebo inak vážne	Oprávnené osoby (pôvodcovia), generálni riaditelia, vedúci služieb. [17.1]  Pôvodcovia určujú dátum alebo obdobie, kedy je možné obsah utajiť na nižšej úrovni alebo odtajniť. [16.2]  Inak dokumenty revidujú aspoň raz za päť rokov, aby sa zabezpečilo, že je stále potrebná pôvodná úroveň utajenia. [17.3]	EÚ DÔVERNÉ a prípadne bezpečnostný ukazovateľ a/alebo bezpečnostné značenie Európskej bezpečnostnej a obrannej politiky sa priradzuje dokumentom, ktoré sú EÚ DÔVERNÉ, strojovo a ručne, alebo tlačou na predtlačene registrované tlačivá. [16.4, 16.5, 16.3]  Utajenie EÚ a bezpečnostný menovateľ sa uvádza na vrchnej a spodnej časti strany v strede, pričom každá strana je očíslovaná. Všetky dokumenty musia mať referenčné číslo a dátum.  Na prvej strane musí byť zoznam všetkých príloh a dodatkov. [21.1]	Zníženie úrovne utajenia alebo odtajnenie spočíva výlučne na pôvodcovi, ktorý o zmenách informuje akýchkoľvek následných adresátov, ktorým zaslal alebo kopíroval dokument. [17.3]  Dokumenty EÚ DÔVERNÉ likviduje register, ktorý je za nich zodpovedný, za dozoru preverenej osoby. Ich likvidácia musí byť zaznamenaná v súlade s národnými pravidlami, a v prípade komisie alebo decentralizovaných agentúr EÚ podľa pokynov predsedu. [22.5]	Prebytočné kópie a dokumenty, ktoré nie sú viac potrebné, sa musia zlikvidovať. [22.5]  Dokumenty EÚ DÔVERNÉ vrátane utajeného odpadu z prípravy dokumentov EÚ DÔVERNÉ, napríklad pokazené kópie, pracovné návrhy, písané poznámky a prepisovací papier, sa musia zlikvidovať spálením, rozdrvením, skartovaním alebo inou deštrukciou na formu, ktorá nie je spoznatelná a obnoviteľná. [22.5]

Utajenie	Kedy	Kto	Označenie	Zníženie utajenia/ odtajnenie/likvidácia	
				Kto	Kedy
	znemožniť významné činnosti EÚ.				

Utajenie	Kedy	Kto	Označenie	Zníženie utajenia/ odtajnenie/likvidácia	
				Kto	Kedy
EÚ VYHRADENÉ: Toto utajenie sa vzťahuje na informácie a materiály, ktorých neoprávnené zverejnenie by nevýhodné pre záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov. [16.1]	Odcudzenie položiek klasifikovaných ako EÚ VYHRADENÉ by mohlo: - nepriaznivo poškodiť diplomatické vzťahy - zapríčiniť ťažkosti jednotlivcom - sťažiť zachovanie operačnej účinnosti alebo bezpečnosti členských štátov alebo iných podporných síl - zapríčiniť finančnú stratu alebo umožniť neprímeraný zisk alebo výhodu jednotlivcom alebo spoločnostiam - porušiť príslušné záväzky zachovať dôvernosť informácií, ktoré poskytli tretie strany - porušiť štatutárne obmedzenia platné pre zverejňovanie informácií - poškodiť vyšetrenie alebo umožniť spáchanie zločinu - znevýhodniť EÚ alebo členské štáty pri obchodných alebo politických rokovaníach s ostatnými - zabrániť účinný	Oprávnené osoby (pôvodcovia), generálni riaditelia, vedúci služieb. [17.1]  Pôvodcovia určujú dátum alebo obdobie, kedy je možné obsah utajiť na nižšej úrovni alebo odtajniť. [16.2]  Inak dokumenty revidujú aspoň raz za päť rokov, aby sa zabezpečilo, že je stále potrebná pôvodná úroveň utajenia. [17.3]	EÚ VYHRADENÉ a prípadne bezpečnostný ukazovateľ a/alebo bezpečnostné značenie Európskej bezpečnostnej a obrannej politiky sa priraduje dokumentom, ktoré sú EÚ VYHRADENÉ, strojovo alebo elektronicky. [16.4, 16.5, 16.3]  Utajenie EÚ a bezpečnostný menovateľ sa uvádza na vrchnej a spodnej časti strany v strede, pričom každá strana je očíslovaná. Všetky dokumenty musia mať referenčné číslo a dátum. [21.1]	Odtajnenie spočíva výlučne na pôvodcovi, ktorý o zmenách informuje akýchkoľvek následných adresátov, ktorým zaslal alebo kopíroval dokument. [17.3]  Dokumenty EÚ VYHRADENÉ likviduje register, ktorý je za nich zodpovedný, alebo užívateľ podľa pokynov predsedu. [22.5]	Prebytočné kópie a dokumenty, ktoré nie sú viac potrebné, sa musia zlikvidovať. [22.5]

Utajenie	Kedy	Kto	Označenie	Zníženie utajenia/ odtajnenie/likvidácia	
				Kto	Kedy
	rozvoj alebo pôsobenie politík EÚ - poškodiť príslušné riadenie EÚ a jej činností.				

*DODATOK 3*

Usmernenia o uvoľnení utajovaných informácií EÚ tretím štátom alebo medzinárodným organizáciám: Úroveň spolupráce 1

## POSTUPY

1. Oprávnenie zverejniť utajované informácie krajinám, ktoré nie sú členmi Európskej únie, alebo iným medzinárodným organizáciám, ktorých bezpečnostná politika a nariadenia sú porovnateľné s EÚ, spočíva výlučne na komisii ako kolektívnom orgáne.
2. Až do uzavretia bezpečnostnej dohody je za bezpečnostné záležitosti zodpovedný člen komisie, ktorý má právo preskúmať žiadosti o zverejnenie utajovaných informácií EÚ.
3. V takomto prípade, musí:
  - získať stanovisko pôvodcov utajovaných informácií EÚ, ktoré sa majú zverejniť;
  - nadviazať potrebné kontakty s bezpečnostnými orgánmi prijímajúcich krajín alebo medzinárodných organizácií, aby overil, či ich bezpečnostná politika a ustanovenia sú také, aby mohli zaručiť, že zverejnené utajované informácie sa budú chrániť v súlade s týmito bezpečnostnými ustanoveniami;
  - získa stanovisko poradnej skupiny komisie pre bezpečnostnú politiku, pokiaľ ide o dôveru, ktorú možno priznať prijímajúcim štátom alebo medzinárodným organizáciám.
4. Člen komisie zodpovedný za bezpečnostné záležitosti postúpi žiadosť a stanovisko poradnej skupiny komisie pre bezpečnostnú politiku komisii na rozhodnutie.

## BEZPEČNOSTNÉ USTANOVENIA, KTORÉ MUSIA UPLATŇOVAŤ PRÍJEMCOVIA

5. Člen komisie zodpovedný za bezpečnostné záležitosti oznámi prijímajúcim štátom alebo medzinárodným organizáciám rozhodnutie komisie o schválení zverejnenia utajovaných informácií EÚ.
6. Rozhodnutie nadobúda účinnosť až vtedy, keď príjemcovia predložia písomné uistenie, že:
  - nepoužijú informácie na iné ako dohodnuté účely;
  - informácie budú chrániť v súlade s týmito bezpečnostnými ustanoveniami, najmä zvláštnymi pravidlami uvedenými nižšie.

## 7. Personál

- (a) Počet úradníkov s prístupom k utajovaným informáciám EÚ musí byť podľa zásady potreby oboznámenia sa prísne obmedzený na tie osoby, ktorých povinnosti takýto prístup vyžadujú.
- (b) Všetci úradníci alebo štátni príslušníci, ktorí majú oprávnenie na prístup k utajovaným informáciám EÚ DÔVERNÉ alebo vyššej úrovne utajenia, musia mať potvrdenie o bezpečnostnom preverení pre príslušnú úroveň alebo rovnocennom preverení, ktoré vydala vláda ich vlastného štátu.

#### 8. Prenos dokumentov

- (a) Praktické postupy pre prenos dokumentov sa stanovujú v dohode. Až do uzavretia takejto dohody sa uplatňujú ustanovenia oddielu 21. Dohoda musí najmä určiť registre, ktorým musia byť utajované informácie postúpené.
- (b) Ak utajované informácie, ktorých zverejnenie komisia oprávnila, zahŕňa informácie EÚ PRÍSNE TAJNÉ, prijímajúci štát alebo medzinárodná organizácia založí centrálny register EÚ a prípadne vedľajšie registre EÚ. Tieto registre musia dôsledne uplatňovať ustanovenia, ktoré sú rovnocenné s ustanoveniami v oddieli 22 týchto bezpečnostných ustanovení.

#### 9. Registrácia

Len čo register obdrží dokument EÚ utajený ako EÚ DÔVERNÉ alebo na vyššej úrovni utajenia, zaeviduje dokument v zvláštnom registri, ktorý má organizácia a ktorý obsahuje stĺpce pre dátumy prijatia, údaje o dokumente (dátum, referenčné číslo a číslo kópie), jeho utajenie, názov, meno alebo postavenie príjemcu, dátum vrátenia potvrdenia o prijímaní a dátum vrátenia dokumentu pôvodcovi v EÚ a likvidácie.

#### 10. Likvidácia

- (a) Utajované dokumenty EÚ sa likvidujú v súlade s pokynmi uvedenými v oddieli 22 týchto bezpečnostných ustanovení. Kópie potvrdení o likvidácii pre dokumenty EÚ TAJNÉ a EÚ PRÍSNE TAJNÉ sa zasielajú do registra EÚ, ktorý dokumenty postúpil.
- (b) Utajované dokumenty musia byť zahrnuté v plánoch núdzovej likvidácie pre vlastné utajované dokumenty orgánov príjemcu.

#### 11. Ochrana dokumentu

Musia sa prijať všetky potrebné opatrenia, aby sa zabránilo prístupu neoprávnených osôb k utajovaným informáciám EÚ.

#### 12. Kópie

Bez oprávnenia vedúceho príslušnej bezpečnostnej organizácie sa nesmú robiť žiadne fotokópie ani preklad dokumentu EÚ DÔVERNÉ alebo EÚ TAJNÉ a ani výpisy z takéhoto dokumentu. Vedúci príslušnej bezpečnostnej organizácie zaeviduje a skontroluje kópie, preklady alebo výpisy z nich a podľa potreby ich opečiatkuje.

Reprodukcii alebo preklad dokumentu EÚ PRÍSNE TAJNÉ môže oprávniť iba úrad pôvodcu, ktorý stanoví počet oprávnených kópií; ak úrad pôvodcu nie je možné stanoviť, žiadosť sa postúpi bezpečnostnej službe komisie.

### 13. Porušenie bezpečnosti

Ak dôjde k porušeniu bezpečnosti, ktoré zahŕňa utajovaný dokument EÚ, alebo vzniklo podozrenie, že k takémuto porušeniu došlo, okamžite sa prijímajú nasledujúce opatrenia, ktoré podliehajú uzavretiu bezpečnostnej dohody.

- (a) Vykoná sa šetrenie, aby sa stanovili okolnosti, za ktorých došlo k porušeniu bezpečnosti;
- (b) upovedomí sa bezpečnostný úrad komisie, príslušný národný bezpečnostný úrad a úrad pôvodcu, alebo sa jasne uvedie, že úrad pôvodcu nebol oboznámený, ak k tomu nedošlo;
- (c) prijímajú sa opatrenia na minimalizovanie účinkov porušenia bezpečnosti;
- (d) opätovne sa zväžia a zavedú opatrenia, aby sa zabránilo opakovaniu;
- (e) zavedú sa akékoľvek opatrenia, ktoré odporúča bezpečnostný úrad komisie na zabránenie opakovania.

### 14. Inšpekcie

Na základe dohôd s danými štátmi alebo medzinárodnými organizáciami sa povolí, aby bezpečnostný úrad komisie posúdil účinnosť opatrení na ochranu zverejnených utajovaných informácií EÚ.

### 15. Hlásenie

S podmienkou uzavretia bezpečnostnej dohody, pokiaľ daný štát alebo organizácia má k dispozícii utajované informácie EÚ, ročne musí predkladať do dátumu určeného pri uvoľnení utajovaných informácií správu, ktorá potvrdí, že sa tieto bezpečnostné ustanovenia naďalej dodržiavajú.

*DODATOK 4*

Usmernenia o uvoľnení utajovaných informácií EÚ tretím štátom alebo medzinárodným organizáciám: Úroveň spolupráce 2

## POSTUPY

1. Oprávnenie zverejniť utajované informácie tretím štátom alebo iným medzinárodným organizáciám, ktorých bezpečnostná politika a nariadenia sú výrazne odlišné od EÚ, spočíva výlučne na pôvodcovi. Oprávnenie uvoľniť utajované informácie EÚ vypracované v rámci komisie spočíva na komisii ako kolektívnom orgáne.
2. V zásade ide o utajované informácie utajené až do úrovne EÚ TAJNÉ vrátane; nie sú zahrnuté utajované informácie, ktoré sú chránené zvláštnymi bezpečnostnými označeniami alebo znakmi.
3. Až do uzavretia bezpečnostnej dohody je za bezpečnostné záležitosti zodpovedný člen komisie, ktorý má právo preskúmať žiadosti o zverejnenie utajovaných informácií EÚ.
4. V takomto prípade, musí:
  - získať stanovisko pôvodcov utajovaných informácií EÚ, ktoré sa majú zverejniť;
  - naviazať potrebné kontakty s bezpečnostnými orgánmi prijímajúcich krajín alebo medzinárodných organizácií, aby zistila informácie o ich bezpečnostnej politike a ustanoveniach, a najmä aby vypracoval tabuľku porovnávajúcu utajovanie uplatňované v EÚ a v danom štáte alebo organizácii;
  - zabezpečí zasadnutie poradnej skupiny komisie pre bezpečnostnú politiku alebo tichým postupom, ak bude potrebné, informuje sa u národných bezpečnostných úradov členských štátov ohľadne získania stanoviska poradnej skupiny komisie pre bezpečnostnú politiku.
5. Stanovisko poradnej skupiny komisie pre bezpečnostnú politiku sa týka nasledujúceho:
  - dôvery, ktorú možno priznať prijímajúcim štátom alebo medzinárodným organizáciám so zreteľom na posúdenie bezpečnostných rizík, ktoré vzniknú pre EÚ alebo jej členské štáty;
  - posúdenie schopnosti príjemcov chrániť utajované informácie, ktoré EÚ uvoľnila;
  - návrhov ohľadne praktických postupov pre narábanie s utajovanými informáciami EÚ (napríklad zabezpečenie cenzurovaných verzií textu) a dokumentmi, ktoré sa prenášajú (zachovanie alebo odstránenie hlavičiek utajovania EÚ, osobitné znaky atď.);
  - zníženia úrovne utajenia alebo odtajnenia pred uvoľnením informácie prijímajúcim krajinám alebo medzinárodným organizáciám.

6. Člen komisie zodpovedný za bezpečnostné záležitosti postúpi žiadosť a stanovisko poradnej skupiny komisie pre bezpečnostnú politiku komisii na rozhodnutie.

#### BEZPEČNOSTNÉ USTANOVENIA, KTORÉ MUSIA UPLATŇOVAŤ PRÍJEMCOVIA

7. Člen komisie zodpovedný za bezpečnostné záležitosti oznámi prijímajúcim štátom alebo medzinárodným organizáciám rozhodnutie komisie o schválení zverejnenia utajovaných informácií EÚ a jeho obmedzeniach.
8. Rozhodnutie nadobúda účinnosť až vtedy, keď príjemcovia predložia písomné uistenie, že:
  - nepoužijú informácie na iné ako dohodnuté účely;
  - informácie budú chrániť v súlade s bezpečnostnými ustanoveniami, ktoré určí komisia.
9. Uplatňujú sa nasledujúce pravidlá ochrany, ak komisia po získaní technického stanoviska poradnej skupiny komisie pre bezpečnostnú politiku nerozhodne o určitom postupe pre narábanie s utajovanými dokumentmi EÚ (odstránenia označenia utajenia EÚ, osobitné znaky atď.).

#### 10. Personál

- (a) Počet úradníkov s prístupom k utajovaným informáciám EÚ musí byť podľa zásady potreby oboznámenia sa prísne obmedzený na tie osoby, ktorých povinnosti takýto prístup vyžadujú.
- (b) Všetci úradníci alebo štátni príslušníci, ktorí majú oprávnenie na prístup k utajovanými informáciám EÚ, musia mať potvrdenie o národnom bezpečnostnom preverení alebo oprávnenia prístupu k príslušnej úrovni ekvivalentnej úrovni EÚ, ako sú definované v porovnávacjej tabuľke;
- (d) Tieto národné bezpečnostné preverenia sa postupujú predsedovi na informovanie.

#### 11. Prenos dokumentov

Praktické postupy pre prenos dokumentov sa stanovujú v dohode. Až do uzavretia takejto dohody sa uplatňujú ustanovenia oddielu 21. Dohoda musí najmä určiť registre, ktorým musia byť utajované informácie postúpené a presné adresy, na ktoré sa dokumenty zašlú, rovnako ako kuriérske služby alebo poštové služby, ktoré sa na prenos utajovaných informácií EÚ použijú.

#### 12. Registrácia pri príchode

Národný bezpečnostný úrad štátu adresáta alebo jeho ekvivalent v štáte, ktorý obdrží v mene vlády utajované informácie postúpené komisiou, alebo bezpečnostný úrad prijímajúcej medzinárodnej organizácie ustanovia zvláštny register na zaznamenávanie utajovaných informácií EÚ pri ich príchode. Register obsahuje stĺpce uvádzajúce dátum prijatia, údaje od dokumentu (dátum, referenčné číslo a číslo kópie), jeho utajenie, názov, meno adresáta alebo

jeho postavenie, dátum návratu potvrdenia o príjme a dátum návratu dokumentu do EÚ alebo jeho likvidácie.

### 13. Návrat dokumentov

Keď príjemca vráti utajovaný dokument komisii, postupuje, ako je uvedené v odseku „Prenos dokumentov“ vyššie.

### 14. Ochrana dokumentu

- (a) Ak sa dokumenty nepoužívajú, skladujú sa v bezpečnostných schránkach, ktoré sú schválené na skladovanie národne utajených materiálov rovnakej úrovne utajenia. Schránka nenesie žiadne označenie svojho obsahu. Ak sa používajú kombinačné zámky, kombinácie sú známe iba tým úradníkom v danom štáte alebo organizácii, ktorí majú prístup k utajovaným informáciám EÚ uloženým v schránke. Kombinácie sa menia každých šesť mesiacov alebo častejšie, ak je niektorý úradník preložený, ak sa odoberie bezpečnostné preverenie niektorému z úradníkov, ktorí poznali kombináciu, alebo ak vznikne nebezpečenstvo odcudzenia.
- (b) Utajené dokumenty EÚ odstraňujú z bezpečnostnej schránky iba tí úradníci, ktorí sú preverení na prístup k utajovaným informáciám EÚ a majú potrebu oboznámenia sa. Sú naďalej zodpovední za uschovávanie týchto dokumentov, pokiaľ sú v ich vlastníctve, a najmä za zabezpečenie toho, aby žiadna neoprávnená osoba nemala prístup k dokumentom. Zabezpečujú tiež, aby sa dokumenty po ich konzultovaní a po pracovných hodinách uložili do bezpečnostnej schránky.
- (c) Bez oprávnenia bezpečnostného úradu komisie sa nesmú robiť žiadne fotokópie ani výpisy dokumentov klasifikovaných ako EÚ DÔVERNÉ a vyššej úrovne utajovania.
- (d) Postup pre rýchlu a úplnú likvidáciu dokumentov v núdzovom stave určí a potvrdí bezpečnostný úrad komisie.

### 15. Fyzická bezpečnosť

- (a) Bezpečnostné schránky, keď sa nepoužívajú na skladovanie utajovaných dokumentov EÚ, sa uchovávajú sústavne zamknuté;
- (b) Ak je potrebné, aby do miestnosti, kde sa nachádzajú bezpečnostné schránky, vstúpil údržbársky alebo čistiaci personál, alebo aby takýto personál pracoval v takýchto miestnostiach, musí byť sústavne sprevádzaný členom bezpečnostnej služby daného štátu alebo organizácie, alebo úradníkom zvlášť zodpovedným za dohľad nad bezpečnosťou danej miestnosti;

- (c) Mimo zvyčajných pracovných hodí (v noci, cez víkendy a v dni štátnych sviatkov), bezpečnostné schránky obsahujúce utajované dokumenty EÚ musia byť chránené strážnou službou alebo automatickým poplašným zariadením.

#### 16. Porušenie bezpečnosti

Ak dôjde k porušeniu bezpečnosti, ktoré zahŕňa utajovaný dokument EÚ, alebo vzniklo podozrenie, že k takémuto porušeniu došlo, okamžite sa prijímajú nasledujúce opatrenia:

(a) okamžite sa predloží správa bezpečnostnému úradu komisie alebo národnému bezpečnostnému úradu členského štátu, ktorý inicioval zaslanie dokumentov (s kópiou bezpečnostnému úradu komisie);

(b) vykoná sa vyšetrovanie a o tomto vyšetrovaní sa predloží správa bezpečnostnému orgánu (pozri (a) vyššie). Potom sa prijímajú opatrenia potrebné na nápravu situácie.

#### 17. Inšpekcie

Na základe dohôd s danými štátmi alebo medzinárodnými organizáciami sa povolí, aby bezpečnostný úrad komisie vykonal posúdenie účinnosti opatrení na ochranu zverejnených utajovaných informácií EÚ.

#### 18. Hlásenie

S podmienkou uzavretia bezpečnostnej dohody, pokiaľ daný štát alebo organizácia má k dispozícii utajované informácie EÚ, ročne musí predkladať do dátumu určeného pri uvoľnení utajovaných informácií správu, ktorá potvrdí, že sa tieto bezpečnostné ustanovenia naďalej dodržiavajú.

*DODATOK 5*

Usmernenia o uvoľnení utajovaných informácií EÚ tretím štátom alebo medzinárodným organizáciám: Úroveň spolupráce 3

## POSTUPY

1. Komisia môže mať za určitých okolností z času na čas záujem o spoluprácu so štátmi a organizáciami, ktoré nemôže poskytnúť uistenia požadované týmito pravidlami, ale takáto spolupráca môže vyžadovať zverejnenie utajovaných informácií EÚ.

2. Oprávnenie zverejniť utajované informácie EÚ tretím štátom alebo medzinárodným organizáciám, ktorých bezpečnostná politika a nariadenia sú výrazne odlišné od politiky a nariadení EÚ, spočíva výlučne na pôvodcovi. Oprávnenie zverejniť utajované informácie EÚ, ktoré vznikli v rámci komisie, spočíva výlučne na komisii ako kolektívnom orgáne.

V zásade sa jedná o informácie utajené až po úroveň EÚ TAJNÉ vrátane; nevzťahuje sa to na utajované informácie chránené zvláštnymi bezpečnostnými označeniami a znakmi.

3. Komisia zváži primeranosť zverejnenia utajovaných informácií, posúdi potrebu príjemcu oboznámenia sa a rozhodne o povahe utajovaných informácií, ktoré sa môžu komunikovať.

4. Ak je komisia za, člen komisie zodpovedný za bezpečnostné záležitosti

- získa stanovisko pôvodcov utajovaných informácií EÚ, ktoré sa majú zverejniť;
- zabezpečí zasadnutie poradnej skupiny komisie pre bezpečnostnú politiku alebo tichým postupom, ak bude potrebné, sa informuje u národných bezpečnostných úradov členských štátov ohľadne získania stanoviska poradnej skupiny komisie pre bezpečnostnú politiku.

5. Stanovisko poradnej skupiny komisie pre bezpečnostnú politiku sa týka:

- (a) vyhodnotenia bezpečnostných rizík, ktoré vzniknú EÚ alebo jej členským štátom;
- (b) úrovne utajovania informácií, ktoré sa môžu zverejniť;
- (c) zníženia úrovne utajenia alebo odtajnenia pred tým, ako sa informácia zverejní;
- (d) postupov pre manipuláciu s dokumentmi, ktoré sa majú zverejniť (pozri odsek nižšie);
- (e) možných metód prenosu (použitie verejných poštových služieb, verejných alebo bezpečnostných telekomunikačných systémov, diplomatických vriec, preverených kuriérov atď.).

6. Dokumenty, ktoré sa zverejnia štátom alebo organizáciám, na ktoré sa vzťahuje tento dodatok, musia byť v zásade pripravené bez odkazu na zdroj alebo utajenie EÚ. Poradná skupina komisie pre bezpečnostnú politiku môže odporúčať:

- použitie osobitného označenia alebo kódového mena;
- použitie osobitného systému klasifikácie, ktorý spája citlivosť informácií s požadovanými kontrolnými opatreniami metód príjemcu na prenos dokumentov.

7. Predseda postúpi komisii stanovisko poradnej skupiny komisie pre bezpečnostnú politiku na rozhodnutie.

8. Po schválení komisie zverejnenia utajovaných informácií EÚ a praktických vykonávajúcich postupov, bezpečnostný úrad komisie zabezpečí potrebný kontakt s bezpečnostným orgánom daného štátu alebo organizácie, aby sa umožnilo uplatnenie predpokladaných bezpečnostných opatrení.

9. Člen komisie zodpovedný za bezpečnostné opatrenia informuje členské štáty o povahe a utajení informácií, pričom uvedie zoznam krajín a organizácií, ktorým sa dané informácie môžu zverejniť, ako o tom rozhodla komisia.

10. Bezpečnostný úrad komisie prijme všetky potrebné opatrenia, aby sa umožnil odhad následnej škody a preskúmali postupy.

Ak sa zmenia podmienky spolupráce, komisia záležitosť opätovne zváži.

#### BEZPEČNOSTNÉ USTANOVENIA, KTORÉ MUSIA UPLATŇOVAŤ PRÍJEMCOVIA

11. Člen komisie zodpovedný za bezpečnostné záležitosti oznámi prijímajúcim štátom alebo medzinárodným organizáciám rozhodnutie komisie o schválení zverejnenia utajovaných informácií EÚ a jeho obmedzeniach, spolu s podrobnými pravidlami ochrany, ktoré navrhla a schválila poradná skupina komisie pre bezpečnostnú politiku.

12. Rozhodnutie nadobúda účinnosť až vtedy, keď príjemcovia predložia písomné uistenie, že:

- nepoužijú informácie na iné účely ako účely, o ktorých rozhodla komisia;
- informácie budú chrániť tak, ako to vyžaduje komisia.

#### 13. Prenos dokumentov

(a) Dohodnú sa praktické postupy pre prenos dokumentov medzi bezpečnostným úradom komisie a bezpečnostnými orgánmi prijímajúcich štátov alebo medzinárodných organizácií. Takéto postupy špecifikujú najmä presné adresy, na ktoré sa dohody musia doručovať.

(b) Dokumenty EÚ DÔVERNÉ a vyššej úrovne utajenia sa musia prenášať v dvojitom obale. Vnútorňa obálka je označená zvláštnou pečiatkou alebo kódovým označením, o ktorom sa rozhodne, a uvádza zvláštne utajenie schválené pre dokument. Pre každý utajený dokument sa zvlášť priloží tlačivo o prijíme. Tlačivo o prijíme, ktoré samo o sebe

nie je utajované, uvádza iba údaje o dokumente (jeho referenčné označenie, dátum, číslo kópie) a jazyk, ale nie názov.

(c) Do vonkajšej obálky sa potom vloží vnútorná obálka. Na vonkajšej obálke je uvedené číslo zásielky pre účely príjmu. Bezpečnostné utajenie nie je na vonkajšej obálke uvedené.

(d) Kuriérom sa vždy odovzdá potvrdenie o príjme, na ktorom je uvedené číslo zásielky.

#### 14. Registrácia pri príchode

Národný bezpečnostný úrad štátu adresáta alebo jeho ekvivalent v štáte, ktorý obdrží v mene vlády utajované informácie postúpené komisiou, alebo bezpečnostný úrad prijímajúcej medzinárodnej organizácie ustanovia zvláštny register na zaznamenávanie utajovaných informácií EÚ pri ich príchode. Register obsahuje stĺpce uvádzajúce dátum prijatia, údaje od dokumente (dátum, referenčné číslo a číslo kópie), jeho utajenie, názov, meno adresáta alebo jeho postavenie, dátum návratu potvrdenia o príjme a dátum návratu dokumentu do EÚ alebo jeho likvidácie.

#### 15. Použitie a ochrana vymenených utajovaných informácií

(a) S informáciami na úrovni EÚ TAJNÉ narábajú zvláštno určení úradníci, ktorí majú oprávnenie na prístup k informáciám s takýmto utajením. Uschovávajú sa v kvalitných bezpečnostných kartotékach, ktoré môžu otvoriť iba osoby s oprávnením na prístup k informáciám, ktoré obsahujú. Oblasti, v ktorých sú takéto kartotéky umiestnené, musia byť sústavne strážené a musí byť zavedený overovací systém, aby sa zabezpečilo, že iba príslušne oprávnené osoby vstúpia do tejto oblasti. Informácie úrovne EÚ TAJNÉ sa doručujú v diplomatických vreciach, bezpečnostnými poštovými službami alebo bezpečnostnými komunikáciami. Dokument EÚ tajný sa môže kopírovať iba s písomným súhlasom úradu pôvodcu. Všetky kópie musia byť zaregistrované a monitorujú sa. Pre všetky operácie týkajúce sa dokumentov EÚ TAJNÉ sa vydávajú potvrdenia o príjme;

(b) S informáciami EÚ DÔVERNÉ narábajú príslušne menovaní úradníci oprávnení na to, aby boli poučení o danom predmete. Dokumenty sa uschovávajú v uzamknutých bezpečnostných kartotékach v kontrolovaných oblastiach;

Informácie úrovne DÔVERNÉ sa doručujú v diplomatických vreciach, bezpečnostnými poštovými službami alebo bezpečnostnými komunikáciami. Dokument EÚ tajný môže prijímajúci orgán kopírovať, pričom počty kópií a ich distribúcia sa zaznamenáva v zvláštnych registroch;

(c) S informáciami EÚ VYHRADENÉ sa narába v priestoroch, ku ktorým nemajú prístup neoprávnené osoby, a uschovávajú sa v uzavretých schránkach. Dokumenty sa môžu zasielať verejnými poštovými službami ako doporučená pošta v dvojitej obálke a v núdzových situáciách počas operácií nechránenými verejnými telekomunikačnými systémami. Prijemcovia môžu zhotovovať kópie;

(d) Neutajené informácie nevyžadujú zvláštno ochranné opatrenia a môžu sa zasielať poštovými službami a verejnými telekomunikačnými systémami. Adresáti môžu zhotovovať kópie.

#### 16. Likvidácia

Dokumenty, ktoré už nie sú potrebné, sa musia zlikvidovať. V prípade dokumentov EÚ VYHRADENÉ a EÚ DÔVERNÉ sa vykoná príslušný záznam v zvláštnom registri. V prípade dokumentov EÚ TAJNÉ sa vydávajú potvrdenia o likvidácii, ktoré podpíšu dve osoby, ktoré boli svedkami likvidácie.

#### 17. Porušenie bezpečnosti

Ak sa informácie EÚ DÔVERNÉ alebo EÚ TAJNÉ odcudzia, alebo ak existuje podozrenie z odcudzenia, národný bezpečnostný úrad daného štátu alebo vedúci bezpečnosti príslušnej organizácie uskutočnia vyšetrovanie okolností odcudzenia. Bezpečnostnému úradu komisie sa oznámi výsledok vyšetrovania. Prijmú sa potrebné kroky na odstránenie nevhodných postupov alebo skladovacích metód, ak takéto postupy alebo metódy boli príčinou odcudzenia.

*DODATOK 6*

## ZOZNAM SKRATIEK

ACPC	Poradný výbor pre obstarávanie a zmluvy
CrA	Úrad pre kódovanie
CISO	Centrálny informačný bezpečnostný referent
COMPUSEC	Počítačová bezpečnosť
COMSEC	Komunikačná bezpečnosť
CSO	Bezpečnostný úrad komisie
ESDP	Európska bezpečnostná a obranná politika
EUCI	Utajované informácie EÚ
IA	Úrad INFOSEC
INFOSEC	Informačná bezpečnosť
IO	Majiteľ informácií
ISO	Medzinárodná organizácia pre normalizáciu
IT	Informačná technológia
LISO	Miestny informačný bezpečnostný referent
LSO	Miestny bezpečnostný referent
MSO	Bezpečnostný referent zasadnutia
NSA	Národný bezpečnostný úrad
PC	Osobný počítač
RCO	Kontrolný referent registra
SAA	Bezpečnostný akreditačný úrad
SecOPS	Bezpečnostné prevádzkové postupy
SSRS	Vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke
TA	Úrad pre búrkové poruchy
TSO	Majiteľ technických systémov