Tento dokument slúži čisto na potrebu dokumentácie a inštitúcie nenesú nijakú zodpovednosť za jeho obsah

►**B**

ROZHODNUTIE KOMISIE

z 29. novembra 2001,

ktorým sa mení a dopĺňa jej rokovací poriadok

(oznámené pod číslom dokumentu C(2001) 3031)

(2001/844/ES, ESUO, Euratom)

(Ú. v. ES L 317, 3.12.2001, s. 1)

Zmenené a doplnené:

		Úradný vestník		
		Č.	Strana	Dátum
►**M1**	Rozhodnutie Komisie 2005/94/ES, Euratom z 3. februára 2005	L 31	66	4.2.2005
►**M2**	Rozhodnutie Komisie 2006/70/ES, Euratom z 31. januára 2006	L 34	32	7.2.2006
►**M3**	Rozhodnutie Komisie 2006/548/ES, Euratom z 2. augusta 2006	L 215	38	5.8.2006
►**M4**	Nariadenie Komisie (EÚ) č. 519/2013 z 21. februára 2013	L 158	74	10.6.2013

▼B

ROZHODNUTIE KOMISIE

z 29. novembra 2001,

ktorým sa mení a dopĺňa jej rokovací poriadok

(oznámené pod číslom dokumentu C(2001) 3031)

(2001/844/ES, ESUO, Euratom)

KOMISIA EURÓPSKYCH SPOLOČENSTIEV,

so zreteľom na Zmluvu o založení Európskeho spoločenstva, najmä na jej článok 218 ods. 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 ods. 1 a článok 41 ods. 1,

ROZHODLA TAKTO:

Článok 1

Ustanovenia Komisie o bezpečnosti, ktorých znenie je priložené k tomuto rozhodnutiu, sa týmto pripájajú k rokovaciemu poriadku Komisie ako príloha.

Článok 2

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

Uplatňuje sa od 1. decembra 2001.

▼B

PRÍLOHA

USTANOVENIA KOMISIE O BEZPEČNOSTI

Keďže:

(1) Aby sa rozvíjali činnosti spoločenstva v oblastiach, ktoré vyžadujú určitý stupeň dôvernosti, je vhodné, aby sa zaviedol komplexný bezpečnostný systém platný pre Komisiu, ostatné orgány, inštitúcie, úrady a agentúry zriadené podľa alebo na základe Zmluvy o založení ES alebo Zmluvy o Európskej únii, členské štáty rovnako ako akéhokoľvek iného príjemcu utajovaných skutočností Európskej únie, ďalej len „utajované skutočnosti EÚ“.

(2) Aby sa zabezpečila účinnosť bezpečnostného systému takto vytvoreného, Komisia sprístupní utajované skutočnosti 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, ktorým sa vykonáva článok 24 Zmluvy o založení Európskeho spoločenstva pre atómovú energiu [1], nariadenie Rady (ES) č. 1588(90) z 11. júna 1990 o prenose údajov, ktoré podliehajú štatistickému utajovaniu, do Štatistického úradu Európskych spoločenstiev [2], a rozhodnutie Komisie C(95) 1510 konečné z 23. novembra 1995 o ochrane informačných systémov.

(4) Bezpečnostný systém Komisie je založený na zásadách, ktoré sú uvedené v rozhodnutí Rady 2001/264/ES z 19. marca 2001, ktorým sa prijímajú bezpečnostné predpisy Rady [3] s cieľom zabezpečiť hladké fungovanie procesov rozhodovania únie.

(5) Komisia podčiarkuje dôležitosť prípadného stotožnenia sa ostatných orgánov 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 orgánu.

(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 prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie [4].

▼M2

(8) Tieto ustanovenia sa nedotýkajú článku 286 zmluvy a nariadenia Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov.

▼B

Článok 1

Bezpečnostné predpisy Komisie sú uvedené v prílohe.

---

[1] Ú. v. ES 17/58, 6.10.1958, s. 406/58.
[2] Ú. v. ES L 151, 15.6.1990, s. 1.
[3] Ú. v. ES L 101, 11.4.2001, s. 1.
[4] Ú. v. ES L 145, 31.5.2001, s. 43.

▼B

Článok 2

1. Člen Komisie zodpovedný za bezpečnostné záležitosti prijme primerané opatrenia, aby zabezpečil, že úradníci a ostatní zamestnanci Komisie a pridelení zamestnanci Komisie budú pri narábaní s utajovanými skutočnosťami v rámci Komisie rovnako ako v rámci všetkých priestorov Komisie vrátane reprezentácií a úradov v únii a jej delegácií v tretích krajinách, a externí dodávatelia Komisie dodržiavať predpisy uvedené v článku 1.

▼M3

Ak zmluva alebo dohoda o poskytnutí grantu medzi Komisiou a externým dodávateľom alebo príjemcom predpokladá spracovanie utajovaných skutočností EÚ v priestoroch dodávateľa alebo príjemcu, primerané opatrenia, ktoré má uvedený externý dodávateľ alebo príjemca prijať na zabezpečenie dodržania pravidiel podľa článku 1 v prípade narábania s utajovanými skutočnosťami EÚ, tvoria neoddeliteľnú súčasť zmluvy alebo dohody o poskytnutí grantu.

▼B

2. Členské štáty, iné orgány, inštitúcie, úrady a agentúry zriadené podľa zmlúv alebo na ich základe sú oprávnené obdržať utajované skutočnosti pod podmienkou, že zabezpečia, aby sa pri narábaní s utajovanými skutočnosťami v rámci ich útvarov a priestorov dodržiavali predpisy rovnocenné s predpismi, ktoré sú uvedené v článku 1, najmä, aby ich dodržiavali:

a) členovia stálych reprezentácií členských štátov v Európskej únii rovnako ako členovia ich národných delegácií, ktorí sa zúčastňujú zasadnutí Komisie alebo jej orgánov, alebo ktorí sa zúčastňujú iných činností Komisie;

b) ostatní členovia národných správ členských štátov, ktoré narábajú s utajovanými skutočnosťami, bez ohľadu na to, či pôsobia na území členského štátu alebo v zahraničí;

c) externí dodávatelia a pridelení zamestnanci, ktorí narábajú s utajovanými skutočnosťami EÚ.

Článok 3

Tretie štáty, organizácie a iné orgány môžu obdržať utajované skutočnosti pod podmienkou, že zabezpečia, aby sa pri narábaní s takýmito utajovanými skutočnosťami dodržiavali predpisy, ktoré sú rovnocenné s predpismi uvedenými v článku 1.

Článok 4

Pri dodržaní základných zásad a minimálnych noriem bezpečnosti uvedených v prvej časti tejto prílohy môže člen Komisie, ktorý je zodpovedný za bezpečnostné záležitosti prijať opatrenia v súlade s druhou časťou tejto prílohy.

Článok 5

Tieto ustanovenie odo dňa ich uplatňovania nahrádzajú:

a) rozhodnutie Komisie C(94) 3282 z 30. novembra 1994 o bezpečnostných opatreniach vzťahujúcich sa na utajované skutočnosti, 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, na základe ktorých majú úradníci a iní zamestnanci Európskej Komisie povolený prístup k utajovaným skutočnostiam, ktoré má Komisia k dispozícii.

▼B

Článok 6

Od dátumu uplatňovania týchto ustanovení všetky utajované skutočnosti, ktoré má Komisia k dispozícii k tomuto dátumu s výnimkou utajovaných skutočností Euratom:

a) ak ich vytvorila Komisia, sa automaticky považujú za prekvalifikované na VYHRADENÉ SKUTOČNOSTI EÚ, pokiaľ ich pôvodca do 31. januára 2002 nerozhodne, že sa im pridelí iné utajenie. V takomto prípade pôvodca musí informovať všetkých adresátov príslušného dokumentu;

b) ak ich vytvorili pôvodcovia mimo Komisie, ponechajú si svoje pôvodné utajenie, a preto sa budú považovať za utajované skutočnosti EÚ rovnocenného stupňa, pokiaľ pôvodca nebude súhlasiť so zrušením stupňa utajenia alebo pridelením nižšieho stupňa utajenia.

▼B

PRÍLOHA

BEZPEČNOSTNÉ PREDPISY

Obsah

PRVÁ I:	**ZÁKLADNÉ ZÁSADY A MINIMÁLNE BEZPEČNOSTNÉ NORMY**
1.	ÚVOD
2.	VŠEOBECNÉ ZÁSADY
3.	ZÁKLADY BEZPEČNOSTI
4.	ZÁSADY INFORMAČNEJ BEZPEČNOSTI
4.1.	**Ciele**
4.2.	**Vymedzenie pojmov**
4.3.	**Utajovanie**
4.4.	**Ciele bezpečnostných opatrení**
5.	ORGANIZÁCIA BEZPEČNOSTI
5.1	**ORGANIZÁCIA BEZPEČNOSTI**
5.2.	**Organizácia**
6.	PERSONÁLNA BEZPEČNOSŤ
6.1.	**Bezpečnostné previerky personálu**
6.2.	**Záznamy o bezpečnostných previerkach personálu**
6.3.	**Bezpečnostné pokyny pre personál**
6.4.	**Zodpovednosti riadenia**
6.5.	**Bezpečnostné postavenie personálu**
7.	FYZICKÁ BEZPEČNOSŤ
7.1.	**Potreba ochrany**
7.2.	**Kontrolovanie**
7.3.	**Bezpečnosť budov**
7.4.	**Havarijné plány**
8.	BEZPEČNOSŤ UTAJOVANÝCH SKUTOČNOSTÍ
9.	BOJ PROTI SABOTÁŽI A KONTROLA INÝCH FORIEM ZLOMYSEĽNÝCH ŠKÔD
10.	POSKYTNUTIE UTAJOVANÝCH SKUTOČNOSTÍ 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
14.	►**M2** RIADITEĽSTVO KOMISIE PRE BEZPEČNOSŤ ◄
15.	BEZPEČNOSTNÉ INŠPEKCIE
16.	UTAJOVANIE, VYMEDZENIE UTAJENIA A OZNAČOVANIE
16.1.	**Stupne utajenia**

▼B

16.2. **Bezpečnostné vymedzenie utajenia**

16.3. **Označovanie**

16.4. **Uvedenie utajenia**

16.5. **Uvedenie bezpečnostného vymedzenia utajenia**

17. RIADENIE UTAJOVANIA

17.1. **Všeobecne**

17.2. **Uplatňovanie utajovania**

17.3. **Zníženie stupňa utajenia a zrušenie stupňa utajenia**

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 ZÁSADY „POTREBA POZNAŤ“ A BEZPEČNOSTNÉ PREVIERKY PERSONÁLU EÚ

19.1. **Všeobecne**

19.2. **Osobitné pravidlá o prístupe k utajovaným skutočnostiam ►M1 TRES SECRET UE/EU TOP SECRET ◄**

19.3. **Osobitné pravidlá o prístupe k utajovaným skutočnostiam ►M1 SECRET UE ◄ a utajovaným skutočnostiam ►M1 CONFIDENTIEL UE ◄**

19.4. **Osobitné pravidlá o prístupe k utajovaným skutočnostiam ►M1 RESTREINT UE ◄**

19.5. **Presuny**

19.6. **Osobitné pokyny**

▼B

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 SKUTOČNOSTÍ EÚ

21.1. **Príprava**

21.2. **Distribúcia**

21.3. **Prenášanie utajovaných dokumentov EÚ**

21.3.1. *Balenie, príjem*

21.3.2. *Prenášanie v rámci budovy alebo skupiny budov*

21.3.3. *Prenášanie v rámci krajiny*

21.3.4. *Prenášanie zo štátu do štátu*

21.3.5. *Prenášanie dokumentov EÚ vyhradené*

21.4. **Bezpečnosť kuriérov**

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

21.6. **Zvláštne kópie a preklady výpisov a výpisy z utajovaných dokumentov EÚ**

22. REGISTRE UTAJOVANÝCH SKUTOČNOSTÍ EÚ, PREHLIADKY, KONTROLY, ARCHÍVNE SKLADOVANIE A LIKVIDÁCIA UTAJOVANÝCH SKUTOČNOSTÍ EÚ

22.1. **Miestne registre utajovaných skutočností EÚ**

22.2. **Register utajovaných skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄**

22.2.1. *Všeobecne*

22.2.2. *Centrálny register utajovaných skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄*

22.2.3. *Vedľajšie registre utajovaných skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄*

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

22.4. **Archívne skladovanie utajovaných dokumentov EÚ**

22.5. **Likvidácia utajovaných dokumentov EÚ**

22.6. **Likvidácia v naliehavých situáciách**

23. BEZPEČNOSTNÉ OPATRENIA PRE OSOBITNÉ ZASADNUTIA, KTORÉ SA KONAJÚ MIMO PRIESTOROV KOMISIE A ZAHŕŇAJÚ UTAJOVANÉ SKUTOČNOSTI EÚ

23.1. **Všeobecne**

23.2. **Právomoci**

23.2.1. ►M2 *Riaditeľstvo Komisie pre bezpečnosť* ◄

23.2.2. *Bezpečnostný úradník zasadnutia (MSO)*

23.3. **Bezpečnostné opatrenia**

23.3.1. *Bezpečnostné oblasti*

23.3.2. *Priepustky*

23.3.3. *Kontrola fotografického a audio zariadenia*

▼B

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 skutočností EÚ*

24. PORUŠENIE BEZPEČNOSTI A OHROZENIE UTAJOVANÝCH SKUTOČNOSTÍ EÚ

24.1. **Vymedzenie pojmov**

24.2. **Hlásenie porušenia bezpečnosti**

24.3. **Právne opatrenia**

25. OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ EÚ, S KTORÝMI SA NARÁBA V INFORMAČNEJ TECHNOLÓGII 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 (OSBP)*

25.1.5. *Bezpečnostné režimy prevádzky*

25.2. **Vymedzenie pojmov**

25.3. **Bezpečnostné právomoci**

25.3.1. *Všeobecne*

25.3.2. *Bezpečnostný akreditačný úrad (BAÚ)*

25.3.3. *Úrad INFOBEZ (IÚ)*

25.3.4. *Vlastník technických systémov (VTS)*

25.3.5. *Vlastník utajovaných skutočností (VUS)*

25.3.6. *Užívatelia*

25.3.7. *Odborné vzdelávanie INFOBEZ*

25.4. **Iné ako technické bezpečnostné opatrenia**

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 utajovaných skutočností*

25.5.2. *Kontrola a zodpovednosť za utajované skutočnosti*

25.5.3. *Manipulácia a kontrola odstrániteľných počítačových uložných médií*

▼B

25.5.4. *Zrušenie stupňa utajenia a likvidácia počítačových úložných 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 škodného softwaru/počítačových vírusov*

25.6.4. *Údržba*

25.7. **Verejné obstarávanie**

25.7.1. *Všeobecne*

25.7.2. *Akreditácia*

25.7.3. *Vyhodnotenie a certifikácia*

25.7.4. *Bežná kontrola bezpečnostných funkcií pre neustálu akreditáciu*

25.8. **Dočasné alebo príležitostné použitie**

25.8.1. *Bezpečnosť mikropočítačov/osobných počítačov*

25.8.2. *Použitie súkromného informačného systému pre oficiálnu prácu Komisie*

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

26. POSKYTNUTIE UTAJOVANÝCH SKUTOČNOSTÍ EÚ TRETÍM ŠTÁTOM ALEBO MEDZINÁRODNÝM ORGANIZÁCIÁM

26.1.1. *Zásady, ktorými sa riadi poskytovanie utajovaných skutočností EÚ*

26.1.2. *Úrovne*

26.1.3. *Dohody o bezpečnosti*

DODATOK 1: **Porovnanie národných stupňov bezpečnostného utajenia**

DODATOK 2: **Praktický návod na utajovanie**

DODATOK 3: **Usmernenia o poskytovaní utajovaných skutočností EÚ tretím štátom alebo medzinárodným organizáciám: Úroveň spolupráce 1**

DODATOK 4: **Usmernenia o poskytovaní utajovaných skutočností EÚ tretím štátom alebo medzinárodným organizáciám: Úroveň spolupráce 2**

DODATOK 5: **Usmernenia o poskytovaní utajovaných skutočností EÚ tretím štátom alebo medzinárodným organizáciám: Úroveň spolupráce 3**

DODATOK 6: **Zoznam skratiek**

▼B

PRVÁ I: ZÁKLADNÉ ZÁSADY A MINIMÁLNE BEZPEČNOSTNÉ NORMY

1. ÚVOD

Tieto ustanovenia určujú základné zásady a minimálne bezpečnostné normy, ktoré Komisia musí primeraným spôsobom rešpektovať na všetkých úrovniach zamestnania, rovnako ako všetci príjemcovia utajovaných skutočnosti EÚ (USEÚ) tak, aby sa zaručila bezpečnosť a všetci zainteresovaní si mohli byť istí, že je zabezpečená spoločná 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 zákonnosť, transparentnosť, zodpovednosť a subsidiaritu (proporcionalitu).

Zákonnosť predstavuje potrebu zostať striktne v právnom rámci pri vykonávaní bezpečnostných funkcií a potrebu byť v súlade s právnymi požiadavkami. Znamená to tiež, že zodpovednosti v oblasti bezpečnosti musia vychádzať z náležitých právnych ustanovení. Ustanovenia v personálnom poriadku sa plne uplatňujú, najmä jeho článok 17 o povinnosti zamestnancov uplatňovať rozvážnosť s ohľadom na utajované skutočnosti Komisie a jeho hlavu VI o disciplinárnych opatreniach. Napokon, zákonnosť 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 trestnej legislatívy.

Transparentnosť predstavuje potrebu jednoznačnosti v súvislosti so všetkými bezpečnostnými predpismi, rovnováhy medzi rozličnými útvarmi a rozličnými oblasťami (fyzická bezpečnosť oproti ochrane utajovaných skutočností atď.) a potrebu dôslednej a štruktúrovanej politiky, ktorá sa týka bezpečnostného povedomia. Vymedzuje tiež potrebu jasných písomných usmernení na zavedenie bezpečnostných opatrení.

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

Subsidiarita alebo proporcionalita znamená, že bezpečnosť sa musí organizovať na najnižšej možnej úrovni a čo najbližšie ku generálnym riaditeľstvám a útvarom Komisie. Tiež predstavuje skutočnosť, 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 činnostiach, a

   2. poskytovanie informácií a rád vláde a prostredníctvom tohto Komisii o povahe bezpečnostných hrozieb a o prostriedkoch proti ich ochrane.

▼B

b) V rámci každého členského štátu a v rámci Komisie technický orgán INFOBEZ (IO) 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 úradmi a zodpovedajúcimi útvarmi európskych orgánov, aby sa stanovilo resp. odporúčalo:

1. ktoré osoby, informácie a zdroje sa musia chrániť a

2. spoločné normy ochrany.

d) Úzka spolupráca medzi ►M2 riaditeľstvom Komisie pre bezpečnosť ◄ a bezpečnostnými službami ostatných európskych orgánov a s Bezpečnostným úradom NATO (BÚN).

4. ZÁSADY INFORMAČNEJ BEZPEČNOSTI

4.1. **Ciele**

Informačná bezpečnosť má tieto hlavné ciele:

a) chrániť utajované skutočnosti EÚ (USEÚ) pred špionážou, ohrozením alebo neoprávneným sprístupnením;

b) chrániť utajované skutočnosti EÚ, s ktorými sa narába v komunikačných a informačných systémoch a sieťach, pred ohrozením ich dôvernosti, celistvosti a dostupnosti;

c) chrániť priestory Komisie, v ktorých sa uchovávajú utajované skutočnosti EÚ, pred sabotážou a zlomyseľným poškodením;

d) v prípade zlyhania posúdiť spôsobenú škodu, obmedziť jej dôsledky a prijať potrebné nápravné opatrenia.

4.2. **Vymedzenie pojmov**

Na účely týchto ustanovení:

a) Výraz „utajované skutočnosti EÚ“ (USEÚ) znamená ľubovoľnú informáciu a materiál, ktorých neoprávnené sprístupnenie by mohlo spôsobiť rozličné stupne poškodenia záujmov EÚ alebo jednému alebo viacerým jej členským štátom, tiež keď takáto utajovaná skutočnosť pochádza z EÚ alebo sa prijme z členských štátov, tretích štátov alebo medzinárodných organizácií.

b) Výraz „dokument“ znamená ľubovoľný list, poznámku, zápisnicu, správu, memorandum, signál/odkaz, náčrt, fotografiu, diapozitív, film, mapu, tabuľku, plán, zápisník, šablónu, prepisovací papier, písací stroj alebo pásku do písacieho stroja, magnetofónovú pásku, kazetu, počítačový disk, CD-ROM alebo iný hmotný nosič, na ktorom sa zaznamenala informácia.

c) Výraz „materiál“ znamená „dokument“ ako je vymedzený v b) a tiež ľubovoľná časť zariadenia, už vyrobeného alebo v procese výroby.

d) Výraz „potreba poznať“ znamená potrebu jednotlivého zamestnanca mať prístup k utajovaným skutočnostiam EÚ, aby mohol vykonávať funkciu alebo úlohu.

e) „Oprávnenie“ znamená rozhodnutie ►M2 riaditeľa Riaditeľstva Komisie pre bezpečnosť ◄ udeliť jednotlivcovi prístup k USEÚ až do príslušného stupňa na základe pozitívneho preverenia v rámci bezpečnostnej previerky, ktoré vykoná Národný bezpečnostný úrad podľa vnútroštátnych právnych predpisov.

▼B

f) Výraz „utajovanie“ znamená pridelenie primeraného stupňa bezpečnosti pre dané utajované skutočnosti, ktorých neoprávnené sprístupnenie môže spôsobiť určitý stupeň škody pre Komisiu alebo záujmy členských štátov.

g) Výraz „zníženie“ (déclassement) znamená zníženie stupňa utajenia.

h) Výraz „zrušenie stupňa utajenia“ (déclassification) znamená zrušenie akéhokoľvek stupňa utajenia.

i) Výraz „pôvodca“ znamená oprávneného autora utajených dokumentov. V rámci Komisie môžu vedúci úradov oprávniť svojich zamestnancov, aby vytvorili USEÚ.

j) Výraz „úrady Komisie“ znamená úrady a útvary Komisie, vrátane kancelárií, na všetkých miestach zamestnanosti, vrátane spoločného výskumného centra, reprezentácií a úradov v únii 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 potrebe jednotlivých informácií a materiálu, ktorý treba chrániť. Aby sa zabezpečil hladký tok informácií, prijmú sa opatrenia, aby sa vyhlo 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 skutočnosti, a najdôležitejšie body v rámci takýchto priestorov.

c) Zodpovednosť za utajovanie informácií spočíva výlučne na pôvodcovi danej informácie.

d) Stupeň utajenia môže závisieť výlučne na obsahu danej informácie.

e) Ak je viacero informácií spolu zoskupených, stupeň utajenia, ktorý sa vzťahuje na celok, musí byť aspoň na takom stupni, ako je najvyšší stupeň utajenia. Súbor informácií však môže mať pridelený vyšší stupeň utajenia, ako jeho jednotlivé časti.

f) Utajovanie sa prideľuje iba vtedy, ak je potrebné a na dobu, na akú je to potrebné.

4.4. **Cieľ bezpečnostných opatrení**

Bezpečnostné opatrenia:

a) sa vzťahujú na všetky osoby, ktoré majú prístup k utajovaným skutočnostiam, médiá prenášajúce utajované skutočnosti, všetky priestory, v ktorých sa nachádzajú takéto utajované skutočnosti a dôležitým zariadenia;

b) sú navrhnuté tak, aby sa zistili osoby, ktorých postavenie môže ohroziť bezpečnosť utajovaných skutočností a dôležitých zariadení, ktoré uchovávajú utajované skutočnosti, a umožnili vylúčenie alebo odvolanie takýchto osôb;

▼B

c) zabraňujú nepovolanej osobe v prístupe k utajovaným skutočnostiam alebo zariadeniam, ktoré ich obsahujú;

d) zabezpečujú, aby sa utajované skutočnosti rozširovali výlučne na základe zásady „potreba poznať“, ktorá je zásadná pre všetky aspekty bezpečnosti;

e) zabezpečujú celistvosť (prevencia pred zneužitím alebo neoprávnenou zmenou alebo neoprávneným vymazaním) a dostupnosť (t. j. prístup nie je zamietnutý tým, ktorí majú prístup) všetkých skutočností, utajovaných aj neutajovaných, a najmä takých skutočností, ktoré sa uchovávajú, spracovávajú alebo prenášajú v elektromagnetickej forme.

5. ORGANIZÁCIA BEZPEČNOSTI

5.1. **Všeobecné minimálne normy**

Komisia zabezpečuje, aby všeobecné minimálne normy bezpečnosti dodržiavali všetci príjemcovia USEÚ v vnútri orgánov a podľa svojich právomocí, napríklad všetky úrady a dodávatelia tak, aby utajované skutočnosti EÚ bolo možné odovzdať ako dôverné, s ktorými sa budú oboznamovať s rovnakou starostlivosťou. Takéto minimálne normy zahŕňajú kritériá udeľovania oprávnení pre personál a postupy na ochranu utajovaných skutočnosti EÚ.

Komisia umožní prístup k USEÚ vonkajším orgánom iba za podmienky, že zabezpečia, aby sa pri oboznamovaní sa s USEÚ dodržiavali ustanovenia aspoň na rovnocennej úrovni, ako je úroveň týchto minimálnych noriem.

▼M3

Tieto minimálne normy sa uplatňujú takisto v prípade, ak Komisia na základe zmluvy alebo dohody o poskytnutí grantu zverí úlohy zahŕňajúce, predpokladajúce a/alebo obsahujúce utajované skutočnosti EÚ priemyselným alebo iným subjektom: tieto spoločné minimálne normy sú uvedené v časti II oddiele 27.

▼B

5.2. **Organizácia**

V rámci Komisie sa bezpečnosť organizuje na dvoch úrovniach:

a) Na úrovni Komisie ako celku existuje ►M2 riaditeľstvo Komisie pre bezpečnosť ◄ s Bezpečnostným akreditačným orgánom (BAO), ktorý pôsobí tiež ako orgán pre kódovanie (OK) a ako orgán TEMPEST, a s orgánom INFOBEZ (IO) a jeden alebo viacero centrálnych registrov USEÚ, pričom každý z nich má jedného alebo viacerých registračných kontrolných úradníkov (RKÚ).

b) Na úrovni úradov Komisie zodpovednosť za bezpečnosť spočíva na jednom alebo viacerých miestnych bezpečnostných úradníkoch, jednom alebo viacerých centrálnych informačných bezpečnostných úradníkoch, miestnych informačných bezpečnostných úradníkoch a miestnych registroch utajovaných skutočností EÚ s jedným alebo viacerými registračnými kontrolnými úradníkmi.

c) Ústredné bezpečnostné orgány zabezpečia pre miestne bezpečnostné orgány prevádzkové usmernenia.

6. PERSONÁLNA BEZPEČNOSŤ

6.1. **Bezpečnostné previerky personálu**

Všetky osoby, ktoré žiadajú o prístup k utajovaným skutočnostiam ►M1 CONFIDENTIEL UE ◄ alebo vyššieho stupňa, musia byť primerane preverené skôr, ako sa im takýto prístup povolí. Podobné preverenie sa vyžaduje v prípade osôb, ktorých povinnosti zahŕňajú technickú prevádzku alebo údržbu komunikačných a informačných systémov obsahujúcich utajované skutočnosti. Toto preverenie sa vykonáva tak, aby sa určilo, či takíto jednotlivci:

a) majú nespochybnenú lojalitu;

▼B

b) majú takú povahu a rozvahu, že niet pochýb o ich bezúhonnosti pri narábaní s utajovanými skutočnosťami, alebo

c) môžu podľahnúť tlaku zahraničných alebo iných zdrojov.

Osobitná pozornosť pri preverovaní v rámci bezpečnostných previerok sa musí uplatniť v prípade osôb:

d) ktorým sa má povoliť prístup k utajovaným skutočnostiam ►M1 TRES SECRET UE/EU TOP SECRET ◄;

e) ktoré sú na pozíciách, ktoré zahŕňajú pravidelný prístup k značnému množstvu utajovaných skutočností ►M1 SECRET UE ◄;

f) ktorých povinnosti im dávajú osobitný prístup k bezpečnostným komunikačným alebo informačným systémom, a tak majú možnosť získať neoprávnený prístup k veľkému množstvu utajovaných skutočností EÚ alebo spôsobiť vážnu škodu pri vykonávaní svojej úlohy tým, že vykonali kroky technickej sabotáže.

Za okolností uvedených vyššie v písm. d), e) a f) sa čo najviac využíva technika vyšetrovanie pozadia.

Ak osoby, u ktorých sa neuplatní zásada „potreba poznať“, sú zamestnané za okolností, pri ktorých môžu mať prístup k utajovaným skutočnostiam EÚ (napríklad kuriéri, bezpečnostní agenti, personál zabezpečujúci údržbu alebo upratovanie atď.), musia sa takéto osoby najprv primerane bezpečnostne preveriť.

6.2. **Záznamy o personálnych previerkach**

Všetky úrady Komisie, ktoré sa oboznamujú s utajovanými skutočnosťami EÚ, alebo uchovávajú bezpečnostné komunikačné alebo informačné systémy, musia viesť záznam o previerkach, ktorými prešiel personál pridelený do daného úradu. Všetky previerky sa musia overiť podľa potreby, aby sa zabezpečilo, že sú primerané pre aktuálne pridelenie danej osoby; opätovne sa revidujú podľa potrebnej priority vždy, keď sa prijme nová utajovaná skutočnosť naznačujúca, že pokračujúce pridelenie na práce súvisiace s utajením už nie je viac v súlade so záujmami bezpečnosti. Miestny bezpečnostný úradník úradu Komisie vedie záznam o previerkach v rámci svojej pôsobnosti.

6.3. **Bezpečnostné pokyny pre personál**

Všetci členovia personálu, ktorí sú zamestnaní na pozíciách, kde by mohli mať prístup k utajovaným skutočnostiam, musia byť pri prevzatí úlohy dôsledne inštruovaní a v pravidelných intervaloch podľa potreby o bezpečnosti a postupoch zaručujúcich bezpečnosť. 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 pri práci prichádzajú do styku s utajovanými skutočnosťami, alebo ktorí majú prístup k bezpečnostným komunikačným alebo informačným systémom, a hlásiť akékoľvek prípady alebo zjavné poruchy, o ktorých je pravdepodobné, že majú dopad na bezpečnosť.

6.5. **Bezpečnostné postavenie personálu**

Vypracujú sa postupy, ktoré zabezpečia, že v prípade objavenia sa nepriaznivej informácie o jednotlivcovi, sa určí, či jednotlivec pracuje s utajovanými skutočnosťami alebo má prístup k bezpečnostným komunikačným alebo informačným systémom, a ►M2 riaditeľ Komisie pre bezpečnosť ◄ je o tejto utajovanej skutočnosti informovaný. Ak sa prijme záver, že takýto jednotlivec predstavuje bezpečnostné riziko, pozastaví sa mu vykonávanie danej činnosti alebo sa mu takáto pracovná činnosť odníme, ak by mohol ohroziť bezpečnosť.

▼B

7. FYZICKÁ BEZPEČNOSŤ

7.1. **Potreba ochrany**

Stupeň opatrení fyzickej ochrany, ktoré sa majú uplatňovať, aby sa zabezpečila ochrana utajovaných skutočností EÚ, musí byť primeraný utajeniu, objemu a ohrozeniu vlastnených informácií a materiálu. Všetky osoby, ktoré majú k dispozícii utajované skutočnosti EÚ musia dodržiavať jednotné postupy utajovania skutočností a spĺňať všeobecné normy ochrany ohľadne spravovania, prenosu a likvidovania informácií a materiálov vyžadujúcich si ochranu.

7.2. **Kontrolovanie**

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

7.3 **Bezpečnosť budov**

Budovy, v ktorých sa uchovávajú utajované skutočnosti EÚ alebo bezpečnostné komunikačné alebo informačné systémy, sa chránia proti neoprávnenému prístupu. Povaha ochrany vo vzťahu k utajovaným skutočnostiam 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, množstva 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 vo vzťahu ku komunikačným a informačným systémom podobne závisí od posúdenia hodnoty majetku, o ktorý ide, a potenciálnej škody, ak by došlo k zníženiu stupňa 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 skutočností počas miestnej alebo celoštátnej havarijnej situácie.

8. BEZPEČNOSŤ UTAJOVANÝCH SKUTOČNOSTÍ

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

▼B

9. BOJ PROTI SABOTÁŽI A KONTROLA INÝCH FORIEM ZLOMYSEĽNÝCH ŠKÔD

Fyzické opatrenia na ochranu dôležitých zariadení uchovávajúcich utajované skutočnosti sú najlepšie ochranné bezpečnostné opatrenia proti sabotáži a zlomyseľnému poškodeniu, a samotné previerky personálu nie sú účinnou náhradou. Príslušný vnútroštátny orgán sa požiada, aby poskytol tajné informácie so zreteľom špionáž, sabotáž, terorizmus a inú podvratnú činnosť.

10. POSKYTNUTIE UTAJOVANÝCH SKUTOČNOSTÍ TRETÍM ŠTÁTOM ALEBO MEDZINÁRODNÝM ORGANIZÁCIÁM

Rozhodnutie poskytnúť utajované skutočnosti EÚ pochádzajúce od Komisie tretiemu štátu alebo medzinárodnej organizácii prijíma Komisia ako kolégium. Ak pôvodcom utajovanej skutočnosti, o ktorej poskytnutie sa žiada, nie je Komisia, Komisia najprv získa súhlas pôvodcu s poskytnutím. Ak nie je možné určiť pôvodcu, zodpovednosť pôvodcu prevezme Komisia.

Ak Komisia obdrží utajované skutočnosti od tretích štátov, od medzinárodných organizácií alebo od iných tretích strán, týmto utajovaným skutočnostiam sa pridelí ochrana primeraná ich utajeniu a rovnocenná normám stanoveným v týchto ustanoveniach pre utajované skutočnosti EÚ alebo také vyššie normy, ktorých dodržanie môže prípadne požadovať tretia strana, ktorá takéto utajované skutočnosti poskytuje. Je možné dojednať vzájomné kontroly.

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

DRUHÁ 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 pridelí Komisia alebo jej príslušný orgán;

c) skúma otázky, ktoré súvisia so zmenami v bezpečnostnej politike Komisie v úzkej spolupráci s národnými bezpečnostnými (alebo inými vhodnými) úradmi členských štátov (ďalej len „NBÚ“).

Člen Komisie zodpovedný za bezpečnostné záležitosti je zodpovedný najmä za:

a) koordináciu všetkých bezpečnostných záležitostí, ktoré sa týkajú činností Komisie;

b) postúpenie žiadostí určeným úradom členských štátov, aby NBÚ zabezpečili bezpečnostné previerky personálu zamestnaného v Komisii v súlade s oddielom 20;

c) vyšetrovanie alebo nariadenia vyšetrovania ľubovoľného úniku utajovaných skutočností EÚ, ku ktorému v Komisii podľa jasného dôkazu došlo;

d) požadovanie, aby príslušné bezpečnostné úrady začali vyšetrovanie, ak podľa všetkého došlo k úniku utajovaných skutočností EÚ mimo Komisie, a koordinovanie vyšetrovania, ak sa týka viacerých bezpečnostných úradov;

e) vykonávanie pravidelných previerok bezpečnostných zabezpečení na ochranu utajovaných skutočností EÚ;

▼B

f) zachovanie úzkej spolupráce so všetkými danými bezpečnostnými úradmi, 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 vypracoval ►M2 riaditeľstvo Komisie pre bezpečnosť ◄.

12. PORADNÁ SKUPINA KOMISIE PRE BEZPEČNOSTNÚ POLITIKU

Vytvára 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 orgánov môžu byť tiež prizvaný. Zástupcovia príslušných decentralizovaných agentúr ES 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 ktoréhokoľvek jej člena. Skupina má za úlohu preskúmať a posúdiť všetky príslušné bezpečnostné otázky a Komisii podľa potreby predložiť odporúčania.

▼M2

13. BEZPEČNOSTNÁ RADA KOMISIE

Zriaďuje sa Bezpečnostná rada Komisie. Skladá sa z generálneho riaditeľa pre personál a administratívu, ktorý jej predsedá, člena kabinetu komisára zodpovedného za bezpečnostné záležitosti, člena kabinetu predsedu, zástupcu generálneho tajomníka, ktorý predsedá krízovému manažmentu Komisie, generálneho riaditeľa pre právny útvar, vonkajšie vzťahy, spravodlivosť, slobodu a bezpečnosť, spoločné výskumné centrum, informatiku, Útvaru vnútorného auditu a vedúceho Bezpečnostného úradu Komisie, alebo ich zástupcov. 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.

▼B

14. ►M2 RIADITEĽSTVO KOMISIE PRE BEZPEČNOSŤ ◄

Aby sa splnili povinnosti uvedené v oddieli 11, člen Komisie zodpovedný za bezpečnostné záležitosti má k dispozícii na koordinovanie, dohliadanie a zavádzanie bezpečnostných opatrení ►M2 riaditeľstvo Komisie pre bezpečnosť ◄.

►M2 Riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ je hlavným poradcom člena Komisie zodpovedného za bezpečnostného záležitosti v 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 potreby s medzinárodnými organizáciami spojenými s Komisiou na základe bezpečnostných dohôd. V tomto zmysle pôsobí ako styčný úradník.

►M2 Riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ je zodpovedný za akreditáciu informačných systémov a sietí v rámci Komisie. ►M2 Riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ rozhoduje po dohode s príslušným NBÚ o akreditácii informačných systémov a sietí, ktoré sa týkajú Komisie na jednej strane a ľubovoľného príjemcu utajovaných skutočností EÚ na strane druhej.

▼B

15. BEZPEČNOSTNÉ INŠPEKCIE

►M2 Riaditeľstvom Komisie pre bezpečnosť ◄ vykonáva pravidelné inšpekcie bezpečnostných zariadení na ochranu utajovaných skutočností EÚ.

►M2 Riaditeľstvom Komisie pre bezpečnosť ◄ môžu pri tejto úlohe pomáhať bezpečnostné útvary ostatných orgánov EÚ, ktoré majú k dispozícii USEÚ, alebo národné bezpečnostné úrady členských štátov ([1]).

Na žiadosť ktoréhokoľvek členského štátu môže jeho NBÚ vykonať inšpekciu USEÚ v rámci Komisie spoločne s bezpečnostnou službou Komisie a po vzájomnej dohode.

16. UTAJOVANIE, VYMEDZENIE UTAJENIA A OZNAČOVANIE

16.1. **Stupne utajenia** ([2])

Skutočnosti sú utajované v rámci týchto stupňov utajenia (pozri tiež Dodatok č. 2):

►M1 TRES SECRET UE/EU TOP SECRET ◄: Toto utajovanie sa vzťahuje iba na informácie a materiál, ktorých neoprávnené sprístupnenie by mohlo zapríčiniť mimoriadne závažné dopady na podstatné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov.

►M1 SECRET UE ◄: Toto utajovanie sa vzťahuje iba na informácie a materiály, ktorých neoprávnené sprístupnenie by mohlo vážne poškodiť podstatné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov.

►M1 CONFIDENTIEL UE ◄: Toto utajovanie sa vzťahuje na informácie a materiály, ktorých neoprávnené sprístupnenie by mohlo poškodiť podstatné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov.

►M1 RESTREINT UE ◄: Toto utajovanie sa vzťahuje na informácie a materiály, ktorých neoprávnené sprístupnenie by bolo nevýhodným pre záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov.

Žiadne iné stupne utajenia nie sú povolené.

16.2. **Bezpečnostné vymedzenie utajenia**

Na určenie limitov platnosti utajenia (pre utajované skutočnosti predstavujúce automatické zníženie stupňa utajenia alebo zrušenie stupňa utajenia) sa môže použiť 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 osobitného narábania s utajovanou skutočnosťou v porovnaní s tým, čo určuje bezpečnostná klasifikácia.

Bezpečnostné vymedzenia utajenia sa používajú iba v kombinácii s utajením.

16.3. **Označovanie**

Označovanie sa môže používať iba na špecifikovanie oblasti, na ktorú sa vzťahuje dokument alebo konkrétne distribuovanie na základe princípu potreby poznať alebo (pre neutajované skutočnosti) na označenie konca zákazu.

Označovanie sa nerovná utajovaniu a nesmie sa používať namiesto utajovania.

([1]) Bez toho, aby bol dotknutý Viedenský dohovor z roku 1961 o diplomatických stykoch a Protokol o výsadách a imunitách Európskych spoločenstiev z 8. apríla 1965.

([2]) Pozri komparatívnu tabuľku bezpečnostných klasifikácií EÚ, NATO, ZEÚ a členských štátov v Dodatku 1.

▼B

Označenie EBOP (Európska bezpečnostná a obranná politika) sa vzťahujú 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. **Uvedenie utajenia**

Utajenie sa uvádza takto:

a) na dokumenty ►M1 RESTREINT UE ◄ mechanickými alebo elektronickými prostriedkami;

b) na dokumenty ►M1 CONFIDENTIEL UE ◄ mechanickými prostriedkami alebo ručne alebo tlačou na vopred opečiatkovaný zaevidovaný papier;

c) na dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ ALEBO TAJNÉ mechanickými prostriedkami alebo ručne.

16.5. **Uvedenie bezpečnostného vymedzenia utajenia**

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

17. RIADENIE UTAJOVANIA

17.1. **Všeobecne**

Skutočnosti sa utajujú iba vtedy, ak je to potrebné. Utajovanie musí byť jasne a správne označené a musí sa ponechať tak dlho, ako to vyžaduje ochrana utajovaných skutočností.

Zodpovednosť za utajovanie skutočností a za následné zníženie stupňa utajenia alebo zrušenie stupňa utajenia spočíva výlučne na pôvodcovi utajovanej skutočnosti.

Úradníci a ostatní zamestnanci Komisie utajujú, znižujú stupne utajenia alebo zrušujú stupne utajenia skutočnosti podľa pokynov alebo po dohode s vedúcim svojho úradu.

Podrobné postupy o oboznamovaní sa s utajovanými dokumentmi sú tak koncipované, aby sa zabezpečilo, že podliehajú ochrane, ktorá zodpovedá utajovanej skutočnosti, ktorú obsahujú.

Počet osôb oprávnených vypracovať dokumenty s ►M1 TRES SECRET UE/EU TOP SECRET ◄ sa udržuje na minime a ich mená sú uvedené na zozname vypracovanom ►M2 Riaditeľstvo Komisie pre bezpečnosť ◄.

17.2. **Uplatňovanie utajovania**

Utajovanie dokumentov je určené úrovňou citlivosti ich obsahu v súlade s vymedzením v oddieli 16. Je dôležité, aby sa utajovanie používalo správne a obozretne. Uvedené sa vzťahuje najmä na utajovanie ►M1 TRES SECRET UE/EU TOP SECRET ◄.

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 uvedené v Dodatku č. 2.

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

▼B

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

Prístup verejnosti sa spravuje nariadením (ES) č. 1049/2001.

17.3. **Zníženie stupňa utajenia a zrušenie stupňa utajenia**

Utajovaným dokumentom EÚ sa môžu znížiť stupne utajenia, alebo sa môžu zrušiť stupne utajenia iba so súhlasom pôvodcu a prípadne po diskusii s ostatnými zainteresovanými stranami. Zníženie stupňa utajenia alebo zrušenie stupňa utajenia 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 na nižšom stupni, alebo sa s ohľadom na obsah môže zrušiť stupeň utajenia. V ostatných prípadoch revidujú dokumenty aspoň raz za päť rokov, aby sa presvedčili, že pôvodné utajenie je potrebné.

18. FYZICKÁ BEZPEČNOSŤ

18.1. **Všeobecne**

Hlavným cieľom fyzických bezpečnostných opatrení je zabrániť nepovolanej osobe, aby získala prístup k utajovaným informáciám a/alebo materiálom EÚ, zabrániť krádeži a znehodnoteniu zariadenia a iného majetku a zabrániť vyhrážkam 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 dochádza k oboznamovaniu sa s utajovanými informáciami a/alebo dokumentmi, musia byť chránené primeranými fyzickými bezpečnostnými opatreniami.

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

a) úroveň utajenia informácií a/alebo materiálu;

b) množstvo a forma (napríklad tvrdá väzby, počítačové úložné médium) uchovávaných utajovaných skutočností;

c) miestne posúdená hrozba zo strany tajných služieb, ktorých cieľom je EÚ, členské štáty a/alebo iné orgány alebo tretie strany, ktoré majú utajované skutočnosti EÚ, teda hrozba sabotáže, terorizmu a iných podvratných a/alebo kriminálnych činností.

Uplatňované fyzické bezpečnostné opatrenia musia byť navrhnuté tak, aby:

a) zabránili tajnému alebo násilnému vstupu nepovolanej osoby;

b) odradili, zabránili a identifikovali kroky nelojálnych členov personálu;

c) tým, ktorí nemajú „potrebu poznať“, zabránili prístup k utajovaným skutočnostiam EÚ.

▼B

18.3. **Fyzické bezpečnostné opatrenia**

18.3.1. *Bezpečnostné oblasti*

Oblasti, kde sú utajované skutočnosti EÚ, klasifikované ako DÔVERNÉ alebo vyššieho stupňa utajenia, skladujú alebo kde sa s nimi dá oboznámiť, musia byť organizované a štruktúrované tak, aby zodpovedali niektorej z týchto tried:

a) Bezpečnostná oblasť triedy I: oblasť, kde sa utajované skutočnosti EÚ, klasifikované ako DÔVERNÉ alebo vyššieho stupňa utajenia, skladujú alebo kde sa s nimi dá oboznámiť tak, že vstup do tejto oblasti predstavuje pre všetky praktické účely prístup k utajovaným skutočnostiam. 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 príslušným spôsobom preverení a majú osobitné oprávnenie na vstup do danej oblasti;

   iii) špecifikáciu utajenia skutočnosti, ktorá sa zvyčajne v danej oblasti uchováva, t. j. utajená skutočnosť, ku ktorej vstup do oblasti vedie k jej prístupu.

b) Bezpečnostná oblasť triedy II: oblasť, kde sa utajované skutočnosti EÚ, klasifikované ako DÔVERNÉ alebo vyššieho stupňa utajenia, skladujú alebo kde sa s nimi dá oboznámiť tak, že ich možno chrániť pred prístupom nepovolaných osôb prostredníctvom vnútorne zavedených kontrol, napríklad priestory, kde sa nachádzajú služby, kde sa pravidelne uchovávajú utajované skutočnosti EÚ klasifikované ako DÔVERNÉ alebo vyššieho stupňa utajenia, alebo kde sa s takýmito utajovanými skutočnosťami pravidelne dá oboznámiť. 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 príslušným spôsobom preverené a majú osobitné oprávnenie na vstup do danej oblasti. Pre všetky ostatné osoby sa musí zabezpečiť sprievod alebo zodpovedajúce kontroly, aby sa zabránilo neoprávnenému vstupu k utajovaným skutočnostiam 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 obvyklom pracovnom čase, aby sa zaručilo, že utajované skutočnosti 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 môže sa oboznamovať iba so skutočnosťami ►M1 RESTREINT UE ◄ a neutajovanými skutočnosťami.

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 skutočnostiam 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.

▼B

18.3.4 *Strážne obhliadky*

Obhliadky bezpečnostných oblastí triedy I a triedy II sa uskutočňujú mimo zvyčajného pracovného času 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 skutočností EÚ sa používajú tri triedy schránok:

— trieda A: schránky schválené na vnútroštátnej úrovni na uskladňovanie utajovaných skutočností ►**M1** TRES SECRET UE/EU TOP SECRET ◄ v rámci bezpečnostných oblastí triedy I a triedy II;

— trieda B: schránky schválené na vnútroštátnej úrovni na uskladňovanie utajovaných skutočností ►**M1** SECRET UE ◄ a DÔVERNÉ v rámci bezpečnostných oblastí triedy I alebo triedy II;

— trieda C: služobný nábytok vhodný iba na uskladňovanie utajovaných skutočností ►**M1** RESTREINT UE ◄.

V zabezpečených miestnostiach vybudovaných v rámci bezpečnostnej oblasti triedy I alebo triedy II a pre všetky bezpečnostné oblasti triedy I, kde sa utajované skutočnosti ►**M1** CONFIDENTIEL UE ◄ a vyššieho stupňa 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 utajovaných skutočností rovnakého stupňa utajenia.

18.3.6. *Zámky*

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

— skupina A: schválené na vnútroštátnej úrovni pre schránky triedy A;

— skupina B: schválené na vnútroštátnej úrovni 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 úradu 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.

▼B

18.3.8. *Poplašné detekčné zariadenie*

Ak sa na ochranu utajovaných skutočností 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 dozorujúci personál.

18.3.9. *Schválené zariadenie*

►M2 Riaditeľstvo Komisie pre bezpečnosť ◄ uchováva aktualizované zoznamy podľa typu a modelu bezpečnostných zariadení, ktoré schválil na ochranu utajovaných skutočností za rozličných špecifikovaných okolností a podmienok. ►M2 Riaditeľstvo Komisie pre bezpečnosť ◄ vychádza pri týchto zoznamoch okrem iného z utajovaných skutočností od národných bezpečnostných úradov.

18.3.10. *Fyzická ochrana kopírovacích a faxových prístrojov*

Kopírovacie a faxové prístroje musia byť fyzicky chránené v potrebnom rozsahu, aby sa zabezpečilo, že iba oprávnené osoby ich môžu používať na spracovávanie utajovaných skutočností a že všetky utajované výrobky 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 nepovolané osoby nemajú možnosť zazrieť utajované skutočnosti EÚ ani náhodne.

18.4.2. *Odpočúvanie*

Služby alebo oblasti, kde sa o utajovaných skutočnostiach ►M1 SECRET UE ◄ a vyššieho stupňa utajenia pravidelne diskutuje, musia byť chránené proti pokusom o pasívne a aktívne odpočúvanie, ak to tak riziká vyžadujú. Posúdenie rizika takýchto pokusov je v právomoci Bezpečnostného úradu Komisie po prípadných porade 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 stupni utajenia ►M1 SECRET UE ◄ a vyššom stupni utajenia, sa môžu podrobiť kontrole technických bezpečnostných špecialistov národných bezpečnostných úradov na žiadosť vedúceho Bezpečnostného úradu Komisie.

▼B

18.5 **Technicky bezpečné oblasti**

Určité oblasti možno vyčleniť ako technicky bezpečné oblasti. Vykonáva sa osobitná vstupná kontrola. Takéto oblasti sa určeným spôsobom uzamykajú, ak nie sú obsadené, a so všetkými kľúčmi sa narába ako s bezpečnostnými kľúčmi. Takéto oblasti sú predmetom pravidelných fyzických inšpekcií, 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 sa nevykonala hĺbková inšpekcia osobitne odborne vyškoleného bezpečnostného personálu, ktorá má odhaliť akékoľvek odpočúvacie zariadenia. Vo všeobecnosti, inštalácia komunikačných liniek v technicky bezpečných oblastiach nie je povolená bez predchádzajúceho povolenia príslušného orgánu.

19. VŠEOBECNÉ PRAVIDLÁ ZÁSADY „POTREBA POZNAŤ“ A BEZPEČNOSTNÉ PREVIERKY PERSONÁLU EÚ

19.1. **Všeobecne**

Prístup k utajovaným skutočnostiam EÚ sa udeľuje iba osobám, ktoré majú „potrebu poznať“, aby mohli vykonávať svoje povinnosti alebo úlohy. Prístup k skutočnostiam ►**M1** TRES SECRET UE/EU TOP SECRET ◄, TAJNÉ a DÔVERNÉ sa udeľuje iba osobám, ktoré úspešne prešli príslušnou bezpečnostnou previerkou.

Zodpovednosť za určenie „potreby poznať“ spočíva na úrade, v ktorom daná osoba pracuje.

Žiadosť o preverenie personálu je povinnosťou jednotlivých úradov.

Uvedené vedie k vydaniu „osobného bezpečnostného certifikátu EÚ“, ktorý uvádza stupeň utajenia skutočností, ku ktorým môže mať preverená osoba prístup, a dátum skončenia platnosti.

Osobný bezpečnostný certifikát EÚ pre dané utajenie oprávňuje držiteľa na prístup k utajovaným skutočnostiam s nižším stupňom 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 skutočnosti EÚ zverejniť, sa musia podrobiť osobnej bezpečnostnej previerke EÚ, pokiaľ ide o utajované skutočnosti EÚ, a musia byť oboznámení s ich zodpovednosťou za bezpečnosť.

Prístup verejnosti je naďalej upravený nariadením (ES) č. 1049/2001.

19.2. **Osobitné pravidlá prístupu k utajovaným skutočnostiam ►M1 TRES SECRET UE/EU TOP SECRET ◄**

Všetky osoby, ktoré majú prístup k utajovaným skutočnostiam ►**M1** TRES SECRET UE/EU TOP SECRET ◄, musia najprv prejsť previerkou na prístup k týmto informáciám.

Všetky osoby, ktoré majú prístup k utajovaným skutočnostiam ►**M1** TRES SECRET UE/EU TOP SECRET ◄, vymenuje člen Komisie zodpovedný za bezpečnostné záležitosti a ich mená sú uvedené v príslušnom registri utajovaných skutočností ►**M1** TRES SECRET UE/EU TOP SECRET ◄. Tento register vytvorí a vedie ►**M2** riaditeľstvo Komisie pre bezpečnosť ◄.

▼B

Všetky osoby predtým, ako získajú prístup k utajovaným skutočnostiam ►M1 TRES SECRET UE/EU TOP SECRET ◄, musia podpísať vyhlásenie, v ktorom uvedú, že boli oboznámené s bezpečnostnými postupmi Komisie a že si plne uvedomujú svoju osobitnú zodpovednosť za ochranu utajovaných skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄ a dôsledky, ktoré ustanovujú predpisy EÚ a vnútroštátne právne predpisy alebo správne opatrenia, ak sa utajované skutočnosti dostanú do nepovolaných rúk zámerne alebo v dôsledku nedbanlivosti.

V prípade osôb, ktoré majú prístup k utajovaným skutočnostiam ►M1 TRES SECRET UE/EU TOP SECRET ◄ na zasadnutiach atď., príslušný kontrolný úradník danej služby alebo orgánu, kde daná osoba pracuje, upovedomí orgán, ktorý organizuje zasadnutie, že príslušné osoby majú takéto oprávnenie.

Mená všetkých osôb, ktoré už nevykonávajú úlohy vyžadujúce si prístup k utajovaným skutočnostiam ►M1 TRES SECRET UE/EU TOP SECRET ◄, sa vyškrtnú zo zoznamu ►M1 TRES SECRET UE/EU TOP SECRET ◄. Okrem toho, všetky takéto osoby sa znova upozornia na ich osobitnú zodpovednosť za ochranu utajovaných skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄. Podpíšu tiež vyhlásenie, v ktorom sa uvedie, že nepoužijú ani neposkytnú utajované skutočnosti ►M1 TRES SECRET UE/EU TOP SECRET ◄, ktoré majú k dispozícii.

19.3. **Osobitné pravidlá o prístupe k utajovaným skutočnostiam ►M1 SECRET UE ◄ alebo ►M1 CONFIDENTIEL UE ◄**

Všetky osoby, ktoré majú prístup k utajovaným skutočnostiam ►M1 SECRET UE ◄ alebo ►M1 CONFIDENTIEL UE ◄, musia najprv prejsť previerkou pre daný stupeň.

Všetky osoby, ktoré majú prístup k utajovaným skutočnostiam ►M1 SECRET UE ◄ alebo ►M1 CONFIDENTIEL UE ◄, musia byť oboznámené s bezpečnostnými predpismi a musia si byť vedomé následkov ich zanedbania.

V prípade osôb, ktoré majú prístup k utajovaným skutočnostiam ►M1 SECRET UE ◄ alebo ►M1 CONFIDENTIEL UE ◄ 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 prístupu k utajovaným skutočnostiam ►M1 RESTREINT UE ◄**

Osoby s prístupom k utajovaným skutočnostiam ►M1 RESTREINT UE ◄ sa oboznámia s týmito bezpečnostnými predpismi a s následkami ich zanedbania.

19.5. **Presuny**

Ak je zamestnanec presunutý z miesta, ktoré zahŕňa oboznamovanie sa s utajovanými skutočnosťami EÚ, register dozrie na príslušný presun tohto materiálu od odchádzajúceho zamestnanca k prichádzajúcemu zamestnancovi.

Ak je zamestnanec presunutý na iné miesto, ktoré zahŕňa oboznamovanie sa s utajovaným materiálom EÚ, miestny bezpečnostný úradník ho s uvedenou utajovanou skutočnosťou v príslušnej miere oboznámi.

19.6. **Osobitné pokyny**

Osoby, ktoré sa oboznamujú s utajovanými skutočnosťami EÚ, by mali byť oboznámené najprv pri prevzatí svojich povinností a potom pravidelne, o:

a) rizikách pre bezpečnosť, ktoré vyplývajú z indiskrétnych rozhovorov;

b) opatreniach, ktoré musia prijať v súvislosti s tlačou a predstaviteľmi osobitných záujmových skupín;

▼B

c) nebezpečenstve, ktoré predstavujú činnosti tajných služieb, ktoré sa zameriavajú na EÚ a členské štáty, pokiaľ ide o utajované skutočnosti a činnosti EÚ;

d) povinnosti okamžite nahlásiť príslušným bezpečnostným úradom akékoľvek oslovenie alebo manéver, ktorý vedie k podozreniu o špionážnej činnosti, alebo akékoľvek nezvyčajné okolnosti, ktoré sa týkajú bezpečnosti.

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

Neexistujú žiadne bezpečnostné predpisy Komisie, ktoré sa týkajú súkromných ciest do akýchkoľvek cieľových miest personálu, ktorý prešiel previerkami pre prístup k utajovaným skutočnostiam EÚ. ►**M2** Riaditeľstvo Komisie pre bezpečnosť ◄ však oboznámi úradníkov a ostatných zamestnancov, ktorí patria do jeho právomoci, s predpismi vzťahujúcimi sa na takéto cesty, ktoré sa na nich môžu prípadne vzťahovať.

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 mať vedomosť alebo musia pracovať s utajovanými skutočnosťami, ktoré má k dispozícii Komisia, majú prístup k takýmto utajovaným skutočnostiam.

b) Na získanie prístupu k utajovaným skutočnostiam klasifikovaným ako „►**M1** TRES SECRET UE/EU TOP SECRET ◄“, „►**M1** SECRET UE ◄“ a „►**M1** CONFIDENTIEL UE ◄“, osoby uvedené v písm. a) vyššie musia byť oprávnené v súlade s postupom uvedeným v písm. 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 písm. i) až n).

d) ►**M2** Riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ je zodpovedný za udeľovanie oprávnení uvedených v písm. a), b) a c).

e) ►**M2** Riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ udelí oprávnenie po získaní stanoviska príslušných vnútroštátnych orgánov členských štátov na základe bezpečnostných previerok, ktoré sa vykonali v súlade s písm. i) až n).

f) ►**M2** Riaditeľstvo Komisie pre bezpečnosť ◄ vedie aktualizovaný zoznam všetkých citlivých pracovných miest, ktoré poskytujú príslušné úrady Komisie, a všetkých osôb, ktorým sa udelilo (dočasné) oprávnenie.

g) Oprávnenie, ktoré je platné na obdobie piatich rokov, nesmie prekročiť trvanie úloh, na základe ktorých bolo udelené. Môže sa obnoviť v súlade s postupom uvedeným v písm. e).

h) ►**M2** Riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ odoberie oprávnenie, ak usúdi, že existujú na to opodstatnené dôvody. Rozhodnutie odobrať oprávnenie sa oznámi danej osobe a príslušnému vnútroštátnemu orgánu. Osoba, ktorej sa oprávnenie odobralo, môže požiadať ►**M2** riaditeľa riaditeľstva Komisie pre bezpečnosť ◄ o vypočutie.

▼B

i) Bezpečnostné preverovanie sa vykonáva za pomoci danej osoby a na žiadosť ►M2 riaditeľa riaditeľstva Komisie pre bezpečnosť ◄. Príslušný vnútroštátny orgán na preverovanie je úradom členského štátu, ktorého je osoba podliehajúca oprávneniu štátnym príslušníkom. Ak daná osoba nie je štátnym príslušníkom členského štátu EÚ, ►M2 riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ požiada o bezpečnostné preverenie členský štát EÚ, kde má daná osoba bydlisko (domicil) alebo kde sa zvyčajne zdržiava.

j) Ako súčasť previerkového postupu sa daná osoba vyzve, aby vyplnila osobné informačné tlačivo.

k) ►M2 Riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ vo svojej žiadosti upresní typ a stupeň utajovaných skutočností, ktoré sa majú sprístupniť danej osobe tak, aby príslušné vnútroštátne orgány mohli vykonať previerku a poskytnúť svoje stanovisko v súvislosti so stupňom oprávnenia, ktorý by bolo vhodné udeliť takejto osobe.

l) Celý bezpečnostný preverovací proces spolu so získanými výsledkami podlieha príslušným pravidlám a predpisom, ktoré sú platné v danom členskom štáte vrátane tých, ktoré sa týkajú odvolania.

m) Ak príslušné vnútroštátne orgány členského štátu vyjadria pozitívne stanovisko, môže ►M2 riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ danej osobe oprávnenie udeliť.

n) Negatívne stanovisko príslušných vnútroštátnych orgánov sa oznámi danej osobe, ktorá môže ►M2 riaditeľa riaditeľstva Komisie pre bezpečnosť ◄ požiadať o vypočutie. Ak ►M2 riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ usúdi, že je potrebné, aby príslušné vnútroštátne orgány 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 písm. d) a e), obdržia v čase udelenia oprávnenia a potom v pravidelných intervaloch akékoľvek potrebné pokyny, ktoré sa týkajú utajovaných skutočností a prostriedkov zabezpečenia ich ochrany. Takéto osoby podpíšu vyhlásenie, v którom potvrdia, že obdržali takéto pokyny, a zaviažu sa, že ich budú dodržiavať.

p) ►M2 Riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ prijme všetky potrebné opatrenia, aby uplatňoval tento oddiel, najmä pokiaľ ide o pravidlá, ktoré upravujú prístup k zoznamu oprávnených osôb.

q) ►M2 Riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ môže výnimočne, ak o to požiada útvar, udeliť po predložení oznámenia príslušných vnútroštátnych orgánov a ak príslušné vnútroštátne orgány neodpovedia do jedného mesiaca, dočasné oprávnenie na obdobie nepresahujúce šesť mesiacov, očakávajúc výsledok previerky uvedenej v písm. i).

r) Dočasné a predbežné oprávnenia takto udelené neumožňujú prístup k utajovaným skutočnostiam ►M1 TRES SECRET UE/EU TOP SECRET ◄; takýto prístup je vyhradený pre úradníkov, ktorí sa už skutočne podrobili previerke s pozitívnymi výsledkami v súlade s písm. i). Úradníci, ktorí požiadali, aby boli preverení na stupni utajenia skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄ a ešte stále očakávajú výsledok previerky, môžu dočasne a predbežne získať oprávnenie na prístup k utajovaným skutočnostiam so stupňom utajenia až po stupeň ►M1 SECRET UE ◄ vrátane tohto stupňa.

▼B

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

21.1. **Príprava**

1. Utajovanie skutočností EÚ sa uplatňuje tak, ako je ustanovené v oddieli 16, a s ohľadom na utajované skutočnosti ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia 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 ►M1 TRES SECRET UE/EU TOP SECRET ◄ a ►M1 SECRET UE ◄ 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 ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia.

2. Dokumenty klasifikované ako ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia, môžu prepisovať, prekladať, uschovávať, fotokopírovať a reprodukovať magneticky alebo mikrofilmami iba osoby, ktoré boli preverené na prístup k utajovaným skutočnostiam EÚ aspoň do bezpečnostného stupňa utajenia daného dokumentu.

3. Ustanovenia, ktoré upravujú elektronické vyhotovovanie utajovaných dokumentov, sú uvedené v oddieli 25.

21.2. **Distribúcia**

1. Utajované skutočnosti EÚ sa distribuujú iba osobám, ktoré ich potrebujú poznať a majú príslušnú bezpečnostnú previerku. Pôvodca utajovaných skutočností označuje počiatočnú distribúciu.

2. Dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ sa dostávajú do obehu prostredníctvom registrov ►M1 TRES SECRET UE/EU TOP SECRET ◄ (pozri oddiel 22.2). V prípade správ ►M1 TRES SECRET UE/EU TOP SECRET ◄ môže príslušný register oprávniť vedúceho komunikačného centra, aby vyhotovil určitý počet kópií, ktorý sa upresní s ohľadom na zoznam adresátov.

3. Dokumenty klasifikované ako ►M1 SECRET UE ◄ a nižšieho stupňa utajenia môže pôvodný adresát ďalej distribuovať ďalším adresátom podľa zásady potreba poznať. Úrady, ktoré sú pôvodcami takýchto dokumentov, však jednoznačne uvedú 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 ako ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia musí pri vstupe alebo pri výstupe z generálneho riaditeľstva alebo útvaru zaznamenať miestny register USEÚ daného úradu. 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. **Prenášanie utajovaných dokumentov EÚ**

21.3.1. *Balenie, príjem*

1. Dokumenty klasifikované ako ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia sa prenášajú v odolných, nepriesvitných dvojitých obálkach. Vnútorná obálka sa označí príslušným bezpečnostným stupňom utajenia EÚ a, ak je možné, tiež úplnými údajmi o názve funkcie príjemcu a adrese.

▼B

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. Vnútorná obálka sa vkladá do vonkajšej obálky, na ktorej je číslo balíka na účely prijatia. Za žiadnych okolností sa na vonkajšej obálke nesmie uvádzať bezpečnostné stupeň utajenia.

5. V prípade dokumentov klasifikovaných ako ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia, kuriéri a poslovia obdržia príjmové tlačivo proti číslam balíkov.

21.3.2. *Prenášanie 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 stupeň utajenia prenášaných dokumentov.

21.3.3. *Prenášanie v rámci krajiny*

1. V rámci krajiny by sa dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ mali zasielať iba prostredníctvom oficiálnej kuriérskej služby alebo prostredníctvom osôb oprávnených na prístup k utajovaným skutočnostiam ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. Ak sa na prenášanie dokumentu ►M1 TRES SECRET UE/EU TOP SECRET ◄ 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 ►M1 TRES SECRET UE/EU TOP SECRET ◄ zostanú po celý čas pod priamym dozorom zodpovedného referenta.

3. Výnimočne môžu aj referenti iní ako kuriéri prenášať dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ mimo budovy alebo skupiny budov pre miestne použitie na zasadnutiach a rokovaniach, ak:

   a) daný posol má oprávnenie na prístup k takýmto dokumentom ►M1 TRES SECRET UE/EU TOP SECRET ◄;

   b) spôsob dopravy je v súlade s pravidlami uplatňovanými na prenášanie dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄;

   c) za žiadnych okolností nenechá daný posol dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ bez dozoru;

   d) je zabezpečené, že zoznam dokumentov takto prenášaných je uvedený v registri dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄ a je zaznamenaný v knihe, pričom sa zoznam skontroluje oproti tomuto zápisu v čase návratu dokumentov.

4. V rámci danej krajiny sa dokumenty ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄ môžu zasielať poštou, ak je takýto prenos povolený vnútroštátnymi právnymi predpismi a je v súlade s ustanoveniami týchto právnych predpisov, alebo kuriérskou službou alebo osobami, ktoré sú preverené na prístup k utajovaným skutočnostiam EÚ.

▼B

5. ►M2 Riaditeľstvo Komisie pre bezpečnosť ◄ 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:

a) zostať mimo dosahu doručiteľa, pokiaľ nie sú v bezpečnej úschove v súlade s ustanoveniami uvedenými v oddieli 18;

b) zostať bez dozoru v prostriedkoch verejnej dopravy alebo súkromných prepravných prostriedkoch, 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. *Prenášanie zo štátu do štátu*

1. Materiál klasifikovaný ako ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia sa prenáša diplomatickými službami EÚ alebo vojenskými kuriérskymi službami EÚ.

2. Je však možné povoliť osobný prenos materiálu klasifikovaného ako ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄, ak sú opatrenia na prenos také, že zabezpečia, že sa dané dokumenty nedostanú do rúk nepovolaných osôb.

3. Člen Komisie zodpovedný za bezpečnostné záležitosti môže oprávniť osobný prenos, ak nie sú k dispozícii diplomatickí ani vojenskí kuriéri, alebo ak by použitie takýchto kuriérov viedlo k zdržaniu, ktoré by mohlo mať škodlivý vplyv na operatívne činnosti EÚ a materiál je súrne potrebný pre určeného príjemcu. ►M2 Riaditeľstvo Komisie pre bezpečnosť ◄ pripraví pokyny, ktoré sa vzťahujú na osobný prenos zo štátu do štátu utajovaného materiálu až do stupňa utajenia ►M1 SECRET UE ◄ vrátane prenosu inými osobami, ako sú diplomatickí a vojenskí kuriéri. Pokyny musia požadovať, aby:

a) doručiteľ mal príslušnú bezpečnostnú previerku;

b) sa viedol záznam v príslušnom úrade 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 ustanovené;

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 dopravných prostriedkov, ktoré sa majú použiť, boli v súlade s predpismi EÚ alebo – ak sú vnútroštátne predpisy pre takéto činnosti prísnejšie – v súlade s takýmito právnymi predpismi;

g) materiál sa nesmie dostať mimo dosahu doručiteľa, pokiaľ nie je uschovaný v súlade s ustanoveniami o bezpečnej úschove, ktoré sú uvedené 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.).

▼B

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 *Prenášanie dokumentov* ►M1 *RESTREINT UE* ◄

Pre prenos dokumentov ►M1 RESTREINT UE ◄ nie sú stanovené žiadne osobitné ustanovenia s výnimkou, že by mali byť také, aby sa zabezpečilo, že sa nedostanú do rúk nepovolaných osôb.

21.4. **Bezpečnosť kuriérov**

Všetci kuriéri a poslovia, ktorí sú určení na prenos dokumentov ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄, musia prejsť príslušnou bezpečnostnou previerkou.

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

1. Komunikačné bezpečnostné opatrenia sú navrhnuté tak, aby zabezpečili bezpečný prenos utajovaných skutočností EÚ. Podrobné pravidlá, ktoré sa vzťahujú na prenos takýchto utajovaných skutočností EÚ sú uvedené v oddieli 25.

2. Iba akreditované komunikačné centrá a siete a/alebo terminály a systémy môžu prenášať utajované skutočnosti ►M1 CONFIDENTIEL UE ◄ a ►M1 SECRET UE ◄.

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

1. Iba pôvodca môže autorizovať kópiu alebo preklad dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. Ak osoby bez preverenia pre stupeň utajenia ►M1 TRES SECRET UE/EU TOP SECRET ◄ žiadajú utajované skutočnosti, ktoré, aj keď sú uvedené v dokumente ►M1 TRES SECRET UE/EU TOP SECRET ◄, nemajú tento stupeň utajenia, vedúci registra dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄ (pozri oddiel 22.2) môže povoliť vyhotovenie potrebného počtu výpisov z týchto dokumentov. Súčasne prijme potrebné opatrenia, aby zabezpečil, že sa týmto výpisom pridelí príslušná klasifikácia utajenia.

3. Dokumenty klasifikované ako ►M1 SECRET UE ◄ a nižšieho stupňa utajenia môže adresát reprodukovať a prekladať v rámci týchto bezpečnostných ustanovení a pod podmienkou, že sa dodržiava zásada potreba poznať. Bezpečnostné opatrenia, ktoré sa vzťahujú na originálny dokument sa tiež vzťahujú na jeho reprodukcie a/alebo preklady.

22. REGISTRE UTAJOVANÝCH SKUTOČNOSTÍ EÚ, PREHLIADKY, KONTROLY, ARCHÍVNE SKLADOVANIA A LIKVIDÁCIA UTAJOVANÝCH SKUTOČNOSTÍ EÚ

22.1. **Miestne registre utajovaných skutočností EÚ**

1. V rámci Komisie v každom úrade je jeden prípadne viacero miestnych registrov USEÚ zodpovedných za registráciu, reprodukciu, rozosielanie, archivovanie a likvidáciu dokumentov klasifikovaných ako ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄.

2. Ak úrad nemá miestny register USEÚ, jeho funkciu vykonáva miestny register USEÚ generálneho sekretariátu.

3. Miestne registre USEÚ podliehajú vedúcemu úradu, od ktorého dostávajú pokyny. Vedúci takýchto registrov sú registračnými kontrolnými úradníkmi.

▼B

4. Miestne registre USEÚ podliehajú dohľadu miestneho bezpečnostného úradníka, pokiaľ ide o uplatňovanie ustanovení, ktoré sa týkajú oboznamovania sa s dokumentmi USEÚ a súlad s príslušnými bezpečnostnými opatreniami.

5. Úradníci pridelení do miestnych registrov USEÚ musia mať oprávnenie na prístup k USEÚ v súlade s oddielom 20.

6. Pod dozorom príslušného vedúceho oddelenia miestne registre USEÚ:

   a) riadia operácie týkajúce sa registrácie, reprodukcie, prekladu, prenosu, rozosielania a likvidácie takýchto dokumentov;

   b) aktualizujú zoznam údajov o utajovaných skutočnostiach;

   c) pravidelne overujú potrebu zachovávať utajovanie skutočností.

7. Miestne registre USEÚ vedú register s týmito údajmi:

   a) dátum vypracovania utajovaných skutočností;

   b) stupeň utajenia;

   c) dátum ukončenie platnosti utajenia;

   d) meno a úrad vydavateľa;

   e) príjemca alebo príjemcovia spolu so sériovým číslom;

   f) predmet;

   g) počet;

   h) počet kópií v obehu;

   i) príprava súpisu utajovaných skutočností predložených úradu;

   j) evidencia zrušenia stupňa utajenia a zníženia stupňa utajenia skutočností.

8. Všeobecné pravidlá ustanovené v oddieli 21 sa vzťahujú na miestne registre USEÚ Komisie, pokiaľ nie sú upravené osobitnými pravidlami ustanovenými v tomto oddieli.

22.2. **Register utajovaných skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄**

22.2.1. *Všeobecne*

1. Centrálny register utajovaných skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄ zabezpečuje zaznamenávanie, manipuláciu a distribúciu dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄ v súlade s týmito bezpečnostnými ustanoveniami. Vedúci registra ►M1 TRES SECRET UE/EU TOP SECRET ◄ je kontrolným úradníkom registra ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. Centrálny register utajovaných skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄ pôsobí ako hlavný prijímajúci a odosielajúci orgán v Komisii voči ostatným orgánom EÚ, členským štátom, medzinárodným organizáciám a tretím štátom, s ktorými má Komisia dohody o bezpečnostných postupoch pri výmene utajovaných skutočností.

3. V prípade potreby sa zakladajú vedľajšie registre, ktoré sú zodpovedné za vnútorné riadenie dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄; vedú aktualizované záznamy o obehu všetkých dokumentov, za ktoré je takýto vedľajší register zodpovedný.

▼B

4. Vedľajšie registre ►M1 TRES SECRET UE/EU TOP SECRET ◄ sa zakladajú podľa ustanovení uvedených v časti 22.2.3. ako odpoveď na dlhodobé potreby a sú priradené k centrálnemu registru ►M1 TRES SECRET UE/EU TOP SECRET ◄. Ak je potrebné nahliadnuť do dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄ iba dočasne a príležitostne, je možné tieto dokumenty poskytnúť bez založenie vedľajšieho registra ►M1 TRES SECRET UE/EU TOP SECRET ◄, ak sú ustanovené pravidlá, ktoré zabezpečujú, aby dokumenty zostali pod kontrolou príslušného registra ►M1 TRES SECRET UE/EU TOP SECRET ◄ a aby sa dodržiavali všetky fyzické a osobné bezpečnostné opatrenia.

5. Vedľajšie registre nesmú dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ prenášať priamo ostatným vedľajším registrom toho istého centrálneho registra ►M1 TRES SECRET UE/EU TOP SECRET ◄ bez výslovného súhlasu centrálneho registra ►M1 TRES SECRET UE/EU TOP SECRET ◄.

6. Všetky výmeny dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄ medzi vedľajším registrami, ktoré nie sú priradené tomu istému centrálnemu registru, sa vykonávajú cez centrálne registre ►M1 TRES SECRET UE/EU TOP SECRET ◄.

22.2.2. *Centrálny register utajovaných skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄*

Vedúci centrálneho registra ►M1 TRES SECRET UE/EU TOP SECRET ◄ je ako kontrolný úradník zodpovedný za:

a) prenos dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄ v súlade s ustanoveniami upravenými v oddieli 21.3;

b) vedenie zoznamu všetkých podriadených vedľajších registrov ►M1 TRES SECRET UE/EU TOP SECRET ◄ spolu s menami a podpismi menovaných kontrolných úradníkov a ich oprávnených zástupcov;

c) uchovávanie potvrdení o príjmoch z registrov pre všetky dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄, ktoré distribuuje centrálny register;

d) vedenie záznamu o dokumentoch ►M1 TRES SECRET UE/EU TOP SECRET ◄, ktoré uchováva a distribuuje;

e) vedenie aktualizovaného zoznamu všetkých centrálnych registrov ►M1 TRES SECRET UE/EU TOP SECRET ◄, s ktorými zvyčajne koresponduje, spolu s menami a podpismi ich menovaných kontrolných úradníkov a ich oprávnených zástupcov;

f) fyzické ochraňovanie všetkých dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄, ktoré sa uchovávajú v registri, v súlade s pravidlami uvedenými v oddieli 18.

22.2.3. *Vedľajšie registre ►M1 TRES SECRET UE/EU TOP SECRET ◄*

Vedúci vedľajšieho registra ►M1 TRES SECRET UE/EU TOP SECRET ◄ je ako kontrolný úradník zodpovedný za:

a) prenos dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄ v súlade s ustanoveniami uvedenými v oddieli 21.3;

b) vedenie aktualizovaného zoznamu všetkých osôb, ktoré majú prístup k utajovaným skutočnostiam ►M1 TRES SECRET UE/EU TOP SECRET ◄ pod jeho kontrolou;

c) distribúciu dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄ v súlade s pokynmi pôvodcu alebo podľa zásady potreba poznať, pričom najprv skontroluje, či adresát má potrebné bezpečnostné preverenie;

d) vedenie aktualizovaného záznamu všetkých dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄, ktoré sa uchovávajú alebo ktoré sú v obehu pod jeho kontrolou, alebo ktoré boli postúpené iným registrom ►M1 TRES SECRET UE/EU TOP SECRET ◄, a za uchovávanie príslušných príjmových tlačív;

▼B

e) vedenie aktualizovaného zoznamu registrov utajovaných skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄, s ktorými má oprávnenie vymieňať si dokumenty úrady PRÍSNE TAJNÉ, spolu s menami a podpismi ich kontrolných referentov a ich oprávnených zástupcov;

f) fyzickú ochranu všetkých dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄, 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 utajovaných skutočností ►M1 TRES SECRET UE/EU TOP SECRET ◄, ako sú uvedené v tomto oddieli, každoročne vykonávajú súpis dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄ podľa položiek. Dokument sa považuje za zaevidovaný v registri, ak register dokument fyzicky obhliadne alebo má doklad o príjme od registra ►M1 TRES SECRET UE/EU TOP SECRET ◄, do ktorého bol dokument prevedený, potvrdenie o likvidácii dokumentu alebo o znížení stupňa utajenia, alebo príkaz na zrušenie stupňa utajenia dokumentu. Zistenia ročných súpisov sa predkladajú členovi Komisie zodpovednému za bezpečnostné záležitosti najneskôr do 1. apríla každého roka.

2. Vedľajšie registre ►M1 TRES SECRET UE/EU TOP SECRET ◄ predkladajú zistenia ročných súpisov centrálnemu registru, ktorému podliehajú, ku dňu, ktorý takýto centrálny register určí.

3. Utajované skutočnosti EÚ nižšieho stupňa utajenia ako ►M1 TRES SECRET UE/EU TOP SECRET ◄ sú predmetom interných kontrol v súlade s pokynmi člena Komisie zodpovedného za bezpečnostné záležitosti.

4. Tieto opatrenia majú umožniť, aby držitelia predložili svoje stanoviská s ohľadom na:

   a) možnosti znížiť stupeň utajenia alebo zrušiť stupeň utajenia určitých dokumentov;

   b) dokumenty, ktoré sa majú zlikvidovať.

22.4. **Archívne skladovanie utajovaných skutočností EÚ**

1. USEÚ sa musia skladovať za podmienok, ktoré sú v súlade s príslušnými požiadavkami uvedenými v oddieli 18.

2. Aby sa minimalizovali skladovacie problémy, kontrolní úradníci všetkých registrov musia mať oprávnenie, aby mohli mať dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄ v podobe mikrofilmy alebo iným spôsobom zaznamenané na magnetických alebo optických médiách na účely archivácie za predpokladu, že:

   a) proces zhotovenia mikrofilmov/skladovania vykonáva personál s platnou bezpečnostnou previerkou pre zodpovedajúci stupeň utajenia;

   b) mikrofilm/skladovacie médium má priradenú tú istú bezpečnostnú ochranu ako pôvodné dokumenty;

   c) zhotovovanie mikrofilmu/skladovanie ľubovoľného dokumentu ►M1 TRES SECRET UE/EU TOP SECRET ◄ sa oznámi pôvodcovi;

   d) zvitky filmu alebo iný typ podpory obsahujú iba dokumenty rovnakého stupňa utajenia ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ alebo ►M1 CONFIDENTIEL UE ◄;

▼B

e) zhotovenie mikrofilmov/skladovanie akéhokoľvek dokumentu ►M1 TRES SECRET UE/EU TOP SECRET ◄ alebo ►M1 SECRET UE ◄ je zreteľne zaznačené 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 vzťahujú na akúkoľvek formu oprávneného skladovania, ako napríklad elektromagnetické médiá a optický disk.

22.5. **Likvidácia utajovaných dokumentov EÚ**

1. Aby sa zabránilo zbytočnému zhromažďovaniu utajovaných dokumentov EÚ, tie dokumenty, o ktorých vedúci jednotky, ktorá ich má k dispozícii usúdi, že sú neaktuálne a v nadbytočnom počte, sa zlikvidujú, len čo je to možné, týmto spôsobom:

a) Dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ likviduje iba centrálny register, ktorý je za ne zodpovedný. Všetky dokumenty, ktoré boli zlikvidované, sa uvedú na zozname potvrdenia o likvidácii, ktoré podpíše kontrolný úradník dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄ a úradník, ktorý bol svedkom likvidácie, pričom obidvaja musia mať preverenie na stupeň utajenia ►M1 TRES SECRET UE/EU TOP SECRET ◄. 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 ►M1 TRES SECRET UE/EU TOP SECRET ◄ vrátane celého utajeného odpadu vzniknutého z prípravy dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄, ako napríklad pokazené kópie, pracovné náčrty, rukou písané poznámky alebo diskety, sa musia zničiť pod dohľadom kontrolného úradníka registra pre utajované skutočnosti ►M1 TRES SECRET UE/EU TOP SECRET ◄ spálením, rozdrvením, skartovaním alebo iným zničením tak, aby ich nebolo možné rozpoznať alebo obnoviť.

2. Dokumenty ►M1 SECRET UE ◄ likviduje register, ktorý je za dokumenty zodpovedný, pod dohľadom bezpečnostne preverenej osoby, pričom sa použije niektorý z postupov uvedených v ods. 1 písm. c). Dokumenty ►M1 SECRET UE ◄, ktoré sa zničili, sa uvedú na zozname podpísaných potvrdení o likvidácii, ktoré uchováva register spolu s rozdeľovníkmi počas doby minimálne troch rokov.

3. Dokumenty ►M1 CONFIDENTIEL UE ◄ likviduje register, ktorý je za dokumenty zodpovedný, pod dohľadom bezpečnostne preverenej osoby, pričom sa použije niektorý z postupov uvedených v ods. 1 písm. c). Ich likvidácia sa zaznamenáva podľa pokynov člena Komisie, ktorý je zodpovedný za bezpečnostné záležitosti.

4. Dokumenty ►M1 RESTREINT UE ◄ likviduje register, ktorý je za dokumenty zodpovedný, alebo ich užívateľ v súlade s pokynmi člena Komisie, ktorý je zodpovedný za bezpečnostné záležitosti.

22.6. **Likvidácia v naliehavých situáciách**

1. Úrady Komisie pripravia plány vychádzajúce z miestnych podmienok, ktoré sú zamerané na ochranu utajovaného materiálu EÚ v krízovej situácii, vrátane prípadnej likvidácie, a evakuačné plány. Komisia vyhlási pokyny, ktoré sa považujú za potrebné na zabránenie situácii, že utajované skutočnosti EÚ sa dostanú do nepovolaných rúk.

▼B

2. Úpravy, ktoré sa týkajú ochrany a/alebo likvidácie materiálov ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄ v krízovej situácii nesmú v žiadnom prípade nepriaznivo ovplyvniť ochranu alebo likvidáciu materiálov ►M1 TRES SECRET UE/EU TOP SECRET ◄, vrátane kódovacieho zariadenia, oboznamovanie sa s ktorými má prednosť pred všetkými ostatnými úlohami.

3. Opatrenia, ktoré sa musia prijať na ochranu a likvidáciu kódovacieho zariadenia v prípade naliehavej situácie, musia byť upravené v osobitných pokynoch.

4. Takéto pokyny musia byť dostupné priamo na mieste v zapečatenej obálke. Dostupné musia byť aj prostriedky/nástroje na likvidáciu.

23. BEZPEČNOSTNÉ OPATRENIA PRE OSOBITNÉ ZASADNUTIA, KTORÉ SA KONAJÚ MIMO PRIESTOROV KOMISIE A ZAHŕŇAJÚ UTAJOVANÉ SKUTOČNOSTI EÚ

23.1. **Všeobecne**

Ak sa zasadnutia Komisie alebo iné dôležité zasadnutia konajú mimo priestorov Komisie a ak je to odôvodnené konkrétnymi bezpečnostnými požiadavkami, ktoré sa týkajú vysokej citlivosti diskutovaných záležitostí alebo utajovaných skutočností, prijmú sa bezpečnostné opatrenia, ktoré sú popísané nižšie. Tieto opatrenia sa týkajú iba ochrany utajovaných skutočností EÚ; ostatné bezpečnostné opatrenia bude možno potrebné naplánovať.

23.2. **Právomoci**

23.2.1. ►M2 *Riaditeľstvo Komisie pre bezpečnosť* ◄

►M2 Riaditeľstvo Komisie pre bezpečnosť ◄ spolupracuje s príslušnými orgánmi členského štátu, na území ktorého sa zasadnutie koná (hostiteľský členský štát), aby sa zaručila 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.

►M2 Riaditeľstvo Komisie pre bezpečnosť ◄ koná ako poradca pre bezpečnosť pri príprave zasadnutia; pri príprave by mal byť zastúpený, aby podľa potreby pomohol a poradil bezpečnostnému úradníkovi zasadnutia a delegáciám.

Každá jednotlivá delegácia na zasadnutí sa vyzve, aby menovala bezpečnostného úradníka, ktorý bude zodpovedný za vybavovanie bezpečnostných záležitostí v rámci svojej delegácie a za vykonávanie funkcie prostredníka s bezpečnostným úradníkom zasadnutia rovnako, ako prípadne so zástupcom ►M2 riaditeľstva Komisie pre bezpečnosť ◄.

23.2.2. *Bezpečnostný úradník zasadnutia (BÚZ)*

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

a) ochranných opatrení na mieste zasadnutia, ktoré zaručia, že zasadnutie sa uskutoční bez incidentu, ktorý by mohol ohroziť bezpečnosť akýchkoľvek utajovaných skutočností EÚ, ktoré sa na zasadnutí prípadne používajú;

▼B

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 orgánmi hostiteľského členského štátu a s Bezpečnostným úradom Komisie;

d) zaradenie bezpečnostných inštrukcií do spisov zasadnutia s príslušným upozornením na požiadavky uvedené v týchto bezpečnostných predpisoch a akékoľvek iné bezpečnostné pokyny, ktoré sa považujú za potrebné.

23.3. **Bezpečnostné opatrenia**

23.3.1. *Bezpečnostné oblasti*

Určujú sa tieto bezpečnostné oblasti:

a) bezpečnostná oblasť triedy II, ktorá pozostáva z pracovnej miestnosti, kancelárií Komisie a reprografického zariadenia rovnako ako prípadne 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 úradník 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 fotografi a zvukoví technici s príslušným povolením od bezpečnostného úradníka 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 skontrolovania. V prípade balíkov pre delegácie, delegácia môže prevziať doručený balík, ktorý sa podrobí inšpekcii bezpečnostného úradníka delegácie, preverí osobitným zariadením alebo ho otvorí bezpečnostný personál na inšpekciu. Ak to bezpečnostný úradník zasadnutia považuje za potrebné, môžu sa prijať prísnejšie opatrenia na inšpekciu aktoviek a balíkov.

▼B

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 skontrolovanie 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 úradníka zasadnutia proti potvrdeniu o prijatí tak, aby bezpečnostný úradník zasadnutia mohol 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 úradník zasadnutia prijme príslušné opatrenia.

23.3.9 *Likvidácia odpadu utajovaných skutočností 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 úradníkovi zasadnutia, ktorý zabezpečí jeho likvidáciu v súlade s týmito bezpečnostnými predpismi.

Na konci zasadnutia sa všetky dokumenty, ktoré majú Komisia alebo delegácie k dispozícii, avšak ich už nepotrebujú, považujú za odpad. Pred tým, ako sa zrušia bezpečnostné opatrenia prijaté pre zasadnutie, sa vykoná dôkladná prehliadka priestorov Komisie a delegácií. Dokumenty, vo vzťahu ku ktorým sa podpísalo potvrdenie o prijatí, sa podľa možností čo najviac zlikvidujú, ako je uvedené v oddieli 22.5.

24. PORUŠENIE BEZPEČNOSTI A OHROZENIE UTAJOVANÝCH SKUTOČNOSTÍ EÚ

24.1. **Vymedzenie pojmov**

K porušenie bezpečnosti dochádza v dôsledku konania alebo opomenutia v rozpore s bezpečnostnými predpismi Komisie, ktoré by mohlo ohroziť alebo spôsobiť ohrozenie utajovaných skutočností EÚ.

K ohrozeniu utajovaných skutočností EÚ dochádza, keď sa celé alebo ich časť dostanú do rúk nepovolaných osôb, t. j. osôb, ktoré nemajú príslušnú bezpečnostnú previerku alebo nespĺňajú zásadu potreba poznať, alebo ak existuje pravdepodobnosť, že k takejto udalosti došlo.

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

24.2. **Hlásenie porušenia bezpečnosti**

Všetky osoby, ktoré musia narábať s utajovanými skutočnosťami EÚ, sú náležito poučené o svojej zodpovednosti v tejto oblasti. Okamžite musia nahlásiť akékoľvek porušenie bezpečnosti, o ktorom sa dozvedia.

▼B

Ak miestny bezpečnostný úradník alebo bezpečnostný úradník zasadnutia objaví alebo je informovaný o porušení bezpečnosti, ktorá sa týka utajovaných skutočností EÚ, alebo o strate alebo zmiznutí utajovaných materiálov EÚ, okamžite podnikne opatrenia na:

a) ochranu dôkazov;

b) konštatovanie faktov;

c) posúdenie a minimalizovanie vzniknutej škody;

d) zabránenie opakovaniu;

e) oznámenie príslušným orgánom o dôsledkoch porušenia bezpečnosti.

V tejto súvislosti sa musia zabezpečiť nasledujúce informácie:

i) opis danej utajovanej skutočnosti, vrátane stupňa jej utajenia, 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 utajovaná skutočnosť vystavená odcudzeniu;

iii) vyhlásenie, či bol pôvodca 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 ►M2 riaditeľstvu Komisie pre bezpečnosť ◄.

Prípady, ktoré zahŕňajú utajované skutočnosti ►M1 RESTREINT UE ◄, 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 skutočnosti;

b) požiadať príslušné bezpečnostné úrady, aby začali vyšetrovanie;

c) koordinovať prešetrovanie, 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 stupňa 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 zabránenia opakovania.

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

24.3. **Právne opatrenia**

Každý jednotlivec, ktorý je zodpovedný za ohrozenie utajovaných skutočností EÚ, podlieha disciplinárnym opatreniam podľa príslušných pravidiel a predpisov, najmä hlavy VI personálneho poriadku. Takéto opatrenie nemá dopad na akékoľvek iné právne opatrenie.

V primeraných prípadoch na základe správy, ktorá je uvedená v oddieli 24.2 člen Komisie zodpovedný za bezpečnostné záležitosti prijme všetky potrebné opatrenia, aby príslušným vnútroštátnym orgánom umožnil začať trestné konanie.

▼B

25. OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ EÚ, S KTORÝMI SA DÁ OBOZNÁMIŤ V INFORMAČNEJ TECHNOLÓGII 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), v ktorých sa dá oboznámiť s utajovanými skutočnosťami ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia. Uplatňujú sa ako dodatok k rozhodnutiu Komisie C(95) 1510 konečné z 23. novembra 1995 o ochrane informačných systémov.

Systémy, v ktorých sa dá oboznámiť s utajovanými skutočnosťami ►M1 RESTREINT UE ◄ tiež vyžadujú bezpečnostné opatrenia na ochranu dôvernosti týchto utajovaných skutočností. Všetky systémy vyžadujú bezpečnostné opatrenia na ochranu celistvosti a dostupnosti týchto systémov a utajovaných skutočností, ktoré obsahujú.

Bezpečnostná politika pre informačné technológie, ktorú uplatňuje Komisia, má tieto prvky:

— tvorí neoddeliteľnú súčasť bezpečnosti vo všeobecnosti a dopĺňa všetky prvky informačnej bezpečnosti, personálnej bezpečnosti a fyzickej bezpečnosti,

— rozdelenie zodpovedností medzi vlastníkmi technických systémov, vlastníkmi utajovaných skutočností EÚ, ktoré sú uložené alebo s ktorými sa dá oboznámiť 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 orgánom,

— zohľadnenie osobitných hrozieb a zraniteľnosti v oblasti informačnej technológie.

25.1.2. *Hrozby a zraniteľnosť systémov*

Hrozbu možno vymedziť 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 vymedziť ako slabinu alebo nedostatok kontroly, ktorý by umožnil alebo povolil vyvolanie hrozby voči určitému majetku alebo cieľu.

Utajované a neutajované skutočnosti 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 utajovaným skutočnostiam nepovolanými užívateľmi, alebo naopak odoprenie prístupu oprávneným osobám. Zahŕňajú tiež riziká neoprávneného sprístupnenia, zneužitia, úpravy alebo vymazania utajovaných skutočností. Okrem toho, zložité a niekedy krehké zariadenia sú drahé a často náročné na rýchlu opravu alebo nahradenie.

25.1.3. *Hlavný účel bezpečnostných opatrení*

Hlavným účelom bezpečnostných opatrení uvedených v tomto oddieli je poskytnúť ochranu proti neoprávnenému sprístupneniu utajovaných skutočností EÚ (strata dôvernosti) a proti strate celistvosti a dostupnosti takýchto utajovaných skutočností. Aby sa dosiahla primeraná bezpečnostná ochrana systému, ktorý narába s utajovanými skutočnosťami EÚ, ►M2 riaditeľstvo Komisie pre bezpečnosť ◄ určí primerané normy všeobecnej bezpečnosti spolu s primeranými osobitnými bezpečnostnými postupmi a technikami navrhnutými konkrétne pre každý systém.

▼B

25.1.4. *Vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke (OSBP)*

V prípade všetkých systémov, v ktorých sa dá oboznámiť s utajovanými skutočnosťami ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia, sa od vlastníka technického systému (VTS, pozri oddiel 25.3.4) a vlastník utajovaných skutočností (VUS, 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 INFOBEZ – 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 utajovaných skutočností ►M1 RESTREINT UE ◄ alebo neutajovaných skutočností 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 skutočnosťami ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia, musia mať akreditáciu na vykonávanie činnosti v jednom alebo, ak je to odôvodnené požiadavkami počas rozličných časových období, viacerých z nasledujúcich bezpečnostných režimov prevádzky alebo ich vnútroštátnych ekvivalentov:

a) jednoúčelový.

b) systém vysoký a

c) viacúrovňový.

25.2. **Vymedzenie pojmov**

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

Poznámka:

Takáto akreditácia by sa mala priznať, ak 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 akým stupňom (stupňami) utajenia skutočností sa dá oboznamovať a aký systém alebo sieťový bezpečnostný režim (režimy) sa navrhujú;

b) vypracovanie prehľadu riadenia rizík, aby sa identifikovali hrozby a citlivé miesta 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.

▼B

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

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

„Komunikačná bezpečnosť (KOMBEZ)“ znamená: uplatňovanie bezpečnostných opatrení na telekomunikačné zariadenia, aby sa nepovolaným osobám odopreli utajované skutočnosti so stupňom utajenia, ktoré by sa mohli získať držbou a analýzou takýchto telekomunikačných zariadení, alebo zabezpečenie autentickosti takýchto telekomunikačných zariadení.

Poznámka:

Takéto opatrenia zahŕňajú kódovaciu, prenosovú alebo vysielaciu bezpečnosť a tiež sa vzťahujú na procesnú, personálnu, dokumentačnú a počítačovú bezpečnosť.

„Počítačová bezpečnos“ (POČBEZ) znamená: uplatňovanie bezpečnostných funkcií, ktoré sa týkajú hardwaru, firmwaru a softwaru, na počítačový systém s cieľom ochrany pred alebo zabráneniu neoprávneného sprístupnenia, manipulácie, zmeny/vymazania utajovaných skutočností alebo zamietnutia vstupu do systému.

„Počítačový bezpečnostný výrobok“ znamená: všeobecná počítačová bezpečnostná položka, ktorá je určená na začlenenie do systému informačnej technológie na používane pri zlepšovaní alebo zabezpečovaní dôvernosti, celistvosti alebo dostupnosti utajovaných skutočností, s ktorými sa dá oboznámiť.

„Jednoúčelový bezpečnostný režim prevádzky“ znamená: režim prevádzky, v ktorom sú VŠETCI jednotlivci s prístupom do systému preverení pre najvyšší stupeň utajenia skutočností v rámci systému a so všeobecnou potrebou poznať utajované skutočnosti, s ktorými sa dá oboznámiť v rámci systému.

Poznámky:

1. Všeobecná potreba poznať naznačuje, že neexistuje žiadna povinná požiadavka, aby počítačové bezpečnostné funkcie zabezpečovali oddeľovanie utajovaných skutočností v rámci systému.

2. Ostatné bezpečnostné funkcie (napríklad fyzické, personálne a procesné) musia zodpovedať požiadavkám najvyššieho stupňa utajenia a pre všetky označenia kategórií utajovaných skutočností, s ktorými sa dá oboznámiť v rámci systému.

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

Poznámky:

1. Vyhodnotenie skúma prítomnosť požadovanej bezpečnostnej funkčnosti a neprítomnosť ohrozujúcich vedľajších účinkov takejto funkčnosti a posudzuje nezneužiteľnosť takejto funkčnosti.

2. Vyhodnotenie určuje rozsah, v akom sú splnené bezpečnostné požiadavky systému alebo bezpečnostné nároky na počítačový bezpečnostný výrobok, a stanovuje úroveň zabezpečenia spoľahlivej funkcie systému alebo kódovacieho alebo počítačového bezpečnostného výrobku.

„Vlastník utajovaných skutočností (VUS)“ znamená orgán (vedúci úradu), ktorý je zodpovedný za vytvorenie, spracovanie a použitie utajovaných skutočností vrátane rozhodovania, komu sa umožní prístup k týmto utajovaným skutočnostiam.

▼B

„Informačná bezpečnosť“ (INFOBEZ) znamená: uplatňovanie bezpečnostných opatrení na ochranu utajovaných skutočností, 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 INFOBEZ“ zahŕňajú opatrenia počítačovej, prenosovej, vysielacej a kódovacej bezpečnosti, zistenie a dokumentáciu hrozieb a prechádzanie hrozbám pre utajované skutočnosti a systémy.

„Oblasť informačnej technológie“ znamená: oblasť, ktorá obsahuje jeden alebo viacej počítačov, ich miestne periférne a úložné 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 mechanizmy na označovanie a postupy, prístupové kontroly, programy a dôsledky auditov) potrebné na zabezpečenie prijateľnej úrovne ochrany utajovaných skutočností.

„Informačný systém“ znamená: súbor zariadení, metód a postupov a prípadne personál, ktorý je organizovaný takým spôsobom, aby mohol vykonávať funkcie spracovávania informácií.

Poznámky:

1. Treba to chápať ako súbor zariadení, ktoré sú nastavené tak, aby mohli v rámci systému narábať s utajovanými skutočnosťami.

2. Takéto systémy môžu predstavovať podporu pre konzultačné, príkazové, kontrolné, komunikačné, vedecké alebo administratívne aplikácie vrátane prác s textom.

3. Hranice systému sa vo všeobecnosti určujú ako prvky, ktoré sú pod kontrolou jediného VTS.

4. Informačný systém môže obsahovať podsystémy, z ktorých niektoré samotné sú informačnými systémami.

▼B

„Bezpečnostné funkcie informačného systému“ sa skladajú zo všetkých hardwarových/firmwarových/softwarových 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 skutočností, s ktorými sa má narábať v informačnom systéme.

„Miestny úradník informačnej bezpečnosti (MÚIB)“ znamená: úradník v úrade 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 pre najvyšší stupeň utajenia skutočností, s ktorými sa dá oboznámiť v rámci systému, a NIE VŠETCI jednotlivci s prístupom do systému majú všeobecnú potrebu poznať utajované skutočnosti, s ktorými sa dá oboznámiť v rámci systému.

Poznámky:

1. Tento režim prevádzky povoľuje súčasne narábať s utajovanými skutočnosťami rozličného stupňa utajenia a s utajovanými skutočnosťami rozličného označenia kategórií.

2. Skutočnosť, že nie všetci jednotlivci sú preverení pre najvyšší stupeň utajenia, v spojení s nedostatkom všeobecnej potreby poznať naznačuje, že existuje požiadavka, aby počítačové bezpečnostné funkcie zabezpečovali selektívny prístup k utajovaným skutočnostiam v rámci systému a oddeľovanie utajovaných skutočností 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, ktorá je oddelená od oblasti informačnej technológie.

„Bezpečnostné prevádzkové postupy“ znamená: postupy, ktoré vypracoval vlastník technických systémov a ktoré vymedzujú zásady, ktoré sa majú prijať pre bezpečnostné záležitosti a prevádzkové postupy, ktoré treba dodržiavať, ako aj zodpovednosť personálu.

„Bezpečnostný prevádzkový režim SYSTÉM VYSOKÉHO ZABEZPEČENIA“ znamená: režim prevádzky, v ktorom VŠETCI jednotlivci s prístupom do systému sú preverení pre najvyšší stupeň utajenia skutočností, s ktorými sa dá oboznámiť v rámci systému, ale NIE VŠETCI jednotlivci s prístupom do systému majú všeobecnú potrebu poznať utajované skutočnosti, s ktorými sa dá oboznámiť v rámci systému.

Poznámky:

1. Nedostatok všeobecnej potreby poznať naznačuje, že existuje požiadavka, aby počítačové bezpečnostné funkcie zabezpečovali selektívny prístup k utajovaným skutočnostiam v rámci systému a oddeľovanie týchto utajovaných skutočností.

2. Ostatné bezpečnostné funkcie (napríklad fyzické, personálne a procesné) musia zodpovedať požiadavkám pre najvyšší stupeň utajenia a všetky označenia kategórií utajovaných skutočností, s ktorými sa dá oboznámiť v systéme.

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

▼B

„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 ukazovateľmi, ktoré sa vzťahujú na prevádzkové prostredie, najnižším stupňom personálneho bezpečnostného preverenia, najvyšším stupňom utajenia skutočností, s ktorými sa dá oboznámiť, bezpečnostným režimom prevádzky alebo užívateľskými požiadavkami. Vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke je jednotnou časťou projektovej dokumentácie, ktorá sa predkladá príslušným orgánom 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.

„Vlastník technických systémov (VTS)“ znamená orgán, ktorý je zodpovedný za tvorbu, údržbu, prevádzku a uzatvorenie systému.

„Tempest (spôsob zaručenia bezpečnosti elektromagnetického impulzu terminálu)“ protiopatrenia: bezpečnostné opatrenia určené na ochranu zariadenia a komunikačnej infraštruktúry proti ohrozeniu utajovaných skutočností v dôsledku neúmyselného elektromagnetického žiarenia a v dôsledku vodivosti.

25.3. **Bezpečnostné právomoci**

25.3.1. *Všeobecne*

Poradné právomoci Poradnej skupiny Komisie pre bezpečnostnú politiku, vymedzenej v oddieli 12, zahŕňajú záležitosti INFOBEZ. Táto skupina organizuje svoje činnosti tak, aby mohla poskytovať odborné rady vo vyššie uvedených záležitostiach.

►**M2** Riaditeľstvo Komisie pre bezpečnosť ◄ je zodpovedný za vydávanie podrobných ustanovení INFOBEZ podľa ustanovení tejto kapitoly.

V prípade problémov, ktoré sa týkajú bezpečnosti (nehody, porušenia atď.) ►**M2** Riaditeľstvo Komisie pre bezpečnosť ◄ okamžite prijme opatrenia.

►**M2** Riaditeľstvo Komisie pre bezpečnosť ◄ má jednotku INFOBEZ.

25.3.2. *Bezpečnostný akreditačný úrad (BAÚ)*

Vedúci bezpečnostného úradu je Bezpečnostný akreditačný úrad pre Komisiu. Bezpečnostný akreditačný úrad má právomoci vo všeobecnej oblasti bezpečnosti a v špecializovaných oblastiach INFOBEZ, 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 skutočnosťami EÚ po stanovený stupeň utajenia 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 INFOBEZ (IÚ)*

Vedúci jednotky INFOBEZ ►**M2** riaditeľstva Komisie pre bezpečnosť ◄ je INFOBEZ orgánom pre Komisiu. Úrad INFOBEZ je zodpovedný za:

— poskytovanie technického poradenstva a pomoci bezpečnostnému akreditačnému úradu,

— pomáhanie pri vypracovávaní vyhlásenia o osobitnej systémovej bezpečnostnej požiadavke

▼B

— skúmanie vyhlásenia o osobitnej systémovej bezpečnostnej požiadavke, aby sa zabezpečila zhoda s týmito bezpečnostnými predpismi a zásadami INFOBEZ a architektonickými plánmi;

— účasť v akreditačných porotách/radách, ak sa to požaduje a za poskytovanie odporúčaní INFOBEZ o akreditácii bezpečnostnému akreditačnému úradu;

— poskytovanie podpory odbornému vzdelávaniu INFOBEZ a vzdelávacím akciám;

— poskytovanie technického poradenstva pri skúmaní prípadov súvisiacich s INFOBEZ;

— vypracovaním usmernení o technickej politike, aby sa zabezpečilo, že sa používa iba jeden autorizovaný software.

25.3.4. *Vlastník technických systémov (VTS)*

Zodpovednosť za zavedenie a vykonávanie kontroly a osobitných bezpečnostných funkcií systému spočíva na vlastníkovi tohto systému, vlastníkovi technických systémov (VTS). V prípade centrálne vlastnených systémov sa vymenuje úradník pre centrálnu informačnú bezpečnosť. Každý úrad vymenuje podľa potreby miestneho úradníka pre informačnú bezpečnosť. Zodpovednosť vlastníka technických systémov zahŕňa tvorbu bezpečnostných prevádzkových postupov a vzťahuje sa na celý životný cyklus systému od projektového plánu až po konečnú likvidáciu.

Vlastník technických systémov určuje bezpečnostné normy a prax, ktoré musí dodávateľ systému splniť.

Vlastník technických systémov môže prípadne delegovať časť svojich právomocí na miestneho úradníka pre informačnú bezpečnosť. Jedna osoba môže vykonávať rôzne funkcie INFOBEZ.

25.3.5. *Vlastník utajovaných skutočností (VUS)*

Vlastník utajovaných skutočností je zodpovedný za utajované skutočnosti EÚ (a ostatné skutočnosti), ktoré sa musia zaviesť, spracovať a vyrobiť v technických systémoch. Vymedzuje požiadavky na prístup k týmto utajovaným skutočnostiam v systémoch. Túto právomoc 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. *Odborné vzdelávanie INFOBEZ*

Všeobecné vzdelávanie a odborné vzdelávanie v oblasti INFOBEZ musí byť dostupné pre všetkých zamestnancov, ktorí ho potrebujú.

25.4. **Iné ako technické bezpečnostné opatrenia**

25.4.1. *Personálna bezpečnosť*

Užívatelia systému sú preverení a majú potrebu poznať, ako to vyžaduje utajenie a obsah utajovaných skutočností, s ktorými sa dá oboznámiť v rámci určitého systému. Na prístup k určitému zariadeniu alebo utajovaným skutočnostiam osobitným pre bezpečnosť systémov sa vyžaduje osobitné preverenie, ktoré sa prideľuje podľa postupov Komisie.

Bezpečnostný akreditačný úrad menuje všetky citlivé pracovné miesta a špecifikuje stupeň preverenia a dohľadu, ktorá sa vyžaduje od všetkých členov personálu, ktorí sú na týchto pracovných miestach.

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

▼B

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 vymedzené v oddieli 25.2), v ktorých sa narába s utajovanými skutočnosťami ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia s prostriedkami informačných technológií, alebo kde je možný potenciálny prístup k takýmto utajovaným skutočnostiam, sa musia stanoviť ako bezpečnostné oblasti utajovaných skutočností EÚ triedy I prípadne triedy II.

25.4.3. *Kontrola prístupu k systému*

Všetky informácie a materiál, ktoré umožňujú kontrolovať prístup k systému sú chránené opatreniami, ktoré sú rovnocenné opatreniam najvyššieho stupňa utajenia a určením kategórie utajovaných skutočností, ku ktorým môžu povoliť 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 utajovaných skutočností*

Je povinnosťou pôvodcu utajovaných skutočností, aby identifikoval a klasifikoval všetky dokumenty, ktoré obsahujú utajované skutočnosti, bez ohľadu na to, či sú výstupy v tlačenej forme alebo uložené na počítačových médiách. Každá strana tlačenej formy musí byť označená stupňom utajenia v hornej a dolnej časti. Výstup v tlačenej forme alebo uložený na počítačovom médiu musí mať taký istý stupeň utajenia ako utajovaná skutočnosť, ktorá sa použila na jeho tvorbu. Spôsob operácie systému tiež môže mať dopad na utajenie výstupov z tohto systému.

Je povinnosťou úradov Komisie a tých, ktorí majú utajované skutočnosti k dispozícii, aby zohľadnili problémy hromadenia sa jednotlivých prvkov utajovaných skutočností a ich vzájomného pôsobenia, ktoré možno získať z príbuzných prvkov, a stanovili, či nie je pre výsledný súhrn utajovaných skutočností primeraný vyšší stupeň utajenia.

Skutočnosť, že utajovaná skutočnosť môže byť v skrátenom kóde, prenosovom kóde alebo akokoľvek inak dvojako vyjadrená, nepredstavuje žiadnu bezpečnostnú ochranu, a preto by nemala mať vplyv na utajovanie skutočností.

Ak sa utajované skutočnosti prenášajú z jedného systému do iného, utajovaná skutočnosť musí byť chránená počas prenosu a v prijímajúcom systéme spôsobom, ktorý je rovnocenný pôvodnému utajeniu a kategorizácii utajovaných skutočností.

So všetkými úložnými počítačovými médiami sa musí narábať spôsobom, ktorý je rovnocenný najvyššiemu stupňu utajenia uložených utajovaných skutočností alebo označeniu média, a musia byť sústavne primerane chránené.

Opakovane použiteľné počítačové úložné médiá používané na záznam utajovaných skutočností EÚ si musia zachovať najvyšší stupeň utajenia, pre ktoré boli použité, až kým sa nezníži stupeň utajenia príslušnej utajovanej skutočnosti alebo s ohľadom na túto utajovanú skutočnosť nedošlo k zrušeniu stupňa utajenia, a príslušne médiá preklasifikované alebo vo vzťahu ku ktorým sa zrušil stupeň utajenia alebo zničené v súlade s postupom schváleným bezpečnostným akreditačným úradom (pozri 25.5.4).

▼B

25.5.2. *Kontrola a zodpovednosť za utajované skutočnosti*

Ako záznamy o prístupe k utajovaným skutočnostiam so stupňom utajenia ►M1 SECRET UE ◄ a vyšším sa vedú automatizované (audítorské reťazce) alebo manuálne záznamové knihy. Tieto záznamy sa uchovávajú v súlade s týmito bezpečnostnými predpismi.

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

Ak systém, v ktorom sa dá oboznámiť s utajovanými skutočnosťami 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 utajovaných skutočností ►M1 SECRET UE ◄ a vyššieho stupňa utajenia takéto postupy zahŕňajú osobitné pokyny s ohľadom na zodpovednosť za utajované skutočnosti.

25.5.3. *Manipulácia a kontrola odstrániteľných počítačových úložných médií*

Všetky odstrániteľné počítačové úložné médiá klasifikované ako utajované skutočnosti ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia sa považujú za materiál, na ktorý sa vzťahujú všeobecné pravidlá. Konkrétny fyzický vzhľad médií sa upraví prostredníctvom príslušnej identifikácie a stupňa utajenia tak, aby sa umožnilo ich jednoduché rozlíšenie.

Užívatelia sú zodpovední za zabezpečenie, že všetky utajované skutočnosti EÚ sa ukladajú na médiách s príslušným označením a ochranou. Ustanovia sa postupy, aby sa zaručilo, že pre všetky stupne utajovaných skutočností EÚ sa ukladanie týchto utajovaných skutočností na počítačových úložných médiách vykonáva v súlade s týmito bezpečnostnými predpismi.

25.5.4 *Zrušenie stupňa utajenia a likvidácia počítačových úložných médií*

V prípade počítačových úložných médií používaných na záznam utajovaných skutočností EÚ sa môže znížiť stupeň utajenia alebo môže byť zrušený stupeň utajenia v súlade s postupom, ktorý schválil Bezpečnostný akreditačný úrad.

V prípade počítačových úložných médií, na ktorých boli uložené utajované skutočnosti ►M1 TRES SECRET UE/EU TOP SECRET ◄ alebo inej osobitnej kategórie, nesmie byť zrušený stupeň utajenia ani sa nesmú opakovane používať.

Ak v prípade počítačových úložných médií nie je možné zrušiť stupeň utajenia alebo sa nesmú opakovane použiť, musia sa zlikvidovať v súlade s vyššie uvedeným postupom.

25.5.5. *Komunikačná bezpečnosť*

►M2 Riaditeľ riaditeľstva Komisie pre bezpečnosť ◄ je šifrovacím úradom.

Ak sa utajované skutočnosti EÚ prenášajú elektromagneticky, zavedú sa osobitné opatrenia na ochranu dôvernosti, celistvosti a dostupnosti takýchto prenosov. Bezpečnostný akreditačný úrad určí požiadavky na ochranu prenosov pred odhalením a zachytením utajovaných skutočností. Utajované skutočnosti, 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 výrobky musia byť osobitne schválené na daný účel bezpečnostným akreditačným úradom ako šifrovacím úradom.

▼B

Počas prenosu sa dôvernosť utajovaných skutočností ►M1 SECRET UE ◄ a vyššieho stupňa utajenia chráni šifrovacími metódami alebo výrobkami schválenými členom Komisie zodpovedným za bezpečnostné záležitosti po porade s Poradnou skupinou Komisie pre bezpečnostnú politiku. Počas prenosu sa dôvernosť utajovaných skutočností ►M1 CONFIDENTIEL UE ◄ alebo ►M1 RESTREINT UE ◄ chráni šifrovacími metódami alebo výrobkami schválenými šifrovacím úradom Komisie po porade s Poradnou skupinou Komisie pre bezpečnostnú politiku.

Podrobné pravidlá, ktoré sa vzťahujú na prenos utajovaných skutočností EÚ sú uvedené v osobitných bezpečnostných pokynoch schválených ►M2 riaditeľstvom Komisie pre bezpečnosť ◄ po porade s Poradnou skupinou Komisie pre bezpečnostnú politiku.

Za výnimočných okolností je možné utajované skutočnosti ►M1 RESTREINT UE ◄, ►M1 CONFIDENTIEL UE ◄ a ►M1 SECRET UE ◄ prenášať v nešifrovanom texte za predpokladu, že každý takýto konkrétny prenos je výslovne schválený a primerane registrovaný vlastníkom utajovaných skutočností. Takýmito výnimočnými okolnosťami sú:

a) počas hroziacej alebo aktuálnej krízy, konfliktu alebo vojnovej situácie a

b) ak rýchlosť doručenia má mimoriadny význam a šifrovacie prostriedky nie sú k dispozícii a posúdi sa, že prenos utajovaných skutočností nemôže byť zneužitý tak rýchlo, aby nepriaznivo ovplyvnil operácie.

Systém musí mať schopnosť pozitívneho odmietnutia prístupu k utajovaným skutočnostiam EÚ na ktorejkoľvek zo všetkých pracovných staníc alebo vzdialených terminálov, ak sa požaduje fyzickým odpojením alebo zvláštnymi softwarovými funkciami schválenými bezpečnostným akreditačným úradom.

25.5.6
Inštalačná a radiačná bezpečnosť

Počiatočná 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 skutočnostiam EÚ až do stupňa, ktorý sa rovná najvyššiemu stupňu utajenia, s ktorými sa má v systéme oboznámiť a ktoré sa majú v systéme uchovávať.

Systémy, v ktorých sa dá oboznámiť s utajovanými skutočnosťami ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia musia byť chránené tak, aby ich bezpečnosť nebolo možné ohroziť nebezpečným žiarením a/alebo vodivosťou, pričom analýza a kontrola týchto faktorov sa označuje ako „Tempest (spôsob zaručenia bezpečnosti elektromagnetického impulzu terminálu)“.

Protiopatrenia súvisiace so spôsobom zaručenia bezpečnosti elektromagnetického impulzu terminálu (Tempest) skúma a schvaľuje Úrad pre spôsob zaručenia bezpečnosti elektromagnetického impulzu terminálu (Úrad Tempest, pozri 25.3.2).

25.6. **Bezpečnosť počas manipulácie**

25.6.1. *Bezpečnostné prevádzkové postupy (BEZPP)*

Bezpečnostné prevádzkové postupy vymedzujú zásady, ktoré sa prijímajú s ohľadom na bezpečnostné záležitosti, prevádzkové postupy, ktoré sa musia dodržiavať, a zodpovednosť personálu. Bezpečnostné prevádzkové postupy sa pripravujú v rámci zodpovednosti vlastníka technických systémov (VTS).

25.6.2. *Riadenie softwarovej ochrany/konfigurácie*

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

▼B

Nové ani modifikované verzie softwaru sa na prácu s utajovanými skutočnosťami EÚ nesmú používať, pokiaľ nie sú overené VTS.

25.6.3. *Kontrola prítomnosti škodného softwaru/počítačových vírusov*

Kontrola zameraná na zisťovanie, či nie je prítomný škodný software/počítačové vírusy, sa vykonáva pravidelne v súlade s požiadavkami BAÚ.

Všetky počítačové úložné médiá prichádzajúce do Komisie sa predtým, ako sa zavedú do ktoréhokoľvek systému, musia overiť, či neobsahujú škodný software alebo počítačové vírusy.

25.6.4. *Údržba*

Zmluvy a postupy pre plánovanú a pohotovostnú údržbu systémov, pre ktoré boli vytvorené vyhlásenia o OSBP, musia špecifikovať požiadavky a opatrenia pre údržbárov a ich súvisiace zariadenie, ktoré vstupuje do oblasti informačných technológií.

Požiadavky musia byť vo vyhláseniach o OSBP zreteľne uvedené, ako aj postupy v BEZPP. Dodávateľská údržba, ktorá vyžaduje postupy pre vzdialený diagnostický prístup, je povolená iba vo výnimočných prípadoch za prísnej bezpečnostnej kontroly a iba so súhlasom BAÚ.

25.7. **Verejné obstarávanie**

25.7.1. *Všeobecne*

Ľubovoľný bezpečnostný produkt na používanie so systémom, ktorý sa má obstarať, musí byť vyhodnotený a certifikovaný, alebo práve v procese vyhodnocovania a certifikovania príslušným vyhodnocujúcim 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 úložné médiá, mali prenajať, a nie zakúpiť, sa musí pamätať na to, že takéto zariadenie, keď sa už používalo na prácu s utajovanými skutočnosťami EÚ, nie je možné uvoľniť mimo primerane bezpečnostného prostredia bez toho, aby sa najprv nezrušil stupeň utajenia so súhlasom BAÚ a že takýto súhlas nie je vždy možný.

25.7.2. *Akreditácia*

Všetky systémy, pre ktoré je nutné vypracovať vyhlásenia o OSBP, musia byť pred prácou s utajovanými skutočnosťami EÚ akreditované BAÚ podľa informácií uvedených vo vyhláseniach o OSBP, BEZPP 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 definovaným zo strany BAÚ.

25.7.3. *Vyhodnotenie a certifikácia*

Pred akreditáciou sa v niektorých prípadoch musí vyhodnotiť systémové bezpečnostné funkcie softwaru, firmwaru a hardwaru a certifikovať ako schopné chrániť utajované skutočnosti na určenom stupni utajenia.

Požiadavky na vyhodnotenie a certifikáciu sa musia zahrnúť do systémového plánovania a jasne uviesť vo vyhláseniach o OSBP.

▼B

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

Tímy môže poskytnúť vymenovaný hodnotiaci alebo certifikačný úrad členského štátu alebo jeho vymenovaní 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 výrobkoch.

25.7.4. *Bežná kontrola bezpečnostných funkcií pre stálu akreditáciu*

VTS 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 BAÚ, musia byť jednoznačne určené a uvedené vo vyhláseniach o OSBP. Po ľubovoľnej modifikácii, oprave alebo zlyhaní, ktoré by mohli ovplyvniť bezpečnostné funkcie systému, VTS zabezpečí, aby sa skontrolovala správna operácia bezpečnostných funkcií. Stála akreditácia systému zvyčajne závisí od uspokojivého ukončenia kontrol.

Všetky systémy, v ktorých sa zaviedli bezpečnostné funkcie, BAÚ pravidelne preveruje a preskúmava. V prípade systémov, v ktorých sa dá oboznámiť s utajovanými skutočnosťami ►**M1** TRES SECRET UE/EU TOP SECRET ◄, sa inšpekcie vykonávajú aspoň raz ročne.

25.8 **Dočasné alebo príležitostné použitie**

25.8.1. *Bezpečnosť mikropočítačov/osobných počítačov*

Mikropočítače/osobné počítače s pevnými diskami (alebo inými úložnými médiami udržujúcimi 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 diskami sa považujú za informačné úložné médiá v rovnakom zmysle ako diskety alebo iné odstrániteľné počítačové úložné médiá.

Zariadeniu sa priraďuje stupeň ochrany z hľadiska prístupu, manipulácie, ukladania a prepravy, ktorý je rovnocenný s najvyšším stupňom utajenia skutočností, v akom vôbec boli tieto utajované skutočnosti ukladané alebo spracovávané (až pokiaľ nedôjde k zníženiu stupňa utajenia alebo k zrušeniu stupňa utajenia v súlade so schválenými postupmi).

25.8.2. *Použitie súkromného informačného systému pre oficiálnu prácu Komisie*

Zakázané je použitie súkromných prenosných počítačových úložných médií, softwaru a hardwaru (napríklad osobné počítač a prenosné počítačové zariadenia) s úložnými kapacitami na manipuláciu s utajovanými skutočnosťami EÚ.

Súkromný software, hardware a médiá sa nesmú prinášať do oblasti triedy I alebo triedy II, kde sa narába s utajovanými skutočnosťami EÚ, bez písomného oprávnenia ►**M2** riaditel' riaditeľstva Komisie pre bezpečnosť ◄. Toto oprávnenie je možné poskytnúť iba vo výnimočných prípadoch z technických dôvodov.

▼B

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 ►M2 riaditel' riaditeľstva Komisie pre bezpečnosť ◄. 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 ktoromkoľvek prípade, ak sa zariadenie informačnej technológie má používať na manipuláciu s utajovanými skutočnosťami EÚ, musí sa konzultovať s BAÚ, aby sa primerane zohľadnili a zaviedli prvky INFOBEZ, ktoré sa vzťahujú na použitie daného zariadenia.

26. POSKYTNUTIE UTAJOVANÝCH SKUTOČNOSTÍ TRETÍM ŠTÁTOM ALEBO MEDZINÁRODNÝM ORGANIZÁCIÁM

26.1.1. *Zásady, ktorými sa riadi poskytovanie utajovaných skutočností EÚ*

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

— povahy a obsahu takýchto utajovaných skutočností,

— potreby poznať s ohľadom na prijímateľov,

— miery výhod pre EÚ.

Pôvodca utajovaných skutočností EÚ, ktoré sa majú poskytnúť, sa požiada 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 prejaviť – čo vyplýva z úrovne bezpečnosti, ktorá by sa vzťahovala na utajované skutočnosti EÚ zverené týmto štátom alebo organizáciám a zo súladu medzi bezpečnostnými predpismi uplatňovanými v daných tretích štátoch alebo medzinárodných organizáciách a v EÚ. Poradná skupina Komisie pre bezpečnostnú politiku predloží Komisii s ohľadom na tento bod svoje technické stanovisko.

Prijatie utajovaných skutočností EÚ tretími štátmi alebo medzinárodnými organizáciami v sebe zahŕňa uistenie, že sa utajované skutočnosti nebudú používať na iné účely, ako sú účely, na ktoré sa dané utajované skutočnosti poskytli alebo vymenili, a že sa zabezpečí ochrana týchto utajovaných skutočností v miere, ktorú požaduje Komisia.

26.1.2. *Úrovne*

Komisia po svojom rozhodnutí, že utajované skutočnosti EÚ možno poskytnúť alebo si vymeniť s daným štátom alebo medzinárodnou organizáciou, rozhodne o úrovni spolupráce, ktorá je možná. Toto bude závisieť najmä od bezpečnostnej politiky a právnych predpisov, ktoré uplatňuje daný štát alebo organizácia.

Existujú tri úrovne spolupráce:

Úroveň 1

Spolupráca s tretími štátmi alebo s medzinárodnými organizáciami, ktorých bezpečnostná politika a právne predpisy sú veľmi blízke bezpečnostnej politike a právnym aktom EÚ.

Úroveň 2

Spolupráca s tretími štátmi alebo s medzinárodnými organizáciami, ktorých bezpečnostná politika a právne predpisy sú značne rozdielne od bezpečnostnej politiky a právnych aktov EÚ.

▼B

Úroveň 3

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

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

26.1.3. *Dohody o bezpečnosti*

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

V prípade úrovne 3, občasná spolupráca, ktorá je svojím vymedzením obmedzená časom a účelom, môže jednorázové memorandum o porozumení vymedzujúce povahu utajovaných skutočností, ktoré sa majú vymieňať a recipročné povinnosti ohľadne týchto utajovaných skutočností, nahradiť „dohodu o postupoch pre výmenu utajovaných skutočností“ za podmienky, že utajované skutočnosti nemajú vyšší stupeň utajenia ako ►M1 RESTREINT UE ◄.

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 utajované skutočnosti, ktoré sa majú poskytnúť, používali a chránili v súlade s ustanoveniami dohôd o bezpečnostných postupoch alebo v súlade s memorandom o porozumení.

▼M3

27. SPOLOČNÉ MINIMÁLNE NORMY PRE PRIEMYSELNÚ BEZPEČNOSŤ

27.1. **Úvod**

Tento oddiel sa zaoberá bezpečnostnými aspektmi priemyselnej činnosti špecifickými pre rokovanie o zmluvách alebo dohodách o poskytnutí grantu, na základe ktorých sa zverujú úlohy zahŕňajúce, predpokladajúce a/alebo obsahujúce utajované skutočnosti EÚ, pre ich zadávanie, ako aj vykonávanie priemyselnými alebo inými subjektmi, vrátane poskytnutia alebo sprístupnenia utajovaných skutočností EÚ v rámci procesu verejného obstarávania a výziev na predkladanie ponúk (obdobie predkladania ponúk a rokovania pred uzatvorením zmluvy).

27.2. **Vymedzenie pojmov**

Na účely týchto spoločných minimálnych noriem platia nasledujúce definície:

a) „zmluva podliehajúca utajeniu“: každá zmluva alebo dohoda o poskytnutí grantu na dodanie výrobkov, vykonanie prác alebo poskytnutie služieb, pričom výkon týchto činností vyžaduje alebo zahŕňa prístup k utajovaným skutočnostiam EÚ alebo ich vytvorenie;

b) „subdodávateľská zmluva podliehajúca utajeniu“: zmluva medzi dodávateľom alebo príjemcom grantu a iným dodávateľom (t. j. subdodávateľom) o dodaní tovaru, vykonaní prác alebo poskytnutí služieb, ktorej realizácia vyžaduje alebo zahŕňa prístup k utajovaným skutočnostiam EÚ alebo ich vytvorenie;

c) „dodávateľ“: hospodársky subjekt alebo právnická osoba s právnou spôsobilosťou na uzatváranie zmlúv alebo prijímanie grantov;

▼M3

d) „určený bezpečnostný úrad (UBÚ)“: orgán podliehajúci národnému bezpečnostnému úradu (NBÚ) členského štátu EÚ, ktorý je zodpovedný za oboznamovanie priemyselných alebo iných subjektov s vnútroštátnou politikou vo všetkých oblastiach priemyselnej bezpečnosti a za usmerňovanie a podporu pri jej vykonávaní. Funkcie UBÚ môže vykonávať NBÚ;

e) „bezpečnostná previerka zariadenia (FSC)“: administratívne potvrdenie zo strany NBÚ/UBÚ, že z pohľadu bezpečnosti je zariadenie schopné zabezpečiť primeranú bezpečnostnú ochranu utajovaných skutočností EÚ s určitým stupňom utajenia a jeho zamestnanci, ktorí požadujú prístup k utajovaným skutočnostiam EÚ, boli náležite bezpečnostne preverení a upovedomení o nevyhnutných bezpečnostných požiadavkách na prístup k utajovaným skutočnostiam EÚ a ich ochranu;

f) „priemyselný alebo iný subjekt“: dodávateľ alebo subdodávateľ, ktorý dodáva tovar, vykonáva práce alebo poskytuje služby; toto môže zahŕňať priemyselné, obchodné, vedecké, výskumné, vzdelávacie alebo rozvojové subjekty, alebo subjekty pôsobiace v oblasti služieb;

g) „priemyselná bezpečnosť“: uplatňovanie ochranných opatrení a postupov na zabránenie, odhalenie a vyriešenie úniku alebo vyzradenia utajovaných skutočností EÚ, s ktorými zaobchádzal dodávateľ alebo subdodávateľ počas rokovaní pred uzavretím zmluvy a v súvislosti so zmluvami podliehajúcimi utajeniu;

h) „národný bezpečnostný úrad (NBÚ)“: orgán štátnej správy členského štátu EÚ s konečnou zodpovednosťou za ochranu utajovaných skutočností EÚ v rámci daného členského štátu;

i) „celkový stupeň bezpečnostného utajenia zmluvy“: stanovenie bezpečnostného utajenia celej zmluvy alebo dohody o poskytnutí grantu založené na utajení skutočností a/alebo materiálu, ktorý bude alebo môže byť vytvorený, poskytnutý alebo sa k nemu bude môcť dostať v rámci každého prvku celkovej zmluvy. Celkový stupeň bezpečnostného utajenia zmluvy nesmie byť nižší než najvyšší stupeň utajenia akéhokoľvek jej prvku, ale môže byť vyšší v dôsledku súhrnného efektu;

j) „kniha bezpečnostných aspektov (SAL)“: súbor osobitných zmluvných podmienok vydaných obstarávateľom, ktorý identifikuje bezpečnostné požiadavky alebo prvky vyžadujúce bezpečnostnú ochranu a ktorý tvorí neoddeliteľnú súčasť zmluvy podliehajúcej utajeniu zahŕňajúcej vytvorenie utajovaných skutočností EÚ alebo prístup k nim;

k) „pokyny k bezpečnostnému utajovaniu (SCG)“: dokument, ktorý opisuje prvky programu, zmluvy alebo dohody o poskytnutí grantu, ktoré sú utajené, pričom uvádza uplatniteľné stupne bezpečnostného utajenia. SCG sa môžu v priebehu programu, zmluvy alebo dohody o poskytnutí grantu rozšíriť a stupeň utajenia prvkov informácií sa môže zmeniť alebo znížiť. SCG musia byť súčasťou SAL.

27.3. **Organizácia**

a) Komisia môže na základe zmluvy podliehajúcej utajeniu zveriť úlohy zahŕňajúce, predpokladajúce a/alebo obsahujúce utajované skutočnosti EÚ priemyselným alebo iným subjektom registrovaným v členskom štáte.

b) Komisia zabezpečí, že pri uzatváraní zmluvy podliehajúcej utajeniu sú splnené všetky požiadavky vyplývajúce z uvedených minimálnych noriem.

c) Na účely uplatňovania týchto minimálnych noriem na priemyselnú bezpečnosť Komisia zapojí príslušný(-é) NBÚ. NBÚ môžu tieto úlohy delegovať na jeden alebo viacero UBÚ.

▼M3

d) Konečnú zodpovednosť za ochranu utajovaných skutočností EÚ v rámci priemyselných alebo iných subjektov má vedenie týchto subjektov.

e) V prípade uzavretia zmluvy alebo subdodávateľskej zmluvy podliehajúcej utajeniu, na ktorú sa vzťahujú tieto minimálne normy, Komisia a/alebo prípadne NBÚ/UBÚ bezodkladne informuje NBÚ/UBÚ členského štátu, v ktorom je dodávateľ alebo subdodávateľ registrovaný.

27.4. **Zmluvy podliehajúce utajeniu a rozhodnutia o grantoch**

a) Bezpečnostné utajenie zmlúv alebo dohôd o poskytnutí grantu musí zohľadňovať tieto zásady:

— Komisia určí podľa potreby aspekty zmluvy podliehajúcej utajeniu, ktoré vyžadujú ochranu a následné bezpečnostné utajenie; musí pri tom zohľadniť pôvodné bezpečnostné utajenie, ktoré pôvodca pridelil informáciám vytvoreným pred uzatvorením zmluvy podliehajúcej utajeniu,

— celkový stupeň utajenia zmluvy nesmie byť nižší ako najvyššia úroveň utajenia ktoréhokoľvek z jej prvkov,

— utajované skutočnosti EÚ, ktoré vznikli počas zmluvných činností, sú utajované v súlade s pokynmi k bezpečnostnému utajovaniu,

— Komisia je v prípade potreby zodpovedná za zmenu celkového stupňa utajenia zmluvy alebo bezpečnostného utajenia ktoréhokoľvek z prvkov zmluvy, pričom spolupracuje s pôvodcom a informuje všetky zainteresované strany,

— utajené skutočnosti sprístupnené dodávateľovi alebo subdodávateľovi alebo vytvorené v rámci zmluvnej činnosti nesmú byť použité na iné účely než tie, ktoré sú vymedzené zmluvou podliehajúcou utajeniu, a nesmú byť sprístupnené tretím stranám bez predchádzajúceho písomného súhlasu pôvodcu.

b) Komisia a NBÚ/UBÚ príslušných členských štátov sú zodpovedné za zabezpečenie toho, že dodávatelia a subdodávatelia, s ktorými uzatvorili zmluvy podliehajúce utajeniu zahŕňajúce informácie označené ako CONFIDENTIEL UE alebo vyšším stupňom utajenia, prijmú všetky kroky potrebné na ochranu takýchto utajovaných skutočností EÚ, ktoré im boli vydané alebo boli nimi vytvorené pri výkone zmluvy podliehajúcej utajeniu v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi. Nedodržiavanie bezpečnostných požiadaviek môže viesť k ukončeniu zmluvy podliehajúcej utajeniu.

c) Všetky priemyselné alebo iné subjekty, ktoré sú stranami zmlúv podliehajúcich utajeniu, ktoré zahŕňajú prístup k skutočnostiam so stupňom utajenia CONFIDENTIEL UE alebo vyšším, musia byť držiteľmi národnej FSC. FSC vydáva NBÚ/UBÚ členského štátu s cieľom potvrdiť, že zariadenie je schopné zabezpečiť a poskytnúť adekvátnu bezpečnostnú ochranu utajovaných skutočností EÚ do príslušného stupňa utajenia.

d) V prípade uzatvorenia zmluvy podliehajúcej utajeniu bezpečnostný pracovník zariadenia (FSO) určený vedením dodávateľa alebo subdodávateľa zodpovedá za požiadanie o osobnú bezpečnostnú previerku (PSC) všetkých osôb, ktoré sú zamestnané v priemyselných alebo iných subjektoch registrovaných v členskom štáte EÚ a ktorých funkcia vyžaduje prístup ku skutočnostiam so stupňom utajenia CONFIDENTIEL UE alebo vyšším na základe zmluvy podliehajúcej utajeniu, ktorú má vykonať NBÚ/UBÚ daného členského štátu v súlade s jeho vnútroštátnymi právnymi predpismi.

▼M3

e) Zmluvy podliehajúce utajeniu musia zahŕňať SAL, ako je vymedzená v bode 27.2 písm. j). SAL musí obsahovať SCG.

f) Pred začatím rokovaní o zmluve podliehajúcej utajeniu sa Komisia spojí s NBÚ/UBÚ členského štátu, v ktorom sú dotknuté priemyselné alebo iné subjekty registrované, s cieľom získať potvrdenie, že sú držiteľmi platnej FSC zodpovedajúcej stupňu bezpečnostného utajenia zmluvy.

g) Obstarávateľ nesmie uzavrieť zmluvu podliehajúcu utajeniu s prednostným hospodárskym subjektom predtým, ako tento získa platné osvedčenie FSC.

h) Pokiaľ vnútroštátne zákony a iné právne predpisy členského štátu nestanovujú inak, FSC sa nevyžaduje pre zmluvy, ktoré zahŕňajú skutočnosti so stupňom utajenia RESTREINT UE.

i) V prípade ponúk na zmluvy podliehajúce utajeniu musí výzva obsahovať ustanovenie, že hospodársky subjekt, ktorý nepredloží ponuku alebo nie je vybratý, bude povinný vrátiť všetky dokumenty v stanovenej časovej lehote.

j) Môže dôjsť k situácii, že dodávateľ bude musieť rokovať so subdodávateľmi na rôznych úrovniach o subdodávateľských zmluvách podliehajúcich utajeniu. Dodávateľ je zodpovedný za zabezpečenie toho, aby boli všetky subdodávateľské činnosti realizované v súlade so spoločnými minimálnymi normami stanovenými v tomto oddiele. Dodávateľ však nesmie postúpiť utajované skutočnosti alebo materiály EÚ subdodávateľovi bez predchádzajúceho písomného súhlasu pôvodcu.

k) Podmienky, za ktorých môže dodávateľ uzatvárať subdodávateľské zmluvy, musia byť definované vo verejnej súťaži, resp. výzve na predkladanie ponúk, a v zmluve. So subjektmi registrovanými v štáte, ktorý nie je členským štátom EÚ, sa nemôže uzavierať žiadna subdodávateľská zmluva bez výslovného písomného povolenia Komisie.

l) Počas celého trvania zmluvy bude Komisia v spolupráci s príslušným NBÚ/UBÚ sledovať súlad so všetkými jej bezpečnostnými ustanoveniami. Oznamovanie bezpečnostných udalostí sa vykonáva v súlade s ustanoveniami stanovenými v časti II oddiele 24 týchto bezpečnostných predpisov. Zmena alebo odobratie FSC sa bezodkladne oznamuje Komisii a všetkým ostatným NBÚ/UBÚ, ktorým bola oznámená.

m) Ukončenie zmluvy podliehajúcej utajeniu alebo subdodávateľskej zmluvy podliehajúcej utajeniu oznámi Komisia a/alebo prípadne NBÚ/UBÚ bezodkladne NBÚ/UBÚ členského štátu, v ktorom je dodávateľ alebo subdodávateľ registrovaný.

n) Po vypovedaní alebo ukončení zmluvy podliehajúcej utajeniu alebo subdodávateľskej zmluvy podliehajúcej utajeniu dodávatelia a subdodávatelia naďalej dodržiavajú spoločné minimálne normy stanovené v tomto oddiele a dôvernosť utajovaných skutočností.

o) Osobitné ustanovenia pre likvidáciu utajovaných skutočností po skončení zmluvy sa stanovia v SAL alebo v iných príslušných ustanoveniach bezpečnostných nariadení.

p) Povinnosti a podmienky uvedené v tomto oddiele sa vzťahujú *mutatis mutandis* na postupy poskytovania grantov na základe rozhodnutí, a najmä na príjemcov takýchto grantov. Rozhodnutie o poskytnutí grantu stanovuje všetky povinnosti príjemcu.

▼M3

27.5. **Návštevy**

Návštevy zamestnancov Komisie uskutočňované v členských štátoch v súvislosti so zmluvami podliehajúcimi utajeniu u priemyselných alebo iných subjektov realizujúcich zmluvy podliehajúce utajeniu EÚ sa musia pripraviť v spolupráci s dotknutým NBÚ/UBÚ. Návštevy zamestnancov priemyselných alebo iných subjektov v rámci zmlúv podliehajúcich utajeniu EÚ sa musia pripraviť v spolupráci medzi dotknutými NBÚ/UBÚ. NBÚ/UBÚ, ktorých sa týka zmluva podliehajúca utajeniu EÚ, sa však môžu dohodnúť na postupe, pri ktorom sa návštevy zamestnancov priemyselných alebo iných subjektov môžu pripravovať priamo.

27.6. **Odovzdávanie a preprava utajovaných skutočností EÚ**

a) Pokiaľ ide o odovzdávanie utajovaných skutočností EÚ, uplatňujú sa ustanovenia časti II oddielu 21 týchto bezpečnostných predpisov. S cieľom doplniť tieto ustanovenia sa budú uplatňovať akékoľvek existujúce platné postupy medzi členskými štátmi.

b) Medzinárodná preprava utajovaného materiálu EÚ týkajúceho sa zmlúv podliehajúcich utajeniu sa uskutočňuje v súlade s vnútroštátnymi postupmi členských štátov. Pri preskúmaní bezpečnostných opatrení medzinárodnej prepravy sa uplatnia tieto zásady:

   — bezpečnosť je zabezpečená vo všetkých etapách prepravy a za všetkých okolností, od miesta pôvodu do miesta konečného určenia,

   — úroveň ochrany zásielky je stanovená najvyšším stupňom utajenia materiálu v nej obsiahnutého,

   — pre spoločnosti realizujúce prepravu sa v prípade potreby vykoná FSC. V takýchto prípadoch sa zamestnanci pracujúci so zásielkou musia podrobiť bezpečnostnej previerke v súlade so spoločnými minimálnymi normami stanovenými v tomto oddiele,

   — cesty sa vykonávajú priamo z miesta pôvodu do miesta určenia a uskutočňujú sa v čo najkratšom možnom čase,

   — ak je to možné, cesta by mala prechádzať cez územia členských štátov EÚ. Cesty cez štáty, ktoré nie sú členmi EÚ, sa realizujú len v prípade, ak s nimi súhlasia NBÚ/UBÚ štátov odosielateľa a príjemcu,

   — pred akýmkoľvek presunom utajovaného materiálu EÚ odosielateľ vypracuje plán prepravy, ktorý schváli dotknutý NBÚ/UBÚ.

▼M1

Dodatok 1

POROVNANIE NÁRODNÝCH BEZPEČNOSTNÝCH UTAJENÍ

Utajenie EÚ	TRES SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Utajenie ZEÚ	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Utajenie Euratom	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Utajenie NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
Belgicko	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Česká republika	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dánsko	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Nemecko	Streng geheim	Geheim	VS ([1]) — Vertraulich	VS — Nur für den Dienstgebrauch
Estónsko	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Grécko	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Španielsko	Secreto	Reservado	Confidencial	Difusión Limitada
Francúzsko	Très Secret Défense ([2])	Secret Défense	Confidentiel Défense	
▼M4				
Croatia	Vrlo tajno	Tajno	Povjerljivo	Ograničeno
▼M1				
Írsko	Top Secret	Secret	Confidential	Restricted
Taliansko	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Lotyšsko	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo

▼**M1**

Luxembursko	Très Secret	Secret	Confidentiel	Diffusion restreinte
Maďarsko	Szigorúan titkos !	Titkos !	Bizalmas !	Korlátozott terjesztésű !
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Holandsko	Stg ([3]). Zeer Geheim	Stg. Geheim	Stg. Confidentieel	Departementaal-vertrouwelijk
Rakúsko	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poľsko	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalsko	Muito Secreto	Secreto	Confidencial	Reservado
Slovinsko	Strogo tajno	Tajno	Zaupno	SVN Interno
Slovensko	Prísne tajné	Tajné	Dôverné	Vyhradené
Fínsko	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Švédsko	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Spojené kráľovstvo	Top Secret	Secret	Confidential	Restricted

([1]) VS = Verschlusssache.
([2]) Utajenie Trés Secret Défense, ktoré sa vzťahuje na prioritné otázky vlády, možno zmeniť len na základe oprávnenia predsedu vlády.
([3]) Stg = staatsgeheim.

▼B

Dodatok 2

PRAKTICKÝ NÁVOD NA UTAJOVANIE

Tento návod je iba orientačný a nie je ho možné chápať tak, že mení podstatné ustanovenia, ktoré sú upravené v oddieloch 16, 17, 20 a 21.

Utajenie	Kedy	Kto	Označenie	Zníženie stupňa utajenia/zrušenie stupňa utajenia/likvidácia	
				Kto	Kedy
►M1 TRES SECRET UE/EU TOP SECRET ◄: Toto utajenie sa vzťahuje iba na informácie a materiály, ktorých neoprávnené sprístupnenie by mohlo spôsobiť mimoriadne vážne poškodenie najdôležitejších záujmov Európskej únie alebo jedného alebo viacerých jej členských štátov [16.1].	Odcudzenie položiek klasifikovaných ako ►M1 TRES SECRET UE/EU TOP SECRET ◄ by mohlo: — ohroziť priamo vnútornú stabilitu EÚ alebo jedného alebo viacerých jej členských štátov alebo spriatelených štátov — mimoriadne vážne poškodiť vzťahy so spriatelenými 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 útvarov [17.1]. Pôvodcovia určujú dátum, obdobie alebo udalosť, kedy je možné obsah utajiť na nižšom stupni utajenia alebo zrušiť stupeň utajenia [16.2]. Inak dokumenty revidujú aspoň raz za päť rokov, aby sa zabezpečilo, že je stále potrebný pôvodný stupeň utajenia [17.3].	►M1 TRES SECRET UE/EU TOP SECRET ◄ a prípadne bezpečnostný ukazovateľ a/alebo bezpečnostné značenie Európskej bezpečnostnej a obrannej politiky sa priraďuje dokumentom, ktoré sú ►M1 TRES SECRET UE/EU TOP SECRET ◄, 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 stupňa utajenia alebo zrušenie stupňa utajenia spočíva výlučne na pôvodcovi, ktorý o zmenách informuje akýchkoľvek následných adresátov, ktorým zaslal alebo kopíroval dokument [17.3]. Dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ likviduje centrálny register alebo vedľajší register, ktorý je za nich zodpovedný. Všetky zlikvidované dokumenty musia byť uvedené v potvrdení o likvidácii podpísanom kontrolným úradníkom ►M1 TRES SECRET UE/EU TOP SECRET ◄ a úradníkom, ktorý bol svedkom likvidácie. V knihe sa urobí zápis o likvidácii. Register uchováva potvrdenia o likvidácii spolu s rozdeľovníkmi desať rokov [22.5].	Nadbytočné kópie a dokumenty, ktoré nie sú viac potrebné, sa musia zlikvidovať. [22.5] Dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ vrátane utajeného odpadu z prípravy dokumentov ►M1 TRES SECRET UE/EU TOP SECRET ◄, napríklad pokazené kópie, písané poznámky a prepisovací papier, sa musia zlikvidovať za dozoru kontrolného úradníka ►M1 TRES SECRET UE/EU TOP SECRET ◄ spálením, rozdrvením, skartovaním alebo inou deštrukciou tak, aby ich nebolo možné rozpoznať alebo obnoviť [22.5].

▼B

Utajenie	Kedy	Kto	Označenie	Zníženie stupňa utajenia/zrušenie stupňa utajenia/likvidácia	
				Kto	Kedy
►M1 SECRET UE ◄: Toto utajenie sa vzťahuje iba na informácie a materiály, ktorých neoprávnené sprístupnenie by mohlo spôsobiť vážne poškodenie najdôležitejších záujmov Európskej únie alebo jedného alebo viacerých jej členských štátov [16.1].	Odcudzenie položiek klasifikovaných ako ►M1 SECRET UE ◄ by mohlo: — zvýšiť medzinárodné napätie — vážne poškodiť vzťahy so spriatelenými 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 útvarov [17.1]. Pôvodcovia určujú obdobie kedy je možné obsah utajiť na nižšom stupni utajenia alebo zrušiť stupeň utajenia [16.2]. Inak dokumenty revidujú aspoň raz za päť rokov, aby sa zabezpečilo, že je stále potrebný pôvodný stupeň utajenia [17.3].	►M1 SECRET UE ◄ a prípadne bezpečnostný ukazovateľ a/alebo bezpečnostné značenie Európskej bezpečnostnej a obrannej politiky sa priraďuje dokumentom, ktoré sú ►M1 SECRET UE ◄, 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 stupňa utajenia alebo zrušenie stupňa utajenia spočíva výlučne na pôvodcovi, ktorý o zmenách informuje akýchkoľvek následných adresátov, ktorým zaslal alebo kopíroval dokument [17.3]. Dokumenty ►M1 SECRET UE ◄ likviduje register alebo vedľajší register, ktorý je za nich zodpovedný pod dohľadom osoby s bezpečnostnou previerkou. Všetky zlikvidované dokumenty ►M1 SECRET UE ◄ musia byť uvedené v potvrdení o likvidácii. Register uchováva potvrdenia o likvidácii spolu s rozdeľovníkmi tri roky [22.5].	Nadbytočné kópie a dokumenty, ktoré nie sú viac potrebné, sa musia zlikvidovať [22.5]. Dokumenty ►M1 SECRET UE ◄ vrátane utajeného odpadu z prípravy dokumentov ►M1 SECRET UE ◄, napríklad pokazené kópie, pracovné návrhy, písané poznámky a prepisovací papier, sa musia zlikvidovať spálením, rozdrvením, skartovaním alebo inou deštrukciou tak, aby ich nebolo možné rozpoznať alebo obnoviť [22.5].
►M1 CONFIDENTIEL UE ◄:	Odcudzenie položiek klasifikovaných ako ►M1 CONFIDENTIEL UE ◄ by mohlo: — vážne poškodiť diplomatické vzťahy, t. j. viesť k formálnym protestom alebo iným sankciám	Oprávnené osoby (pôvodcovia), generálni riaditelia, vedúci útvarov [17.1].	►M1 CONFIDENTIEL UE ◄ a prípadne bezpečnostný ukazovateľ a/alebo bezpečnostné značenie Európskej bezpečnostnej a obrannej politiky sa priraďuje dokumentom, ktoré sú ►M1 CONFIDENTIEL UE ◄, strojovo a ručne, alebo tlačou na predtlačené registrované tlačivá [16.4, 16.5, 16.3].	Zníženie stupňa utajenia alebo zrušenie stupňa utajenia spočíva výlučne na pôvodcovi, ktorý o zmenách informuje akýchkoľvek následných adresátov, ktorým zaslal alebo kopíroval dokument [17.3].	Nadbytočné kópie a dokumenty, ktoré nie sú viac potrebné, sa musia zlikvidovať [22.5].

▼B

Utajenie	Kedy	Kto	Označenie	Zníženie stupňa utajenia/zrušenie stupňa utajenia/likvidácia	
				Kto	Kedy
Toto utajenie sa vzťahuje na informácie a materiály, ktorých neoprávnené sprístupnenie by mohlo spôsobiť poškodenie dôležitých záujmov Európskej únie alebo jedného alebo viacerých jej členských štátov [16.1].	— 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 situáciu významných organizácií — znemožniť vyšetrovanie alebo umožniť spáchanie vážnych zločinov; — pracovať významne proti finančným, peňažným, ekonomickým a obchodným záujmom EÚ alebo jej členských štátov; — vážne ohroziť rozvoj alebo realizáciu významných politík EÚ; — ukončiť alebo inak vážne znemožniť významné činnosti EÚ.	Pôvodcovia určujú dátum alebo obdobie, kedy je možné obsah utajiť na nižšom stupni utajenia alebo zrušiť stupeň utajenia. Inak dokumenty revidujú aspoň raz za päť rokov, aby sa zabezpečilo, že je stále potrebný pôvodný stupeň utajenia. [17.3]	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].	Dokumenty ►**M1** CONFIDENTIEL UE ◄ likviduje register, ktorý je za nich zodpovedný, za dozoru preverenej osoby. Ich likvidácia musí byť zaznamenaná v súlade s vnútroštátnymi právnymi predpismi a v prípade Komisie alebo decentralizovaných agentúr EÚ podľa pokynov ►**M2** člena Komisie zodpovedného za bezpečnostné záležitosti ◄ [22.5].	Dokumenty ►**M1** CONFIDENTIEL UE ◄ vrátane utajeného odpadu z prípravy dokumentov ►**M1** CONFIDENTIEL UE ◄, napríklad pokazené kópie, pracovné návrhy, písané poznámky a prepisovací papier, sa musia zlikvidovať spálením, rozdrvením, skartovaním alebo inou deštrukciou tak, aby ich nebolo možné rozpoznať alebo obnoviť [22.5].

▼B

Utajenie	Kedy	Kto	Označenie	Zníženie stupňa utajenia/zrušenie stupňa utajenia/likvidácia	
				Kto	Kedy
►M1 RESTREINT UE ◄: Toto utajenie sa vzťahuje na informácie a materiály, ktorých neoprávnené sprístupnenie by mohlo byť nevýhodné pre záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov [16.1].	Odcudzenie položiek klasifikovaných ako ►M1 RESTREINT UE ◄ 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 neprimeraný zisk alebo výhodu jednotlivcom alebo spoločnostiam — porušiť príslušné záväzky zachovať dôvernosť utajovaných skutočností, ktoré poskytli tretie strany — porušiť štatutárne obmedzenia platné pre sprístupnenie utajovaných skutočností — poškodiť vyšetrovanie alebo umožniť spáchanie zločinu — znevýhodniť EÚ alebo členské štáty pri obchodných alebo politických rokovaniach s ostatnými — zabrániť účinnému rozvoju alebo pôsobeniu politík EÚ — poškodiť príslušné riadenie EÚ a jej činností.	Oprávnené osoby (pôvodcovia), generálni riaditelia, vedúci útvarov [17.1]. Pôvodcovia určujú dátum alebo obdobie, kedy je možné obsah utajiť na nižšom stupni utajenia alebo zrušiť stupeň utajenia [16.2]. Inak dokumenty revidujú aspoň raz za päť rokov, aby sa zabezpečilo, že je stále potrebný pôvodný stupeň utajenia [17.3].	►M1 RESTREINT UE ◄ a prípadne bezpečnostný ukazovateľ a/alebo bezpečnostné značenie Európskej bezpečnostnej a obrannej politiky sa priraďuje dokumentom, ktoré sú ►M1 RESTREINT UE ◄, 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].	Zrušenie stupňa utajenia spočíva výlučne na pôvodcovi, ktorý o zmenách informuje akýchkoľvek následných adresátov, ktorým zaslal alebo kopíroval dokument [17.3]. Dokumenty ►M1 RESTREINT UE ◄ likviduje register, ktorý je za nich zodpovedný, alebo užívateľ podľa pokynov ►M2 člena Komisie zodpovedného za bezpečnostné záležitosti ◄ [22.5].	Nadbytočné kópie a dokumenty, ktoré nie sú viac potrebné, sa musia zlikvidovať [22.5].

▼B

Dodatok 3

Usmernenia o poskytovaní utajovaných skutočností EÚ tretím štátom alebo medzinárodným organizáciám: Úroveň spolupráce 1

POSTUPY

1. Oprávnenie poskytnúť utajované skutočnosti krajinám, ktoré nie sú členmi Európskej únie, alebo iným medzinárodným organizáciám, ktorých bezpečnostná politika a právne predpisy sú porovnateľné s EÚ, spočíva výlučne na Komisii ako kolektívnom orgáne.

2. Až do uzavretia dohody o bezpečnosti je za bezpečnostné záležitosti zodpovedný člen Komisie, ktorý má právo preskúmať žiadosti o poskytnutí utajovaných skutočností EÚ.

3. V takomto prípade, musí:

   — získať stanovisko pôvodcov utajovaných skutočností EÚ, ktoré sa majú poskytnúť;

   — nadviazať potrebné kontakty s bezpečnostnými orgánmi prijímajúcich krajín alebo medzinárodných organizácií, aby overil, či ich bezpečnostná politika a predpisy sú také, aby mohli zaručiť, že poskytnuté utajované skutočnosti sa budú chrániť v súlade s týmito bezpečnostnými predpismi;

   — 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 PREDPISY, KTORÉ MUSIA UPLATŇOVAŤ PRÍJEMCOVIA

5. Člen Komisie zodpovedný za bezpečnostné záležitosti oznámi prijímajúcim štátom alebo medzinárodným organizáciám rozhodnutie Komisie o schválení poskytnutia utajovaných skutočností EÚ.

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

   — nepoužijú utajované skutočnosti na iné ako dohodnuté účely,

   — utajované skutočnosti budú chrániť v súlade s týmito bezpečnostnými predpismi, najmä osobitnými pravidlami uvedenými nižšie.

7. Personál

   a) Počet úradníkov s prístupom k utajovaným skutočnostiam EÚ musí byť podľa zásady potreba poznať obmedzený výlučne na tie osoby, ktorých povinnosti takýto prístup vyžadujú.

   b) Všetci úradníci alebo štátni príslušníci, ktorí majú oprávnenie na prístup k utajovaným skutočnostiam ►M1 CONFIDENTIEL UE ◄ alebo vyššieho stupňa utajenia, musia mať potvrdenie o bezpečnostnej previerke pre príslušný stupeň alebo potvrdenie o rovnocennej previerke, ktoré vydala vláda ich vlastného štátu.

8. Prenos dokumentov

   a) Praktické postupy pre prenos dokumentov sa ustanovia v dohode. Až do uzavretia takejto dohody sa uplatňujú ustanovenia oddielu 21. Dohoda musí najmä určiť registre, ktorým musia byť utajované skutočnosti postúpené.

▼B

b) Ak utajované skutočnosti, ktorých poskytnutie Komisia povolila, zahŕňajú utajované skutočnosti ►M1 TRES SECRET UE/EU TOP SECRET ◄, prijímajúci štát alebo medzinárodná organizácia založí centrálny register EÚ a prípadne vedľajšie registre EÚ. Tieto registre musia dôsledne uplatňovať predpisy, ktoré sú rovnocenné s ustanoveniami v oddieli 22 týchto bezpečnostných predpisov.

9. Registrácia

Len čo register obdrží dokument EÚ utajený ako ►M1 CONFIDENTIEL UE ◄ alebo na vyššom stupni utajenia, zaeviduje dokument v osobitnom 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 príjme a dátum vrátenia dokumentu pôvodcovi v EÚ a dátum likvidácie.

10. Likvidácia

a) utajované dokumenty EÚ sa likvidujú v súlade s pokynmi uvedenými v oddieli 22 týchto bezpečnostných predpisov. Kópie potvrdení o likvidácii pre dokumenty ►M1 SECRET UE ◄ a ►M1 TRES SECRET UE/EU TOP SECRET ◄ sa zasielajú do registra EÚ, ktorý dokumenty postúpil.

b) utajované dokumenty musia byť zahrnuté v plánoch likvidácie v núdzových situáciách pre vlastné utajované dokumenty orgánov príjemcu.

11. Ochrana dokumentu

Musia sa prijať všetky potrebné opatrenia, aby sa zabránilo prístupu nepovolaných osôb k utajovaným skutočnostiam EÚ.

12. Kópie, preklady a výpisy

Bez oprávnenia vedúceho príslušnej bezpečnostnej organizácie sa nesmú robiť žiadne fotokópie ani preklad dokumentu ►M1 CONFIDENTIEL UE ◄ alebo ►M1 SECRET UE ◄ a ani výpisy z takéhoto dokumentu. Vedúci dotknutej bezpečnostnej organizácie zaeviduje a skontroluje kópie, preklady alebo výpisy z nich a podľa potreby ich opečiatkuje.

Reprodukciu alebo preklad dokumentu ►M1 TRES SECRET UE/EU TOP SECRET ◄ môže povoliť iba úrad pôvodcu, ktorý určí počet oprávnených kópií; ak úrad pôvodcu nie je možné určiť, 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 prijmú nasledujúce opatrenia, ktoré podliehajú uzavretiu dohody o bezpečnosti:

a) záležitosť sa prešetrí, aby sa stanovili okolnosti, za ktorých došlo k porušeniu bezpečnosti;

b) upovedomí sa ►M2 riaditeľstvo Komisie pre bezpečnosť ◄, príslušný národný bezpečnostný úrad a úrad pôvodcu, alebo sa jasne uvedie, že úrad pôvodcu nebol oboznámený, ak k tomu nedošlo;

c) prijmú sa opatrenia na minimalizovanie účinkov porušenia bezpečnosti;

d) opätovne sa zvážia a zavedú opatrenia, aby sa zabránilo opakovaniu;

e) zavedú sa akékoľvek opatrenia, ktoré odporúča ►M2 riaditeľstvo Komisie pre bezpečnosť ◄ na zabránenia opakovania.

▼B

14. Inšpekcie

Na základe dohôd s danými štátmi alebo medzinárodnými organizáciami sa povolí, aby ►M2 riaditeľstvo Komisie pre bezpečnosť ◄ posúdil účinnosť opatrení na ochranu poskytnutých utajovaných skutočností EÚ.

15. Podávanie správ

Za predpokladu uzavretia dohody o bezpečnosti, pokiaľ daný štát alebo organizácia má k dispozícii utajované skutočnosti EÚ, ročne predkladá v termíne určenom pri poskytnutí utajovaných skutočností správu, ktorá potvrdí, že sa tieto bezpečnostné predpisy naďalej dodržiavajú.

▼B

Dodatok 4

Usmernenia o poskytovaní utajovaných skutočností EÚ tretím štátom alebo medzinárodným organizáciám: Úroveň spolupráce 2

POSTUPY

1. Oprávnenie poskytnúť utajované skutočnosti tretím štátom alebo iným medzinárodným organizáciám, ktorých bezpečnostná politika a nariadenia sú výrazne odlišné od EÚ, spočíva výlučne na pôvodcovi. Oprávnenie poskytnúť utajované skutočnosti EÚ vypracované v rámci Komisii spočíva na Komisii ako kolektívnom orgáne.

2. V zásade ide o utajované skutočnosti utajené až do stupňa utajenia ►M1 SECRET UE ◄ vrátane; nie sú zahrnuté utajované skutočnosti, ktoré sú chránené osobitnými bezpečnostnými označeniami alebo znakmi.

3. Až do uzavretia dohody o bezpečnosti je za bezpečnostné záležitosti zodpovedný člen Komisie, ktorý má právo preskúmať žiadosti o poskytnutie utajovaných skutočností EÚ.

4. V takomto prípade, musí:

   — získať stanovisko pôvodcov utajovaných skutočností EÚ, ktoré sa majú poskytnúť,

   — nadviazať potrebné kontakty s bezpečnostnými orgánmi prijímajúcich krajín alebo medzinárodných organizácií, aby sa zistili informácie o ich bezpečnostnej politike a právnych predpisoch, a najmä aby sa vypracovala tabuľka porovnávajúcu utajovanie uplatňované v EÚ a v danom štáte alebo organizácii,

   — zabezpečí zasadnutie Poradnej skupiny Komisie pre bezpečnostnú politiku alebo v rámci tichého postupu, ak je to potrebné, informuje sa u národných bezpečnostných úradov členských štátov v súvislosti so získaním 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 skutočnosti, ktoré EÚ poskytla,

   — návrhov, ktoré sa týkajú praktických postupov pre oboznamovanie sa s utajovanými skutočnosťami EÚ (napríklad zabezpečenie cenzurovaných verzií textu) a dokumentmi, ktoré sa prenášajú (zachovanie alebo odstránenie hlavičiek utajovania EÚ, osobitné znaky atď.),

   — zníženia stupňa utajenia alebo zrušenie stupňa utajenia pred poskytnutím utajovaných skutočností 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 PREDPISY, KTORÉ MUSIA UPLATŇOVAŤ PRÍJEMCOVIA

7. Člen Komisie zodpovedný za bezpečnostné záležitosti oznámi prijímajúcim štátom alebo medzinárodným organizáciám rozhodnutie Komisie o schválení poskytnutia utajovaných skutočností EÚ a jeho obmedzeniach.

▼B

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

— nepoužijú utajované skutočnosti na iné ako dohodnuté účely,

— utajované skutočnosti budú chrániť v súlade s bezpečnostnými predpismi, 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 oboznamovanie sa s utajovanými dokumentmi EÚ (odstránenia označenia utajenia EÚ, osobitné znaky atď.).

10. Personál

a) počet úradníkov s prístupom k utajovaným skutočnostiam EÚ musí byť podľa zásady potreba poznať obmedzený výlučne na tie osoby, ktorých povinnosti takýto prístup vyžadujú;

b) všetci úradníci alebo štátni príslušníci, ktorí majú oprávnenie na prístup k utajovanými skutočnostiam EÚ, musia mať potvrdenie o národnej bezpečnostnej previerke alebo oprávnenia na prístup na zodpovedajúcom stupni utajenia, ktoré je porovnateľné so stupňom utajenia EÚ, ako je vymedzené v porovnávacej tabuľke;

c) tieto národné bezpečnostné previerky sa postupujú ►M2 riaditeľovi riaditeľstva Komisie pre bezpečnosť ◄ na informáciu.

11. Prenos dokumentov

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

12. Registrácia pri príchode

Národný bezpečnostný úrad štátu adresáta alebo zodpovedajúci v štáte, ktorý obdrží v mene vlády utajované skutočnosti postúpené Komisiou, alebo bezpečnostný úrad prijímajúcej medzinárodnej organizácie vytvoria osobitný register na zaznamenávanie utajovaných skutočností EÚ pri ich príchode. Register obsahuje stĺpce uvádzajúce dátum prijatia, údaje o dokumente (dátum, referenčné číslo a číslo kópie), jeho utajenie, názov, meno adresáta alebo jeho postavenie, dátum návratu potvrdenia o prijatí a dátum návratu dokumentu do EÚ alebo dátum jeho likvidácie.

13. Návrat dokumentov

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

14. Ochrana

a) Ak sa dokumenty nepoužívajú, skladujú sa v bezpečnostných schránkach, ktoré sú schválené na skladovanie vnútroštátnych utajovaných materiálov rovnakého stupňa 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 skutočnostiam 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, ktorý poznal kombináciu, alebo ak vznikne nebezpečenstvo odcudzenia.

▼B

b) Utajené dokumenty EÚ odstraňujú z bezpečnostnej schránky iba tí úradníci, ktorí sú preverení na prístup k utajovaným skutočnostiam EÚ a majú potrebu poznať. Sú naďalej zodpovední za uschovávanie týchto dokumentov, pokiaľ ich majú k dispozícii, a najmä za zabezpečenie toho, aby žiadna nepovolaná osoba nemala prístup k dokumentom. Zabezpečujú tiež, aby sa dokumenty po ich konzultovaní a po pracovných hodinách uložili do bezpečnostnej schránky.

c) Bez oprávnenia ►M2 riaditeľstva Komisie pre bezpečnosť ◄ sa nesmú robiť žiadne fotokópie ani výpisy dokumentov klasifikovaných ako ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia.

d) Postup pre rýchlu a úplnú likvidáciu dokumentov v núdzovom stave určí a potvrdí ►M2 riaditeľstvo Komisie pre bezpečnosť ◄.

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 hodín (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 prijmú tieto opatrenia:

a) okamžite sa predloží správa ►M2 Riaditeľstvu Komisie pre bezpečnosť ◄ alebo národnému bezpečnostnému úradu členského štátu, ktorý dal podnet na zaslanie dokumentov (s kópiou ►M2 Riaditeľstvu Komisie pre bezpečnosť ◄);

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

17. Inšpekcie

Na základe dohôd s danými štátmi alebo medzinárodnými organizáciami sa povolí, aby ►M2 riaditeľstvo Komisie pre bezpečnosť ◄ vykonal posúdenie účinnosti opatrení na ochranu poskytnutých utajovaných skutočností EÚ.

18. Podávanie správ

Za predpokladu uzavretia dohody o bezpečnosti, pokiaľ daný štát alebo organizácia má k dispozícii utajované skutočnosti EÚ, ročne predkladá v termíne určenom pri poskytnutí utajovaných skutočností správu, ktorá potvrdí, že sa tieto bezpečnostné predpisy naďalej dodržiavajú.

▼B

Dodatok 5

Usmernenia o poskytnutí utajovaných skutočností 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 predpismi, ale takáto spolupráca môže vyžadovať poskytnutie utajovaných skutočností EÚ.

2. Oprávnenie poskytnúť utajované skutočnosti EÚ tretím štátom alebo medzinárodným organizáciám, ktorých bezpečnostná politika a právne predpisy sú výrazne odlišné od politiky a právnych aktov EÚ, spočíva výlučne na pôvodcovi. Oprávnenie poskytnúť utajované skutočnosti EÚ, ktoré vznikli v rámci Komisie, spočíva výlučne na Komisii ako kolektívnom orgáne.

   V zásade sa jedná o skutočnosti utajené až do stupňa utajenia ►M1 SECRET UE ◄ vrátane; nevzťahuje sa to na utajované skutočnosti chránené osobitnými bezpečnostnými označeniami a znakmi.

3. Komisia zváži primeranosť poskytnutia utajovaných skutočností, posúdi potrebu príjemcu poznať a rozhodne o povahe utajovaných skutočností, ktoré sa môžu odoslať.

4. Ak Komisia vyjadrí súhlas, člen Komisie zodpovedný za bezpečnostné záležitosti

   — získa stanovisko pôvodcov utajovaných skutočností EÚ, ktoré sa majú poskytnúť,

   — zabezpečí zasadnutie Poradnej skupiny Komisie pre bezpečnostnú politiku alebo v rámci tichého postupu, ak je to potrebné, sa informuje u národných bezpečnostných úradov členských štátov v súvislosti so získaním 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) stupňa utajenia skutočností, ktoré sa môžu poskytnúť;

   c) zníženia stupňa utajenia alebo zrušenie stupňa utajenia pred tým, ako sa utajované skutočnosti poskytnú;

   d) postupov pre oboznamovanie sa s dokumentmi, ktoré sa majú poskytnúť (pozri odsek nižšie);

   e) možných spôsobov prenosu (použitie verejných poštových služieb, verejných alebo bezpečnostných telekomunikačných systémov, diplomatickej pošty, preverených kuriérov atď.).

6. Dokumenty, ktoré sa poskytnú 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 utajovaných skutočností s požadovanými kontrolnými opatreniami spôsobov príjemcu na prenos dokumentov.

▼B

7. ►M2 Člen Komisie zodpovedný za bezpečnostné záležitosti ◄ postúpi Komisii stanovisko Poradnej skupiny Komisie pre bezpečnostnú politiku na rozhodnutie.

8. Po schválení Komisie, ktoré sa týka poskytnutia utajovaných skutočností EÚ a praktických vykonávajúcich postupov, ►M2 riaditeľstvo Komisie pre bezpečnosť ◄ zabezpečí potrebné spojenie s bezpečnostným úradom daného štátu alebo organizácie, aby sa umožnilo uplatnenie predpokladaných bezpečnostných opatrení.

9. Člen Komisie zodpovedný za bezpečnostné opatrenia informuje členské štáty o povahe a stupni utajenia utajovaných skutočností, pričom uvedie zoznam krajín a organizácií, ktorým sa dané utajované skutočnosti môžu poskytnúť, ako o tom rozhodla Komisia.

10. ►M2 Riaditeľstvo Komisie pre bezpečnosť ◄ prijme všetky potrebné opatrenia, aby sa umožnil odhad následnej škody a preskúmali postupy.

Ak sa zmenia podmienky spolupráce, Komisia záležitosť opätovne zváži.

BEZPEČNOSTNÉ PREDPISY, KTORÉ MUSIA UPLATŇOVAŤ PRÍJEMCOVIA

11. Člen Komisie zodpovedný za bezpečnostné záležitosti oznámi prijímajúcim štátom alebo medzinárodným organizáciám rozhodnutie Komisie o schválení poskytnutia utajovaných skutočností 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 utajované skutočnosti na iné účely ako sú účely, o ktorých rozhodla Komisia,

— utajované skutočnosti budú chrániť tak, ako to vyžaduje Komisia.

13. Prenos dokumentov

a) dohodnú sa praktické postupy na prenos dokumentov medzi ►M2 riaditeľstvom Komisie pre bezpečnosť ◄ a bezpečnostnými úradmi prijímajúcich štátov alebo medzinárodných organizácií. Takéto postupy špecifikujú najmä presné adresy, na ktoré sa dohody musia doručovať;

b) dokumenty ►M1 CONFIDENTIEL UE ◄ a vyššieho stupňa utajenia sa musia prenášať v dvojitom obale. Vnútorná obálka je označená zvláštnou pečiatkou alebo kódovým označením, o ktorom sa rozhodne, a uvádza osobitné utajenie schválené pre dokument. Pre každý utajený dokument sa zvlášť priloží tlačivo o prijatí. Tlačivo o prijatí, ktoré samo o sebe nie je utajené, 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 na účely prijatia. Bezpečnostné utajenie nie je na vonkajšej obálke uvedené;

d) kuriérom sa vždy odovzdá potvrdenie o prijatí, na ktorom je uvedené číslo zásielky.

▼B

14. Registrácia pri príchode

Národný bezpečnostný úrad štátu adresáta alebo zodpovedajúci orgán v štáte, ktorý obdrží v mene vlády utajované skutočnosti postúpené Komisiou, alebo bezpečnostný úrad prijímajúcej medzinárodnej organizácie vytvoria osobitný register na zaznamenávanie utajovaných skutočností 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 prijatí a dátum návratu dokumentu do EÚ alebo dátum jeho likvidácie.

15. Použitie a ochrana vymenených utajovaných skutočností

a) s utajovanými skutočnosťami so stupňom utajenia ►M1 SECRET UE ◄ sa oboznamujú osobitne určení úradníci, ktorí majú oprávnenie na prístup k utajovaným skutočnostiam s takýmto stupňom utajenia. Uschovávajú sa v kvalitných bezpečnostných kartotékach, ktoré môžu otvoriť iba osoby s oprávnením na prístup k utajovaným skutočnostiam, 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. Utajované skutočnosti so stupňom utajenia ►M1 SECRET UE ◄ sa doručujú diplomatickou poštou, bezpečnostnými poštovými službami alebo bezpečnostnými komunikáciami. Dokument ►M1 SECRET UE ◄ sa môže kopírovať iba s písomným súhlasom úradu pôvodcu. Všetky kópie musia byť zaregistrované a monitorujú sa. Pre všetky operácie, ktoré sa týkajú dokumentov ►M1 SECRET UE ◄ sa vydávajú potvrdenia o prijatí;

b) s utajovanými skutočnosťami ►M1 CONFIDENTIEL UE ◄ sa oboznamujú náležito vymenovaní úradníci, ktorí sú oprávnení na získanie informácií o danom predmete. Dokumenty sa uschovávajú v uzamknutých bezpečnostných kartotékach v kontrolovaných oblastiach;

Utajované skutočnosti so stupňom utajenia DÔVERNÉ sa doručujú diplomatickou poštou, bezpečnostnými poštovými službami alebo bezpečnostnými komunikáciami. Kópie dokumentov môže prijímajúci orgán urobiť, pričom počty kópií a ich distribúcia sa zaznamenáva v osobitných registroch;

c) s utajovanými skutočnosťami ►M1 RESTREINT UE ◄ sa dá oboznámiť v priestoroch, ku ktorým nemajú prístup mepovolané 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. Príjemcovia môžu zhotovovať kópie;

d) neutajené skutočnosti nevyžadujú osobitné 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 ►M1 RESTREINT UE ◄ a ►M1 CONFIDENTIEL UE ◄ sa vykoná príslušný záznam v osobitnom registri. V prípade dokumentov ►M1 SECRET UE ◄ sa vydávajú potvrdenia o likvidácii, ktoré podpíšu dve osoby, ktoré boli svedkami likvidácie.

17. Porušenie bezpečnosti

Ak sa utajované skutočnosti ►M1 CONFIDENTIEL UE ◄ alebo ►M1 SECRET UE ◄ odcudzia, alebo ak existuje podozrenie z odcudzenia, národný bezpečnostný úrad daného štátu alebo vedúci bezpečnosti príslušnej organizácie uskutočnia vyšetrovanie okolností odcudzenia. ►M2 Riaditeľstvu Komisie pre bezpečnosť ◄ sa oznámi výsledok vyšetrovania. Prijmú sa potrebné opatrenia na odstránenie nevhodných postupov alebo spôsobov skladovania, ak takéto postupy alebo spôsoby boli príčinou odcudzenia.

▼B

Dodatok 6

ZOZNAM SKRATIEK

PVVOZ	Poradný výbor pre verejné obstarávanie a zmluvy
ÚpK	Úrad pre kódovanie
CIBÚ	Centrálny informačný bezpečnostný úradník
POČBEZ	Počítačová bezpečnosť
KOMBEZ	Komunikačná bezpečnosť
BÚK	►M2 Riaditeľstvo Komisie pre bezpečnosť ◄
EBOP	Európska bezpečnostná a obranná politika
USEÚ	Utajované skutočnosti EÚ
IÚ	Úrad INFOBEZ
INFOBEZ	Informačná bezpečnosť
VUS	Vlastník utajovaných skutočností
ISO	Medzinárodná organizácia pre normalizáciu
IT	Informačná technológia
MIBÚ	Miestny informačný bezpečnostný úradník
MBÚ	Miestny bezpečnostný úradník
BÚZ	Bezpečnostný úradník zasadnutia
NBÚ	Národný bezpečnostný úrad
PC	Osobný počítač
KÚR	Kontrolný úradník registra
BAÚ	Bezpečnostný akreditačný úrad
BPP	Bezpečnostné prevádzkové postupy
OSBP	Vyhlásenie o osobitnej systémovej bezpečnostnej požiadavke
TEMPEST	Úrad pre spôsob zaručenia bezpečnosti elektromagnetického impulzu terminálu
VTS	Vlastník technických systémov

▼M3

UBÚ	určený bezpečnostný úrad
FSC	bezpečnostná previerka zariadenia
FSO	bezpečnostný pracovník zariadenia
PSC	osobná bezpečnostná previerka
SAL	kniha bezpečnostných aspektov
SCG	pokyny k bezpečnostnému utajovaniu