Tento dokument je třeba brát jako dokumentační nástroj a instituce nenesou jakoukoli odpovědnost za jeho obsah

►**B**

ROZHODNUTÍ KOMISE

ze dne 29. listopadu 2001,

kterým se mění její jednací řád

(oznámeno pod číslem K(2001) 3031)

(2001/844/ES, ESUO, Euratom)

(Úř. věst. L 317, 3.12.2001, s. 1)

Ve znění:

		Úřední věstník		
		Č.	Strana	Datum
►**M1**	Rozhodnutí Komise 2005/94/ES, Euratom, ze dne 3. února 2005	L 31	66	4.2.2005
►**M2**	Rozhodnutí Komise 2006/70/ES, Euratom, ze dne 31. ledna 2006	L 34	32	7.2.2006
►**M3**	Rozhodnutí Komise 2006/548/ES, Euratom, ze dne 2. srpna 2006	L 215	38	5.8.2006

▼B

ROZHODNUTÍ KOMISE

ze dne 29. listopadu 2001,

kterým se mění její jednací řád

(oznámeno pod číslem K(2001) 3031)

(2001/844/ES, ESUO, Euratom)

KOMISE EVROPSKÝCH SPOLEČENSTVÍ,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na čl. 218 odst. 2 této smlouvy,

s ohledem na Smlouvu o založení Evropského společenství uhlí a oceli, a zejména na článek 16 této smlouvy,

s ohledem na Smlouvu o založení Evropského společenství pro atomovou energii, a zejména na článek 131 této smlouvy,

s ohledem na Smlouvu o Evropské unii, a zejména na čl. 28 odst. 1 a čl. 41 odst. 1 této smlouvy,

ROZHODLA TAKTO:

Článek 1

Bezpečnostní předpisy Komise, jejichž text je obsažen v příloze k tomuto rozhodnutí, se připojují jako příloha k jednacímu řádu Komise.

Článek 2

Toto rozhodnutí vstupuje v platnost dnem vyhlášení v *Úředním věstníku Evropských společenství*.

Použije se ode dne 1. prosince 2001.

▼B

PŘÍLOHA

BEZPEČNOSTNÍ PŘEDPISY KOMISE

Vzhledem k těmto důvodům:

(1) Pro rozvoj činností Komise v oblastech, které vyžadují určitý stupeň utajení, je důležité vytvořit souborný bezpečnostní systém pro Komisi, další orgány, instituce, úřady a agentury zřízené Smlouvou o založení ES či Smlouvou o Evropské unii nebo na základě těchto smluv, pro členské státy, jakož i pro všechny ostatní příjemce informací Evropské unie, které podléhají utajení (dále jen „utajované skutečnosti EU“).

(2) K zajištění účinnosti takto vytvořeného bezpečnostního systému zpřístupní Komise utajované skutečnosti EU pouze těm vnějším subjektům, které skýtají záruky, že přijaly veškerá nezbytná opatření pro uplatnění pravidel zcela odpovídajících těmto předpisům.

(3) Přijetím těchto předpisů nejsou dotčena nařízení č. 3 ze dne 31. července 1958, kterým se provádí článek 24 Smlouvy o založení Evropského společenství pro atomovou energii ([1]), nařízení Rady (ES) č. 1588/90 ze dne 11. června 1990 o předávání údajů, na které se vztahuje statistická důvěrnost, Statistickému úřadu Evropských společenství ([2]) a rozhodnutí Komise K (95) 1510 v konečném znění ze dne 23. listopadu 1995 o ochraně informačních systémů.

(4) Aby byl zajištěn řádný chod rozhodovacích postupů v Unii, je bezpečnostní systém Komise založen na zásadách stanovených v rozhodnutí Rady 2001/264/ES ze dne 19. března 2001, kterým se přijímají bezpečnostní předpisy Rady ([3]).

(5) Komise upozorňuje, jak je důležité, aby se i ostatní orgány případně připojily k plnění předpisů a norem pro zachování důvěrnosti, které jsou nezbytné pro ochranu zájmů Unie a jejích členských států.

(6) Komise uznává nezbytnost vytvoření své vlastní koncepce bezpečnosti, přičemž bere v úvahu všechny prvky bezpečnosti a zvláštní povahu Komise jakožto orgánu.

(7) Těmito předpisy nejsou dotčeny článek 255 Smlouvy a nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise ([4]).

▼M2

(8) Těmito předpisy nejsou dotčeny článek 286 Smlouvy a nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů.

▼B

Článek 1

Bezpečnostní předpisy Komise jsou uvedeny v příloze.

Článek 2

1. Člen Komise odpovědný za bezpečnostní otázky přijme vhodná opatření, aby zajistil, že při nakládání s utajovanými skutečnostmi EU budou v Komisi úředníci Komise a ostatní zaměstnanci i personál přidělený ke Komisi dodržovat pravidla uvedená v článku 1, a rovněž aby zajistil jejich dodržování na všech pracovištích Komise, včetně jejích zastoupení a kanceláří v Unii a jejích delegací ve třetích zemích, a aby je dodržovali externí smluvní partneři Komise.

([1]) Úř. věst. 17/58, 6.10.1958, s. 406/58.
([2]) Úř. věst. L 151, 15.6.1990, s. 1.
([3]) Úř. věst. L 101, 11.4.2001, s. 1.
([4]) Úř. věst. L 145, 31.5.2001, s. 43.

▼M3

Pokud se smlouva nebo grantová dohoda uzavřená mezi Komisí a externím smluvním partnerem nebo příjemcem týká zpracování utajovaných skutečností EU v prostorách smluvního partnera nebo příjemce, musí být opatření, která má tento smluvní partner nebo příjemce přijmout, aby při nakládání s utajovanými skutečnostmi EU zajistil dodržování pravidel uvedených v článku 1, nedílnou součástí smlouvy nebo grantové dohody.

▼B

2. Členské státy, ostatní orgány jakož i instituce, úřady a agentury zřízené Smlouvami nebo na jejich základě mohou získat utajované skutečnosti EU pod podmínkou, že zajistí, aby se v rámci jejich úřadoven a prostor při práci s utajovanými skutečnostmi dodržovala pravidla zcela odpovídající pravidlům uvedeným v článku 1, což se zejména týká:

a) členů stálých zastoupení členských států při Evropské unii, dále členů národních delegací, kteří se účastní zasedání Komise nebo jejích složek nebo se účastní jiných činností Komise;

b) ostatních členů správních orgánů členských států, kteří nakládají s utajovanými skutečnostmi EU, bez ohledu na to, zda působí na území členských států nebo v cizině;

c) externích smluvních partnerů a přiděleného personálu, kteří nakládají s utajovanými skutečnostmi EU.

Článek 3

Třetím státům, mezinárodním organizacím a dalším orgánům je povoleno získat utajované skutečnosti EU pod podmínkou, že při práci s těmito skutečnostmi zajistí dodržování pravidel zcela odpovídajících pravidlům uvedeným v článku 1.

Článek 4

Při dodržování základních zásad a minimálních bezpečnostních norem uvedených v části I přílohy může člen Komise odpovědný za bezpečnostní otázky přijmout opatření v souladu s částí II přílohy.

Článek 5

Tyto předpisy nahrazují ode dne svého použití:

a) rozhodnutí Komise K (94) 3282 ze dne 30. listopadu 1994 o bezpečnostních opatřeních, která se vztahují na utajované skutečnosti vzniklé nebo předávané v souvislosti s činnostmi Evropské unie;

b) rozhodnutí Komise K (99) 423 ze dne 25. února 1999 o postupech, podle nichž může být úředníkům a ostatním zaměstnancům Evropské komise povolen přístup k utajovaným skutečnostem v držení Komise.

Článek 6

Od dne použití těchto ustanovení platí pro všechny utajované skutečnosti, které jsou k tomuto datu v držení Komise, s výjimkou utajovaných skutečností Euratom, tato pravidla:

a) pokud je vytvořila Komise, považují se za automaticky přeřazené na stupeň utajení ►M1 RESTREINT UE ◄, ledaže autor do 31. ledna 2002 rozhodne o jejich jiném stupni utajení. V takovém případě autor informuje všechny subjekty, jimž je dotčený dokument určen;

▼B

b) pokud je vytvořily osoby mimo Komisi, zachová se jejich původní stupeň utajení, a proto se považují za utajované skutečnosti EU odpovídajícího stupně, ledaže autor souhlasí s odtajněním skutečnosti nebo se snížením stupně jejího utajení.

▼B

PŘÍLOHA

BEZPEČNOSTNÍ PRAVIDLA

Obsah

ČÁST I: ZÁKLADNÍ ZÁSADY A MINIMÁLNÍ BEZPEČNOSTNÍ NORMY

1. ÚVOD
2. OBECNÉ ZÁSADY
3. ZÁKLADY BEZPEČNOSTI
4. ZÁSADY ZABEZPEČENÍ INFORMACÍ
4.1 **Cíle**
4.2 **Definice**
4.3 **Utajování**
4.4 **Cíle bezpečnostních opatření**
5. ORGANIZACE BEZPEČENOSTI
5.1 **Minimální společné normy**
5.2 **Organizace**
6. BEZPEČNOSTNÍ OPATŘENÍ TÝKAJÍCÍ SE PERSONÁLU
6.1 **Bezpečnostní prověrky**
6.2 **Záznamy o prověrkách personálu**
6.3 **Bezpečnostní školení personálu**
6.4 **Odpovědnost vedoucích pracovníků**
6.5 **Bezpečnostní status personálu**
7. FYZICKÁ BEZPEČNOST
7.1. **Potřeba ochrany**
7.2 **Kontrola**
7.3 **Bezpečnost budov**
7.4 **Nouzové plány**
8. BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ
9. OCHRANA PROTI SABOTÁŽI A KONTROLA JINÝCH FOREM ÚMYSLNÉHO POŠKOZENÍ
10. PŘEDÁVÁNÍ UTAJOVANÝCH SKUTEČNOSTÍ TŘETÍM STÁTŮM NEBO MEZINÁRODNÍM ORGANIZACÍM

ČÁST II: ORGANIZACE BEZPEČNOSTI V KOMISI

11. ČLEN KOMISE ODPOVĚDNÝ ZA BEZPEČNOSTNÍ OTÁZKY
12. PORADNÍ SKUPINA PRO BEZPEČNOSTNÍ POLITIKU KOMISE
13. BEZPEČNOSTNÍ VÝBOR KOMISE
14. ► **M2** ŘEDITELSTVÍ PRO BEZPEČNOST KOMISE ◄
15. BEZPEČNOSTNÍ KONTROLY
16. STUPNĚ UTAJENÍ, BEZPEČNOSTNÍ SPECIFIKACE A OZNAČENÍ
16.1 **Stupně utajení**
16.2 **Bezpečnostní specifikace**

▼B

16.3 **Značky**

16.4 **Vyznačení stupně utajení**

16.5 **Vyznačení bezpečnostní specifikace**

17. PRAVIDLA UTAJOVÁNÍ

17.1 **Obecně**

17.2 **Stanovení stupně utajení**

17.3 **Snížení stupně utajení a odtajnění**

18. FYZICKÁ BEZPEČNOST

18.1 **Obecně**

18.2 **Bezpečnostní požadavky**

18.3 **Fyzická bezpečnostní opatření**

18.3.1 *Bezpečnostní oblasti*

18.3.2 *Administrativní oblast*

18.3.3 *Kontroly vstupů a výstupů*

18.3.4 *Pochůzky*

18.3.5 *Bezpečnostní schránky a trezory*

18.3.6 *Zámky*

18.3.7 *Kontrola klíčů a kombinací*

18.3.8 *Zařízení pro odhalování vniknutí*

18.3.9 *Schválené vybavení*

18.3.10 *Fyzická ochrana kopírovacích zařízení a faxů*

18.4. **Opatření proti nahlédnutí a odposlechu**

18.4.1 *Nahlédnutí*

18.4.2 *Odposlech*

18.4.3 *Vnášení elektronického a záznamového zařízení*

18.5 **Technicky chráněné oblasti**

19. OBECNÁ PRAVIDLA TÝKAJÍCÍ SE ZÁSADY „POTŘEBA VĚDĚT“ A BEZPEČNOSTNÍCH PROVĚREK PERSONÁLU EU

19.1 **Obecně**

19.2 **Zvláštní pravidla pro přístup ke skutečnostem se stupněm utajení TRES SECRET UE/EU TOP SECRET**

19.3 **Zvláštní pravidla pro přístup ke skutečnostem se stupněm utajení SECRET UE A CONFIDENTIEL UE**

19.4 **Zvláštní pravidla pro přístup ke skutečnostem se stupněm utajení RESTREINT UE**

19.5. **Převedení na jiné místo**

19.6 **Zvláštní pokyny**

20. BEZPEČNOSTNÍ PROVĚRKY ÚŘEDNÍKŮ A OSTATNÍCH ZAMĚSTNANCŮ KOMISE

21. PŘÍPRAVA, ŠÍŘENÍ, PŘENOS, BEZPEČNOST PERSONÁLU ZÁSILKOVÝCH SLUŽEB A DOPLŇKOVÉ VÝTISKY NEBO PŘEKLADY A VÝPISY Z UTAJOVANÝCH DOKUMENTŮ EU

▼B

21.1 **Příprava**

21.2 **Šíření**

21.3 **Přenos utajovaných dokumentů EU**

21.3.1 *Balení zásilek, potvrzení příjmu*

21.3.2 *Přenos uvnitř budovy nebo skupiny budov*

21.3.3 *Přenos uvnitř země*

21.3.4 *Přenos z jednoho státu do druhého*

21.3.5 *Přenos dokumentů se stupněm utajení RESTREINT UE*

21.4 **Bezpečnost personálu zásilkových služeb**

21.5 **Přenos elektronickými a jinými technickými prostředky**

21.6 **Doplňkové výtisky a překlady a výpisy z utajovaných dokumentů EU**

22. SPISOVNY UTAJOVANÝCH SKUTEČNOSTÍ EU, INVENTURY A KONTROLY, ARCHIVACE A NIČENÍ TĚCHTO SKUTEČNOSTÍ

22.1 **Místní spisovny utajovaných skutečností**

22.2 **Spisovna TRES SECRET UE/EU TOP SECRET**

22.2.1 *Obecně*

22.2.2 *Ústřední spisovna TRES SECRET UE/EU TOP SECRET*

22.2.3 *Spisovny TRES SECRET UE/EU TOP SECRET nižší úrovně*

22.3 **Inventury a kontroly utajovaných dokumentů EU**

22.4 **Archivace utajovaných skutečností EU**

22.5 **Ničení utajovaných dokumentů EU**

22.6 **Zničení v nouzových situacích**

23. BEZPEČNOSTNÍ OPATŘENÍ PRO ZVLÁŠTNÍ ZASEDÁNÍ, KTERÁ SE KONAJÍ MIMO PROSTORY KOMISE A KTERÉ SE TÝKAJÍ UTAJOVANÝCH SKUTEČNOSTÍ EU

23.1 **Obecně**

23.2 **Odpovědnost**

23.2.1 ► **M2** Ředitelství pro bezpečnost Komise ◄

23.2.2 *Bezpečnostní úředník zasedání*

23.3 **Bezpečnostní opatření**

23.3.1 *Bezpečnostní oblasti*

23.3.2 *Propustky*

23.3.3 *Kontrola fotografických a záznamových zařízení*

23.3.4 *Kontrola aktovek, přenosných počítačů a zásilek*

23.3.5 *Technická bezpečnost*

23.3.6 *Dokumenty delegací*

23.3.7 *Bezpečné uložení dokumentů*

23.3.8 *Kontrola kanceláří*

23.3.9 *Odstranění utajovaného odpadu EU*

24. NARUŠENÍ BEZPEČNOSTI A VYZRAZENÍ UTAJOVANÝCH SKUTEČNOSTÍ EU

▼B

24.1 **Definice**

24.2 **Hlášení narušení bezpečnosti**

24.3 **Právní kroky**

25. OCHRANA UTAJOVANÝCH SKUTEČNOSTÍ EU ZPRACOVÁVANÝCH V INFORMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMECH

25.1 **Úvod**

25.1.1 *Obecně*

25.1.2 *Ohrožení a slabá místa systémů*

25.1.3 *Hlavní cíl bezpečnostních opatření*

25.1.4 *Bezpečnostní požadavky vlastní danému systému*

25.1.5 *Bezpečnostní režimy provozu*

25.2 **Definice**

25.3 **Odpovědnost v oblasti bezpečnosti**

25.3.1 *Obecně*

25.3.2 *Orgán pro schvalování z hlediska bezpečnosti (SAA)*

25.3.3 *Orgán pro bezpečnost informačních systémů*

25.3.4 *Vlastník technického systému (TSO)*

25.3.5 *Vlastník informací (IO)*

25.3.6 *Uživatelé*

25.3.7 *Školení INFOSEC*

25.4 **Netechnická bezpečnostní opatření**

25.4.1 *Bezpečnostní opatření týkající se personálu*

25.4.2 *Fyzická bezpečnost*

25.4.3 *Kontrola přístupu k systému*

25.5 **Technická bezpečnostní opatření**

25.5.1 *Bezpečnost skutečností*

25.5.2 *Kontrola a odpovědnost za skutečnosti*

25.5.3 *Nakládání s odnímatelnými nosiči dat a jejich kontrola*

25.5.4 *Odtajnění a zničení nosičů dat*

25.5.5 *Bezpečnost komunikací*

25.5.6 *Bezpečnost instalací a vyzařování*

25.6 **Bezpečnost během zpracování**

25.6.1 *Provozní postupy týkající se bezpečnosti (SecOP)*

25.6.2 *Ochrana softwaru a správa konfigurace*

25.6.3 *Zjišťování přítomnosti softwaru působícího škodu a počítačových virů*

25.6.4 *Údržba*

25.7 **Nabývání**

25.7.1 *Obecně*

25.7.2 *Schvalování*

▼B

25.7.3 *Hodnocení a udělení osvědčení*

25.7.4 *Systematické kontroly bezpečnostních vlastností při prodlužování schválení*

25.8 **Dočasné nebo příležitostné použití**

25.8.1 *Bezpečnost mikropočítačů a osobních počítačů*

25.8.2 *Používání soukromého počítačového vybavení IT k oficiální práci Komise*

25.8.3 *Používání počítačového vybavení IT smluvního partnera nebo vybavení dodaného vnitrostátním dodavatelem k oficiální práci Komise*

26. PŘEDÁVÁNÍ UTAJOVANÝCH SKUTEČNOSTÍ EU TŘETÍM STÁTŮM NEBO MEZINÁRODNÍM ORGANIZACÍM

26.1.1 *Zásady, kterými se řídí předávání utajovaných skutečností EU*

26.1.2 *Stupně*

26.1.3 *Dohody*

DODATEK 1: **Srovnávací tabulka vnitrostátních bezpečnostních stupňů**

DODATEK 2: **Praktický průvodce stupni utajení**

DODATEK 3: **Obecné zásady pro předávání utajovaných skutečností EU třetím státům nebo mezinárodním organizacím: spolupráce na úrovni 1**

DODATEK 4: **Obecné zásady pro předávání utajovaných skutečností EU třetím státům nebo mezinárodním organizacím: spolupráce na úrovni 2**

DODATEK 5: **Obecné zásady pro předávání utajovaných skutečností EU třetím státům nebo mezinárodním organizacím: spolupráce na úrovni 3**

DODATEK 6: **Seznam zkratek**

▼B

ČÁST 1: ZÁKLADNÍ ZÁSADY A MINIMÁLNÍ BEZPEČNOSTNÍ NORMY

1. ÚVOD

Tato pravidla vymezují základní zásady a minimální bezpečnostní normy, které musí Komise odpovídajícím způsobem dodržovat na všech svých pracovištích a které jsou povinni dodržovat rovněž všichni příjemci utajovaných skutečností EU tak, aby byla zajištěna bezpečnost a aby měl každý jistotu, že byly vytvořeny společné normy ochrany.

2. OBECNÉ ZÁSADY

Bezpečnostní politika Komise tvoří nedílnou součást její obecné vnitřní řídící strategie, a proto vychází ze zásad, kterými se řídí její obecná politika.

Mezi tyto zásady patří legalita, transparentnost, odpovědnost a subsidiarita (proporcionalita).

Legalita znamená nezbytnost přísného dodržování právního rámce při výkonu bezpečnostních funkcí a nutnost dodržovat požadavky právních norem. V plném rozsahu se použijí ustanovení služebního řádu, zejména jeho článek 17 týkající se povinnosti úředníků zachovávat mlčenlivost o informacích Komise a jeho hlava VI, týkající se disciplinárních opatření. Tento koncept rovněž znamená, že úkoly v oblasti bezpečnosti se musejí opírat o příslušné právní předpisy. Konečně to znamená, že porušení bezpečnosti v rámci odpovědnosti Komise se musí posuzovat způsobem, který odpovídá koncepci disciplinárních postupů Komise a její politice spolupráce s členskými státy v oblasti trestního soudnictví.

Transparentnost znamená jednoduchost všech bezpečnostních pravidel a předpisů, nezbytnost vyváženosti mezi různými službami a různými oblastmi (fyzická bezpečnost versus ochrana informací atd.) a nezbytnost důsledné a strukturované bezpečnostní politiky. Zároveň představuje nezbytnost srozumitelných písemných pokynů pro plnění bezpečnostních opatření.

Odpovědnost znamená nejen, že se úkoly ve sféře bezpečnosti konkrétně vymezí, ale rovně nutnost pravidelného prověřování, zda se tyto úkoly plní správným způsobem.

Subsidiarita či proporcionalita znamená, že se bezpečnost zaručuje na nejnižší možné úrovni a co nejblíže generálním ředitelstvím a službám Komise. Zároveň to znamená, že se bezpečnostní činnosti omezí pouze na ty skutečnosti, které je skutečně potřebují. A konečně, že bezpečnostní opatření jsou přiměřená zájmům, které mají chránit, a skutečnému nebo potenciálnímu ohrožení těchto zájmů, přičemž umožňují obranu, která způsobuje co nejmenší rušivé vlivy.

3. ZÁKLADY BEZPEČNOSTI

Základem pro zajištění spolehlivého systému bezpečnosti je:

a) vnitrostátní bezpečnostní organizace v každém členském státu zajišťující:

   1. shromažďování a záznam informací o špionáži, sabotáži, terorismu a jiných podvratných činnostech a

   2. poskytování informací vládám a jejich prostřednictvím Komisi o povaze ohrožení bezpečnosti a poskytování rad o prostředcích pro ochranu před ním;

b) v rámci každého členského státu a v rámci Komise technický orgán INFOSEC, který je pověřen spoluprací s příslušným bezpečnostním orgánem při poskytování informací o technickém ohrožení bezpečnosti a při poskytování rad o prostředcích pro ochranu před ním;

c) pravidelná spolupráce mezi útvary vlád a příslušnými útvary Komise s cílem v závislosti na případu určit nebo doporučit:

   1. osoby, informace a zdroje, které mají být chráněny a

▼B

2. společné normy ochrany;

d) úzká spolupráce mezi ►M2 ředitelstvím pro bezpečnost Komise ◄ a bezpečnostními útvary ostatních orgánů Společenství a Bezpečnostním úřadem NATO (NOS).

4. ZÁSADY BEZPEČNOSTI ÚDAJŮ

4.1 **Cíle**

Zajištění bezpečnosti údajů má tyto základní cíle:

a) ochrana utajovaných skutečností EU před špionáží, zneužitím nebo neoprávněným zveřejněním;

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

c) ochrana prostor Komise, v nichž jsou informace EU uloženy, před pokusy o sabotáž a úmyslnými snahami o poškození;

d) v případě selhání zhodnocení způsobené škody, omezení jejích důsledků a přijmutí nezbytných nápravných opatření.

4.2 **Definice**

Pro účely těchto předpisů se výrazem:

a) „utajované skutečnosti EU“ rozumějí všechny informace a materiály, jejichž neoprávněné vyzrazení by mohlo v různých stupních ohrozit zájmy EU nebo jednoho či více členských států, a to bez ohledu na to, zda taková informace pochází z EU nebo byla získána z členských států, třetích států nebo mezinárodních organizací;

b) „dokument“ rozumí jakýkoli dopis, poznámka, zápis, zpráva, memorandum, signál nebo vzkaz, náčrtek, fotografie, diapozitiv, film, mapa, graf, plán, zápisník, rozmnožovací blána, uhlový papír, páska do psacího stroje nebo do tiskárny, magnetická páska, kazeta, počítačová disketa, CD-ROM nebo jiný fyzický nosič, na kterém jsou informace zaznamenány;

c) „materiál“ rozumí dokumenty vymezené v písmenu b) a všechny již vyrobené nebo vyráběné součásti vybavení;

d) „potřeba vědět“ rozumí potřeba jednotlivého pracovníka mít přístup k utajovaným skutečnostem EU, aby byl schopen vykonávat funkci nebo provést úkol;

e) „oprávnění“ rozumí rozhodnutí ►M2 ředitele ředitelství pro bezpečnost Komise ◄ poskytnout individuální přístup k utajované skutečnosti EU, a to až po určitý stupeň utajení, na základě kladného výsledku bezpečnostní prověrky, kterou provádí vnitrostátní bezpečnostní orgán podle vnitrostátních právních předpisů;

f) „utajování“ rozumí přiznání určitého stupně ochrany skutečnosti, jejíž neoprávněné zveřejnění by mohlo v určitém rozsahu poškodit zájmy Komise nebo členského státu;

g) „snížení stupně utajení“ rozumí zařazení na nižší stupeň utajení;

h) „odtajnění“ rozumí odstranění jakéhokoliv utajení;

i) „původce“ rozumí řádně pověřený autor utajovaného dokumentu; v rámci Komise mohou pověřit své zaměstnance vytvářením utajovaných skutečností EU vedoucí útvarů;

j) „útvary Komise“ rozumějí oddělení a útvary Komise, včetně kabinetů, na všech pracovištích, včetně Společného výzkumného střediska, zastoupení a kanceláří Komise v Evropské unii a delegací ve třetích zemích.

▼B

4.3 **Utajování**

a) V oblasti důvěrných informací jsou pro výběr skutečností a materiálů, které mají být chráněny, a pro stanovení potřebného stupně ochrany nezbytné opatrnost a zkušenost. Stupeň ochrany – a jedná se o základní hledisko – musí odpovídat bezpečnostnímu významu informací a materiálů, které mají být chráněny. S cílem zajistit řádný tok informací musí být přijata opatření, aby nedošlo k zařazení na příliš vysoký nebo příliš nízký stupeň utajení.

b) Systém utajování představuje nástroj, který umožňuje uplatňovat tyto zásady; obdobný systém by měl být přijat pro plánování a organizaci boje proti špionáži, sabotáži, terorismu a jiným hrozbám tak, aby byla chráněna nejdůležitější zařízení, v nichž se nacházejí utajované skutečnosti, a nejcitlivější části těchto zařízení.

c) Za utajení skutečnosti odpovídá výlučně její původce.

d) Stanovení stupně utajení vychází výlučně z obsahu těchto skutečností.

e) V případech spojení několika skutečností do jednoho celku musí stupeň utajení, který se vztahuje na tento celek, odpovídat skutečnosti s nejvyšším stupněm utajení. Soubor skutečností může být ale zařazen na vyšší stupeň utajení, než mají jeho dílčí části.

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

4.4 **Cíle bezpečnostních opatření**

Bezpečnostní opatření:

a) se musí vztahovat na všechny osoby, které mají přístup k utajovaným skutečnostem, k prostředkům přenosu utajovaných skutečností, do všech prostor obsahujících takové skutečnosti a ke všem významným zařízením;

b) musí být vytvořena tak, aby určila osoby, jejichž postavení by mohlo ohrozit bezpečnost utajovaných skutečností a významných zařízení obsahujících takové skutečnosti, a zamezit jejich přístupu nebo změnit jejich místo;

c) musí bránit přístupu všech neoprávněných osob k utajovaným skutečnostem nebo zařízením, která je obsahují;

d) musí zajistit, aby utajované skutečnosti byly šířeny výlučně v souladu se zásadou „potřeba vědět“, která je základní pro všechna hlediska bezpečnosti;

e) musí zajistit celistvost (tj. zabránit poškození nebo neoprávněné změně nebo neoprávněnému zničení) a dostupnost (tj. přístup nesmí být odmítnut osobám, které se potřebují se skutečnostmi seznámit a jsou k tomu oprávněny) všech skutečností, utajovaných či nikoli a zejména skutečností uložených, zpracovávaných nebo přenášených v elektromagnetické formě.

5. ORGANIZACE BEZPEČNOSTI

5.1 **Minimální společné normy**

Komise dbá na to, aby všichni příjemci utajovaných skutečností EU, a to jak vnitřní, tak i ti, kteří spadají do její odpovědnosti, jako např. útvary a externí smluvní partneři Komise, dodržovali společné minimální normy bezpečnosti, a aby tak utajované skutečnosti EU mohly být předávány s důvěrou, že zmíněné všichni s nimi budou nakládat stejně obezřetně. Tyto minimální normy musí obsahovat kritéria pro prověřování personálu a opatření, která mají být přijata pro ochranu utajovaných skutečností EU.

Přístup vnějších subjektů k utajovaným skutečnostem EU povolí Komise pouze pod podmínkou, že tyto subjekty zaručí, že při nakládání

▼B

s těmito skutečnostmi dodrží pravidla přinejmenším odpovídající těmto minimálním normám.

▼M3

Tyto minimální normy se rovněž uplatní v případě, kdy Komise smlouvou nebo grantovou dohodou přenáší úkoly, jež se týkají, představují a/nebo obsahují utajované skutečnosti EU týkající se průmyslových nebo jiných subjektů: tyto společné minimální normy jsou uvedeny v oddílu 27 části II.

▼B

5.2 **Organizace**

Bezpečnost je v rámci Komise zajišťována na dvou úrovních:

a) Na úrovni Komise jako celku existuje ►M2 ředitelství pro bezpečnost Komise ◄ s orgánem pro schvalování z hlediska bezpečnosti, který zároveň působí jako orgán pro šifrování (CrA) a jako orgán pro normu TEMPEST, a s orgánem INFOSEC (IA) a jeden nebo více ústředních spisoven utajovaných skutečností EU, z nichž v každé pracuje jeden nebo více kontrolorů spisovny (RCO).

b) Na úrovni útvarů Komise odpovídá za bezpečnost jeden nebo více bezpečnostních pracovníků daného útvaru (LSO), jeden nebo více úředníků pro bezpečnost počítačových systémů na úrovni ústředí (CISO), úředníků pro bezpečnost počítačových systémů na místní úrovni (LISO) a místní spisovny utajovaných informací EU, kde pracuje jeden nebo více kontrolorů spisovny.

c) Ústřední bezpečnostní orgány udílí provozní pokyny bezpečnostním orgánům na úrovni útvarů.

6. BEZPEČNOSTNÍ OPATŘENÍ TÝKAJÍCÍ SE PERSONÁLU

6.1 **Bezpečnostní prověrky**

Všechny osoby, které mají mít přístup k utajovaným skutečnostem se stupněm utajení ►M1 CONFIDENTIEL UE ◄ nebo vyšším, musí nejprve projít řádnou bezpečností prověrkou. Obdobné prověrky se požadují pro osoby, jejichž funkce spočívají v zajišťování technického provozu nebo údržby komunikačních a informačních systémů obsahujících utajované skutečnosti. Při prověrce se musí zjistit, zda:

a) dotčená osoba je nezpochybnitelně loajální;

b) její osobnost a spolehlivost je taková, že není možné nijak zpochybnit její bezúhonnost při nakládání s utajovanými skutečnostmi nebo

c) by mohla ustoupit tlakům ze zahraničních nebo jiných zdrojů.

Zvláštní pozornost musí být věnována provádění prověrek osob, které:

d) mají mít přístup ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄;

e) zastávají funkce, které vyžadují pravidelný přístup k velkému počtu skutečností se stupněm utajení ►M1 SECRET UE ◄;

f) mají z důvodu své funkce zvláštní přístup k zabezpečeným komunikačním a informačním systémům a mohou tak získat neoprávněný přístup k velkému počtu utajovaných skutečností EU nebo vážně ohrozit splnění úkolu prostřednictvím technické sabotáže.

V případech uvedených v písmenech d), e) a f) je třeba co nejvíce využívat metody prošetřování minulosti osob.

Pokud má být zaměstnána do funkce, ve které může získat přístup k utajovaným skutečnostem EU (např. kurýři, bezpečnostní zaměstnanci, personál údržby nebo úklidu apod.) osoba, která nemá „potřebu vědět“, musí nejprve projít řádnou bezpečnostní prověrkou.

▼B

6.2 **Záznamy o prověrkách personálu**

Všechny útvary Komise, kde se nakládá s utajovanými skutečnostmi EU nebo kde jsou instalovány zabezpečené komunikační nebo informační systémy, musí vést záznamy o prověrkách svého personálu. Každá prověrka musí být ověřena, s ohledem na okolnosti, s cílem zjistit, zda odpovídá stupni utajení skutečností a materiálů, se kterými prověřovaná osoba nakládá; nové prověření je nezbytné, kdykoli některá nová informace naznačuje, že ponechání dotčené osoby na místě, které umožňuje přístup k utajovaným skutečnostem, nadále neodpovídá zájmům bezpečnosti. V rámci své působnosti vede záznamy o prověrkách místní bezpečnostní pracovník daného útvaru Komise.

6.3 **Bezpečnostní školení personálu**

Všechny osoby v postavení, ve kterém mohou mít přístup k utajovaným skutečnostem, musí před nástupem do funkce a poté v pravidelných intervalech získat podrobný výklad o nezbytných bezpečnostních opatřeních a souvisejících platných postupech. Tyto osoby písemně potvrdí, že si přečetly a plně porozuměly příslušným bezpečnostním předpisů.

6.4 **Odpovědnost vedoucích pracovníků**

Vedoucí pracovníci musí vědět, kteří z jejich pracovníků nakládají s utajovanými skutečnostmi a kteří mají přístup k zabezpečeným komunikačním a informačním systémům, a musí evidovat a hlásit všechny události nebo zřejmá ohrožení, která by mohla ovlivnit bezpečnost.

6.5 **Bezpečnostní status personálu**

Měly by být stanoveny postupy umožňující určit, jsou-li zjištěny nepříznivé informace o určité osobě, zda tato osoba vykonává funkci vyžadující přístup k utajovaným skutečnostem nebo zda má přístup k zabezpečeným komunikačním nebo informačním systémům, a uvědomit ►M2 ředitelství pro bezpečnost Komise ◄. Zjistí-li se, že tato osoba představuje bezpečnostní riziko, bude odvolána nebo vyřazena z plnění úkolů, při kterém by mohla ohrožovat bezpečnost.

7. FYZICKÁ BEZPEČNOST

7.1 **Potřeba ochrany**

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

7.2 **Kontrola**

Osoby, které odcházejí z prostorů, v nichž se nacházejí jim svěřené utajované skutečnosti EU, se musí ujistit, že jsou bezpečně uloženy a že jsou zapojena všechna bezpečnostní zařízení (zámky, poplašná zařízení atd.). Po pracovní době se provádějí další doplňující kontroly.

7.3 **Bezpečnost budov**

Budovy, v nichž se nacházejí utajované skutečnosti EU nebo zabezpečené komunikační a informační systémy, musí být chráněny před neoprávněným vstupem. Povaha této ochrany (např. mříže na oknech, zámky na dveřích, stráže u vchodů, automatické systémy kontroly přístupu, bezpečnostní inspekce a hlídky, poplašné systémy, systémy odhalující neoprávněné vniknutí a hlídací psi) závisí na:

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

b) jakosti bezpečnostních schránek obsahujících informace a materiály a

c) technických vlastnostech a umístění budovy.

▼B

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

7.4 **Nouzové plány**

Je třeba předem připravit podrobné plány na ochranu utajovaných skutečností v nouzových případech souvisejících s místní nebo vnitrostátní nouzovou situací.

8. BEZPEČNOST INFORMACÍ

Bezpečnost informací (INFOSEC) souvisí s určením a použitím bezpečnostních opatření na ochranu utajovaných skutečností EU zpracovávaných, uchovávaných nebo přenášených komunikačními, informačními a jinými elektronickými systémy před náhodným i úmyslným ohrožením jejich důvěrnosti, celistvosti nebo dostupnosti. Je třeba přijmout vhodná preventivní opatření, aby se zabránilo přístupu neoprávněných uživatelů k utajovaným skutečnostem EU, odmítnutí přístupu k utajovaným skutečnostem EU oprávněným uživatelům a poškození, neoprávněné změně nebo zničení utajovaných skutečností EU.

9. OCHRANA PROTI SABOTÁŽI A KONTROLA JINÝCH FOREM ÚMYSLNÉHO POŠKOZENÍ

Fyzická opatření jsou nejúčinnější prostředky pro zajištění bezpečnosti a ochrany důležitých zařízení obsahujících utajované skutečnosti proti sabotáži nebo jinému úmyslnému poškození; samotné bezpečnostní prověrky personálu je nemohou účinně nahradit. Vnitrostátní orgán odpovědný za bezpečnost shromažďuje poznatky o špionážních, sabotážních, teroristických a jiných podvratných činnostech.

10. PŘEDÁVÁNÍ UTAJOVANÝCH SKUTEČNOSTÍ TŘETÍM STÁTŮM NEBO MEZINÁRODNÍM ORGANIZACÍM

K předání utajovaných skutečností EU pocházejících od Komise některému třetímu státu nebo mezinárodní organizaci uděluje oprávnění sbor členů Komise. Není-li Komise původcem skutečností, které mají být předány, musí Komise předem získat souhlas původce. Nelze-li původce zjistit, převezme Komise jeho odpovědnost.

Získá-li Komise utajované skutečnosti od třetích států, mezinárodních organizací nebo jiných třetích osob, bude jim poskytnuta ochrana v souladu s jejich stupněm utajení, který bude odpovídat normám stanoveným pro utajované skutečnosti EU v tomto předpise, nebo přísnějším normám, které mohou vyžadovat třetí osoby předávající tyto skutečnosti. Je možno zorganizovat vzájemné kontroly.

Výše zmíněné zásady se uplatňují v souladu s podrobnými ustanoveními uvedenými v části II oddíle 26 a v dodatcích 3, 4 a 5.

ČÁST II: ORGANIZACE BEZPEČNOSTI V KOMISI

11. ČLEN KOMISE ODPOVĚDNÝ ZA BEZPEČNOSTNÍ OTÁZKY

Člen Komise odpovědný za bezpečnostní otázky:

a) provádí bezpečnostní politiku Komise;

b) posuzuje bezpečnostní obtíže, které mu předkládá Komise nebo její příslušné útvary;

c) posuzuje v úzkém spojení s vnitrostátními bezpečnostními orgány (nebo jinými příslušnými orgány) členských států otázky týkající se změn bezpečnostní politiky Komise.

Člen Komise odpovědný za bezpečnostní otázky je pověřen zejména:

a) koordinovat všechny bezpečnostní otázky související s činností Komise;

▼B

b) požadovat od vnitrostátních bezpečnostních orgánů členských států, aby zajišťovaly bezpečnostní pověrky personálu zaměstnaného v Komisi v souladu s oddílem 20;

c) vyšetřovat nebo nechat vyšetřit úniky utajovaných skutečností EU, pokud se zdá, že k nim došlo v Komisi;

d) požadovat od příslušných bezpečnostních orgánů, aby zahájily šetření, jestliže se zdá, že k úniku utajovaných skutečností EU došlo vně Komise, a koordinovat vyšetřování, je-li v něm zapojeno více bezpečnostních orgánů;

e) pravidelně posuzovat bezpečnostní opatření přijatá pro ochranu utajovaných skutečností EU;

f) udržovat úzké vztahy se všemi dotčenými bezpečnostními orgány, aby bylo dosaženo celkové koordinace bezpečnosti;

g) trvale posuzovat bezpečnostní politiku a bezpečnostní postupy Komise a případně připravovat vhodná doporučení. V této souvislosti předkládá Komisi její člen odpovědný za bezpečnostní politiku roční plán inspekcí zpracovaný ►M2 ředitelstvím pro bezpečnost Komise ◄.

12. PORADNÍ SKUPINA PRO BEZPEČNOSTNÍ POLITIKU KOMISE

Zřizuje se poradní skupina pro bezpečnostní politiku Komise. Tvoří ji člen Komise odpovědný za bezpečnostní otázky nebo jeho zástupce, který skupině předsedá, a ze zástupců vnitrostátních bezpečnostních orgánů jednotlivých členských států. Je možno přizvat i zástupce dalších evropských orgánů. Zástupci decentralizovaných institucí ES a EU mohou být rovněž vyzváni, aby se účastnili zasedání, jestliže se jich týkají projednávané otázky.

Poradní skupina pro bezpečnostní politiku Komise se schází na žádost jejího předsedy nebo kteréhokoli z jejích členů. Úkolem skupiny je podle potřeby posuzovat a hodnotit všechny závažné bezpečnostní otázky a předkládat Komisi případná doporučení.

▼M2

13. BEZPEČNOSTNÍ VÝBOR KOMISE

Zřizuje se bezpečnostní výbor Komise. Skládá se z generálního ředitele pro personál a administrativu, který výboru předsedá, člena kabinetu komisaře odpovědného za bezpečnostní otázky, člena kabinetu předsedy, zástupce generálního tajemníka, který předsedá skupině Komise krizového řízení, generálních ředitelů právní služby, generálních ředitelství pro vnější vztahy, pro spravedlnost, pro svobodu a bezpečnost, Společného výzkumného střediska a generálního ředitelství pro informatiku a z útvaru interního auditu a ředitele ředitelství pro bezpečnost Komise, nebo jejich zástupců. Je možné přizvat další úředníky Komise. Jeho úkolem je hodnocení bezpečnostních opatření v rámci Komise a předkládání doporučení v této oblasti členovi Komise odpovědnému za bezpečnostní otázky.

▼B

14. ►M2 ŘEDITELSTVÍ PRO BEZPEČNOST KOMISE ◄

Pro plnění úkolů uvedených v oddíle 11 má člen Komise odpovědný za bezpečnostní otázky k dispozici ►M2 ředitelství pro bezpečnost Komise ◄, která koordinuje bezpečnostní opatření, dohlíží na ně a provádí je.

►M2 Ředitel ředitelství pro bezpečnost Komise ◄ je hlavním poradcem člena Komise odpovědného za bezpečnostní otázky a zajišťuje funkci sekretariátu poradní skupiny pro bezpečnostní politiku Komise. V této souvislosti řídí aktualizaci bezpečnostních předpisů a koordinuje bezpečnostní opatření s příslušnými orgány členských států a případně s mezinárodními organizacemi spojenými s Komisí prostřednictvím bezpečnostních dohod. Vykonává při tom úlohu styčné osoby.

▼B

►M2 Ředitel ředitelství pro bezpečnost Komise ◄ odpovídá za schvalování systémů a sítí IT v rámci Komise. ►M2 Ředitel ředitelství pro bezpečnost Komise ◄ po dohodě s dotčenými vnitrostátními bezpečnostními orgány rozhoduje o schválení systémů a sítí IT, v nichž je zapojena Komise na jedné straně a na druhé straně kterýkoli jiný příjemce utajovaných skutečností EU.

15. BEZPEČNOSTNÍ KONTROLY

►M2 Ředitelství pro bezpečnost Komise ◄ uskutečňuje pravidelné kontroly předpisů přijatých pro ochranu utajovaných skutečností EU.

►M2 Ředitelstvím pro bezpečnost Komise ◄ mohou s tímto úkolem pomáhat bezpečnostní služby dalších evropských orgánů EU, které mají v držení utajované informace EU, nebo vnitrostátní bezpečnostní orgány členských států. ([1])

Na žádost členského státu provede jeho vnitrostátní bezpečnostní orgán v rámci Komise kontrolu utajovaných skutečností, a to společně s ►M2 Ředitelství pro bezpečnost Komise ◄ a na základě vzájemné dohody.

16. STUPNĚ UTAJENÍ, BEZPEČNOSTNÍ SPECIFIKACE A OZNAČENÍ

16.1 **Stupně utajení ([2])**

Skutečnosti jsou zařazovány do těchto stupňů utajení (srov. dodatek 2):

►M1 TRES SECRET UE/EU TOP SECRET ◄: tento stupeň se použije výlučně pro informace a materiály, jejichž neoprávněné vyzrazení by mohlo výjimečně závažně poškodit zásadní zájmy Evropské unie nebo jednoho či více jejích členských států.

►M1 SECRET UE ◄: tento stupeň se použije výlučně pro informace a materiály, jejichž neoprávněné vyzrazení by mohlo vážně poškodit základní zájmy Evropské unie nebo jednoho či více členských států.

►M1 CONFIDENTIEL UE ◄: tento stupeň se použije pro informace a materiály, jejichž neoprávněné vyzrazení by mohlo poškodit základní zájmy Evropské unie nebo jednoho či více jejích členských států.

►M1 RESTREINT UE ◄: tento stupeň se použije pro informace a materiály, jejichž neoprávněné vyzrazení by mohlo být nevýhodné pro zájmy Evropské unie nebo jednoho či více jejích členských států.

Žádné jiné stupně utajení nejsou přípustné.

16.2 **Bezpečnostní specifikace**

Za účelem stanovení mezí platnosti utajení (což pro utajované skutečnosti udává automatické snížení stupně utajení nebo přímo odtajnění) se může použít smluvená bezpečnostní specifikace. Jedná se buď o slova „AŽ DO.… (čas/datum)“ nebo „AŽ DO.… (určitá událost)“.

Další bezpečnostní specifikace, jako jsou například „KRYPTO“ (šifrováno) nebo jakékoli jiné bezpečnostní specifikace uznávané EU, se použijí v případech, kdy kromě způsobu nakládání s danou skutečností, který je určen jejím stupněm utajení, existuje navíc potřeba omezeného šíření a zvláštního nakládání.

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

16.3 **Značky**

K upřesnění oblasti, které se týká daný dokument, nebo k označení zvláštního rozšiřování na základě „potřeby vědět“ nebo (u informací nepodléhajících utajení) k označení konce embarga lze použít značky.

([1]) Tímto není dotčena Vídeňská úmluva o diplomatických vztazích z roku 1961 a Protokol o výsadách a imunitách Evropských společenství ze dne 8. dubna 1965.

([2]) Viz srovnávací tabulku bezpečnostních stupňů EU, NATO, Západoevropské unie (WEU) a členských států, která je uvedena v dodatku 1.

▼B

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

Značka EBOP se použije na dokumenty a jejich kopie, které se týkají bezpečnosti a obrany Unie nebo jednoho či více členských států nebo které se týkají vojenského nebo nevojenského řešení krizí.

16.4 **Vyznačení stupně utajení**

Stupeň utajení se vyznačuje následujícími způsoby:

a) na dokumentech se stupněm utajení ►M1 RESTREINT UE ◄ mechanickými nebo elektronickými prostředky;

b) na dokumentech se stupněm utajení ►M1 CONFIDENTIEL UE ◄ mechanickými prostředky nebo ručně nebo vytištěním na předem orazítkovaný a evidovaný list;

c) na dokumentech se stupněm utajení ►M1 SECRET UE ◄ a ►M1 TRES SECRET UE/EU TOP SECRET ◄ mechanickými prostředky nebo ručně.

16.5 **Vyznačení bezpečnostní specifikace**

Bezpečnostní specifikace se vyznačují přímo pod stupeň utajení stejnými způsoby, které se používají pro vyznačení stupně utajení.

17. PRAVIDLA UTAJOVÁNÍ

17.1 **Obecně**

Skutečnost se utajuje pouze, je-li to nezbytné. Utajení je jasně a řádně vyznačeno a trvá pouze po dobu, po kterou skutečnost vyžaduje ochranu.

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

Úředníci a ostatní zaměstnanci Komise utajují skutečnosti, snižují stupeň jejich utajení nebo je odtajňují na pokyn svého vedoucího útvaru nebo s jeho souhlasem.

Podrobné postupy upravující nakládání s utajovanými dokumenty byly vypracovány tak, aby zajišťovaly těmto dokumentům ochranu odpovídající informacím, které obsahují.

Počet osob oprávněných vypracovat dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ musí být omezen na přísné minimum. Jména těchto osob musí být uvedena na seznamu vytvořeném ►M2 ředitelstvím pro bezpečnost Komise ◄.

17.2 **Stanovení stupně utajení**

Stupeň utajení dokumentu se stanoví podle úrovně citlivosti jeho obsahu v souladu s definicemi v oddílu 16. Stupně utajení je nutno používat správně a střídmě. To se týká zvláště stupně ►M1 TRES SECRET UE/EU TOP SECRET ◄.

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

Praktický návod pro stanovení stupně utajení je obsažen v příloze 2.

Stránky, odstavce, oddíly, přílohy, dodatky a připojené části dokumentu mohou vyžadovat různé stupně utajení a musí být podle toho označeny. Stupeň utajení dokumentu jako celku je stanoven podle části s nejvyšším stupněm utajení.

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

Přístup veřejnosti se i nadále řídí nařízením (ES) č. 1049/2001.

▼B

17.3 **Snížení stupně utajení a odtajnění**

Stupeň utajení utajovaného dokumentu EU může být snížen a dokument lze odtajnit pouze se souhlasem jeho původce a, je-li to nezbytné, po konzultaci ostatních zúčastněných stran. Snížení stupně utajení nebo odtajnění musí být potvrzeno písemně. Původce musí uvědomit své příjemce o změně utajení a příjemci jsou povinni na to upozornit další příjemce, kterým předali originál dokumentu nebo jeho kopii.

Je-li to možné, uvede původce na utajovaný dokument datum nebo lhůtu, od kdy lze snížit stupeň utajení skutečnosti, které obsahuje, nebo ji odtajnit. Jinak posuzuje tuto otázku nejpozději každých pět let, aby zjistil, zda je původní stupeň utajení nadále nezbytný.

18. FYZICKÁ BEZPEČENOST

18.1 **Obecně**

Hlavním cílem fyzických bezpečnostních opatření je zabránit neoprávněným osobám získat přístup k utajovaným informacím nebo materiálům EU, zabránit odcizení a znehodnocení zařízení a dalšího majetku a zabránit obtěžování nebo jinému druhu útoku zaměřeného proti zaměstnancům, ostatním pracovníkům a návštěvníkům.

18.2 **Bezpečnostní požadavky**

Všechny objekty, oblasti, budovy, kanceláře, místnosti, komunikační a informační systémy atd., ve kterých jsou uloženy utajované informace a materiály EU nebo ve kterých se s takovými informacemi a materiály nakládá, je třeba chránit pomocí vhodných fyzických bezpečnostních opatření.

Při určování stupně fyzické ochrany, který má být zajištěn, je třeba přihlížet ke všem příslušným faktorům, a zejména:

a) ke stupni utajení informací nebo materiálu;

b) k objemu a formě (např. papír, počítačové nosiče dat) uchovávaných skutečností;

c) k místnímu hodnocení ohrožení ze strany zpravodajských služeb, které se zaměřují na EU, členské státy a/nebo jiné orgány nebo třetí osoby, které disponují utajovanými skutečnostmi EU, zejména sabotáže, terorismu a jiné podvratné a/nebo trestné činnosti.

Cílem použitých fyzických bezpečnostních opatření je:

a) zabránit lstivému nebo násilnému vniknutí;

b) odstrašovat neloajální personál (vnitřní špióny) od podvratných činů, bránit jim a odhalovat je;

c) bránit těm, kteří nemají „potřebu vědět“, v přístupu k utajovaným skutečnostem EU.

18.3 Fyzická bezpečnostní opatření

18.3.1 *Bezpečnostní oblasti*

Oblasti, kde jsou zpracovávány a uchovávány skutečnosti se stupněm utajení ►**M1** CONFIDENTIEL UE ◄ nebo vyšším, musí být organizovány a strukturovány způsobem, který odpovídá jedné z níže uvedených kategorií:

a) bezpečnostní oblast kategorie I: oblast, kde jsou zpracovávány a uchovávány skutečnosti se stupněm utajení ►**M1** CONFIDENTIEL UE ◄ nebo vyšším takovým způsobem, že vstup do takové oblasti představuje ve skutečnosti přístup k těmto skutečnostem. Tato oblast vyžaduje:

   i) jasně vymezit chráněný prostor, jehož vstupy a výstupy jsou kontrolovány;

▼B

ii) zavést systém kontroly vstupů, který umožní vstup pouze řádně prověřeným a zvláště oprávněným osobám;

iii) upřesnit stupeň utajení skutečností, které jsou zde obvykle drženy, tj. skutečností, k nimž se vstupem získá přístup.

b) bezpečnostní oblast kategorie II: oblast, kde jsou zpracovávány a uchovávány skutečnosti se stupněm utajení ►M1 CONFIDENTIEL UE ◄ nebo vyšším takovým způsobem, že je možné chránit je před přístupem neoprávněných osob prostředky vnitřní kontroly, např. prostory, v nichž jsou umístěny kanceláře, kde jsou pravidelně zpracovávány a uchovávány skutečnosti se stupněm utajení ►M1 CONFIDENTIEL UE ◄ nebo vyšším. Tato oblast vyžaduje:

i) jasně vymezit chráněný prostor, jehož vstupy a výstupy jsou kontrolovány;

ii) zavést systém kontroly vstupů, který umožní vstup bez doprovodu pouze řádně prověřeným a zvláště oprávněným osobám. Pro všechny ostatní osoby je nutné zajistit doprovod nebo podobné kontrolní opatření, aby se zabránilo přístupu k utajovaným skutečnostem EU a vstupu do oblastí, které jsou kontrolovány technickým zabezpečením.

Není-li v těchto oblastech personál ve službě 24 hodin denně, provede se ihned po skončení obvyklé pracovní doby kontrola, jejímž cílem je zjistit, zda jsou utajované skutečnosti EU řádně zabezpečeny.

18.3.2 *Administrativní oblast*

Kolem bezpečnostních oblastí kategorie I a II nebo před nimi lze zřídit administrativní oblast s nižší ochranou. Ta musí obsahovat viditelně vyznačený prostor umožňující kontrolu osob a vozidel. V administrativních oblastech je možné zpracovávat a ukládat pouze skutečnosti se stupněm utajení ►M1 RESTREINT UE ◄ a informace nepodléhající utajení.

18.3.3 *Kontroly vstupů a výstupů*

Vstup do bezpečnostních oblastí kategorií I a II a výstup z nich jsou kontrolovány systémem propustek nebo osobní identifikace pro veškerý personál v těchto oblastech běžně pracující. Je třeba rovněž vytvořit systém kontroly návštěvníků, aby se zabránilo všem neoprávněným přístupům k utajovaným skutečnostem EU. K systému propustek lze připojit systém automatické identifikace, který je třeba považovat za doplněk strážní služby, nikoli však za její úplnou náhradu. Změna hodnocení ohrožení, například v době návštěvy významných osob, může mít za následek zesílení kontrolních opatření při vstupu a výstupu.

18.3.4 *Pochůzky*

Mimo obvyklou pracovní dobu je třeba provádět v bezpečnostních oblastech kategorie I a II bezpečnostní pochůzky pro ochranu informací a materiálů EU před vyzrazením, poškozením nebo ztrátou. Frekvence pochůzek je určena v závislosti na místních podmínkách, musí však probíhat přibližně každé 2 hodiny.

18.3.5 *Bezpečnostní schránky a trezory*

Pro uchovávání utajovaných informací EU se používají tři kategorie schránek:

— kategorie A: schránky schválené vnitrostátními normami pro uchovávání skutečností se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ v bezpečnostní oblasti kategorie I nebo kategorie II;

— kategorie B: schránky schválené vnitrostátními normami pro uchovávání skutečností se stupněm utajení ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄v bezpečnostní oblasti kategorie I nebo II;

▼B

— kategorie C: kancelářský nábytek schválený pro uchovávání skutečností se stupněm utajení ►M1 RESTREINT UE ◄.

Pro trezory instalované v bezpečnostních oblastech kategorie I nebo II a pro všechny bezpečnostní oblasti kategorie I, kde jsou skutečnosti se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším uloženy na otevřených policích nebo jsou uvedeny na plánech, mapách atd., musí být stěny, podlahy, stropy, dveře a zámky schváleny orgánem pro bezpečnostní akreditaci, že poskytují odpovídající ochranu jako bezpečnostní schránka kategorie schválená pro skladování skutečností se stejným stupněm utajení.

18.3.6 *Zámky*

Zámky na bezpečnostních schránkách a trezorech, ve kterých jsou uloženy utajované skutečnosti EU, musí odpovídat těmto normám:

— skupina A: schválené podle vnitrostátních norem pro schránky kategorie A;

— skupina B: schválené podle vnitrostátních norem pro schránky kategorie B;

— skupina C: vhodné pouze pro kancelářský nábytek kategorie C.

18.3.7 *Kontrola klíčů a kombinací*

Klíče od bezpečnostních schránek nesmějí být vynášeny mimo budovu. Kombinace se naučí zpaměti pouze osoby, které je potřebují znát. Místní bezpečnostní pracovník má pro případ nouze k dispozici náhradní klíče a záznam jednotlivých kombinací uložené jednotlivě v zapečetěné neprůhledné obálce. Klíče, jejich náhrady a obálky s kombinacemi jsou uchovávány v oddělených bezpečnostních schránkách. Tyto klíče a kombinace musí být chráněny stejně pečlivě jako materiál, ke kterému zajišťují přístup.

Počet osob, které znají kombinace k bezpečnostním schránkám, musí být co nejvíce omezen. Kombinace jsou měněny:

a) při přijetí nové schránky;

b) při jakékoli změně personálu;

c) v případě skutečného vyzrazení nebo vznikne-li podezření z vyzrazení;

d) nejlépe každých šest měsíců a nejméně každých dvanáct měsíců.

18.3.8 *Zařízení pro odhalování vniknutí*

Používají-li se pro ochranu utajovaných skutečností EU poplašné systémy, uzavřené televizní okruhy a jiná elektrická zařízení, musí být k dispozici nouzové zdroje elektřiny, aby byl zajištěn nepřetržitý provoz systému v případě přerušení dodávky elektrické energie. Dalším základním požadavkem je, aby jakýkoli nedostatek funkce systému nebo jakýkoli pokus o odstavení zmíněných systémů vedly ke spuštění poplachu nebo jiného spolehlivého upozornění pro dohlížející personál.

18.3.9 *Schválené vybavení*

►M2 Ředitelství pro bezpečnost Komise ◄ aktualizuje seznamy, vedené podle typu a modelu, bezpečnostního vybavení, které schválila k přímé nebo nepřímé ochraně utajovaných skutečností za různých okolností a podmínek, které budou upřesněny. ►M2 Ředitelství pro bezpečnost Komise ◄ vypracuje tyto seznamy mimo jiné na základě informací poskytnutých vnitrostátními bezpečnostními orgány.

18.3.10 *Fyzická ochrana kopírovacích zařízení a faxů*

Kopírovací zařízení a faxy musí být předmětem opatření fyzické ochrany, která dostatečně zajistí, že je budou moci ke zpracování používat pouze oprávněné osoby a že všechny utajované tisky budou řádně kontrolovány.

▼B

18.4 **Opatření proti nahlédnutí a odposlechu**

18.4.1 *Nahlédnutí*

Je třeba přijmout všechna nezbytná opatření, která ve dne i v noci zajistí, aby žádná neoprávněná osoba neměla možnost vidět, ani náhodně, utajované skutečnosti EU.

18.4.2 *Odposlech*

Kanceláře nebo oblasti, ve kterých se pravidelně projednávají utajované skutečnosti se stupněm utajení ►M1 SECRET UE ◄ nebo vyšším, musí být, odůvodňuje-li to riziko, chráněny před pokusy o pasivní a aktivní odposlech. Hodnocení rizika odposlechů provádí ►M2 ředitelství pro bezpečnost Komise ◄ případně po konzultaci vnitrostátního bezpečnostního orgánu.

18.4.3 *Vnášení elektronického a záznamového zařízení*

Do bezpečnostních oblastí nebo technicky zabezpečených prostor není povoleno vnášet mobilní telefony, soukromé počítače, nahrávací zařízení, kamery nebo jiné elektronické či záznamové zařízení bez předchozího povolení ►M2 ředitele ředitelství pro bezpečnost Komise ◄.

Pro stanovení ochranných opatření, která mají být přijata v citlivých prostorách proti pasivnímu odposlechu (např. izolace stěn, dveří, podlah a stropů, měření vycházejícího hluku) a aktivnímu odposlechu (např. pátrání po mikrofonech), může ►M2 ředitelství pro bezpečnost Komise ◄ požádat o podporu odborníky z vnitrostátního bezpečnostního orgánu.

Podobně mohou odborníci na bezpečnostní techniku vnitrostátních bezpečnostních orgánů na žádost ►M2 ředitele ředitelství pro bezpečnost Komise ◄ ověřovat telekomunikační zařízení a elektrická nebo elektronická kancelářská zařízení jakéhokoli druhu používaná při zasedáních se stupněm utajení ►M1 SECRET UE ◄ a vyšším, vyžadují-li to okolnosti.

18.5 *Technicky chráněné oblasti*

Některé oblasti mohou být určeny jako technicky chráněné oblasti. U vstupu se zde provádějí speciální kontroly. Tyto oblasti musí být uzamčeny, nejsou-li obsazeny, schválenou metodou a se všemi klíči se musí zacházet jako s bezpečnostními klíči. Tyto oblasti musí být pravidelně fyzicky kontrolovány a kontrola musí být provedena také po jakémkoli neoprávněném vstupu nebo při podezření z takového vstupu.

Musí se vést podrobná evidence vybavení a nábytku, aby se zjistil jejich jakýkoli pohyb. Do této oblasti lze vnést jakýkoli nábytek nebo zařízení pouze po pečlivé kontrole speciálně školeným bezpečnostním personálem zaměřené na odhalení jakýchkoli odposlechových zařízení. Obecně není dovoleno instalovat komunikační linky do technicky chráněných oblastí bez předem uděleného souhlasu příslušného orgánu.

19. OBECNÁ PRAVIDLA TÝKAJÍCÍ SE ZÁSADY „POTŘEBA VĚDĚT“ A BEZPEČNOSTNÍCH PROVĚREK PERSONÁLU EU

19.1 **Obecně**

Přístup k utajovaným skutečnostem EU je povolen pouze osobám, které mají pro výkon svých funkcí nebo splnění svého úkolu „potřebu vědět“. Přístup ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄ je povolen pouze osobám, které prošly příslušnou bezpečnostní prověrkou.

„Potřebu vědět“ určuje útvar, ve kterém osoba vykonává své funkce.

Za žádosti o prověrku pracovníků odpovídá jednotlivý útvar.

▼B

Po provedení prověrky je vydáno „bezpečnostní osvědčení“, které upřesňuje stupeň utajovaných skutečností, k nimž může mít prověřovaná osoba přístup, a datum skončení platnosti.

Bezpečnostní osvědčení pracovníka EU vydané pro určitý stupeň může držiteli umožnit přístup ke skutečnostem nižšího stupně.

Jiné osoby než úředníci nebo ostatní zaměstnanci, například externí smluvní partneři, odborníci nebo konzultanti, s nimiž může být nezbytné posuzovat nebo konzultovat utajované skutečnosti EU, musí mít bezpečnostní prověrku pracovníka EU a musí být poučeni o své odpovědnosti v oblasti bezpečnosti.

Přístup veřejnosti se i nadále řídí nařízením (ES) č. 1049/2001.

19.2 **Zvláštní pravidla pro přístup ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄**

Všechny osoby, které mají mít přístup ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, musí nejprve projít bezpečnostní prověrkou umožňující přístup k těmto skutečnostem.

Všechny osoby, které potřebují získat přístup ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, musí být jmenovitě určeny členem Komise odpovědným za bezpečnostní otázky a jejich jména jsou vedena v příslušné spisovně skutečností ►M1 TRES SECRET UE/EU TOP SECRET ◄. Tuto spisovnu vytvoří a spravuje ►M2 ředitelství pro bezpečnost Komise ◄.

Všechny osoby oprávněné k přístupu ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ musí nejprve podepsat potvrzení, že byly poučeny o bezpečnostních postupech Komise a že plně chápou svou zvláštní odpovědnost za ochranu skutečností ►M1 TRES SECRET UE/EU TOP SECRET ◄, jakož i důsledky stanovené v předpisech EU a vnitrostátních právních a správních předpisech pro případ, že se utajované skutečnosti dostanou do neoprávněných rukou, ať už úmyslně, nebo z nedbalosti.

U osob, které mají přístup ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ v průběhu zasedání atd., musí příslušný kontrolní úředník útvaru nebo subjektu, kde jsou zaměstnány, upozornit útvar, který zasedání pořádá, že jsou oprávněny k přístupu ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄.

Jména všech osob, které již nejsou zaměstnány ve funkcích vyžadujících přístup ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, musí být vyškrtnuta z příslušného seznamu. Kromě toho musí být všechny tyto osoby znovu upozorněny na svou zvláštní odpovědnost za ochranu skutečností se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄. Musí rovněž podepsat prohlášení, ve kterém se zavazují, že nepoužijí ani nevyzradí skutečnosti se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, které jsou jim známy.

19.3 **Zvláštní pravidla pro přístup ke skutečnostem se stupněm utajení ►M1 SECRET UE ◄ A ►M1 CONFIDENTIEL UE ◄**

Všechny osoby, které mají mít přístup ke skutečnostem se stupněm utajení ►M1 SECRET UE ◄ nebo ►M1 CONFIDENTIEL UE ◄, musí nejprve projít bezpečnostní prověrkou odpovídajícího stupně.

Všechny osoby, které mají mít přístup ke skutečnostem se stupněm utajení ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄, musí být seznámeny s příslušnými bezpečnostními předpisy a s následky případné nedbalosti.

V případě osob, které mají přístup ke skutečnostem se stupněm utajení ►M1 SECRET UE ◄ nebo ►M1 CONFIDENTIEL UE ◄ v průběhu zasedání atd., musí příslušný bezpečnostní pracovník útvaru

▼B

nebo subjektu, kde jsou zaměstnány, upozornit útvar, který zasedání pořádá, že jsou oprávněny k přístupu k těmto skutečnostem.

19.4. **Zvláštní pravidla pro přístup ke skutečnostem se stupněm utajení ►M1 RESTREINT UE ◄**

Všechny osoby s přístupem ke skutečnostem se stupněm utajení ►M1 RESTREINT UE ◄ musí být upozorněny na tyto bezpečnostní předpisy a na následky případné nedbalosti.

19.5 **Převedení na jiné místo**

Při převedení personálu z funkce, která vyžaduje nakládání s utajovanými skutečnostmi EU, musí spisovna dohlédnout na řádné předání materiálu mezi odcházejícím a nastupujícím úředníkem.

Pokud je někdo z personálu převeden na jiné pracovní místo, kde přijde do styku s utajovanými materiály EU, místní bezpečnostní pracovník jej odpovídajícím způsobem poučí.

19.6 **Zvláštní pokyny**

Osoby, které mají mít přístup k utajovaným skutečnostem EU, jsou při nástupu do funkce a potom pravidelně upozorňovány na:

a) ohrožení bezpečnosti neuváženými rozhovory;

b) opatření přijatá pro vztah k tisku a k zástupcům zvláštních zájmových skupin;

c) ohrožení činnostmi zpravodajských služeb, které se zaměřují na EU a členské státy a které se zajímají o utajované skutečnosti a činnosti EU;

d) povinnost okamžitě oznámit příslušným bezpečnostním orgánům všechny pokusy o přiblížení nebo jednání, které vzbuzují podezření, že jde o špionážní činnost, nebo jakékoli neobvyklé okolnosti související s bezpečností.

Všechny osoby, které obvykle přicházejí často do styku se zástupci zemí, jejichž zpravodajské služby se zaměřují na EU a členské státy a zajímají se o utajované skutečnosti a činnosti EU, jsou poučeny o známých technikách různých špionážních služeb.

Neexistují bezpečnostní předpisy Komise pro soukromé cesty, a to nezávisle na jejich cíli, personálu zmocněného pro přístupu k utajovaným skutečnostem EU. ►M2 Ředitelství pro bezpečnost Komise ◄ však seznámí úředníky a jiné zaměstnance spadající do její působnosti s předpisy platnými pro cestování, které by se jich mohly týkat.

20. BEZPEČNOSTNÍ PROVĚRKY ÚŘEDNÍKŮ A OSTATNÍCH ZAMĚSTNANCŮ KOMISE

a) Přístup k utajovaným skutečnostem EU mají pouze úředníci a ostatní zaměstnanci Komise nebo osoby pracující v rámci Komise, kteří mají z důvodu svých funkcí a pro splnění požadavků daného útvaru znát utajované skutečnosti v držení Komise nebo s nimi nakládat.

b) Pro přístup k utajovaným skutečnostem se stupněm utajení „ ►M1 TRES SECRET UE/EU TOP SECRET ◄“, „ ►M1 SECRET UE ◄“ a „ ►M1 CONFIDENTIEL UE ◄“ musí všechny osoby uvedené v odstavci a) nejprve získat oprávnění pro tento účel postupem podle odstavců c) a d).

c) Oprávnění se uděluje pouze osobám, které prošly bezpečnostní prověrkou příslušných vnitrostátních orgánů členských států postupem podle odstavců i) až n).

d) ►M2 Ředitel ředitelství pro bezpečnost Komise ◄ odpovídá za udělování oprávnění podle odstavců a) až c).

e) ►M2 Ředitel ředitelství pro bezpečnost Komise ◄ udělí oprávnění po převzetí stanoviska příslušných vnitrostátních orgánů členských

▼B

států na základě bezpečnostní prověrky provedené v souladu s odstavci i) až n).

f) ►M2 Ředitelství pro bezpečnost Komise ◄ vede a aktualizuje seznam všech citlivých pracovních míst, která jí nahlásily příslušné útvary Komise, a všech osob, kterým bylo uděleno (dočasné) oprávnění.

g) Oprávnění, které má dobu platnosti pět let, nesmí být uděleno na dobu delší než je doba výkonu funkcí odůvodňujících jeho udělení. Platnost oprávnění může být prodloužena postupem podle odstavce e).

h) ►M2 Ředitel ředitelství pro bezpečnost Komise ◄ odejme oprávnění, má-li za to, že jsou k tomu oprávněné důvody. Jakékoli rozhodnutí o odnětí oprávnění je sděleno dotčené osobě, která může žádat o vyslechnutí ►M2 ředitele ředitelství pro bezpečnost Komise ◄, a rovněž příslušnému vnitrostátnímu orgánu.

i) Bezpečnostní šetření se provádí s pomocí dotčené osoby a na žádost ►M2 ředitele ředitelství pro bezpečnost Komise ◄. Za příslušný vnitrostátní orgán, který je oprávněn provádět šetření, se považuje orgán toho členského státu, jehož je osoba, na kterou se vztahuje oprávnění, státním příslušníkem. V případech, kdy dotčená osoba není státním příslušníkem členského státu EU, si ►M2 ředitel ředitelství pro bezpečnost Komise ◄ vyžádá bezpečnostní šetření od členského státu EU, ve kterém má tato osoba bydliště nebo kde se obvykle zdržuje.

j) V rámci šetření je dotčená osoba povinna vyplnit osobní prohlášení.

k) ►M2 Ředitel ředitelství pro bezpečnost Komise ◄ ve své žádosti upřesní typ a stupeň utajení utajovaných skutečností, které má dotčená osoba znát, aby příslušné vnitrostátní orgány mohly provést šetření a vydat své stanovisko k úrovni oprávnění, které má být uděleno dotčené osobě.

l) Pro celý průběh a výsledky bezpečnostního šetření se uplatňují pravidla a předpisy platné v této oblasti v dotčeném členském státu včetně pravidel a předpisů pro případné opravné prostředky.

m) Vydají-li příslušné vnitrostátní orgány členského státu kladné stanovisko, může ►M2 ředitel ředitelství pro bezpečnost Komise ◄ udělit dotčené osobě oprávnění.

n) Vydají-li příslušné vnitrostátní orgány záporné stanovisko, oznámí se smysl tohoto stanoviska dotčené osobě, která může požádat ►M2 ředitele ředitelství pro bezpečnost Komise ◄ o vyslechnutí. Považuje-li to ►M2 ředitel ředitelství pro bezpečnost Komise ◄ za nezbytné, může požádat příslušné vnitrostátní orgány o doplňující vysvětlení, která tyto orgány mohou poskytnout. Je-li záporné stanovisko potvrzeno, nelze oprávnění udělit.

o) Všechny osoby oprávněné ve smyslu odstavců d) a e) dostanou v okamžiku udělení oprávnění a poté v pravidelných intervalech pokyny nezbytné k ochraně utajovaných skutečností a ke způsobu zajištění této ochrany. Tyto osoby podepíší prohlášení potvrzující, že přijaly pokyny a že se zavazují je dodržovat.

p) ►M2 Ředitel ředitelství pro bezpečnost Komise ◄ přijme všechna nezbytná opatření k provedení tohoto oddílu, zejména opatření týkající se úpravy přístupu k seznamu oprávněných osob.

q) Výjimečně a vyžaduje-li to útvar, může ►M2 ředitel ředitelství pro bezpečnost Komise ◄ poté, co předběžně uvědomí vnitrostátní příslušné orgány, a pokud od nich nezíská ve lhůtě jednoho měsíce žádnou reakci, udělit dočasné oprávnění na dobu nepřesahující šest měsíců, dokud nebude znám výsledek šetření uvedeného v odstavci i).

▼B

r) Takto udělená prozatímní a dočasná oprávnění neumožňují přístup ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄; přístup k nim je vyhrazen úředníkům, u nichž bylo účinně s kladnými výsledky provedeno šetření v souladu s odstavcem i). Do vydání výsledků šetření mohou úředníci, u kterých se požaduje prověrka pro stupeň ►M1 TRES SECRET UE/EU TOP SECRET ◄, dostat dočasné a prozatímní oprávnění pro přístup k utajovaným skutečnostem se stupněm utajení nejvýše ►M1 SECRET UE ◄ včetně.

21. PŘÍPRAVA, ŠÍŘENÍ, PŘENOS, BEZPEČNOST PERSONÁLU ZÁSILKOVÝCH SLUŽEB A DOPLŇKOVÉ VÝTISKY NEBO PŘEKLADY A VÝPISY Z UTAJOVANÝCH DOKUMENTŮ EU

21.1 **Příprava**

1. Jak je stanoveno v oddílu 16 a pro stupeň ►M1 CONFIDENTIEL UE ◄ a vyšší se uvádějí stupně a označení uprostřed nahoře a dole každé stránky a každá stránka musí být očíslována. Na každém utajovaném dokumentu EU musí být uvedeno spisové číslo a datum. U dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ a ►M1 SECRET UE ◄ je spisové číslo uvedeno na každé stránce. Mají-li být utajované dokumenty šířeny ve více výtiscích, musí být každý z nich označen na první stránce číslem výtisku a celkovým počtem stránek. Na první stránce dokumentu se stupněm utajení ►M1 CONFIDENTIEL UE ◄ nebo vyšším musí být uveden seznam všech příloh a připojených částí.

2. Dokumenty se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším mohou psát na stroji, překládat, archivovat, kopírovat, ukládat na magnetické nosiče nebo na mikrofilmy pouze osoby prověřené pro přístup k utajovaným skutečnostem EU nejméně až do bezpečnostní kategorie odpovídající dotčenému dokumentu.

3. Ustanovení pro zpracování utajovaných dokumentů s využitím výpočetní techniky jsou uvedena v oddíle 25.

21.2 **Šíření**

1. Utajované skutečnosti EU lze šířit pouze mezi osoby, které mají „potřebu vědět“ a prošly příslušnou bezpečnostní prověrkou. Počáteční šíření upřesní původce dokumentu.

2. Dokumenty se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ se rozšiřují prostřednictvím spisoven ►M1 TRES SECRET UE/EU TOP SECRET ◄ (viz oddíl 22.2). V případě sdělení se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ může příslušná spisovna pověřit vedoucího střediska komunikace, aby připravil počet kopií odpovídající seznamu příjemců.

3. Dokumenty se stupněm utajení ►M1 SECRET UE ◄ a nižším může původní příjemce dále šířit dalším příjemcům na základě „potřeby vědět“. Původci dokumentů však musí jasně uvést všechna omezení, která zamýšlejí uložit. Jakmile jsou tato omezení uložena, mohou příjemci dokumenty dále šířit pouze s povolením jejich původce.

4. Všechny dokumenty se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším se evidují při příchodu na generální ředitelství nebo službu a při odchodu z nich. Tento úkol přísluší místní spisovně utajovaných skutečností EU v daném útvaru. Do knihy nebo na speciálně chráněné nosiče dat se zaznamenávají údaje (spisové číslo, datum a případně číslo výtisku), které umožňují dokumenty identifikovat (viz oddíl 22.1).

▼B

21.3 **Přenos utajovaných dokumentů EU**

21.3.1 *Balení zásilek, potvrzení příjmu*

1. Dokumenty se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším jsou přenášeny v trvanlivých neprůhledných dvojitých obálkách. Vnitřní obálka je orazítkována a označena příslušným stupněm utajení EU a pokud možno všemi údaji o funkci a adrese příjemce.

2. Otevřít vnitřní obálku a potvrdit příjem vložených dokumentů smí pouze kontrolor spisovny (viz oddíl 22.1) nebo jeho zástupce, nemá-li obálka určitého příjemce. V tom případě eviduje příslušná spisovna (viz oddíl 22.1) přijetí obálky a otevřít vnitřní obálku a potvrdit přijetí dokumentů, které obsahuje, smí pouze osoba, které je obálka určena.

3. Do vnitřní obálky se vkládá potvrzení o příjmu. Potvrzení, které není utajovaným dokumentem, obsahuje spisové číslo, datum a číslo výtisku dokumentu, nikdy však předmět.

4. Vnitřní obálka je uzavřena do vnější obálky označené číslem zásilky pro účely převzetí. Za žádných okolností se na vnější obálce nesmí objevit stupeň utajení.

5. K dokumentům se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším stupněm dostanou kurýři a poslíčci potvrzení o příjmu s uvedením čísla zásilky.

21.3.2 *Přenos uvnitř budovy nebo skupiny budov*

Uvnitř budovy nebo skupiny budov se utajované dokumenty mohou přenášet v jediné uzavřené obálce označené pouze jménem příjemce, pokud je přenáší osoba prověřená pro daný stupeň utajení dokumentů.

21.3.3 *Přenos uvnitř země*

1. Uvnitř jedné země jsou dokumenty se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ přenášeny výlučně prostřednictvím úřední zásilkové služby nebo osobami oprávněnými k přístupu ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. Kdykoli se pro přenos dokumentu se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ mimo rámec budovy nebo skupiny budov použije zásilková služba, je vhodné použít ustanovení o balení a potvrzování příjmu uvedená v této kapitole. Zásilkové služby mají takový personál, aby bylo zajištěno, že balíčky obsahující dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ zůstanou pod přímým a stálým dohledem odpovědné osoby.

3. Výjimečně mohou dokumenty se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ přenášet mimo rámec budovy nebo skupiny budov pro místní použití na zasedáních a jednáních jiní úředníci než kurýři, pokud:

   a) je osoba, která je přenáší, oprávněna k přístupu k těmto dokumentům ►M1 TRES SECRET UE/EU TOP SECRET ◄;

   b) způsob dopravy vyhovuje pravidlům, kterými se řídí přenos dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄;

   c) osoba, která je přenáší, nenechává za žádných okolností přenášené dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ bez dozoru;

   d) jsou přijata ustanovení, aby byl seznam takto přenášených dokumentů uložen ve spisovně ►M1 TRES SECRET UE/EU TOP SECRET ◄ a zaznamenán do rejstříku a umožnil tak kontrolu těchto dokumentů při návratu.

▼B

4. Uvnitř jedné země lze dokumenty se stupněm utajení ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄ přenášet jak poštou, je-li tento způsob přenosu povolen podle vnitrostátních právních předpisů a v souladu s nimi, tak zásilkovou službou, nebo osobami oprávněnými pro přístup k utajovaným skutečnostem EU.

5. ►M2 Ředitelství pro bezpečnost Komise ◄ vypracuje na základě těchto pravidel pokyny pro osobní přenos utajovaných dokumentů EU. Osoba, která dokumenty přenáší, si tyto pokyny přečte a podepíše je. Pokyny zejména jasně stanoví, že dokumenty:

   a) musí za všech okolností zůstat v rukou osoby, která je přenáší, ledaže jsou pod dozorem podle ustanovení oddílu 18;

   b) nesmějí být ponechány bez dozoru v prostředcích hromadné dopravy ani v soukromých vozidlech ani na veřejných místech, jako jsou restaurace a hotely. Nesmějí být uloženy v hotelových sejfech ani ponechány bez dozoru v hotelových pokojích;

   c) nesmějí se číst na veřejných místech, například v letadle nebo ve vlaku.

21.3.4 *Přenos z jednoho státu do druhého*

1. Materiál se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším je přenášen z jednoho členského státu do jiného diplomatickou nebo vojenskou zásilkovou službou.

2. Přenos materiálu se stupněm utajení ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄ osobami však lze však povolit, poskytují-li opatření přijatá pro přenos záruky, že dokumenty se nemohou dostat do rukou neoprávněné osoby.

3. Člen Komise odpovědný za bezpečnostní otázky může povolit přenos zajišťovaný osobou, pokud nelze využít diplomatické ani vojenské kurýry nebo pokud by jejich využití znamenalo zpoždění schopné poškodit operace EU a pokud příjemce požaduje materiál naléhavě. ►M2 Ředitelství pro bezpečnost Komise ◄ vypracuje pokyny pro mezinárodní přepravu materiálu se stupněm utajení ►M1 SECRET UE ◄ včetně jinými osobami, než jsou diplomatičtí a vojenští kurýři. Tyto pokyny vyžadují, aby:

   a) osoba, která je přenáší, prošla příslušnou bezpečnostní prověrkou;

   b) všechny takto přenášené materiály byly evidovány v příslušném útvaru nebo spisovně;

   c) balíky nebo tašky obsahující materiál EU měly oficiální pečeť zamezující nebo předcházející celní kontrole a identifikační nálepky s pokyny pro nálezce;

   d) osoba, která je přenáší, byla držitelem osvědčení kurýra nebo pověření k úkolu uznávaného všemi členskými státy EU a opravňujícího k přenosu řádně označeného balíčku;

   e) osoba, která je přenáší, nepřekročila při přepravě pozemní cestou hranice ani území třetího státu, ledaže tento stát poskytne odesílajícímu státu zvláštní záruku;

   f) pokud jde o místo určení, trasa a dopravní prostředky, odpovídají předpisy týkající se cesty předpisům EU nebo vnitrostátním předpisům, jsou-li přísnější;

   g) osoba, která je přenáší, má materiál stále u sebe, ledaže je zajištěn dozor nad ním v souladu s bezpečnostními ustanoveními uvedenými v oddíle 18;

   h) materiály nejsou ponechány bez dozoru v prostředcích hromadné dopravy nebo v soukromých vozidlech ani na veřejných místech, jako jsou restaurace nebo hotely. Nesmí se ukládat do hotelových sejfů ani nechávat bez dozoru v hotelových pokojích;

▼B

i) pokud přenášený materiál obsahuje dokumenty, nesmějí se číst na veřejných místech (například v letadle, ve vlaku atd.).

4. Osoba pověřená přenosem utajovaného materiálu si musí přečíst a podepsat bezpečnostní pokyny, které obsahují alespoň výše uvedené pokyny a uvádějí postupy pro případy nouze nebo pro případ, že balíček obsahující utajovaný materiál budou kontrolovat celní orgány nebo bezpečnostní orgány na letišti.

21.3.5 *Přenos dokumentů se stupněm utajení* ►M1 *RESTREINT UE* ◄

Pro přenos dokumentů se stupněm utajení ►M1 RESTREINT UE ◄ nejsou stanovena žádná zvláštní pravidla; pouze musí probíhat tak, aby se nedostaly do rukou neoprávněné osoby.

21.4 **Bezpečnost personálu zásilkových služeb**

Všichni kurýři a poslíčci používaní pro přenos dokumentů se stupněm utajení ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄ musí projít příslušnou bezpečnostní prověrkou.

21.5 **Přenos elektronickými a jiné jinými způsoby technického technickými prostředky**

1. Bezpečnostní opatření v oblasti telekomunikací mají zajistit bezpečný přenos utajovaných skutečností EU. Podrobná pravidla, která je třeba dodržovat při přenosu utajovaných skutečností EU, jsou uvedena v oddílu 25.

2. Skutečnosti se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a ►M1 SECRET UE ◄ mohou přenášet pouze schválená přenosová centra a sítě nebo terminály a systémy.

21.6 **Doplňkové výtisky a překlady a výpisy z utajovaných dokumentů EU**

1. Kopírování nebo překlady dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ může povolit pouze původce dokumentu.

2. Jestliže osoby, které neprošly bezpečnostní prověrkou pro stupeň utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, potřebují informace obsažené v dokumentu se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, které však samy o sobě takto zařazeny nejsou, může být vedoucí spisovny ►M1 TRES SECRET UE/EU TOP SECRET ◄ (viz oddíl 22.2) pověřen vytvořit potřebný počet výpisů z daného dokumentu. Vedoucí zároveň přijme potřebná opatření, aby těmto výpisům byl přidělen odpovídající stupeň utajení.

3. Dokumenty se stupněm utajení ►M1 SECRET UE ◄ a nižším může rozmnožovat a překládat příjemce v souladu s těmito bezpečnostními opatřeními a za podmínky, že přísně dodržuje zásadu „potřeba vědět“. Bezpečnostní opatření vztahující se na původní dokument se rovněž použijí na rozmnoženiny nebo překlady dokumentu.

22. SPISOVNY UTAJOVANÝCH INFORMACÍ SKUTEČNOSTÍ EU, INVENTURY A KONTROLY, ARCHIVACE A NIČENÍ TĚCHTO SKUTEČNOSTÍ

22.1 **Místní spisovny utajovaných skutečností**

1. V rámci Komise, v případě potřeby v rámci každého útvaru, se vytvoří jedna nebo více místních spisoven pro správu utajovaných skutečností EU. Odpovídají za evidování, rozmnožování, rozesílání, archivaci a ničení dokumentů se stupněm utajení ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄.

2. Jestliže útvar nemá místní spisovnu utajovaných skutečností EU, tuto činnost vykonává místní spisovna generálního sekretariátu.

3. Místní spisovny utajovaných skutečností EU podávají zprávy vedoucímu útvaru, od kterého dostávají pokyny. Vedoucím těchto spisoven je kontrolor spisovny (RCO).

▼B

4. Pokud jde o používání předpisů týkajících se nakládání s dokumenty obsahujícími utajované skutečnosti a o dodržování odpovídajících bezpečnostních opatření, jsou podřízeny bezpečnostnímu pracovníkovi daného útvaru.

5. Úředníci pracující v místních spisovnách utajovaných skutečností EU musí mít oprávnění k přístupu k utajovaným skutečnostem EU v souladu s oddílem 20.

6. Za odpovědnosti příslušného vedoucího útvaru místní spisovny utajovaných skutečností EU:

   a) řídí operace, které se týkají evidence, rozmnožování, překladů, přenosu, odesílání a ničení takových skutečností;

   b) aktualizují rejstřík utajovaných skutečností;

   c) pravidelně prověřují potřebu nadále zachovávat utajení skutečností.

7. Místní spisovny utajovaných informací EU vedou rejstříky obsahující tyto údaje:

   a) datum vyhotovení utajované skutečnosti;

   b) stupeň utajení;

   c) datum skončení utajení;

   d) jméno a útvar původce skutečnosti;

   e) příjemce nebo příjemci s uvedením pořadového čísla;

   f) předmět;

   g) číslo;

   h) počet rozšiřovaných výtisků;

   i) informace o vypracování evidence utajovaných skutečností předložených útvaru;

   j) rejstřík, kde jsou zaznamenány operace odtajnění a snížení stupně utajení.

8. Na spisovny utajovaných informací EU se vztahují obecná pravidla uvedená v oddíle 21, aniž jsou tím dotčeny změny vyplývající ze zvláštních pravidel stanovených v tomto oddíle.

22.2 **Spisovna ►M1 TRES SECRET UE/EU TOP SECRET ◄**

22.2.1 *Obecně*

1. Ústřední spisovna ►M1 TRES SECRET UE/EU TOP SECRET ◄ zajišťuje evidenci dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, nakládání s nimi a jejich šíření v souladu s těmito bezpečnostními předpisy. Vedoucím spisovny ►M1 TRES SECRET UE/EU TOP SECRET ◄ je kontrolor spisovny ►M1 TRES SECRET UE/EU TOP SECRET ◄.

2. Ústřední spisovna ►M1 TRES SECRET UE/EU TOP SECRET ◄ působí jako hlavní orgán pro příjem a šíření pro Komisi, ostatní instituce EU, členské státy, mezinárodní organizace a pro třetí státy, s nimiž Komise uzavřela dohody o bezpečnostních postupech při výměně utajovaných skutečností.

3. Podle potřeby se zřizují spisovny nižší úrovně, které zajišťují vnitřní nakládání s dokumenty se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄; aktualizují záznamy o každém dokumentu, který mají na starosti.

4. Spisovny ►M1 TRES SECRET UE/EU TOP SECRET ◄ nižší úrovně se zřizují, jak je uvedeno v oddílu 22.2.3, aby se vyhovělo dlouhodobé potřebě, a jsou napojeny na ústřední spisovnu

▼B

►M1 TRES SECRET UE/EU TOP SECRET ◄. Je-li potřeba nahlížet do dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ pouze dočasná a příležitostná, lze tyto dokumenty poskytnout, aniž je zřízena spisovna ►M1 TRES SECRET UE/EU TOP SECRET ◄ nižší úrovně, pokud stanovená pravidla zajišťují, že tyto dokumenty zůstanou pod kontrolou příslušné spisovny ►M1 TRES SECRET UE/EU TOP SECRET ◄, a pokud budou dodržována všechna fyzická bezpečnostní opatření a bezpečnostní opatření týkající se personálu.

5. Spisovny nižší úrovně nesmějí bez výslovného souhlasu ústřední spisovny ►M1 TRES SECRET UE/EU TOP SECRET ◄ předávat dokumenty se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ přímo jiným spisovnám nižší úrovně podřízeným stejné ústřední spisovně ►M1 TRES SECRET UE/EU TOP SECRET ◄.

6. Všechny výměny dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ mezi spisovnami nižší úrovně podřízenými různým ústředním spisovnám se provádějí prostřednictvím ústředních spisoven ►M1 TRES SECRET UE/EU TOP SECRET ◄.

22.2.2 *Ústřední spisovna* ►M1 TRES SECRET UE/EU TOP SECRET ◄

Jako kontrolor odpovídá vedoucí spisovny ►M1 TRES SECRET UE/EU TOP SECRET ◄ za:

a) zajištění přenášení dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ v souladu s pravidly stanovenými v oddíle 21.3;

b) aktualizaci seznamu všech podřízených spisoven ►M1 TRES SECRET UE/EU TOP SECRET ◄ nižší úrovně spolu se jmény a podpisy pověřených kontrolních úředníků a jejich oprávněných zástupců;

c) uchovávání potvrzení o převzetí od spisoven pro všechny dokumenty se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ šířené ústřední spisovnou;

d) vedení záznamů o držených a rozšiřovaných dokumentech se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄;

e) aktualizaci seznamu všech ústředních spisoven ►M1 TRES SECRET UE/EU TOP SECRET ◄, s nimiž obvykle udržuje písemný styk, spolu se jmény a podpisy pověřených kontrolorů a jejich oprávněných zástupců;

f) zajištění fyzické bezpečnosti všech dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ držených ve spisovně v souladu s pravidly uvedenými v oddíle 18.

22.2.3 *Spisovny* ►M1 *TRES SECRET UE/EU TOP SECRET* ◄ *nižší úrovně*

Jako kontrolor odpovídá vedoucí spisovny ►M1 TRES SECRET UE/EU TOP SECRET ◄ nižší úrovně za:

a) zajištění přenášení dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ v souladu s pravidly vymezenými v oddíle 21.3;

b) aktualizaci seznamu všech osob oprávněných k přístupu ke skutečnostem se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, které kontroluje;

c) šíření dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ v souladu s pokyny původce nebo v závislosti na „potřebě vědět“, poté co se ujistí, že příjemce prošel bezpečnostní prověrkou požadovaného stupně;

▼B

d) aktualizaci seznamu všech dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ držených nebo obíhajících pod jeho kontrolou nebo které byly předány jiným spisovnám ►M1 TRES SECRET UE/EU TOP SECRET ◄, a za uchovávání odpovídajících potvrzení o převzetí;

e) aktualizaci seznamu spisoven ►M1 TRES SECRET UE/EU TOP SECRET ◄, se kterými je oprávněn vyměňovat dokumenty se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, spolu se jmény a podpisy pověřených kontrolorů a jejich oprávněných zástupců;

f) zajištění fyzické bezpečnosti všech dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ uložených ve spisovně nižší úrovně v souladu s pravidly stanovenými v oddíle 18.

22.3 **Inventury a kontroly utajovaných dokumentů EU**

1. Každý rok provede každá spisovna ►M1 TRES SECRET UE/EU TOP SECRET ◄ podrobnou inventuru všech dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄. Dokument se považuje za zkontrolovaný, jestliže spisovna dokument fyzicky zkontroluje nebo má potvrzení o převzetí od spisovny ►M1 TRES SECRET UE/EU TOP SECRET ◄, které byl dokument předán, nebo zápis o zničení dokumentu nebo pokyn ke snížení stupně utajení daného dokumentu nebo k jeho odtajnění. Spisovny předají výsledky svých ročních inventur členovi Komise odpovědnému za bezpečnostní otázky, a to nejpozději do 1. dubna každého roku.

2. Spisovny ►M1 TRES SECRET UE/EU TOP SECRET ◄ nižší úrovně předávají výsledky své roční inventury ústřední spisovně, které jsou podřízeny, ke dni stanovenému ústřední spisovnou.

3. Kontrola utajovaných dokumentů EU zařazených do nižšího stupně než je stupeň ►M1 TRES SECRET UE/EU TOP SECRET ◄ se provádí podle pokynů vydaných členem Komise odpovědným za bezpečnostní otázky.

4. Tyto činnosti poskytují možnost zjistit stanoviska držitelů, zda:

   a) je možno snížit stupeň utajení určitých dokumentů nebo je případně odtajnit;

   b) lze určité dokumenty zničit.

22.4 **Archivace utajovaných skutečností EU**

1. Utajované skutečnosti EU se archivují za podmínek odpovídajícím všem příslušným ustanovením uvedeným v oddíle 18.

2. Aby byly obtíže s archivací co nejmenší, jsou všichni kontroloři všech spisoven oprávněni převádět dokumenty se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄ na mikrofilmy nebo je uložit na magnetický nebo optický nosič pro účely archivace, pokud:

   a) převedení na mikrofilmy nebo archivaci provádějí osoby, které prošly platnou bezpečnostní prověrkou pro odpovídající stupeň utajení;

   b) je pro mikrofilmy nebo záznamy zaručena stejná bezpečnost jako pro původní dokumenty;

   c) převedení dokumentu se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ na mikrofilmy nebo archivace jsou oznámeny původci;

   d) cívky filmu nebo jiné typy nosiče obsahují pouze dokumenty se stejným stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ nebo ►M1 CONFIDENTIEL UE ◄;

▼B

e) převedení dokumentů se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ nebo ►M1 SECRET UE ◄ na mikrofilm nebo archivace budou jasně vyznačeny v rejstříku používaném při roční inventuře;

f) původní dokumenty, které byly převedeny na mikrofilmy nebo jinak archivovány, se zničí v souladu s pravidly uvedenými v oddíle 22.5.

3. Tato pravidla se rovněž uplatňují na všechny ostatní způsoby povolené archivace, jako jsou například elektromagnetické nosiče a optické disky.

22.5 **Ničení utajovaných dokumentů EU**

1. Aby se zabránilo zbytečnému hromadění utajovaných dokumentů EU, zničí se dokumenty považované vedoucím subjektu, který je drží, za zastaralé a nadbytečné, jakmile je to možné, těmito způsoby:

a) dokumenty se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ ničí výlučně ústřední spisovna, která je tím pověřena. Každý zničený dokument je uveden v zápise o zničení podepsaném kontrolorem ►M1 TRES SECRET UE/EU TOP SECRET ◄ a svědkem, který prošel bezpečnostní prověrkou stupně ►M1 TRES SECRET UE/EU TOP SECRET ◄. Zničení je zaznamenáno do knihy;

b) spisovna archivuje zápisy o zničení spolu s doklady o rozdělení po dobu deseti let. Kopie se předávají původci nebo příslušné ústřední spisovně, pouze jsou-li výslovně požadovány;

c) dokumenty se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ včetně utajovaného odpadu, který vzniká při přípravě těchto dokumentů (např. poškozené výtisky, koncepty, na stroji psané poznámky a diskety) se zničí pod dohledem úředníka prověřeného pro stupeň ►M1 TRES SECRET UE/EU TOP SECRET ◄ spálením, rozdrcením, roztrháním nebo jiným způsobem tak, aby je nebylo možné identifikovat a znovu sestavit.

2. Dokumenty se stupněm utajení ►M1 SECRET UE ◄ zničí spisovna, která je tím pověřená, pod dohledem osoby, jež prošla bezpečnostní prověrkou, a to jedním z postupů uvedených v odstavci 1 c). Zničení dokumentů se stupněm utajení ►M1 SECRET UE ◄ je uvedeno v podepsaných zápisech, které spisovna archivuje spolu s doklady o rozdělení nejméně tři roky.

3. Dokumenty se stupněm utajení ►M1 CONFIDENTIEL UE ◄ zničí spisovna, která je tím pověřena, pod dohledem osoby, jež prošla bezpečnostní prověrkou, jedním z postupů uvedených v odstavci 1 c). Jejich zničení se eviduje v souladu s pokyny člena Komise odpovědného za bezpečnostní otázky.

4. Dokumenty se stupněm utajení ►M1 RESTREINT UE ◄ zničí spisovna, která je tím pověřena, nebo uživatel v souladu s pokyny člena Komise odpovědného za bezpečnostní otázky.

22.6 **Zničení v nouzových situacích**

1. Útvary Komise vypracují s ohledem na místní podmínky plány pro zabezpečení utajovaných materiálů EU v případě krize včetně případných plánů na zničení a vyklizení v případech nouze. Vyhlásí pokyny, které považují za nezbytné pro zamezení tomu, aby se utajované skutečnosti EU dostaly do neoprávněných rukou.

2. Ustanovení přijatá pro zabezpečení a/nebo zničení materiálů se stupněm utajení ►M1 SECRET UE ◄ a ►M1 CONFIDENTIEL UE ◄ nesmí za žádných okolností ovlivnit zabezpečení ani zničení materiálů se stupněm utajení ►M1 TRES SECRET UE/EU

▼B

TOP SECRET ◄, zejména kódovacího zařízení, jejichž opatrování má přednost před všemi ostatními úkoly.

3. Opatření, která mají být přijata k zabezpečení a zničení kódovacího zařízení v případě nouze, se řídí zvláštními pokyny.

4. Je nezbytné, aby byly pokyny k dispozici přímo na místě v zapečetěné obálce. K dispozici musí být rovněž prostředky či nástroje určené pro zničení.

23. BEZPEČNOSTNÍ OPATŘENÍ PRO ZVLÁŠTNÍ ZASEDÁNÍ, KTERÁ SE KONAJÍ MIMO PROSTORY KOMISE A KTERÉ SE TÝKAJÍ UTAJOVANÝCH SKUTEČNOSTÍ EU

23.1 **Obecně**

Konají-li se zasedání Komise nebo jiná významná zasedání mimo prostory Komise v Bruselu a Lucemburku a odůvodňují-li to zvláštní bezpečnostní požadavky vyplývající z vysoké citlivosti projednávaných otázek nebo skutečností, přijmou se níže uvedená opatření. Tato opatření se týkají pouze ochrany utajovaných skutečností EU; může se ukázat jako nezbytné stanovit jiná bezpečnostní opatření.

23.2 **Odpovědnost**

23.2.1 ►M2 *Ředitelství pro bezpečnost Komise* ◄

►M2 Ředitelství pro bezpečnost Komise ◄ spolupracuje s příslušnými orgány členského státu, na jehož území se má zasedání uskutečnit (hostitelský členský stát), s cílem zajistit bezpečnost zasedání Komise nebo jiného významného zasedání a zajistit bezpečnost delegátů a jejich spolupracovníků. V oblasti ochrany bezpečnosti musí zajistit, aby:

a) byly vypracovány plány, které budou řešit ohrožení bezpečnosti a incidenty s bezpečností související, přičemž tato opatření se týkají zejména ochrany utajovaných dokumentů EU uvnitř prostor;

b) byla přijata opatření zajišťující případný přístup k telekomunikačnímu systému Komise za účelem příjmu a zasílání utajovaných sdělení EU. Hostitelský členský stát rovněž zajistí případný přístup k chráněným telefonním systémům.

►M2 Ředitelství pro bezpečnost Komise ◄ působí jako poradce v otázkách bezpečnosti při přípravě zasedání; měla by zde být zastoupena, aby podle potřeby pomohla a poradila úředníkovi odpovědnému za bezpečnost zasedání a delegacím.

Každá delegace na zasedání se vyzve k tomu, aby určila jednoho bezpečnostního úředníka, který bude řešit bezpečnostní otázky ve své delegaci a udržovat kontakt s bezpečnostním úředníkem zasedání a se zástupcem ►M2 ředitelství pro bezpečnost Komise ◄.

23.2.2 *Bezpečnostní úředník zasedání*

Je určen bezpečnostní úředník zasedání, který odpovídá za obecnou přípravu a kontrolu obecných opatření vnitřní bezpečnosti a za koordinaci s ostatními dotčenými bezpečnostními orgány. Opatření, která přijme, se obecně týkají:

a) ochranných opatření v místě zasedání zajišťujících, že zasedání proběhne bez incidentů, které by mohly narušit bezpečnost utajovaných skutečností EU, které se mohou při zasedání používat;

b) kontroly personálu, který má přístup na místo zasedání, do oblastí vyhrazených delegacím a do konferenčních sálů, a kontroly vnesených materiálů;

c) trvalé koordinace s příslušnými orgány hostitelského členského státu a s ►M2 ředitelstvím pro bezpečnost Komise ◄;

d) zařazení bezpečnostních pokynů do dokumentace k zasedání s ohledem na požadavky stanovené v těchto bezpečnostních před-

▼B

pisech a v jakýchkoli jiných bezpečnostních pokynech považovaných za nezbytné.

23.3 **Bezpečnostní opatření**

23.3.1 *Bezpečnostní oblasti*

Vytvářejí se tyto bezpečnostní oblasti:

a) bezpečnostní oblast kategorie II, zahrnující případně redakční místnost, kanceláře a rozmnožovací zařízení Komise a kanceláře delegací;

b) bezpečností oblast kategorie I, zahrnující konferenční místnost a kabiny tlumočníků a zvukových techniků;

c) administrativní oblasti zahrnující zařízení pro tisk a sektory vyhrazené pro administrativu, stravování a ubytování, i oblast bezprostředně přiléhající k tiskovému středisku a k místu zasedání.

23.3.2 *Propustky*

Úředník odpovědný za bezpečnost zasedání musí vydat visačky příslušného typu podle požadavků delegací. Podle potřeby lze odlišit povolení vstupu do jednotlivých bezpečnostních oblastí.

Bezpečnostní pokyny pro zasedání stanoví, že všechny dotčené osoby musí v místě zasedání neustále nosit svou visačku na viditelném místě, aby je mohl bezpečnostní personál podle potřeby kontrolovat.

Kromě účastníků vybavených visačkou bude přístup na místo zasedání povolen co nejmenšímu počtu osob. Úředník odpovědný za bezpečnost zasedání povolí delegacím států přijímat návštěvy během zasedání pouze na jejich žádost. Návštěvníci dostanou zvláštní visačku pro návštěvníky. Je jim vystavena propustka, která obsahuje jejich jméno a jméno osoby, která je přijme. Návštěvníky musí stále doprovázet bezpečnostní stráž nebo osoba, která je přijme. Propustku návštěvníka nese doprovázející osoba, která ji vrátí spolu s visačkou návštěvníka bezpečnostnímu personálu po odchodu návštěvníka z místa zasedání.

23.3.3 *Kontrola fotografických a záznamových zařízení*

Do bezpečnostní oblasti kategorie I se nesmějí vnášet žádná fotografická ani záznamová zařízení s výjimkou zařízení vnesených fotografy a zvukovými techniky, kteří mají řádné povolení od úředníka odpovědného za bezpečnost zasedání.

23.3.4 *Kontrola aktovek, přenosných počítačů a zásilek*

Držitelé propustek, které jim umožňují přístup do určité bezpečnostní oblasti, mohou běžně bez kontroly vnášet své aktovky a přenosné počítače (pouze s vlastním zdrojem energie). Delegace mohou přijímat pro ně určené zásilky, poté co je zkontroluje bezpečnostní úředník delegace nebo speciální zařízení, nebo po otevření bezpečnostním personálem. Považuje-li to úředník odpovědný za bezpečnost zasedání považuje za nezbytné, mohou být stanovena přísnější opatření pro kontroly aktovek a zásilek.

23.3.5 *Technická bezpečnost*

Technický bezpečnostní tým může zaručit technickou bezpečnost zasedací místnosti a rovněž může zajistit elektronický dozor během zasedání.

23.3.6 *Dokumenty delegací*

Delegace odpovídají za přepravu utajovaných dokumentů EU na zasedání a z něj. Rovněž odpovídají za kontrolu a bezpečnost těchto dokumentů při jejich používání v prostorách, jež jim jsou přiděleny. Pro přepravu utajovaných dokumentů na zasedání a ze zasedání lze žádat o pomoc hostitelský stát.

▼B

23.3.7 *Bezpečné uložení dokumentů*

Jestliže Komise nebo delegace nejsou schopny uložit své utajované dokumenty v souladu se schválenými normami, mohou tyto dokumenty svěřit v zapečetěné obálce proti potvrzení o převzetí bezpečnostnímu úředníkovi zasedání, který odpovídá za jejich uložení v souladu se schválenými normami.

23.3.8 *Kontrola kanceláří*

Bezpečnostní úředník zasedání zajistí na konci každého pracovního dne kontroly kanceláří Komise a delegací, aby zajistil, že všechny utajované dokumenty EU jsou bezpečně uloženy; není-li tomu tak, přijme vhodná opatření.

23.3.9 *Odstranění utajovaného odpadu EU*

Veškerý odpad se považuje za utajovaný odpad EU a koše nebo pytle na papír se předávají Komisi a delegacím ke zničení. Komise a delegace musí před odchodem z místností, které jim byly přiděleny, předat odpad úředníkovi odpovědnému za bezpečnost zasedání, který zajistí jeho zničení podle pravidel.

Na konci zasedání se se všemi dokumenty, které Komise nebo delegace drží, avšak nadále je nepotřebují, zachází jako s odpadem. Před zrušením bezpečnostních opatření přijatých pro zasedání musí být provedena důkladná prohlídka kanceláří Komise a delegací. Dokumenty, ke kterým bylo podepsáno potvrzení o příjmu, musí být podle možností zničeny, jak je uvedeno v oddíle 22.5.

24. NARUŠENÍ BEZPEČNOSTI A VYZRAZENÍ UTAJOVANÝCH SKUTEČNOSTÍ EU

24.1 **Definice**

K narušení bezpečnosti dochází jednáním nebo opomenutím proti bezpečnostním předpisům Komise nebo vnitrostátním bezpečnostním předpisům, které může ohrozit nebo vyzradit utajované skutečnosti EU.

K vyzrazení utajovaných skutečností EU dojde, pokud se tyto skutečnosti dostanou zcela nebo zčásti do rukou neoprávněných osob, tj. osob, které neprošly příslušnou bezpečnostní prověrkou nebo nemají „potřebu vědět“, nebo je-li pravděpodobné, že k takové události došlo.

Utajované skutečnosti EU mohou být vyzrazeny následkem neopatrnosti, nedbalosti nebo nerozvážnosti anebo činností služeb, které se zaměřují na EU nebo členské státy a zajímají se o utajované skutečnosti a činnost EU, nebo činností podvratných organizací.

24.2 **Hlášení narušení bezpečnosti**

Všechny osoby, které mají nakládat s utajovanými skutečnostmi EU, jsou důkladně poučeny o svých povinnostech v této oblasti. Jsou povinny ihned ohlásit každé narušení bezpečnosti, jakmile se o něm dozvědí.

Zjistí-li bezpečnostní pracovník daného útvaru nebo úředník odpovědný za bezpečnost zasedání nebo je-li upozorněn, že byly porušeny bezpečnostní předpisy týkající se utajovaných skutečností EU nebo že se ztratily nebo zmizely utajované materiály EU, musí neprodleně jednat, aby:

a) zajistil důkazy;

b) zjistil skutkový stav;

c) zhodnotil a snížil na minimum způsobenou škodu;

d) zabránil opakování;

e) uvědomil příslušné orgány o důsledcích narušení bezpečnosti.

V této souvislosti jsou poskytovány tyto informace:

▼B

i) popis dotčených skutečností, zejména s upřesněním jejich stupně utajení, spisového čísla a čísla výtisku, data, původce, předmětu a rozsahu dokumentu;

ii) stručný popis okolností narušení bezpečnosti včetně data a období, během něhož mohly být skutečnosti vyzrazeny;

iii) prohlášení uvádějící, zda byl informován původce.

Každý bezpečnostní orgán, jakmile byl upozorněn, že mohlo dojít k narušení bezpečnosti, je povinen skutečnost okamžitě oznámit ►M2 ředitelstvím pro bezpečnost Komise ◄.

O případech, které se týkají skutečností se stupněm utajení ►M1 RESTREINT UE ◄ se podává zpráva, mají-li neobvyklou povahu.

Jakmile je člen Komise odpovědný za bezpečnostní otázky informován o narušení bezpečnosti:

a) oznámí to původci, který utajovanou skutečnost vydal;

b) vyzve příslušné bezpečnostní orgány, aby zahájily vyšetřování;

c) koordinuje vyšetřování, týká-li se věc více bezpečnostních orgánů;

d) získá zprávu o okolnostech narušení, datu nebo období, během kterého mohlo k narušení dojít, o datu a místě jeho zjištění a podrobný popis obsahu a stupně utajení dotčených dokumentů. Rovněž je třeba uvést poškození zájmů EU nebo jednoho či více členských států a opatření přijatá s cílem zabránit jakémukoli opakování.

Původce uvědomí příjemce a dá jim potřebné pokyny.

24.3 **Právní kroky**

V souladu s příslušnými pravidly a předpisy, zejména s hlavou VI služebního řádu, a aniž je dotčena možnost soudního postihu, mohou být přijata disciplinární opatření proti jakékoli osobě, která je odpovědná za vyzrazení utajovaných skutečností EU.

V odůvodněných případech, na základě zprávy zmíněné v oddíle 24.2 podnikne člen Komise odpovědný za bezpečnostní otázky všechny nezbytné kroky umožňující příslušným vnitrostátním orgánům zahájit trestní stíhání.

25. OCHRANA UTAJOVANÝCH SKUTEČNOSTÍ EU ZPRACOVÁVANÝCH V INFORMAČNÍCH A V KOMUNIKAČNÍCH SYSTÉMECH

25.1 **Úvod**

25.1.1 *Obecně*

Bezpečnostní politika a bezpečnostní požadavky se uplatňují na všechny komunikační a informační systémy a sítě (dále jen „systémy“), v nichž se zpracovávají skutečnosti se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším. Použijí se jako doplněk rozhodnutí Komise K (95) 1510 v konečném znění ze dne 23. listopadu 1995 o ochraně informačních systémů.

Systémy, které zpracovávají skutečnosti se stupněm utajení ►M1 RESTREINT UE ◄, vyžadují rovněž uplatňování bezpečnostních opatření na ochranu důvěrnosti těchto skutečností. Všechny systémy vyžadují bezpečnostní opatření umožňující chránit celistvost a dostupnost těchto systémů a skutečností, které obsahují.

Bezpečnostní politika Komise ve vztahu k informačním technologiím (IT) je postavena na následujících základech:

— tvoří nedílnou součást celkového zajištění bezpečnosti a doplňuje všechny prvky zajištění bezpečnosti informací, bezpečnosti personálu a fyzické bezpečnosti,

▼B

— rozdělení povinností mezi vlastníky technických systémů, držiteli utajovaných skutečností EU, které jsou uloženy nebo zpracovávány v technických systémech, a odborníky na bezpečnost IT a uživatele,

— popis bezpečnostních zásad a požadavků jednotlivých systémů IT,

— schválení těchto zásad a požadavků pověřeným orgánem,

— zohlednění zvláštních ohrožení a slabých míst v oblasti IT.

25.1.2 *Ohrožení a slabá místa systémů*

Ohrožení lze vymezit jako možnost náhodného nebo úmyslného narušení bezpečnosti. V případě systémů se toto narušení projevuje ztrátou jedné nebo více vlastností, kterými jsou důvěrnost, celistvost a dostupnost. Slabá místa lze vymezit jako nedostatečnou nebo chybějící kontrolu, která by usnadnila nebo umožnila ohrožení určitého objektu nebo cíle.

Utajované či neutajované skutečnosti EU zpracovávané v systémech v koncentrované podobě, která umožňuje jejich rychlé vyhledání, sdělení a použití, jsou vystaveny mnoha rizikům. Patří mezi ně přístup neoprávněných uživatelů ke skutečnostem nebo naopak odepření přístupu oprávněným uživatelům. Zároveň existují rizika neoprávněného vyzrazení, zkreslení, pozměnění nebo odstranění informací. Kromě toho složité a často choulostivé zařízení je nákladné a často je obtížné rychle jej opravit nebo nahradit.

25.1.3 *Hlavní cíl bezpečnostních opatření*

Hlavním cílem bezpečnostních opatření uvedených v tomto oddíle je zajistit ochranu před neoprávněným vyzrazením utajovaných skutečností EU (ztráta důvěrnosti) a před ztrátou celistvosti a dostupnosti skutečností. Aby bylo dosaženo náležité ochrany systému, který zpracovává utajované skutečnosti EU, upřesní ►M2 ředitelství pro bezpečnost Komise ◄ vhodné normy klasické bezpečnosti a vhodné bezpečnostní postupy a techniky vytvořené zvlášť pro každý systém.

25.1.4 *Bezpečnostní požadavky vlastní danému systému (SSRS)*

Pro všechny systémy, které zpracovávají skutečnosti se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším, musí vlastník technického systému (TSO; viz oddíl 25.3.4) a vlastník informace (viz oddíl 25.3.5), případně s přispěním a za podpory ve osob odpovědných za projekt a ►M2 ředitelství pro bezpečnost Komise ◄ (ve funkci orgánu pro bezpečnost informačních systémů – orgánu INFOSEC; viz oddíl 25.3.3), vypracovat stanovení bezpečnostních požadavků vlastních danému systému (SSRS), který schválí orgán pro schvalování z hlediska bezpečnosti (SAA; viz oddíl 25.3.2.).

Stanovení bezpečnostních požadavků vlastních danému systému se rovněž požaduje, považuje-li orgán pro schvalování z hlediska bezpečnosti dostupnost a celistvost skutečností se stupněm utajení ►M1 RESTREINT UE ◄ nebo neutajovaných skutečností za podstatnou.

Stanovení bezpečnostních požadavků vlastních danému systému bude vypracováno co nejdříve během vytváření projektu a vyvíjí se a zlepšuje postupně s vývojem projektu; plní přitom v jednotlivých fázích projektu a životního cyklu systému různé úlohy.

25.1.5 *Bezpečnostní režimy provozu*

Všechny systémy, které zpracovávají skutečnosti se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším stupněm utajení, se schvalují pro jeden z níže uvedených provozních režimů nebo, odůvodňují-li to potřeby v různých obdobích, pro několik provozních režimů nebo pro jejich vnitrostátní protějšek:

a) „dedicated“;

b) „system high“ a

c) „multi-level“.

▼B

25.2 *Definice*

„Schvalovacím řízením“ se rozumí: schválení systému, které povoluje jeho používání pro zpracování utajovaných skutečností EU v jeho operačním prostředí.

Poznámka:

Ke schvalovacímu řízení dojde po uplatnění všech vhodných bezpečnostních postupů a po dosažení dostatečné úrovně ochrany systémových zdrojů. Schvalování se obvykle uskutečňuje na základě stanovení bezpečnostních požadavků pro daný systém, zejména těchto skutečností:

a) vymezení cíle schválení systému uvádějící zejména stupně utajení skutečností, které se mají v systému zpracovávat, a režim nebo režimy bezpečnostního provozu navrhované pro systém nebo síť;

b) zhodnocení rizik poukazující na ohrožení a slabá místa a stanovení opatření nezbytných pro jejich předcházení;

c) provozní postupy pro zajištění bezpečnosti (SecOP) s podrobným popisem navrhovaných postupů (např. režimy a služby, které mají být poskytovány), a zejména s popisem bezpečnostních vlastností systému, který bude základem schvalovacího řízení;

d) plán pro zavedení a údržbu bezpečnostních vlastností;

e) plán, kterým se stanoví zkoušky, hodnocení a udělení osvědčení zaměřené na zajištění prvotní a následné bezpečnosti systému nebo sítě a

e) udělení osvědčení, je-li požadováno, spolu s ostatními prvky schvalovacího řízení.

„Úředníkem pro bezpečnost informatiky na úrovni ústředí“ (CISO) se rozumí: úředník v ústřední službě IT, který koordinuje a dohlíží na bezpečnostní opatření určená pro centrálně organizované systémy.

„Udělováním osvědčení“ se rozumí: vydávání úředního dokumentu na základě nezávislé kontroly chování a výsledků hodnocení, který uvádí míru, v jaké daný systém plní požadavky bezpečnosti nebo v jaké produkt počítačové bezpečnosti odpovídá předem stanoveným bezpečnostním požadavkům v této oblasti.

„Bezpečnostní komunikací“ (COMSEC) se rozumí: použití bezpečnostních opatření v telekomunikacích, které znemožní neoprávněným osobám získat skutečnosti, které lze získat z přístupu k telekomunikačnímu provozu a z jeho vyhodnocení, nebo které zajistí autentičnost telekomunikačního provozu.

Poznámka:

Tato opatření se vztahují nejen na bezpečnost šifrovacích prostředků, kódování, přenosu a emisí, ale i na bezpečnost týkající se postupů, fyzických prvků, personálu, dokumentů a počítačového systému.

„Počítačovou bezpečností“ (COMPUSEC) se rozumí: zavedení bezpečnostních vlastností hardwaru, firmwaru a softwaru do počítačového systému, aby byl chráněn proti neoprávněnému vyzrazení, úpravě, změnám nebo vymazání skutečností nebo aby jim bylo zabráněno nebo proti odmítnutí přístupu.

„Produktem počítačového zabezpečení“ se rozumí: obecný produkt počítačové bezpečnosti, který má být začleněn do IT systému, aby zlepšil nebo zajistil důvěrnost, celistvost nebo dostupnost zpracovávaných skutečností.

„Bezpečnostním provozním režimem dedicated“ se rozumí: provozní režim, podle kterého jsou VŠECHNY osoby, které mají přístup k systému, prověřeny pro nejvyšší stupeň utajení skutečností zpracovávaných v rámci systému a mají společnou „potřebu vědět“ týkající se VŠECH informací zpracovávaných v rámci systému.

▼B

Poznámky:

1. Protože všichni uživatelé mají společnou „potřebu vědět“, není nezbytné, aby bezpečnostní technika zajišťovala oddělení skutečností v rámci systému.

2. Ostatní bezpečnostní vlastnosti (např. fyzické, personální a procedurální) musí vyhovovat požadavkům stanoveným pro nejvyšší úroveň utajení a pro všechny kategorie skutečností zpracovávaných v systému.

„Zhodnocením“ se rozumí: podrobné technické posouzení provedené příslušným orgánem týkající se aspektů systému, šifrovacích prostředků nebo produktu počítačové bezpečnosti, které souvisejí s jeho bezpečností.

Poznámky:

1. Hodnocení zkoumá přítomnost požadované bezpečnostní funkce, absenci nežádoucích vedlejších účinků vyplývajících z této funkce a její neporušitelnost.

2. Hodnocení určuje míru, do jaké jsou uspokojeny bezpečnostní požadavky systému nebo splněny nároky produktu počítačové bezpečnosti, a stanoví úroveň zajištění systému nebo šifrovacího prostředku nebo funkce produktu počítačové bezpečnosti.

„Vlastníkem informací“ (IO) se rozumí orgán (vedoucí útvaru), který nese odpovědnost za vytvoření, zpracování a užívání skutečností, včetně odpovědnosti za rozhodnutí, komu se povolí přístup k těmto informacím.

„Bezpečností informačních systémů“ (INFOSEC) se rozumí: uplatňování bezpečnostních opatření pro ochranu zpracovávaných, archivovaných nebo předávaných skutečností v komunikačních, informačních a jiných elektronických systémech před, náhodnou nebo úmyslnou, ztrátou důvěrnosti, celistvosti nebo dostupnosti a pro zamezení ztrátě celistvosti a dostupnosti samotných systémů.

„Opatřeními pro bezpečnost informačních systémů“ (opatření INFOSEC) se rozumí: opatření určená pro zabezpečení počítačů, přenosu, vysílání a šifrování a dále opatření ke zjišťování, dokumentaci a obraně proti ohrožení informací a systémů.

„Oblastí IT“ se rozumí: oblast s jedním počítačem nebo více počítači, s jejich místními periferiemi a paměťovými jednotkami, s jejich řídícími jednotkami a vyhrazenými síťovými a komunikačními zařízeními.

Poznámka:

Součástí této oblasti není jakákoli oddělená oblast, kde se nacházejí vzdálené terminály/pracovní stanice nebo periferie, i když jsou tato zařízení připojena k oblasti IT.

„Sítí IT“ se rozumí: zeměpisně rozptýlený soubor tvořený propojenými IT systémy pro výměnu dat, obsahující různé složky propojených systémů IT a jejich rozhraní s datovými a komunikačními sítěmi, které je doplňují.

Poznámky:

1. Síť IT může využívat služeb jedné nebo více komunikačních sítí pro výměnu dat; více IT sítí může využívat služeb společné komunikační sítě.

2. Spojuje-li síť IT více počítačů nacházejících se na stejném místě, označuje se jako „místní síť“.

„Bezpečnostní vlastnosti sítě IT“ zahrnují bezpečnostní vlastnosti každého systému IT, který je součástí sítě, ale rovněž doplňující součásti a vlastnosti spojené v síti jako takové nezbytné pro zajištění dostatečné úrovně ochrany utajovaných skutečností (např. komunikace

▼B

v síti, mechanismy a postupy bezpečnostního označování a identifikace, kontroly přístupu, programy a kontrolní cesty).

„Systémem IT“ se rozumí: soubor zařízení, metod a postupů a případně osob, který je uspořádán tak, aby plnil funkce při zpracování informací.

Poznámky:

1. Jedná se o soubor uspořádaných prostředků pro zpracování skutečností v rámci systému.

2. Tyto systémy mohou být používány pro konzultace, řízení, dohled a komunikaci a pro vědecké nebo administrativní uplatnění včetně zpracování textů.

3. Systém je obecně vymezen jako soubor prvků podléhajících kontrole jednoho vlastníka technického systému.

4. Systém IT může obsahovat subsystémy, z nichž některé jsou rovněž systémy IT.

„Bezpečnostní vlastnosti systému IT“ zahrnují všechny funkce, charakteristiky a vlastnosti hardwaru/firmwaru/softwaru; provozní postupy a postupy vytváření odpovědnosti a kontroly přístupu, oblast IT, oblast vzdálených terminálů/pracovních stanic a pravidla řízení, fyzická zařízení a strukturu a opatření pro kontrolu personálu a komunikací nezbytných pro zajištění přijatelné úrovně ochrany utajovaných skutečností, které mají být zpracovávány v systému IT.

„Úředníkem pro bezpečnost informatiky na místní úrovni“ (LISO) se rozumí: úředník útvaru Komise, který odpovídá za koordinaci a sledování bezpečnostních opatření v rámci jeho působnosti.

„Bezpečnostním provozním režimem multi-level“ se rozumí: provozní režim, ve kterém NEMAJÍ VŠECHNY osoby, jež mají přístup k systému, prověření pro nejvyšší stupeň utajení skutečností zpracovávaných v rámci systému a VŠECHNY osoby s přístupem k systému NEMAJÍ společnou „potřebu vědět“ týkající se skutečností zpracovávaných v rámci systému.

Poznámky:

1. Tento provozní režim zároveň dovoluje zpracovávání skutečností s různým stupněm utajení a různých kategorií.

2. Vzhledem k tomu, že všichni uživatelé nejsou prověřeni pro nejvyšší stupeň utajení a nemají společnou „potřebu vědět“, musí bezpečnostní technika zajistit výběrový přístup ke skutečnostem v rámci systému a oddělení těchto skutečností.

„Oblastí vzdálených terminálů/pracovních stanic“ se rozumí: oblast oddělená od oblasti IT obsahující počítačové vybavení, jeho místní periferie nebo terminály/pracovní stanice a jakékoli s nimi spojené komunikační zařízení.

„Bezpečnostními provozními postupy“ se rozumí: postupy, sestavené vlastníkem technického systému a vymezující zásady, které se mají zavést v bezpečnostních věcech, provozních postupy, které mají být dodržovány, a povinnosti pracovníků.

„Bezpečnostním provozním režimem system-high“ se rozumí: provozní režim, podle kterého jsou VŠECHNY osoby, jež mají přístup k systému, prověřeny pro nejvyšší stupeň utajení skutečností zpracovávaných v rámci systému, avšak VŠECHNY NEMAJÍ společnou „potřebu vědět“ týkající se skutečností zpracovávaných v rámci systému.

Poznámky:

1. Vzhledem k tomu, že dotčené osoby nemají společnou „potřebu vědět“, musí bezpečnostní technika zajistit výběrový přístup ke skutečnostem v rámci systému a oddělení těchto skutečností.

▼B

2. Ostatní bezpečnostní vlastnosti (např. fyzické, personální a procedurální) musí vyhovovat požadavkům stanoveným pro nejvyšší úroveň utajení a pro všechny kategorie skutečností zpracovávaných v systému.

3. Všechny skutečnosti zpracovávané v systému nebo použitelné pro systém v tomto provozním režimu spolu s vytvořeným výstupem musí být chráněny, dokud není prokázán opak, jako by spadaly do kategorie a měly nejvyšší stupeň utajení, ledaže existuje přijatelná úroveň důvěry k některé ze stávajících funkcí označování.

„Bezpečnostními požadavky vlastními danému systému“ (SSRS) se rozumí: úplný a výslovný přehled bezpečnostních zásad, které se musí dodržovat, a podrobných bezpečnostních požadavků, které se musí splnit. Vychází z bezpečnostní politiky Komise a z hodnocení rizika, popřípadě jsou sestaveny na základě parametrů jako jsou provozní prostředí, nejnižší úroveň bezpečnostních prověrek pracovníků, nejvyšší stupeň utajení zpracovávaných informací, bezpečnostní provozní režim nebo požadavky uživatelů. Bezpečnostní požadavky vlastní danému systému tvoří nedílnou součást projektové dokumentace předložené příslušným orgánům ke schválení z technického, rozpočtového a bezpečnostního hlediska. Ve své konečné podobě představuje úplný přehled o tom, co představuje zabezpečení systému.

„Vlastníkem technického systému“ (TSO) se rozumí: orgán odpovědný za vytvoření, údržbu, provoz a ukončení provozu systému.

Bezpečnostními opatřeními „TEMPEST“ (norma pro přechodné elektromagnetické pulzující záření) se rozumí: bezpečnostní opatření určená pro ochranu zařízení a komunikační infrastruktury před vyzrazením utajovaných skutečností neúmyslným elektromagnetickým vyzařováním a vodivostí.

25.3 **Odpovědnost v oblasti bezpečnosti**

25.3.1 *Obecně*

Poradenské úkoly poradní skupiny pro bezpečnostní politiku Komise, vymezené v oddíle 12, zahrnují i otázky INFOSEC. Skupina organizuje svou činnost tak, aby mohla poskytovat odborné rady k výše uvedeným otázkám.

►M2 Ředitelství pro bezpečnost Komise ◄ odpovídá za vydávání prováděcích předpisů INFOSEC, které vycházejí z ustanovení této kapitoly.

V případě obtíží spojených s bezpečností (incidenty, narušení atd.) přijme ►M2 ředitelství pro bezpečnost Komise ◄ neprodleně opatření.

V rámci ►M2 ředitelství pro bezpečnost Komise ◄ je zřízeno oddělení bezpečnosti informačních systémů (oddělení INFOSEC).

25.3.2 *Orgán pro schvalování z hlediska bezpečnosti (SAA)*

►M2 Ředitel ředitelství pro bezpečnost Komise ◄ je pro Komisi orgánem pro schvalování z hlediska bezpečnosti (SAA). Tento orgán odpovídá za celkovou oblast bezpečnosti a za specializované oblasti bezpečnosti informačních systémů, bezpečnosti komunikací, zabezpečení šifrování a zabezpečení na úseku normy TEMPEST.

Orgán pro schvalování z hlediska bezpečnosti odpovídá za soulad systémů s bezpečnostní politikou Komise. Jedním z jeho úkolů je schvalování systému, který má ve svém operačním prostředí zpracovávat utajované skutečnosti EU s určitým stupněm utajení.

Do pravomoci orgánu pro schvalování z hlediska bezpečnosti Komise spadají všechny systémy provozované v prostorách Komise. Spadají-li jednotlivé složky systému do pravomoci orgánu pro schvalování z hlediska bezpečnosti Komise a ostatních orgánů pro schvalování z hlediska bezpečnosti, určí všechny dotčené strany společný výbor

▼B

pro schvalování, jeho koordinaci bude zajišťovat orgán pro schvalování z hlediska bezpečnosti.

25.3.3 *Orgán pro bezpečnost informačních systémů*

►M2 Ředitel ředitelství pro bezpečnost Komise ◄ je pro Komisi orgánem pro bezpečnost informačních systémů (INFOSEC). Orgán INFOSEC odpovídá za:

— poskytování technického poradenství a technické pomoci orgánu pro schvalování z hlediska bezpečnosti,

— pomoc při vypracování stanovení bezpečnostních požadavků pro daný systém,

— kontrolu stanovení bezpečnostních požadavků pro daný systém, aby byla zajištěna jeho slučitelnosti s těmito bezpečnostními předpisy a s politikou INFOSEC a dokumenty týkajícími se jeho architektury,

— účast v komisích nebo výborech pro schvalování podle potřeby a vydávání doporučení INFOSEC pro orgán pro schvalování z hlediska bezpečnosti týkající se schvalování,

— poskytování podpory školicím a vzdělávacím činnostem INFOSEC,

— poskytování technického poradenství při vyšetřování incidentů souvisejících s INFOSEC,

— vypracování obecných zásad s cílem zajistit, že se bude používat pouze povolený software.

25.3.4 *Vlastník technického systému (TSO)*

Odpovědnost za zavedení kontrol a fungování speciálních bezpečnostních vlastností systému nese vlastník tohoto systému, vlastník technického systému (TSO). Pro centrálně vlastněné systémy je třeba jmenovat úředníka pro bezpečnost informatiky na úrovni ústředí (CISO). Každý útvar podle potřeby jmenuje úředníka pro bezpečnost informatiky na místní úrovni (LISO). K povinnostem vlastníka technického systému patří sestavení provozních postupů pro zajištění bezpečnosti (SecOP) a jeho odpovědnost trvá po celou dobu životnosti systému od stádia návrhu projektu až po jeho ukončení.

Vlastník technického systému určuje bezpečnostní normy a provozní předpisy, které dodavatel systému musí dodržet.

Vlastník technického systému může ve vhodných případech delegovat část svých povinností na úředníka pro bezpečnost informatiky na místní úrovni (LISO). Jedna osoba může vykonávat různé funkce související se bezpečností informačních systémů (INFOSEC).

25.3.5 *Vlastník informací (IO)*

Vlastník informací (IO) odpovídá za utajované skutečnosti EU (a další skutečnosti), které se mají zavádět do technických systémů a zde se zpracovávat nebo vytvářet. Určuje požadavky týkající se přístupu k těmto skutečnostem v systémech. Může delegovat svou odpovědnost na správce skutečností nebo správce databáze v rámci své působnosti.

25.3.6 *Uživatelé*

Všichni uživatelé odpovídají za to, že jejich činnosti nepoškodí bezpečnost systému, který používají.

25.3.7 *Školení INFOSEC*

Vzdělávání a školení v oblasti bezpečnosti informačních systémů je k dispozici všem pracovníkům, kteří jej potřebují.

25.4 **Netechnická bezpečnostní opatření**

25.4.1 *Bezpečnostní opatření týkající se personálu*

Uživatelé systému musí projít bezpečnostní prověrkou odpovídající stupni utajení a obsahu zpracovávaných skutečností v jejich systému

▼B

a musí mít „potřebu vědět“. Přístup k některým zařízením nebo informacím specifickým pro bezpečnost systémů vyžaduje zvláštní povolení udělené podle postupů Komise.

Orgán pro schvalování z hlediska bezpečnosti určí všechny citlivé funkce a vymezí stupeň bezpečnostní prověrky a nezbytného dohledu nad pracovníky, kteří tyto funkce vykonávají.

Systémy jsou specifikovány a navrženy tak, aby usnadňovaly rozdělení úkolů a odpovědnosti mezi pracovníky, aby jedna osoba neznala ani zcela nekontrolovala všechny klíčové body systému.

Oblasti IT a oblasti vzdálených terminálů/pracovních stanic, ve kterých lze měnit bezpečnost systému, nesmějí být obsazeny pouze jedním pověřeným úředníkem nebo ostatním zaměstnancem.

Bezpečnostní nastavení systému mohou měnit pouze společně alespoň dva pověření pracovníci.

25.4.2 *Fyzická bezpečnost*

Oblasti IT a oblasti vzdálených terminálů/pracovních stanic (jak jsou vymezeny v oddíle 25.2), ve kterých jsou skutečnosti se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším zpracovávány prostředky IT nebo ve kterých je možný přístup k těmto skutečnostem, jsou označeny podle skutečnosti jako bezpečnostní oblasti EU kategorie I nebo kategorie II.

25.4.3 *Kontrola přístupu k systému*

Všechny informace a materiály, které umožňují kontrolu přístupu k systému, jsou chráněny podle ustanovení pro nejvyšší stupeň utajení a pro kategorii skutečností, ke kterým tento systém může poskytovat přístup.

Informace a materiály umožňující kontrolu přístupu, které již nejsou k tomuto účelu používány, se zničí v souladu s ustanoveními oddílu 25.5.4.

25.5 **Technická bezpečnostní opatření**

25.5.1 *Bezpečnost skutečností*

Původce informace má za úkol zjistit všechny dokumenty obsahující skutečnosti a přiřadit jim stupeň utajení, ať se jedná o výstupy v podobě papírové kopie nebo o nosiče dat. Na každé stránce papírové kopie je nahoře a dole vyznačen příslušný stupeň utajení. Výstupy, ať už v podobě papírové kopie nebo nosiče dat, mají stejný stupeň utajení jako je nejvyšší stupeň utajení skutečností použitých při jeho vytváření. Způsob, jakým je systém provozován, může mít rovněž vliv na stupeň utajení výstupů tohoto systému.

Útvary Komise a ti, kteří jsou v něm držiteli skutečností, musí posoudit otázky související se souborem jednotlivých prvků skutečností a závěrů, které mohou vyplynout z navzájem svázaných prvků, aby určili, zda pro takto svázané prvky nevyžadují vyšší stupeň utajení.

Skutečnost, že informace může mít zkrácenou kódovanou podobu, podobu přenosového kódu nebo jakoukoli binární podobu, jim nezajišťuje žádnou bezpečnostní ochranu a neměla by proto ovlivnit jejich stupeň utajení.

Při přenosu skutečností z jednoho systému do druhého musí být během přenosu a v přijímajícím systému chráněny způsobem odpovídajícím původnímu stupni utajení a kategorii skutečností.

Všechny nosiče dat musí být zpracovány v souladu s nejvyšším stupněm utajení uchovávaných skutečností nebo označení nosiče dat a po celou dobu musí být přiměřeně chráněny.

Znovu použitelné nosiče dat použité pro záznam utajovaných skutečností EU mají zachován nejvyšší stupeň utajení přidělovaný datům, pro které byly použity, dokud není stupeň utajení těchto skutečností řádně

▼B

snížen nebo dokud nejsou odtajněny a nosič s takto změněným stupněm utajení není odtajněn nebo zničen podle postupu, který schválil orgán pro schvalování z hlediska bezpečnosti (viz 25.5.4).

25.5.2 *Kontrola a odpovědnost za skutečnosti*

Přístup ke skutečnostem se stupněm utajení ►M1 SECRET UE ◄ a vyšším stupněm se zaznamenává automaticky („audit trails“) nebo ručně do rejstříku. Rejstříky se uchovávají v souladu s těmito bezpečnostními předpisy.

Utajované výstupy uvnitř oblasti IT lze považovat za jeden soubor utajovaných skutečností a nemusí se evidovat, pokud jsou odpovídajícím způsobem identifikovány, označeny příslušným stupněm utajení a kontrolovány.

Jsou-li data vycházející ze systému, který zpracovává utajované skutečnosti EU, přenášena z oblasti IT do vzdáleného terminálu/pracovní stanice, stanoví se postupy schválené orgánem pro schvalování z hlediska bezpečnosti pro kontrolu a protokolování takto rozptýlených dat. Pro skutečnosti se stupněm utajení ►M1 SECRET UE ◄ a vyšším tyto postupy zahrnují zvláštní pokyny pro odpovědnost za skutečnosti.

25.5.3 *Nakládání s odnímatelnými nosiči dat a jejich kontrola*

Se všemi odnímatelnými nosiči dat se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším se zachází jako s utajovaným materiálem a vztahují se na ně související obecná pravidla. Příslušná identifikace a vyznačení stupně utajení se přizpůsobí jejich fyzickému vzhledu, aby byla jasně rozpoznatelná.

Uživatelé se musí ujistit, že utajované skutečnosti EU jsou zaznamenány na nosičích dat s vyznačením odpovídajícího stupně utajení a že jim je poskytována náležitá ochrana. Je třeba stanovit postupy, kterými se zajistí, že ukládání skutečností na nosiče dat bude probíhat pro všechny úrovně skutečností EU v souladu s těmito bezpečnostními předpisy.

25.5.4 *Odtajnění a zničení nosičů dat*

Stupeň utajení nosičů dat používaných pro záznam utajovaných skutečností EU může být snížen nebo nosiče mohou být odtajněny v souladu s postupem, který schválil orgán pro schvalování z hlediska bezpečnosti.

Nosiče dat, na nichž byly uloženy skutečnosti se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ nebo skutečnosti zvláštní kategorie, nelze odtajnit ani použít znovu.

Nosiče dat, která nelze odtajnit ani použít znovu, se zničí v souladu s výše uvedeným postupem.

25.5.5 *Bezpečnost komunikací*

►M2 Ředitel ředitelství pro bezpečnost Komise ◄ působí jako orgán pro šifrování.

Jsou-li utajované skutečnosti EU přenášeny elektromagnetickou cestou, je třeba přijmout zvláštní opatření na ochranu důvěrnosti, celistvosti a dostupnosti přenášených skutečností. Orgán pro schvalování z hlediska bezpečnosti stanoví požadavky, které mají být splněny pro ochranu přenosů před případným odhalením a odposlouchávaním. Skutečnosti přenášené prostřednictvím komunikačního systému jsou chráněny na základě požadavků nezbytných pro zajištění jejich důvěrnosti, celistvosti a dostupnosti.

Je-li nezbytné pro ochranu důvěrnosti, celistvosti a dostupnosti skutečností využít šifrovací metody, musí být tyto metody nebo s nimi související produkty zvlášť schválené pro tento účel orgánem pro schvalování z hlediska bezpečnosti z pozice orgánu pro šifrování.

Během přenosu je důvěrnost skutečností se stupněm utajení ►M1 SECRET UE ◄ a vyšším chráněna šifrovacími metodami nebo

▼B

produkty schválenými členem Komise odpovědným za bezpečnostní otázky po konzultaci s poradní skupinou pro bezpečnostní politiku Komise. Během přenosů je důvěrnost skutečností se stupněm utajení ►M1 CONFIDENTIEL UE ◄ nebo ►M1 RESTREINT UE ◄ chráněna šifrovacími metodami nebo produkty schválenými orgánem Komise pověřeným šifrováním po konzultaci s poradní skupinou pro bezpečnostní politiku Komise.

Podrobná pravidla uplatňovaná pro přenosy utajovaných skutečností EU musí být uvedena ve zvláštních bezpečnostních pokynech schválených ►M2 ředitelstvím pro bezpečnost Komise ◄ po konzultaci s poradní skupinou pro bezpečnostní politiku Komise.

Za výjimečných okolností lze skutečnosti se stupněm utajení ►M1 RESTREINT UE ◄, ►M1 CONFIDENTIEL UE ◄ a ►M1 SECRET UE ◄ přenášet jako jasný text za podmínky, že každý z těchto přenosů bude zvlášť výslovně schválen a řádně evidován vlastníkem informací. Jedná se o tyto výjimečné podmínky:

(a) případy hrozící nebo skutečné krize, konfliktu nebo války a

(b) v případě výjimečné naléhavosti a nejsou-li k dispozici šifrovací prostředky, má-li se za to, že přenášené skutečnosti nelze včas využít tak, aby ovlivnily probíhající operace.

Systém musí mít schopnost kategoricky zamítnout přístup k utajovaným skutečnostem EU na jednom nebo na všech vzdálených pracovištích nebo terminálech, a to fyzickým odpojením nebo zvláštními funkcemi softwaru schválenými orgánem pro schvalování z hlediska bezpečnosti.

25.5.6 *Bezpečnost instalací a vyzařování*

Pravidla pro první instalaci systému a jakoukoli významnou následnou změnu stanoví, že práce musí provádět technici s nezbytnou bezpečnostní prověrkou za stálého dohledu technicky kvalifikovaného personálu, který má prověrku potřebnou pro přístup k utajovaným skutečnostem EU stupně odpovídajícího nejvyššímu stupni utajení skutečností, které má systém ukládat a zpracovávat.

Systémy zpracovávající skutečnosti se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším jsou chráněny tak, aby jejich bezpečnost nemohla být ohrožena vyzrazujícím vyzařováním, jehož studium a prevence se označují jako „TEMPEST“.

Protiopatření jsou posuzovány a schvalovány schvalovacím orgánem TEMPEST (viz 25.3.2).

25.6 **Bezpečnost během zpracování**

25.6.1 *Provozní postupy pro zajištění bezpečnosti (SecOP)*

Provozní postupy pro zajištění bezpečnosti (SecOP) vymezují zásady k přijetí v oblasti bezpečnosti, provozní postupy, které se mají používat, a odpovědnost personálu. Za vypracování provozních postupů pro zajištění bezpečnosti odpovídá vlastník technického systému (TSO).

25.6.2 *Ochrana softwaru a správa konfigurace*

Úroveň ochrany aplikačních programů se stanoví na základě zhodnocení bezpečnostního stupně vlastního programu spíše než na základě stupně utajení skutečností, které má zpracovávat. Používané verze softwaru musí být pravidelně ověřovány, aby byla zajištěna jejich celistvost a řádné fungování.

Nové nebo pozměněné verze softwaru budou používány pro zpracování utajovaných skutečností EU, až po ověření vlastníkem technických systémů.

25.6.3 Zjišťování přítomnosti softwaru působícího škodu a počítačových virů

Zjišťování přítomnosti softwaru působícího škodu a počítačových virů se provádějí pravidelně v souladu s požadavky orgánu pro schvalování z hlediska bezpečnosti.

▼B

Všechny nosiče dat vstupující do Komise musí být před zavedením do jakéhokoli systému ověřeny, zda neobsahují software působící škodu nebo počítačové viry.

25.6.4 *Údržba*

Smlouvy a postupy pro pravidelnou a mimořádnou údržbu systémů, pro které bylo vypracováno stanovení bezpečnostních požadavků pro daný systém, upřesní požadavky a opatření použitelné pro personál, který údržbu uskutečňuje, a pro jejich zařízení, pokud musí vstoupit do oblasti IT.

Požadavky a postupy musí být jasně uvedeny ve stanovení bezpečnostních požadavků pro daný systém a v provozních postupech pro zajištění bezpečnosti. Údržba prováděná dodavatelem, která vyžaduje použití diagnostických postupů na dálku, je možná pouze za mimořádných okolností a pod přísnou kontrolou a se souhlasem orgánu pro schvalování z hlediska bezpečnosti.

25.7 **Nabývání**

25.7.1 *Obecně*

Bezpečnostní produkty, které mají být použity v nabývaném systému, musí být buď zhodnoceny a osvědčeny podle mezinárodně uznávaných kriterií (např. Společná kritéria pro hodnocení bezpečnosti informačních technologií, viz norma ISO 15408), nebo musí probíhat řízení o jejich hodnocení nebo osvědčení příslušným orgánem pro hodnocení nebo osvědčování jednoho z členských států EU Pro získání souhlasu Poradní komise pro nákupy a veřejné zakázky (ACPC) se vyžadují zvláštní postupy.

Při rozhodování, zda má být zařízení, zejména nosiče dat pro ukládání, spíše pronajato než zakoupeno, je třeba přihlédnout ke skutečnosti, že toto zařízení, je-li jednou použito ke zpracování utajovaných skutečností EU, nesmí již opustit prostory, které mu zajišťují požadovanou ochranu, aniž by nejprve bylo se schválením orgánu pro schvalování z hlediska bezpečnosti odtajněno, a že toto schválení nemusí být vždy možné.

25.7.2 *Schvalování*

Všechny systémy, ke kterým bylo vypracováno stanovení bezpečnostních požadavků pro daný systém, ještě než začnou zpracovávat utajované skutečnosti EU, musí být schváleny orgánem pro schvalování z hlediska bezpečnosti na základě informací ve stanovení bezpečnostních požadavků pro daný systém, v provozních postupech pro zajištění bezpečnosti a v jakékoli jiné dokumentaci. Podsystémy a vzdálené terminály/pracovní stanice musí být schváleny jako součást systémů, ke kterým jsou připojeny. Pokud určitý systém zajišťuje spojení Komise i jiných organizací, dohodne se Komise a dotčené bezpečnostní orgány na otázce schválení.

Schvalovací řízení může probíhat v souladu se schvalovací strategií přijatou pro určitý systém a vymezenou orgánem pro schvalování z hlediska bezpečnosti.

25.7.3 *Hodnocení a udělení osvědčení*

Před schvalovacím řízením je v určitých případech třeba hodnotit bezpečnostní vlastnosti hardwaru, firmwaru a softwaru a udělit pro ně osvědčení o schopnosti systému chránit skutečnosti na zamýšleném stupni utajení.

Požadavky na hodnocení a vystavení osvědčení jsou zahrnuty do plánování systému a jsou jasně uvedeny ve stanovení bezpečnostních požadavků vlastních danému systému.

Hodnocení a udělování osvědčení provádí v souladu se schválenými směrnicemi personál s nezbytnou technickou kvalifikací, který prošel příslušnými bezpečnostními prověrkami a jedná na účet vlastníka technických systémů.

▼B

Personál může poskytnout pověřený orgán pro hodnocení nebo osvědčování některého členského státu nebo jeho pověření zástupci, například příslušný a prověřený smluvní partner.

Hodnocení a udělování osvědčení lze zjednodušit (například mohou se týkat pouze integrace), jsou-li systémy založeny na produktech počítačové bezpečnosti hodnocených a osvědčených na vnitrostátní úrovni.

25.7.4 *Systematické kontroly bezpečnostních vlastností při prodlužování schválení*

Vlastník technického systému stanoví systematickou kontrolu, která zaručí, že všechny bezpečnostní vlastnosti systému jsou stále platné.

Stanovení bezpečnostních požadavků vlastních danému systému musí jasně zjistit a vyhlásit druhy změn, které by byly důvodem k novému schvalovacímu řízení nebo které vyžadují předběžný souhlas orgánu pro schvalování z hlediska bezpečnosti. Pro zajištění řádného fungování vlastností bezpečnosti provádí vlastník technického systému ověřování po každé změně, opravě nebo poruše, která by mohla ovlivnit bezpečnostní vlastnosti systému. Prodloužení schválení pro systém obvykle závisí na uspokojivém výsledku těchto kontrol.

Orgán pro schvalování z hlediska bezpečnosti provádí pravidelně inspekce a přezkoušení všech systémů, které mají bezpečnostní vlastnosti. U systémů, které zpracovávají skutečnosti se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄, se inspekce provádějí alespoň jednou ročně.

25.8 **Dočasné nebo příležitostné použití**

25.8.1 *Bezpečnost mikropočítačů a osobních počítačů*

Mikropočítače a osobní počítače (PC) s pevnými disky (nebo jinými stálými nosiči dat) používané samostatně nebo v síti a přenosné přístroje (např. osobní počítače a elektronické notebooky) s pevnými disky se považují za elektronické nosiče dat stejně jako diskety nebo jiné vyměnitelné nosiče dat.

Pro přístup, zpracování, ukládání a přepravu je těmto zařízením poskytována stejná úroveň ochrany jako skutečnostem s nejvyšším stupněm utajení, které jsou na nich uchovávány nebo zpracovávány (dokud jim není snížen stupeň utajení nebo nejsou odtajněny v souladu se schválenými postupy).

25.8.2 *Používání soukromého počítačového vybavení IT k oficiální práci Komise*

Používání soukromých vyměnitelných nosičů dat, softwaru a hardwaru IT (například osobních počítačů a přenosných elektronických zařízení) s pamětí pro zpracování utajovaných skutečností EU je zakázáno.

Soukromý hardware, software a nosiče dat se nesmějí vnášet do bezpečnostních oblastí kategorie I nebo kategorie II, kde se zpracovávají utajované skutečnosti EU, bez písemného povolení ►M2 ředitele ředitelství pro bezpečnost Komise ◄. Toto povolení se uděluje pouze z technických důvodů ve výjimečných případech.

25.8.3 *Používání počítačového vybavení IT smluvního partnera nebo vybavení dodaného vnitrostátním dodavatelem k oficiální práci Komise*

Používání počítačového vybavení a softwaru smluvního partnera pro oficiální práci Komise může povolit ►M2 ředitel ředitelství pro bezpečnost Komise ◄. Používání počítačového vybavení IT a softwaru poskytnutého vnitrostátním dodavatelem může být rovněž povoleno; v tom případě podléhá IT vybavení inventuře Komise. Má-li být IT vybavení použito ke zpracovávání utajovaných skutečností EU, je nutné v každém případě konzultovat příslušný orgán pro schvalování z hlediska bezpečnosti, aby byly řádně zhodnocena a provedena hlediska INFOSEC, která se vztahují na používání tohoto vybavení.

▼B

26. PŘEDÁVÁNÍ UTAJOVANÝCH SKUTEČNOSTÍ EU TŘETÍM STÁTŮM NEBO MEZINÁRODNÍM ORGANIZACÍM

26.1.1 *Zásady, kterými se řídí předávání utajovaných skutečností EU*

Sbor členů Komise může rozhodnout o tom, že poskytne utajované skutečnosti EU třetím státům nebo mezinárodním organizacím na základě:

— povahy a obsahu těchto skutečností,

— „potřeby vědět“ příjemce,

— výhodnosti pro EU.

Vyžaduje se předběžný souhlas původce utajovaných skutečností EU, které mají být předány.

Tato rozhodnutí jsou přijímána případ od případu v závislosti na:

— požadovaném stupni spolupráce se třetími státy nebo mezinárodními organizacemi,

— důvěře, kterou je jim možno věnovat a která vyplývá z úrovně bezpečnosti, jakou mají utajované skutečnosti EU svěřené těmto státům a organizacím, a v závislosti na slučitelnosti bezpečnostních předpisů platných v daném státě nebo organizaci s bezpečnostními předpisy uplatňovanými v EU. Poradní skupina pro bezpečnostní politiku Komise předá Komisi technické stanovisko k tomuto bodu.

Přijetí utajovaných skutečností EU třetími státy nebo mezinárodními organizacemi s sebou nese ujištění, že tyto skutečnosti nebudou použity k jiným účelům, než pro které byly předány nebo vyměněny, a že jim tyto státy a organizace poskytnou ochranu požadovanou Komisí.

26.1.2 *Úrovně*

Jakmile Komise rozhodne, že lze skutečnosti danému státu nebo mezinárodní organizaci předat nebo s nimi vyměnit, stanoví možnou úroveň spolupráce. Ta bude záviset zejména na bezpečnostní politice a právní úpravě uplatňované daným státem nebo organizací.

Rozlišují se tři úrovně spolupráce:

Úroveň 1

Spolupráce se třetími státy nebo s mezinárodními organizacemi, jejichž bezpečnostní politika a předpisy jsou velmi podobné bezpečnostní politice a předpisům EU.

Úroveň 2

Spolupráce se třetími státy nebo s mezinárodními organizacemi, jejichž bezpečnostní politika a předpisy se od bezpečnostní politiky a předpisů EU výrazně liší.

Úroveň 3

Příležitostná spolupráce se třetími státy nebo s mezinárodními organizacemi, jejichž bezpečnostní politiku a předpisy nelze zhodnotit.

Každá úroveň spolupráce určuje postupy a bezpečnostní ustanovení, které jsou podrobně rozvedeny v dodatcích 3, 4 a 5.

26.1.3 *Dohody*

Rozhodne-li Komise, že existuje stálá nebo dlouhodobá potřeba výměny utajovaných skutečností mezi EU a třetími státy nebo mezinárodními organizacemi, vypracuje s nimi „dohody o bezpečnostních postupech pro výměnu utajovaných skutečností“, které vymezí předmět spolupráce a navzájem uplatňovaná pravidla pro ochranu vyměňovaných skutečností.

V případě příležitostné spolupráce na úrovni 3, která je již ze své definice časově a účelově omezena, lze „dohodu o bezpečnostních

▼B

postupech pro výměnu utajovaných skutečností“ nahradit pouhým memorandem o porozumění, které vymezí povahu utajovaných skutečností, které se mají vyměnit, a vzájemné povinnosti s nimi související, není-li stupeň utajení těchto skutečností vyšší než ►M1 RESTREINT UE ◄.

Návrhy dohod o bezpečnostních postupech nebo memorand o porozumění projedná Poradní skupina pro bezpečnostní politiku Komise a poté je předloží Komisi k rozhodnutí.

Člen Komise odpovědný za bezpečnostní otázky si vyžádá veškerou nezbytnou pomoc od vnitrostátního bezpečnostního orgánu členského státu, aby bylo zajištěno, že jsou předávané skutečnosti použity a chráněny v souladu s dohodami o bezpečnostních postupech nebo o memorandech o porozumění.

▼M3

27. SPOLEČNÉ MINIMÁLNÍ NORMY PRŮMYSLOVÉ BEZPEČNOSTI

27.1 **Úvod**

Tento oddíl se týká bezpečnostních aspektů průmyslových činností, které souvisejí se sjednáváním a udělováním smluv a grantových dohod, jimiž se úkoly týkající se, představující a/nebo obsahující utajované skutečnosti EU a jejich výkon přenáší na průmyslové a jiné subjekty, a to včetně předávání utajovaných skutečností EU a přístupu k nim během zadávání veřejných zakázek a výzev pro předkládání nabídek (v průběhu lhůty pro předkládání nabídek a jednání před uzavřením smlouvy).

27.2 **Definice**

Pro účely těchto společných minimálních norem se použijí tyto definice:

a) „utajovaná smlouva“: jakákoli smlouva nebo grantová dohoda o dodávce zboží, provedení stavebních prací, poskytnutí volných budov nebo poskytování služeb, jejíž výkon vyžaduje nebo znamená přístup k utajovaným skutečnostem EU nebo jejich vytvoření;

b) „utajovaná subdodavatelská smlouva“: smlouva, kterou uzavírá dodavatel nebo příjemce grantu s jiným dodavatelem (tj. subdodavatelem) ohledně dodávky zboží, provedení stavebních prací, poskytnutí budov nebo poskytování služeb, jejíž výkon vyžaduje nebo znamená přístup k utajovaným skutečnostem EU nebo jejich vytvoření;

c) „dodavatel“: hospodářský subjekt nebo právnická osoba, která má právní způsobilost uzavírat smlouvy nebo být příjemcem grantu;

d) „stanovený bezpečnostní úřad (DSA)“: úřad odpovědný Národnímu bezpečnostnímu úřadu (NBÚ) příslušného členského státu, který odpovídá za sdělování národní politiky v otázkách průmyslových tajemství průmyslovým nebo jiným subjektům a za vedení a pomoc při jejím provádění. Funkce DSA mohou být vykonávány NBÚ;

e) „bezpečnostní prověrka zařízení (FSC)“: správní rozhodnutí NBÚ/DSA, že zařízení může z bezpečnostního hlediska zajistit dostatečnou bezpečnostní ochranu utajovaných skutečností EU určitého stupně utajení a že jeho zaměstnanci, kteří musí mít přístup k utajovaným skutečnostem EU, mají vhodnou bezpečnostní prověrku a jsou poučeni o nutných bezpečnostních požadavcích pro přístup k utajovaným skutečnostem a jejich ochraně;

f) „průmyslový a jiný subjekt“: dodavatel nebo subdodavatel podnikající v oblasti dodávek zboží, provádění stavebních prací nebo poskytování služeb; může se jednat o průmyslové, obchodní, vědecké, výzkumné, vzdělávací nebo rozvojové subjekty nebo subjekty poskytující služby;

g) „průmyslové tajemství“: uplatňování ochranných opatření a postupů k předcházení ztrátám nebo vyzrazení utajovaných skutečností EU,

▼M3

které má k dispozici dodavatel nebo subdodavatel v rámci jednání před uzavřením smlouvy i při uzavírání utajované smlouvy, a k zjištění nebo nápravě takových ztrát nebo vyzrazení;

h) „Národní bezpečnostní úřad (NBÚ)“: orgán výkonné moci členského státu EU, který má v rámci tohoto členského státu úplnou odpovědnost v oblasti ochrany utajovaných skutečností EU;

i) „celková úroveň bezpečnostní klasifikace smlouvy“: rozhodnutí o stupni utajení úplné smlouvy nebo grantové dohody vycházející z utajení informace a/nebo materiálu, který má nebo může být vytvořen, předán nebo zpřístupněn na základě jakéhokoli prvku úplné smlouvy nebo grantové dohody. Celkový stupeň utajení smlouvy nesmí být nižší než nejvyšší stupeň utajení některého z jejích prvků; může však být vyšší díky spojení těchto prvků;

j) „bezpečnostní dopis (SAL)“: zvláštní smluvní podmínky vydané zadavatelem, které tvoří nedílnou součást utajované smlouvy, s níž souvisí přístup k utajovaným skutečnostem EU nebo jejich vytvoření, a které identifikují bezpečnostní požadavky nebo prvky utajované smlouvy, které vyžadují bezpečnostní ochranu;

k) „pokyny k utajení“: dokument, který popisuje utajované prvky programu, smlouvy nebo grantové dohody a určuje použitelné stupně utajení. SCG mohou být v průběhu realizace programu, smlouvy nebo grantové dohody rozšířeny a stupně utajení informací mohou být změněny nebo sníženy. SCG musí být součástí SAL.

27.3 **Organizace**

a) Komise může utajovanou smlouvou převést úkoly týkající se, představující a/nebo obsahující utajované skutečnosti EU na průmyslové nebo jiné subjekty v členském státě.

b) Komise zajistí při zadávání utajovaných smluv splnění všech požadavků vyplývajících z těchto minimálních norem.

c) Za účelem uplatňování těchto minimálních norem na průmyslová tajemství Komise zapojí příslušný NBÚ nebo více těchto příslušných úřadů. NBÚ může tyto úkoly převést na jeden nebo více DSA.

d) Úplnou odpovědnost za ochranu utajovaných skutečností EU v průmyslovém nebo jiném subjektu má vedení těchto subjektů.

e) Pokaždé, když se uzavírá utajovaná smlouva s dodavatelem nebo se subdodavatelem, která spadá do působnosti těchto minimálních norem, Komise a/nebo případně NBÚ/DSA bez zbytečného prodlení uvědomí NBÚ/DSA členského státu, ve kterém má dodavatel nebo subdodavatel sídlo.

27.4 **Utajované smlouvy a rozhodnutí o přidělení grantu**

a) Utajení smluv nebo grantových dohod musí zohlednit tyto zásady:

— Komise v případě potřeby určuje takové prvky utajované smlouvy, které vyžadují ochranu a následné utajení; Komise při tom musí vzít do úvahy původní stupeň utajení, který původce informace stanovil před uzavřením utajované smlouvy,

— celkový stupeň utajení smlouvy nesmí být nižší než nejvyšší stupeň utajení kteréhokoli z jejích prvků,

— utajované skutečnosti EU vzniklé v rámci smluvních činností jsou utajovány podle pokynů k utajení,

— Komise v případě potřeby, po konzultaci s původcem a po informování všech zúčastněných stran odpovídá za změnu celkového stupně utajení smlouvy nebo utajení kteréhokoli z jejích prvků,

— utajované skutečnosti předané dodavateli nebo subdodavateli nebo vzniklé v rámci smluvní činnosti nesmí být použity k jiným účelům než těm, které jsou definovány v utajované

▼M3

smlouvě, a bez předchozího písemného souhlasu původce nesmí být sdělovány třetím stranám.

b) Komise a NBÚ/DSA příslušných členských států odpovídají za to, aby dodavatelé a subdodavatelé, s nimiž byla uzavřena utajovaná smlouva obsahující utajované skutečnosti stupně utajení CONFIDENTIEL UE nebo vyššího stupně, přijali v souladu s vnitrostátními právními předpisy veškerá vhodná opatření k ochraně těchto utajovaných skutečností EU, které jim byly předány nebo které vznikly v rámci realizace utajované smlouvy. Nedodržení bezpečnostních požadavků může vyústit v rozvázání utajované smlouvy.

c) Všechny průmyslové nebo jiné subjekty, s nimiž byla uzavřena utajovaná smlouva umožňující přístup k utajovaným skutečnostem stupně utajení CONFIDENTIEL UE nebo vyššího, musí být držiteli vnitrostátního FSC. FSC vydává NBÚ/DSA členského státu a potvrzuje jím, že příslušné zařízení může zajistit vhodnou bezpečnostní ochranu utajovaných skutečností EU, která bude odpovídat danému stupni utajení.

d) Pokud je uzavřena utajovaná smlouva, bezpečnostní pracovník zařízení (FSO) jmenovaný řídícími pracovníky dodavatele nebo subdodavatele odpovídá za podání žádosti o zaměstnanecké bezpečnostní prověrky (PSC) pro všechny osoby zaměstnané průmyslovým nebo jiným subjektem se sídlem v členském státě EU, jejichž úkoly vyžadují přístup k informacím stupně utajení CONFIDENTIEL UE nebo vyššího, které jsou předmětem utajované smlouvy; uvedené prověrky vydává NBÚ/DSA tohoto členského státu podle vnitrostátních právních předpisů.

e) Utajované smlouvy musí obsahovat SAL definované v bodu 27.2 písm. j). SAL musí obsahovat SCG.

f) Před zahájením vyjednávacího řízení směřujícího k uzavření utajované smlouvy Komise kontaktuje NBÚ/DSA členského státu, ve kterém má dotčený průmyslový nebo jiný subjekt sídlo, za účelem získání potvrzení, že tento subjekt je držitelem platné prověrky FSC, která odpovídá stupni utajení smlouvy.

g) Zadavatel nesmí uzavřít utajovanou smlouvu se zvoleným hospodářským subjektem dříve, než obdrží platnou prověrku FSC.

h) Pokud tak nestanoví vnitrostátní právní předpisy členského státu, prověrka FSC se nevyžaduje v případě smluv obsahujících informace stupně utajení RESTREINT UE.

i) Výzvy k předkládání nabídek týkající se utajovaných smluv musí obsahovat požadavek, aby hospodářský subjekt, který nabídku nepředloží nebo není zvolen, vrátil ve stanovené lhůtě veškerou dokumentaci.

j) Dodavatel bude pravděpodobně muset sjednávat utajované smlouvy se subdodavateli na různých úrovních. Dodavatel odpovídá za to, že jsou všechny subdodavatelské činnosti vykonávány v souladu se společnými minimálními normami obsaženými v tomto oddílu. Dodavatel však nesmí utajovanou skutečnost EU nebo materiál subdodavateli předat bez předchozího písemného souhlasu původce.

k) Podmínky, na jejichž základě může dodavatel uzavřít subdodavatelskou smlouvu, musí být uvedeny v oznámení o veřejné zakázce nebo ve výzvě k předkládání nabídek a v utajované smlouvě. Bez výslovného písemného souhlasu Komise nemůže být subdodavatelská smlouva uzavřena se subjekty se sídlem ve státě, který není členem EU.

l) V průběhu realizace utajované smlouvy Komise ve spolupráci s příslušným DSA/NBÚ monitorují dodržování všech těchto bezpečnostních předpisů. Jakékoli události, které by mohly ovlivnit bezpečnost, musí být nahlášeny podle ustanovení části II oddílu 24 těchto

▼M3

bezpečnostních pravidel. Jakákoli změna prověrky FSC nebo její odnětí musí být neprodleně sděleny Komisi a jakémukoli NBÚ/DSA, kterému bylo její udělení oznámeno.

m) Pokud dojde k ukončení utajované smlouvy s dodavatelem nebo subdodavatelem, Komise a/nebo případně NBÚ/DSA bez zbytečného prodlení uvědomí NBÚ/DSA členského státu, ve kterém má dodavatel nebo subdodavatel sídlo.

n) Dodavatelé a subdodavatelé budou dodržovat společné minimální normy obsažené v tomto oddílu a zachovávat důvěrnost utajovaných skutečností i po skončení nebo zrušení utajované smlouvy nebo utajované subdodavatelské smlouvy.

o) V dopise SAL nebo v jiných příslušných předpisech upravujících bezpečnostní požadavky bude upraveno nakládání s utajovanými skutečnostmi po skončení utajované smlouvy.

p) Povinnosti a podmínky uvedené v tomto oddílu se přiměřeně použijí na postupy přijímání rozhodnutí o přidělení grantu a zejména na příjemce těchto grantů. Rozhodnutí o přidělení grantu upraví veškeré povinnosti příjemce.

27.5 **Návštěvy**

Návštěvy pracovníků Komise v souvislosti s utajovanými smlouvami v průmyslových nebo jiných subjektech v členských státech, které provádějí utajované smlouvy, musí být organizovány ve spolupráci s příslušným NBÚ/DSA. Vzájemné návštěvy zaměstnanců průmyslových a jiných subjektů v rámci smlouvy týkající se utajovaných skutečností EU musí být organizovány mezi příslušnými NBÚ/DSA. Příslušné NBÚ/DSA, jichž se smlouva obsahující utajované skutečnosti EU týká, se mohou dohodnout na postupu, na základě něhož mohou být návštěvy zaměstnanců průmyslových a jiných subjektů organizovány přímo.

27.6 **Předávání a přenos utajovaných skutečností EU**

a) Pokud jde o předávání utajovaných skutečností EU, použijí se ustanovení části II oddílu 21 těchto bezpečnostních pravidel. Za účelem doplnění těchto pravidel se použije jakýkoli postup platný mezi členskými státy.

b) Mezinárodní přenos utajovaných materiálů EU týkajících se utajovaných smluv se uskutečňuje v souladu s vnitrostátními postupy členských států. Při kontrole bezpečnostních opatření mezinárodních přenosů se použijí tyto zásady:

— bezpečnost musí být zajištěna ve všech stádiích přenosu za všech okolností, a to z místa původu do místa konečného určení,

— stupeň ochrany příslušné zásilky se určuje podle nevyššího stupně utajení materiálu, který zásilka obsahuje,

— je-li to vhodné, získávají dopravní společnosti prověrku FSC. V těchto případech musí mít zaměstnanec, který se zásilkou nakládá, bezpečnostní prověrku podle těchto společných minimálních norem uvedených v tomto oddíle,

— cesty jsou pokud možno realizovány z místa určení do místa určení bez přerušení a podle okolností co nejrychleji,

— kdykoli je to možné, měly by cesty vést pouze po území členských států EU. Cesty po území státu, který není členem EU, by se měly využívat pouze na základě povolení NBÚ/DSA jak státu, který zásilku vyslal, tak státu, který je jejím příjemcem,

— před jakýmkoli pohybem utajovaného materiálu EU musí vysílající subjekt vypracovat plán přenosu, který schvaluje příslušný NBÚ/DSA.

▼M1

Dodatek 1

SROVNÁVACÍ TABULKA VNITROSTÁTNÍCH BEZPEČNOSTNÍCH KLASIFIKACÍ

Klasifikace EU	TRES SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Klasifikace WEU	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Klasifikac Euratom e	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
Klasifikace NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
Belgie	Très Secret	Secret	Confidentiel	Diffusion restreinte
	Zeer Geheim	Geheim	Vertrouwelijk	Beperkte Verspreiding
Česká republika	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dánsko	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Německo	Streng geheim	Geheim	VS ([1]) — Vertraulich	VS — Nur für den Dienstgebrauch
Estonsko	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Řecko	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
	Abr: ΑΑΠ	Abr: (ΑΠ)	Abr: (ΕΜ)	Abr: (ΠΧ)
Španělsko	Secreto	Reservado	Confidencial	Difusión Limitada
Francie	Très Secret Défense ([2])	Secret Défense	Confidentiel Défense	
Irsko	Top Secret	Secret	Confidential	Restricted
Itálie	Segretissimo	Segreto	Riservatissimo	Riservato
Kypr	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Lotyšsko	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Lucembursko	Très Secret	Secret	Confidentiel	Diffusion restreinte
Maďarsko	Szigorúan titkos !	Titkos !	Bizalmas !	Korlátozott terjesztésű !
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nizozemsko	Stg ([3]). Zeer Geheim	Stg. Geheim	Stg. Confidentieel	Departementaalvertrouwelijk
Rakousko	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Polsko	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalsko	Muito Secreto	Secreto	Confidencial	Reservado
Slovinsko	Strogo tajno	Tajno	Zaupno	SVN Interno
Slovensko	Prísne tajné	Tajné	Dôverné	Vyhradené

▼B

Finsko	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Švédsko	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Spojené království	Top Secret	Secret	Confidential	Restricted

(7) VS = Verschlusssache.
(8) Klasifikaci Très Secret Défense, která se týká všech prioritních vládních záležitostí, lze změnit pouze tehdy, schválí-li to předseda vlády.
(9) Stg = staatsgeheim.

Dodatek 2

PRAKTICKÝ PRŮVODCE STUPNI UTAJENÍ

Tento průvodce je pouze informativní a nelze jej vykládat, jako by měnil základní ustanovení oddílů 16, 17, 20 a 21.

Stupeň utajení	Kdy	Kdo	Způsob označení	Snížení stupně utajení/ odtajnění / zničení	
				Kdo	Kdy
►M1 TRES SECRET UE/EU TOP SECRET ◄: Tento stupeň se použije výlučně pro informace a materiál, jejichž neoprávněné vyzrazení by mohlo výjimečně závažně poškodit základní zájmy Evropské unie nebo jednoho či více členských států [16.1].	Vyzrazení informací nebo materiálu označených ►M1 TRES SECRET UE/EU TOP SECRET ◄ by mohlo: — přímo ohrozit vnitřní stabilitu EU nebo některého z jejích členských států nebo spřátelených zemí, — způsobit výjimečně závažné škody ve vztazích se spřátelenými vládami, — vést přímo k velkým ztrátám na životech, — způsobit výjimečně závažné škody pro schopnost uplatnění nebo pro bezpečnost ozbrojených sil členských států nebo jiných partnerů nebo pro trvalou účinnost výjimečně cenných bezpečnostních nebo zpravodajských operací, — způsobit závažné dlouhodobé škody v hospodářství EU nebo členských států.	Řádně zmocněné osoby (původci), generální ředitelé, vedoucí služeb [17.1]. Původci stanoví datum nebo lhůtu, od kdy lze snížit stupeň utajení nebo odtajnit skutečnosti obsažené v dokumentu [16.2]. Jinak posuzují tuto otázku nejpozději každých pět let, aby zjistili, zda je původní stupeň utajení nadále nezbytný [17.3].	Stupeň utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ se přiděluje dokumentům ►M1 TRES SECRET UE/EU TOP SECRET ◄ a případně souvisí bezpečnostní specifikací a/nebo označením EBOP pořízeným mechanickými prostředky a ručně [16.4, 16.5, 16.3]. Stupeň utajení EU musí být uveden nahoře a dole uprostřed každé stránky a každá stránka musí být očíslovaná. Každý dokument musí obsahovat spisové číslo a datum; toto spisové číslo je uvedeno na každé stránce. Pokud musí být dokumenty rozesílány ve více výtiscích, musí být každý z nich označen na první stránce číslem výtisku a celkovým počtem stránek. Na první stránce musí být uveden úplný seznam všech příloh a připojených částí [21.1].	Rozhodnutí o odtajnění nebo snížení stupně utajení může přijmout výlučně původce, který je povinen uvědomit o změně stupně utajení následné příjemce, kterým předložil originál nebo jeho kopie [17.3]. Dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ ničí ústřední spisovna nebo spisovna nižší úrovně, která je za ně odpovědná. Zničení každého dokumentu je uvedeno v zápise o zničení podepsaném úředníkem, který má na starosti kontrolu ►M1 TRES SECRET UE/EU TOP SECRET ◄, úředníkem, který byl svědkem zničení a který musí projít prověrkou stupně ►M1 TRES SECRET UE/EU TOP SECRET ◄. Záznam o zničení se uvede v příslušné knize. Spisovna archivuje potvrzení o zničení spolu s doklady o rozdělení po dobu deseti let [22.5].	Nadbytečné výtisky a dokumenty, které již nejsou potřeba, je nutné zničit [22.5]. Dokumenty ►M1 TRES SECRET UE/EU TOP SECRET ◄ včetně všeho utajovaného odpadu, který vzniká při přípravě těchto dokumentů ►M1 TRES SECRET UE/EU TOP SECRET ◄, například poškozené výtisky, koncepty, na stroji psané poznámky a uhlový papír, musí být zničeny pod dohledem úředníka prověřeného pro stupeň ►M1 TRES SECRET UE/EU TOP SECRET ◄ spálením, rozdrcením, roztrháním nebo jiným způsobem tak, aby je nebylo možné identifikovat a znovu sestavit [22.5].

Stupeň utajení	Kdy	Kdo	Způsob označení	Snížení stupně utajení/ odtajnění / zničení	
				Kdo	Kdy
►M1 SECRET UE ◄: Tento stupeň se použije výlučně na informace a materiály, jejichž neoprávněné vyzrazení by mohlo vážně poškodit základní zájmy Evropské unie nebo jednoho či více členských států [16.1].	Vyzrazení skutečností nebo materiálu označených ►M1 SECRET UE ◄ by mohlo: — vyvolat mezinárodní napětí, — vážně poškodit vztahy se spřátelenými vládami, — přímo ohrozit lidské životy nebo vážně narušit veřejný pořádek nebo osobní bezpečnost nebo svobodu, — způsobit závažné škody pro schopnost uplatnění nebo pro bezpečnost ozbrojených sil členských států nebo jiných partnerů, nebo pro trvalou účinnost velmi cenných bezpečnostních nebo zpravodajských operací, — způsobit závažné materiální škody finančním, měnovým, hospodářským nebo obchodním zájmům EU nebo některého členského státu.	Zmocněné osoby (původci), generální ředitelé, vedoucí služeb [17.1]. Původci uvedou datum nebo lhůtu, od kdy lze snížit stupeň utajení skutečnosti obsažené v dokumentu nebo ji odtajnit [16.2]. Jinak posuzují tuto otázku nejpozději každých pět let, aby zjistili, zda je původní stupeň utajení nadále nezbytný [17.3].	Stupeň utajení ►M1 SECRET UE ◄, a v případech potřeby bezpečnostní specifikace a/nebo označení – EBOP, se vyznačí na dokumentech se stupněm utajení ►M1 SECRET UE ◄ mechanickými prostředky a ručně [16.4, 16.5, 16.3]. Stupeň utajení EU a bezpečnostní specifikace musí být uvedena nahoře a dole uprostřed každé stránky a každá stránka musí být očíslovaná. Každý dokument musí obsahovat spisové číslo a datum; toto spisové číslo je uvedeno na každé stránce. Pokud musí být dokumenty rozesílány ve více výtiscích, musí být každý z nich označen na první stránce číslem výtisku a celkovým počtem stránek. Na první stránce musí být uveden úplný seznam všech příloh a připojených částí [21.1].	Rozhodnutí o odtajnění nebo snížení stupně utajení může přijmout výlučně původce, který je povinen uvědomit o změně stupně utajení následné příjemce, kterým předložil originál nebo jeho kopie [17.3]. Dokumenty ►M1 SECRET UE ◄ ničí spisovna, která je za ně odpovědná, pod dohledem osoby, která prošla bezpečnostní prověrkou. Každý zničený dokument je uveden v podepsaném zápise o zničení, který musí archivovat spisovna spolu s doklady o rozdělení nejméně po dobu tří let [22.5].	Nadbytečné výtisky a dokumenty, které již nejsou potřeba, je nutné zničit [22.5]. Dokumenty ►M1 SECRET UE ◄ včetně všeho utajovaného odpadu, který vzniká při přípravě těchto dokumentů ►M1 TRES SECRET UE/EU TOP SECRET ◄, například poškozené výtisky, koncepty, na stroji psané poznámky a uhlový papír musí být zničeny spálením, rozdrcením, roztrháním nebo jiným způsobem tak, aby je nebylo možné identifikovat a znovu sestavit [22.5].

Stupeň utajení	Kdy	Kdo	Způsob označení	Snížení stupně utajení/ odtajnění / zničení	
				Kdo	Kdy
►M1 CONFIDENTIEL UE ◄: Tento stupeň se použije pro informace a materiály, jejichž neoprávněné vyzrazení by mohlo poškodit základní zájmy Evropské unie nebo jednoho či více členských států [16.1].	Vyzrazení skutečností nebo materiálu označených ►M1 CONFIDENTIEL UE ◄ by mohlo: — významně poškodit diplomatické vztahy, to znamená vyvolat oficiální protest nebo jiné sankce, — narušit osobní bezpečnost nebo svobodu, — způsobit vážné škody pro schopnost uplatnění nebo pro bezpečnost ozbrojených sil členských států nebo jiných partnerů, nebo trvalou účinnost užitečných bezpečnostních nebo zpravodajských operací, — vážně ohrozit finanční životaschopnost velkých organizací, — bránit vyšetřování nebo závažných trestných činů nebo usnadňovat jejich páchání, — působit významně proti finančním, měnovým, hospodářským nebo obchodním zájmům EU nebo členských států, — závažně narušit vpracování a fungování hlavních politik EU, — způsobit ukončení významných činností EU nebo je významně narušit jakýmkoli způsobem.	Zmocněné osoby (původci), generální ředitelé, vedoucí služeb [17.1]. Původci uvedou datum nebo lhůtu, od kdy lze snížit stupeň utajení skutečnosti obsažené v dokumentu nebo ji odtajnit. Jinak posuzují tuto otázku nejpozději každých pět let, aby zjistili, zda je původní stupeň utajení nadále nezbytný [17.3].	Stupeň utajení ►M1 CONFIDENTIEL UE ◄, a v případech potřeby bezpečnostní specifikace a/nebo označení – EBOP, se vyznačí na dokumentech se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a ručně nebo vytištěním na předem orazítkovaný evidovaný papír [16.4, 16.5, 16.3]. Stupeň utajení EU musí být uveden nahoře a dole uprostřed každé stránky a každá stránka musí být očíslovaná. Každý dokument musí obsahovat spisové číslo a datum. Na první stránce musí být uveden úplný seznam všech příloh a připojených částí [21.1].	Rozhodnutí o odtajnění nebo snížení stupně utajení může přijmout výlučně původce, který je povinen uvědomit o změně stupně utajení následující příjemce, kterým předložili originál nebo jeho kopie [17.3]. Dokumenty ►M1 CONFIDENTIEL UE ◄ ničí spisovna, která je za ně odpovědná, pod dohledem osoby, která prošla bezpečnostní prověrkou. Zničení se eviduje v souladu s vnitrostátními předpisy a v případě Komise nebo decentralizovaných subjektů EU podle pokynů ►M2 člena Komise odpovědného za bezpečnostní otázky ◄ [22.5].	Nadbytečné výtisky a dokumenty, které již nejsou potřeba, je nutné zničit [22.5]. Dokumenty ►M1 CONFIDENTIEL UE ◄, včetně všeho utajovaného odpadu, který vzniká při přípravě těchto dokumentů ►M1 CONFIDENTIEL UE ◄, například poškozené výtisky, koncepty, na stroji psané poznámky a uhlový papír musí být zničeny spálením, rozdrcením, roztrháním nebo jiným způsobem tak, aby je nebylo možné identifikovat a znovu sestavit [22.5].

Stupeň utajení	Kdy	Kdo	Způsob označení	Snížení stupně utajení/ odtajnění / zničení	
				Kdo	Kdy
►M1 RESTREINT UE ◄: Tento stupeň se použije pro informace a materiály, jejichž neoprávněné vyzrazení by mohlo být nevýhodné pro zájmy Evropské unie nebo jednoho či více členských států [16.1].	Vyzrazení skutečností nebo materiálu označených ►M1 RESTREINT UE ◄ by mohlo: — poškodit diplomatické vztahy, — způsobit velké nepříjemnosti jednotlivcům, — způsobit vážné škody pro schopnost uplatnění nebo pro bezpečnost ozbrojených sil členských států nebo jiných partnerů, — způsobit finanční ztrátu nebo usnadnit neoprávněný zisk nebo výhody jednotlivcům nebo společnostem, — porušit řádně přijatý závazek zachovávat důvěrnost informací poskytnutých třetími osobami, — porušit zákonná omezení pro sdělování informací, — poškodit vyšetřování nebo usnadnit páchání závažných trestných činů, — znevýhodnit EU nebo členské státy při obchodních nebo politických jednáních, — narušit účinné vypracování nebo uplatňování politik EU, — ohrožovat řádné řízení EU a jejích činností.	Zmocněné osoby (původci), generální ředitelé, vedoucí služeb [17.1]. Původci uvedou datum nebo lhůtu, od kdy lze snížit stupeň utajení skutečnosti obsažené v dokumentu nebo ji odtajnit [16.2]. Jinak posuzují tuto otázku nejpozději každých pět let, aby zjistili, zda je původní stupeň utajení nadále nezbytný [17.3].	Stupeň utajení ►M1 RESTREINT UE ◄, a v případech potřeby bezpečnostní specifikace a/nebo označení – EBOP, se vyznačí na dokumentech ►M1 RESTREINT UE ◄ mechanickými nebo elektronickými prostředky. [16.4, 16.5, 16.3]. Stupeň utajení EU musí být uveden nahoře a dole uprostřed každé stránky a každá stránka musí být očíslovaná. Každý dokument musí obsahovat spisové číslo a datum [21.1].	Rozhodnutí o odtajnění nebo snížení stupně utajení může přijmout pouze původce, který je povinen uvědomit o změně stupně utajení následné příjemce, kterým předložili originál nebo jeho kopie [17.3]. Dokumenty ►M1 RESTREINT UE ◄ ničí spisovna, která je za ně odpovědná, nebo uživatel podle pokynů ►M2 člena Komise odpovědného za bezpečnostní otázky ◄ [22.5].	Nadbytečné výtisky a dokumenty, které již nejsou potřeba, je nutné zničit [22.5].

▼B

Dodatek 3

Obecné zásady pro předávání utajovaných skutečností EU třetím státům nebo mezinárodním organizacím: spolupráce na úrovni 1

POSTUPY

1. Za předávání utajovaných skutečností EU zemím, které nejsou členy Evropské unie, nebo jiným mezinárodním organizacím, jejichž bezpečnostní politika a předpisy jsou srovnatelné s bezpečnostní politikou a předpisy EU, odpovídá sbor členů Komise.

2. Až do uzavření bezpečnostní dohody je člen Komise odpovědný za bezpečnostní otázky oprávněn prověřovat žádosti o poskytnutí utajovaných skutečností EU.

3. Při tom postupuje takto:

   — získá stanoviska původců utajovaných skutečností EU, které mají být předány;

   — vytvoří nezbytné kontakty s bezpečnostními orgány přijímajících zemí nebo mezinárodních organizací, aby si ověřil, zda jejich bezpečnostní politika a předpisy zaručují, že předávané skutečnosti budou chráněny v souladu s těmito bezpečnostními pravidly,

   — získá stanovisko Poradní skupiny pro bezpečnostní politiku Komise týkající se důvěry, kterou lze věnovat přijímajícím státům nebo mezinárodním orgánům.

4. Člen Komise odpovědný za bezpečnostní otázky předloží žádost a stanovisko Poradní skupiny pro bezpečnostní politiku Komise Komisi, která rozhodne.

BEZPEČNOSTNÍ PRAVIDLA, KTERÁ MUSÍ PŘÍJEMCI DODRŽOVAT

5. Člen Komise odpovědný za bezpečnostní otázky oznámí přijímajícím státům nebo mezinárodním organizacím rozhodnutí Komise povolit předání utajovaných skutečností EU.

6. Rozhodnutí předat skutečnosti je vykonatelné, pouze pokud příjemci přijmou písemný závazek, že:

   — budou používat skutečnosti pouze ke stanoveným účelům,

   — budou chránit skutečnosti v souladu s těmito bezpečnostními pravidly, a zejména s níže uvedenými zvláštními ustanoveními.

7. Personál

   a) Počet zaměstnanců, kteří mají přístup k utajovaným skutečnostem EU, je přísně omezen podle zásady „potřeba vědět“ na osoby, jejichž funkce takový přístup vyžadují.

   b) Všichni zaměstnanci nebo státní příslušníci, jimž je povolen přístup ke skutečnostem se stupněm utajení ►**M1** CONFIDENTIEL UE ◄ nebo vyšším, musí být držitelem bezpečnostního osvědčení příslušné úrovně uděleného vládou jejich státu nebo musí projít bezpečnostní prověrkou odpovídajícího stupně organizovanou daným státem.

8. Předávání dokumentů

   a) Praktický postup při předávání dokumentů je přijat dohodou. Do uzavření této dohody platí ustanovení oddílu 21. Dohoda zejména upřesní, kterým spisovnám jsou utajované skutečnosti EU předávány.

   b) Jestliže utajované skutečnosti, jejichž předání bylo Komisí povoleno, zahrnují skutečnosti se stupněm utajení ►**M1** TRES SECRET UE/EU TOP SECRET ◄, musí přijímající země nebo mezinárodní organizace vytvořit ústřední spisovnu EU, a je-li potřeba spisovny nižší úrovně. Tyto spisovny uplatňují důsledně taková opatření, která odpovídají opatřením oddílu 22 těchto bezpečnostních pravidel.

▼B

9. Evidence

Jakmile některá spisovna přijme dokument EU se stupněm utajení ►M1 CONFIDENTIEL UE ◄ nebo vyšším, zaznamená jej do zvláštního rejstříku vedeného organizací, který je rozdělen na sloupce uvádějící datum přijetí dokumentu, údaje o dokumentu (datum, spisové číslo a číslo výtisku), stupeň utajení dokumentu, předmět, jméno nebo funkci příjemce, datum vrácení potvrzení o převzetí a datum, kdy byl dokument vrácen původci v EU nebo kdy byl zničen.

10. Zničení

a) Utajované dokumenty EU se ničí v souladu s pokyny uvedenými v oddílu 22 těchto bezpečnostních pravidel. Kopie zápisů o zničení dokumentů ►M1 SECRET UE ◄ a ►M1 TRES SECRET UE/EU TOP SECRET ◄ se zasílají spisovně EU, která dokumenty zaslala.

b) Utajované dokumenty EU se zahrnou do plánů ničení utajovaných dokumentů přijímajícího orgánu v nouzových situacích.

11. Ochrana dokumentů

Je třeba přijmout všechna nezbytná opatření, aby se zabránilo přístupu neoprávněných osob k utajovaným skutečnostem EU.

12. Kopie, překlady a výpisy

Je zakázáno pořizovat fotokopie dokumentů se stupněm utajení ►M1 CONFIDENTIEL UE ◄ nebo ►M1 SECRET UE ◄, překládat je a pořizovat z nich výpisy bez povolení vedoucího dotčené bezpečnostní organizace, která kopie, překlady a výpisy eviduje a zkontroluje a připojí k nim nezbytná označení.

Rozmnožování nebo překlad dokumentu se stupněm utajení ►M1 TRES SECRET UE/EU TOP SECRET ◄ může povolit pouze původce, přičemž v povolení uvede počet povolených kopií; jestliže původce nelze určit, je dotaz zaslán ►M2 ředitelstvím pro bezpečnost Komise ◄.

13. Porušení bezpečnosti

Dojde-li k porušení bezpečnosti některého utajovaného dokumentu EU nebo vznikne-li podezření z tohoto porušení, je třeba neprodleně přijmout, s výhradou uzavření bezpečnostní dohody, tato opatření:

a) provést šetření pro zjištění okolností porušení bezpečnosti;

b) upozornit ►M2 ředitelství pro bezpečnost Komise ◄, příslušný vnitrostátní bezpečnostní orgán a původce dokumentu nebo jasně uvést, že posledně uvedený nebyl upozorněn;

c) usilovat o omezení účinků tohoto porušení bezpečnosti na minimum;

d) znovu posoudit a provést opatření, která zamezí opakování;

e) provést veškerá doporučení ►M2 ředitelství pro bezpečnost Komise ◄, která zamezí opakování.

14. Kontroly

►M2 Ředitelství pro bezpečnost Komise ◄ je oprávněna po dohodě s dotčenými státy nebo mezinárodními organizacemi provádět ověřování účinnosti opatření na ochranu předávaných utajovaných skutečností EU.

15. Zprávy

S výhradou uzavření bezpečnostní dohody předkládá země nebo mezinárodní organizace, mají-li v držení utajované skutečnosti EU, každý rok ke dni stanovenému při udělení oprávnění k přijímání skutečností zprávu potvrzující dodržování těchto bezpečnostních pravidel.

▼B

Dodatek 4

Obecné zásady pro předávání utajovaných skutečností EU třetím státům nebo mezinárodním organizacím: spolupráce na úrovni 2

POSTUPY

1. Za předávání utajovaných skutečností EU třetím státům nebo mezinárodním organizacím, jejichž bezpečnostní politika a předpisy se výrazně liší od bezpečnostní politiky a předpisů EU, odpovídá původce. Oprávnění poskytovat utajované skutečnosti EU, které vznikly v Komisi, má sbor členů Komise.

2. Platí zásada, že lze poskytnout pouze skutečnosti do stupně utajení ►M1 SECRET UE ◄ včetně; utajované skutečnosti chráněné zvláštní bezpečnostní specifikací nebo označením není možné poskytovat.

3. Až do uzavření bezpečnostní dohody je člen Komise odpovědný za bezpečnostní otázky oprávněn prověřovat žádosti o poskytnutí utajovaných skutečností EU.

4. Postupuje při tom takto:

   — získá stanoviska původců utajovaných skutečností EU, které se mají poskytnout,

   — vytvoří nezbytné kontakty s bezpečnostními orgány přijímajících států nebo mezinárodních organizací, aby se informoval o jejich bezpečnostní politice a předpisech, a zejména aby vytvořil tabulku pro srovnání stupňů utajení platných v EU a v dotčeném státu nebo organizaci,

   — zorganizuje zasedání Poradní skupiny pro bezpečnostní politiku Komise nebo požádá, případně zjednodušeným písemným postupem, vnitrostátní bezpečnostní orgány členských států o přezkoumání s cílem získat stanovisko Poradní skupiny pro bezpečnostní politiku Komise.

5. Stanovisko Poradní skupiny pro bezpečnostní politiku Komise se týká:

   — důvěry, kterou je možné věnovat přijímajícím státům nebo mezinárodním organizací, s cílem zhodnotit bezpečnostní rizika pro EU nebo její členské státy,

   — hodnocení schopnosti příjemců zajistit ochranu utajovaných skutečností předaných ze strany EU,

   — návrhů na praktické postupy pro nakládání s předávanými utajovanými skutečnostmi EU (např. cenzurování textu) a dokumenty (ponechání nebo odstranění poznámek o stupni utajení, specifického označení atd.),

   — snížení stupně utajení nebo odtajnění skutečnosti původcem před předáním skutečnosti přijímající zemi nebo mezinárodní organizaci.

6. Člen Komise odpovědný za bezpečnostní otázky předá žádost a stanovisko Poradní skupiny pro bezpečnostní politiku Komise Komisi, která rozhodne.

BEZPEČNOSTNÍ PRAVIDLA, KTERÁ MUSÍ PŘÍJEMCI DODRŽOVAT

7. Člen Komise odpovědný za bezpečnostní otázky oznámí přijímajícím státům nebo mezinárodním organizacím rozhodnutí Komise povolit předání utajovaných skutečností EU a o jejích omezeních.

8. Rozhodnutí předat skutečnosti je vykonatelné, pouze pokud příjemci přijmou písemný závazek, že:

   — budou používat skutečnosti pouze ke stanoveným účelům,

▼B

— budou chránit skutečnosti v souladu s předpisy stanovenými Komisí.

9. Nepřijme-li Komise na základě technického stanoviska Poradní skupiny pro bezpečnostní politiku Komise rozhodnutí o zvláštním postupu pro nakládání s utajovanými dokumenty EU (odstranění poznámky o utajení EU, specifická označení atd.), budou stanovena následující pravidla ochrany.

10. Personál

a) Počet zaměstnanců, kteří mají přístup k utajovaným skutečnostem EU, je přísně omezen podle zásady „potřeba vědět“ na osoby, jejichž funkce takový přístup vyžaduje.

b) Všichni zaměstnanci nebo státní příslušníci, jimž je povolen přístup k utajovaným skutečnostem předaným Komisí, musí projít vnitrostátní bezpečnostní prověrkou nebo musí mít vnitrostátní bezpečnostní osvědčení opravňující ho k přístupu k vnitrostátním utajovaným skutečnostem příslušného stupně odpovídajícího bezpečnostnímu stupni EU podle srovnávací tabulky.

c) Tyto vnitrostátní bezpečnostní prověrky nebo osvědčení se předávají pro informaci ►M2 řediteli ředitelství pro bezpečnost Komise ◄.

11. Předávání dokumentů

Praktický postup při předávání dokumentů je přijat dohodou. Do uzavření této dohody se použijí ustanovení oddílu 21. Dohoda zejména upřesní, kterým spisovnám jsou utajované skutečnosti EU předávány, a upřesní adresy, na které se dokumenty zašlou, a zásilkovou nebo poštovní službu použitou pro předání utajovaných skutečností EU.

12. Evidence při převzetí

Vnitrostátní bezpečnostní orgán přijímající země nebo obdobný orgán, který přijímá jménem své vlády utajované skutečnosti předávané Komisí, nebo bezpečnostní kancelář přijímající mezinárodní organizace zavedou zvláštní rejstřík pro evidenci utajovaných dokumentů EU při převzetí. Rejstřík je rozdělen na sloupce uvádějící datum přijetí dokumentu, údaje o dokumentu (datum, spisové číslo a číslo výtisku), stupeň utajení dokumentu, předmět, jméno nebo funkci příjemce, datum vrácení potvrzení o převzetí a datum, kdy byl dokument vrácen původci v EU nebo zničen.

13. Vracení dokumentů

Při vracení utajovaného dokumentu Komisi postupuje příjemce způsobem uvedeným v odstavci „Předávání dokumentů“.

14. Ochrana

a) Dokumenty, které se právě nepoužívají, jsou uzavřeny v bezpečnostní schránce schválené pro archivování vnitrostátních utajovaných materiálů stejného stupně utajení. Na schránce nesmí být žádné označení jejího obsahu, který je přístupný pouze osobám pověřeným k nakládání s utajovanými skutečnostmi EU. Je-li vybavena zámkem s kombinací, je tato kombinace známa pouze zaměstnancům státu nebo organizace, kteří jsou oprávněni pro přístup k utajovaným skutečnostem EU uloženým ve schránce; kombinace se mění každých šest měsíců nebo dříve při odchodu některého zaměstnance nebo při zrušení platnosti bezpečnostní prověrky některého ze zaměstnanců, který zná kombinaci, nebo vznikne-li riziko vyzrazení.

b) Utajované dokumenty EU jsou oprávněni vyjímat z bezpečnostní schránky pouze zaměstnanci, kteří prošli bezpečnostní prověrkou pro přístup k utajovaným dokumentům EU a mají „potřebu vědět“. Musí zajistit dohled nad těmito dokumenty, pokud je

▼B

mají v držení, a zejména zajistit, aby k dokumentům neměla přístup žádná neoprávněná osoba. Musí rovněž zajistit jejich uložení v bezpečnostní schránce, jakmile je přestanou využívat, a mimo pracovní dobu.

c) Bez povolení ►M2 ředitelství pro bezpečnost Komise ◄ je zakázáno pořizovat fotokopie dokumentu se stupněm utajení ►M1 CONFIDENTIEL UE ◄ nebo vyšším nebo z něj pořizovat výpisy.

d) Je třeba vymezit a potvrdit společně s ►M2 ředitelstvím pro bezpečnost Komise ◄ postup pro rychlé a úplné zničení dokumentů v případě nouze.

15. Fyzická bezpečnost

a) Bezpečnostní schránky pro ukládání utajovaných dokumentů UE, které se právě nepoužívají, musí být stále zamčené.

b) Je-li nutné, aby do objektu, kde jsou uloženy bezpečnostní schránky, vstoupili nebo v něm pracovali pracovníci údržby nebo úklidu, musí je stále doprovázet některý člen bezpečnostní služby státu nebo organizace nebo zaměstnanec, který je speciálně pověřen zajištěním bezpečnosti tohoto objektu.

c) Mimo obvyklou pracovní dobu (v noci, o víkendech a o dnech volna) zajišťuje ochranu bezpečnostních schránek obsahujících utajované dokumenty EU stráž nebo automatický poplašný systém.

16. Porušení bezpečnosti

Dojde-li k porušení bezpečnosti některého utajovaného dokumentu EU nebo vznikne-li podezření z tohoto porušení, je třeba neprodleně přijmout následující opatření:

a) neprodleně podat zprávu ►M2 ředitelstvím pro bezpečnost Komise ◄ nebo vnitrostátnímu bezpečnostnímu orgánu členského státu, který převzal iniciativu při přepravě dokumentů (s kopií pro ►M2 ředitelství pro bezpečnost Komise ◄);

b) provést šetření, po jehož ukončení je předložena podrobná zpráva bezpečnostnímu orgánu [viz výše písmeno a)]. Poté je třeba přijmout potřebná opatření pro nápravu situace.

17. Kontroly

►M2 Ředitelství pro bezpečnost Komise ◄ je oprávněna po dohodě s dotčenými státy nebo mezinárodními organizacemi provádět ověření účinnosti opatření na ochranu předávaných utajovaných skutečností EU.

18. Zprávy

Nestanoví-li bezpečnostní dohoda jinak, Má-li stát nebo mezinárodní organizace v držení utajované skutečnosti EU, předkládá každý rok ke dni stanovenému při udělení oprávnění k přijímání skutečností zprávu potvrzující dodržování těchto bezpečnostních pravidel.

▼B

Dodatek 5

Obecné zásady pro předávání utajovaných skutečností EU třetím státům nebo mezinárodním organizacím: spolupráce na úrovni 3

POSTUPY

1. Může dojít k tomu, že se Komise rozhodne za určitých zvláštních okolností spolupracovat se státy nebo organizacemi, které nemohou poskytnout záruky požadované těmito bezpečnostními pravidly, ale spolupráce může vyžadovat předání utajovaných skutečností EU.

2. Oprávnění poskytovat utajované skutečnosti EU třetím státům nebo mezinárodním organizacím, jejichž bezpečnostní politika a předpisy se výrazně odlišují od EU, má původce. Oprávnění poskytovat utajované skutečnosti EU, které vznikly v Komisi, má sbor členů Komise.

   Platí zásada, že poskytnutí informací se omezuje na skutečnosti do stupně utajení ►M1 SECRET UE ◄ včetně; utajované skutečnosti chráněné zvláštní bezpečnostní specifikací nebo označením není možné předat.

3. Komise posoudí, zda je vhodné utajované skutečnosti předat, posoudí potřebu „znalost nutná“ příjemce a rozhodne o povaze utajovaných skutečností, které mohou být předány.

4. Pokud je rozhodnutí Komise kladné, člen Komise odpovědný za bezpečnostní otázky

   — získá stanoviska původců utajovaných skutečností EU, které se mají předat,

   — zorganizuje zasedání Poradní skupiny pro bezpečnostní politiku Komise nebo požádá, případně zjednodušeným písemným postupem, vnitrostátní bezpečnostní orgány členských států o přezkoumání s cílem získat stanovisko Poradní skupiny pro bezpečnostní politiku Komise.

5. Stanovisko Poradní skupiny pro bezpečnostní politiku Komise se týká

   a) hodnocení bezpečnostních rizik vznikajících EU nebo jejím členským státům;

   b) stupně utajení skutečností, které lze sdělit, případně s ohledem na jejich povahu;

   c) snížení stupně utajení nebo odtajnění skutečností před jejich předáním;

   d) postupů pro nakládání s dokumenty, které mají být předány (viz následující odstavec);

   e) možných způsobů předání (využití veřejných poštovních služeb, veřejných nebo chráněných telekomunikačních sítí, diplomatické pošty, prověřených kurýrů atd.).

6. Dokumenty předávané státům nebo organizacím podle této přílohy jsou v zásadě připraveny bez uvedení zdroje a stupně utajení EU. Poradní skupina pro bezpečnostní politiku Komise může doporučit:

   — přijetí zvláštního označení nebo kódovaného jména,

   — přijetí zvláštního systému stupňů utajení, který vytvoří vazbu mezi jednotlivými stupni citlivosti předávaných skutečností a kontrolními opatřeními, jež jsou potřebná na základě metod předávání dokumentů požadovaných od příjemce.

7. ►M2 Člen Komise odpovědný za bezpečnostní otázky ◄ předá Komisi stanovisko Poradní skupiny pro bezpečnostní politiku Komise k rozhodnutí.

8. Jakmile Komise schválí předání utajovaných skutečností EU a praktické prováděcí postupy, naváže ►M2 ředitelství pro bezpeč-

▼B

nost Komise ◄ nezbytné kontakty s bezpečnostní službou dotčeného státu nebo organizace, aby usnadnila uplatňování předpokládaných bezpečnostních opatření.

9. Člen Komise odpovědný za bezpečnostní otázky informuje členské státy o povaze a stupni utajení skutečností, spolu s uvedením organizací a zemí, kterým mohou být na základě rozhodnutí Komise poskytnuty.

10. ►M2 Ředitelství pro bezpečnost Komise ◄ přijme všechna nezbytná opatření, aby usnadnila zhodnocení škody a případné následné přepracování postupů.

Při každé změně podmínek spolupráce je třeba věc znovu předložit Komisi.

BEZPEČNOSTNÍ PRAVIDLA, KTERÁ MUSÍ PŘÍJEMCI DODRŽOVAT

11. Člen Komise odpovědný za bezpečnostní otázky oznámí přijímajícím státům nebo mezinárodním organizacím rozhodnutí Komise povolit předávání utajovaných skutečností EU a předá jim podrobná pravidla ochrany navržená Poradní skupinou pro bezpečnostní politiku Komise a schválená Komisí.

12. Rozhodnutí předat skutečnosti je vykonatelné, pouze pokud příjemci přijmou písemný závazek, že:

— budou používat skutečnosti pouze za účelem spolupráce schválené Komisí,

— chránit skutečnosti podle požadavků Komise.

13. Předávání dokumentů

a) Praktický postup při předávání dokumentů je přijat společnou dohodou ►M2 ředitelství pro bezpečnost Komise ◄ a s bezpečnostními orgány přijímajících států nebo mezinárodních organizací. Tyto postupy uvedou zejména přesné adresy, na které mají být dokumenty zaslány.

b) Dokumenty se stupněm utajení ►M1 CONFIDENTIEL UE ◄ a vyšším se předávají ve dvojité obálce. Vnitřní obálka se označí zvláštním razítkem nebo kódovaným jménem, o kterém bude rozhodnuto, a údajem o stupni utajení. Ke každému utajovanému dokumentu se přiloží formulář potvrzení o převzetí. Formulář potvrzení o převzetí není utajovaný a poskytuje výlučně údaje o daném dokumentu (spisové číslo, datum, číslo výtisku) a jazyk dokumentu, nikoli však předmět.

c) Vnitřní obálka se poté vloží do vnější obálky, na níž se uvede číslo zásilky pro účely přijetí. Na vnější obálce nesmí být uveden stupeň utajení.

d) Kurýrům se vždy předává potvrzení s uvedením čísla zásilky.

14. Evidence při převzetí

Vnitrostátní bezpečnostní orgán přijímajícího státu nebo obdobný orgán, který přijímá jménem své vlády utajované skutečnosti předávané Komisí, nebo bezpečnostní kancelář přijímající mezinárodní organizace zavedou zvláštní rejstřík pro evidenci utajovaných dokumentů EU při převzetí. Rejstřík je rozdělen na sloupce uvádějící datum přijetí dokumentu, údaje o dokumentu (datum, spisové číslo a číslo výtisku), stupeň utajení dokumentu, předmět, jméno nebo funkci příjemce, datum vrácení potvrzení o převzetí a datum, kdy byl dokument vrácen původci v EU nebo zničen.

15. Používání a ochrana vyměňovaných utajovaných skutečností

a) Skutečnosti se stupněm utajení ►M1 SECRET UE ◄ zpracovávají zaměstnanci, kteří jsou výslovně určeni k tomuto účelu a kteří jsou oprávněni k přístupu ke skutečnostem s tímto stupněm utajení. Skutečnosti jsou uchovávány v kvalitních

▼B

bezpečnostních skříňkách, které mohou otevřít pouze osoby oprávněné k přístupu ke skutečnostem obsaženým ve skříňkách. Oblasti, kde jsou tyto skříňky umístěny, jsou stále střeženy, a je vytvořen kontrolní systém, který zajistí vstup pouze řádně oprávněným osobám. Skutečnosti se stupněm utajení ►M1 SECRET UE ◄ jsou zasílány diplomatickou poštou, bezpečnou poštovní službou a bezpečnými telekomunikačními prostředky. Dokument se stupněm utajení ►M1 SECRET UE ◄ lze kopírovat pouze s písemným souhlasem původce. Všechny kopie jsou evidovány a kontrolovány. Pro všechny operace týkající se dokumentů stupně ►M1 SECRET UE ◄ se vydávají potvrzení.

b) Skutečnosti se stupněm utajení ►M1 CONFIDENTIEL UE ◄ zpracovávají řádně určení zaměstnanci, kteří jsou oprávněni získat informace o jejich předmětu. Dokumenty jsou uchovávány v uzavřených bezpečnostních skříňkách v kontrolovaných oblastech.

   Skutečnosti se stupněm utajení ►M1 CONFIDENTIEL UE ◄ se zasílají diplomatickou poštou, vojenskými poštovními službami a bezpečnými telekomunikačními prostředky. Přijímající subjekt je může kopírovat, přičemž jejich počet a rozdělení jsou uvedeny ve zvláštních rejstřících.

c) Skutečnosti se stupněm utajení ►M1 RESTREINT UE ◄ se zpracovávají v objektech, do nichž nemají přístup neoprávněné osoby, a ukládají se do uzavřených schránek. Dokumenty lze zasílat veřejnými poštovními službami jako doporučenou zásilku ve dvojité obálce a v případech nouze nechráněnou veřejnou telekomunikační sítí. Příjemci mohou pořizovat kopie.

d) Neutajované skutečnosti nevyžadují zvláštní ochranná opatření a lze je zasílat poštou a veřejnými telekomunikačními sítěmi. Příjemci mohou pořizovat kopie.

16. Zničení

Dokumenty, které již nejsou potřebné, musí být zničeny. V případě dokumentů se stupněm utajení ►M1 RESTREINT UE ◄ a ►M1 CONFIDENTIEL UE ◄ musí být uveden příslušný záznam o zničení do speciálních rejstříků. V případě dokumentů se stupněm utajení ►M1 SECRET UE ◄ jsou vypracovány zápisy o zničení podepsané dvěma osobami, které byly svědky zničení.

17. Porušení bezpečnosti

Dojde-li k vyzrazení skutečností se stupněm utajení ►M1 CONFIDENTIEL UE ◄ nebo ►M1 SECRET UE ◄ nebo vznikne-li podezření z vyzrazení, provede vnitrostátní bezpečnostní orgán státu nebo vedoucí bezpečnosti organizace šetření okolností vyzrazení. O výsledcích šetření je nutno informovat ►M2 ředitelství pro bezpečnost Komise ◄. Přijmou se nezbytná opatření pro nápravu nevhodných postupů nebo způsobů uložení, pokud způsobily vyzrazení.

▼B

Dodatek 6

SEZNAM ZKRATEK

ANGLICKÁ ZKRATKA	ČESKÝ PŘEKLAD
ACPC	Poradní komise pro nákupy a veřejné zakázky
CrA	orgán pro šifrování
CISO	úředník pro bezpečnost informatiky na úrovni ústředí
COMPUSEC	počítačová bezpečnost
COMSEC	bezpečnostní komunikace
CSO	►M2 ředitelství pro bezpečnost Komise ◄
ESDP	Evropská bezpečnostní a obranná politika
EUCI	utajované údaje EU
IA	úřad INFOSEC
INFOSEC	bezpečnost informačních systémů
IO	vlastník informací
ISO	Mezinárodní organizace pro normalizaci
IT	informační technologie
LISO	úředník pro bezpečnost informatiky na místní úrovni
LSO	bezpečnostní pracovník daného útvaru
MSO	bezpečnostní pracovník zasedání
NSA	vnitrostátní bezpečnostní orgán
PC	osobní počítač
RCO	kontrolor spisovny
SAA	orgán pro schvalování z hlediska bezpečnosti
SecOP	provozní postupy pro zajištění bezpečnosti
SSRS	stanovení bezpečnostních požadavků vlastních danému systému
TA	orgán pro normu TEMPEST
TSO	vlastník technického systému

▼M3

DSA	stanovený bezpečnostní úřad (Designated Security Authority)
FSC	bezpečnostní prověrka zařízení (Facility Security Clearance)
FSO	bezpečnostní pracovník zařízení (Facility Security Officer)
PSC	zaměstnanecká bezpečnostní prověrka (Personnel Security Clearance)
SAL	bezpečnostní dopis (Security Aspects Letter)
SCG	pokyny k utajení (Security Classification Guide)