32001D0264

L 101/1 *ÚŘEDNÍ VĚSTNÍK EVROPSKÝCH SPOLEČENSTVÍ* 11.4.2001

ROZHODNUTÍ RADY
ze dne 19. března 2001,
kterým se přijímají bezpečnostní předpisy Rady

(2001/264/ES)

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o založení Evropského společenství, a zejména na čl. 207 odst. 3 této smlouvy,

s ohledem na rozhodnutí Rady 2000/396/ES, ESUO, Euratom ze dne 5. června 2000, kterým se přijímá jednací řád Rady [1], a zejména na článek 24 uvedeného rozhodnutí,

vzhledem k těmto důvodům:

(1) Aby Rada mohla vyvíjet činnost v oblastech, které vyžadují určitý stupeň utajení, je vhodné zavést komplexní bezpečnostní systém, který se bude vztahovat na Radu, její generální sekretariát a členské státy.

(2) Tento systém musí v jediném textu spojovat úpravu uvedenou ve všech dřívějších rozhodnutích a předpisech přijatých v této oblasti.

(3) V praxi se bude většina skutečností v EU se stupněm utajení „CONFIDENTIEL UE“ a vyšším týkat společné bezpečnostní a obranné politiky.

(4) Aby byla zajištěna účinnost takto vytvořeného bezpečnostního systému, měly by se členské státy účastnit jeho fungování tím, že přijmou vnitrostátní opatření nezbytná pro dodržování tohoto rozhodnutí pro případy, kdy jejich příslušné orgány a úředníci nakládají s utajovanými skutečnostmi EU.

(5) Rada vítá záměr Komise zavést ke dni použitelnosti tohoto rozhodnutí komplexní systém odpovídající přílohám tohoto rozhodnutí s cílem zajistit řádný chod rozhodovacích postupů v Unii.

(6) Rada upozorňuje, jak je důležité, aby se Evropský parlament a Komise případně připojily k plnění předpisů a norem pro zachování důvěrnosti, které jsou nezbytné pro ochranu zájmů Unie a jejích členských států.

(7) Toto rozhodnutí je přijato, aniž je dotčen článek 255 Smlouvy a akty jej provádějící.

(8) Toto rozhodnutí je přijato, aniž jsou dotčeny platné postupy členských států v oblasti informování jejich parlamentů o činnostech Unie,

ROZHODLA TAKTO:

Článek 1

Schvalují se bezpečnostní předpisy Rady uvedené v příloze.

Článek 2

1. Generální tajemník/vysoký představitel přijme vhodná opatření, aby zajistil, že při nakládání s utajovanými skutečnostmi EU budou v generálním sekretariátu Rady (dále jen „GSR“) úředníci a jiní zaměstnanci GSR, externí smluvní partneři GSR a personál přidělený ke GSR dodržovat předpisy uvedené v článku 1, a rovněž aby zajistil jejich dodržování v objektech Rady a v rámci decentralizovaných subjektů EU [2].

[1] Úř. věst. L 149, 23.6.2000, s. 21.

[2] Viz závěry Rady ze dne 10. listopadu 2000.

2. Členské státy přijmou v souladu s vnitrostátními předpisy vhodná opatření, aby zajistily, že při nakládání s utajovanými skutečnostmi EU budou v rámci útvarů a v objektech členských států dodržovat předpisy uvedené v článku 1

a) členové stálých zastoupení členských států při Evropské unii i členové jejich delegací, kteří se účastní zasedání Rady nebo jejích útvarů nebo kteří se účastní jiných činností Rady;

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

c) externí smluvní partneři členských států a přidělený personál, kteří nakládají s utajovanými skutečnostmi EU.

Členské státy neprodleně uvědomí GSR o přijatých opatřeních.

3. Opatření uvedená v odstavcích 1 a 2 budou přijata do 30. listopadu 2001.

Článek 3

Při dodržování základních zásad a minimálních bezpečnostních norem uvedených v části 1 přílohy může generální tajemník, vysoký představitel přijmout opatření v souladu s částí II oddílem 1 body 1 a 2 přílohy.

Článek 4

Toto rozhodnutí nahrazuje ode dne své použitelnosti

a) rozhodnutí Rady 98/319 ES ze dne 27. dubna 1998, o postupech, kterými lze povolit úředníkům a jiným zaměstnancům generálního sekretariátu Rady přístup k utajovaným informacím v držení Rady [1];

b) rozhodnutí generálního tajemníka, vysokého představitele ze dne 27. července 2000 o opatřeních na ochranu utajovaných skutečností použitelných pro generální sekretariát Rady [2];

c) rozhodnutí 433/97 generálního tajemníka Rady ze dne 22. května 1997 o postupu bezpečnostních prověrek úředníků odpovědných za provoz sítě Cortesy.

Článek 5

1. Toto rozhodnutí vstupuje v platnost prvním dnem po zveřejnění.

2. Je použitelné ode dne 1. prosince 2001.

V Bruselu dne 19. března 2001.

Za Radu

předsedkyně

A. LINDH

[1] Úř. věst. L 140, 12.5.1998, s. 12.
[2] Úř. věst. C 239, 23.8.2000, s. 1.

PŘÍLOHA

BEZPEČNOSTNÍ PŘEDPISY RADY EVROPSKÉ UNIE

OBSAH

Strana

Přílohy

ČÁST I

ZÁKLADNÍ ZÁSADY A MINIMÁLNÍ BEZPEČNOSTNÍ NORMY

ÚVOD

1. Tato ustanovení vymezují základní zásady a minimální bezpečnostní normy, které musí Rada, generální sekretariát Rady (dále jen „GSR“), členské státy a decentralizované subjekty Evropské unie (dále jen „decentralizované subjekty EU“) odpovídajícím způsobem dodržovat tak, aby byla zajištěna bezpečnost a aby měl každý jistotu, že byly vytvořeny společné normy ochrany.

2. „Utajovanými skutečnostmi EU“ se rozumí jakýkoli materiál a informace, jejichž neoprávněné vyzrazení by mohlo na různých stupních ohrozit zájmy EU nebo zájmy jednoho či více členských států nezávisle na tom, zda tyto informace pocházejí z EU nebo z členských států, třetích států nebo mezinárodních organizací.

3. Ve zmíněných předpisech se rozumí:

   a) „dokumentem“ 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;

   b) „materiálem“ dokumenty vymezené v písmenu a) a všechny již vyrobené nebo vyráběné součásti výzbroje nebo zbraně.

4. Zajištění bezpečnosti má tyto základní cíle:

   a) ochrana utajovaných skutečností EU před špionáží, zneužitím nebo nepovoleným sdělením;

   b) ochrana utajovaných skutečností EU, které jsou používané v komunikačních a informačních systémech a sítích, před ohrožením jejich celistvosti a dostupnosti;

   c) ochrana zařízení, v nichž jsou skutečnosti EU uloženy, před pokusy o sabotáž a úmyslnými snahami o poškození;

   d) v případě selhání zhodnotit způsobenou škodu, omezit její důsledky a přijmout nezbytná nápravná opatření.

5. Základem pro zajištění spolehlivé bezpečnosti jsou:

   a) vnitrostátní bezpečnostní organizace v každém členském státu zajišťující:

      i) sběr a záznam informací o špionáži, sabotáži, terorismu a jiných podvratných činnostech a

      ii) poskytování informací vládě a jejím prostřednictvím Radě o povaze ohrožení bezpečnosti a poskytování rad o prostředcích pro ochranu před ním;

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

   c) pravidelná spolupráce mezi úředními útvary, zařízeními a příslušnými útvary GSR s cílem určit:

      i) skutečnosti, zdroje a zařízení, která mají být chráněna, a

      ii) společné normy ochrany.

6. Tam, kde se jedná o utajení, 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 skutečností a materiálu, které mají být chráněny. S cílem zajistit řádný tok informací musí být přijata opatření, aby nedošlo ke stanovení příliš vysokého stupně utajení. Klasifikační systém 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 body v těchto zařízeních.

ZÁKLADNÍ ZÁSADY

7. **Bezpečnostní opatření:**

a) se musí vztahovat na všechny osoby, které mají přístup k utajovaným skutečnostem, k prostředkům přenosu utajovaných skutečností, do všech objektů 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 potřebují skutečnosti konzultovat a jsou k tomu oprávněny) všech skutečností, utajovaných či nikoli a zejména skutečností uložených, zpracovávaných nebo přenášených v elektromagnetické formě.

ORGANIZACE BEZPEČNOSTI

Minimální společné normy

8. Rada a každý členský stát musí zajistit, aby všechny správní nebo úřední útvary, jiné instituce, subjekty a smluvní partneři EU dodržovaly společné minimální normy bezpečnosti a aby tak utajované skutečnosti EU mohly být předávány s důvěrou, že zmíněné orgány s nimi budou nakládat se stejnou péčí. Tyto minimální normy musí obsahovat kritéria pro prověřování personálu a opatření, která mají být přijata pro ochranu utajovaných skutečností EU.

BEZPEČNOSTNÍ OPATŘENÍ TÝKAJÍCÍ SE PERSONÁLU

Bezpečnostní prověrky

9. Všechny osoby, které mají mít přístup k utajovaným skutečnostem se stupněm utajení 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;

c) by mohla ustoupit tlakům ze zahraničních nebo jiných zdrojů, např. z důvodu jejího dřívějšího bydliště nebo vztahů z minulosti, které by mohly vytvářet bezpečnostní riziko.

Zvláštní pozornost musí být věnována provádění prověrek osob, které:

d) mají mít přístup k informacím se stupněm utajení TRÈS SECRET UE/EU TOP SECRET;

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

f) mají z důvodu své funkce zvláštní přístup k významným 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 vyšetřování dřívějšího chování.

10. 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.

Záznamy o prověrkách personálu

11. Všechny útvary, subjekty nebo zařízení, kde se nakládá s utajovanými skutečnostmi EU nebo kde jsou instalovány klíčové 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. Záznamy o prověrkách vede bezpečnostní šéf daného útvaru, orgánu nebo zařízení.

Bezpečnostní školení personálu

12. 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. Je užitečné vyžadovat, aby tyto osoby písemně potvrdily, že plně chápou bezpečnostní předpisy, které se vztahují na jejich postavení.

Odpovědnost vedoucích pracovníků

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

Bezpečnostní status personálu

14. 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 ke klíčovým komunikačním nebo informačním systémům, a uvědomit příslušné orgány. Zjistí-li se, že tato osoba představuje bezpečnostní riziko, bude odvolána nebo vyřazena z plnění úkolů, při kterém by mohla ohrožovat bezpečnost.

FYZICKÁ BEZPEČNOST

Potřeba ochrany

15. 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. Je tedy třeba vyhnout se stanovení příliš vysokého nebo naopak příliš nízkého stupně utajení a udělený stupeň utajení pravidelně kontrolovat. Všichni držitelé utajovaných skutečností EU se řídí jednotnými pravidly klasifikace a dodržují společné standardy ochrany týkající se opatrování, přenosu a ničení informací a materiálů vyžadujících ochranu.

Kontrola

16. 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.

Bezpečnost budov

17. Budovy, v nichž se nacházejí utajované skutečnosti EU nebo klíčové 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 pro odhalování neoprávněného vniknutí a hlídací psi) závisí na:

a) klasifikaci, objemu a umístění chráněných informací a materiálů v budově;

b) kvalitě bezpečnostních schránek obsahujících informace a materiály;

c) technických vlastnostech a umístění budovy.

18. 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.

Nouzové plány

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

BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ (INFOSEC)

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

OCHRANA PROTI SABOTÁŽI A JAKÝMKOLI JINÝM FORMÁM ÚMYSLNÉHO POŠKOZENÍ

21. 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.

PŘEDÁVÁNÍ UTAJOVANÝCH SKUTEČNOSTÍ TŘETÍM STÁTŮM NEBO MEZINÁRODNÍM ORGANIZACÍM

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

23. Získá-li Rada 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.

24. Výše zmíněné zásady se uplatňují v souladu s podrobnými ustanoveními uvedenými v části II.

ČÁST II

ODDÍL I

ORGANIZACE BEZPEČNOSTI V RADĚ EVROPSKÉ UNIE

Generální tajemník/vysoký představitel

1. Generální tajemník/vysoký představitel:

   a) uplatňuje bezpečnostní politiku Rady;

   b) posuzuje bezpečnostní obtíže, které mu předkládá Rada 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 Rady. Příloha 1 obsahuje seznam těchto orgánů.

2. Generální tajemník/vysoký představitel je pověřen zejména:

   a) koordinovat všechny bezpečnostní otázky související s činností Rady;

   b) požadovat, aby každý členský stát vytvořil ústřední rejstřík TRÈS SECRET UE/EU TOP SECRET, a požadovat vytvoření tohoto rejstříku případně v decentralizovaných subjektech EU;

   c) požadovat od vnitrostátních bezpečnostních orgánů členských států, aby zajišťovaly bezpečnostní pověrky personálu zaměstnaného v GSR v souladu s oddílem VI;

   d) vyšetřovat nebo nechat vyšetřit úniky utajovaných skutečností EU, pokud se zdá, že k nim došlo v GSR nebo v některém z decentralizovaných subjektů EU;

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

   f) pravidelně posuzovat bezpečnostní opatření přijatá pro ochranu utajovaných skutečností EU v členských státech ve spolupráci s příslušnými vnitrostátními bezpečnostními orgány a po dohodě s nimi;

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

   h) trvale posuzovat bezpečnostní politiku a bezpečnostní postupy Rady a případně připravovat vhodná doporučení. V této souvislosti předkládá Radě roční plán inspekcí zpracovaný bezpečnostní kanceláří GSR.

Bezpečnostní výbor Rady

3. Zřizuje se Bezpečnostní výbor. Tvoří jej zástupci vnitrostátních bezpečnostních orgánů z každého členského státu. Předsedá mu generální tajemník/vysoký představitel nebo jím pověřená osoba. Zástupci decentralizovaných subjektů EU mohou být rovněž vyzváni, aby se účastnili zasedání, jestliže se jich týkají projednávané otázky.

4. Bezpečností výbor se schází podle pokynů Rady na žádost generálního tajemníka/vysokého představitele nebo některého vnitrostátního bezpečnostního orgánu. Výbor je příslušný posuzovat a hodnotit všechny bezpečnostní otázky související s prací Rady a předkládat jí případně doporučení. Jde-li o činnost GSR, je výbor zmocněn podávat doporučení generálnímu tajemníkovi/vysokému představiteli k bezpečnostním otázkám.

Bezpečnostní kancelář generálního sekretariátu Rady

5. Pro plnění odpovědností uvedených v odstavcích 1 a 2 má generální tajemník/vysoký představitel k dispozici bezpečnostní kancelář, která koordinuje bezpečnostní opatření, dohlíží na ně a provádí je.

6. Vedoucí bezpečnostní kanceláře GSR je hlavním poradcem generálního tajemníka/vysokého představitele v bezpečnostních otázkách a zajišťuje funkci sekretariátu Bezpečnostního výboru. V této souvislosti řídí aktualizaci bezpečnostních předpisů a koordinuje bezpečnostní opatření s příslušnými orgány členských států a případně s mezinárodními organizacemi spojenými s Radou prostřednictvím bezpečnostních dohod. Vykonává při tom úlohu styčného důstojníka.

7. Vedoucí bezpečnostní kanceláře GSR odpovídá za schvalování systémů a sítí IT v rámci GSR. Vedoucí bezpečnostní kanceláře GSR a dotčené vnitrostátní bezpečnostní orgány rozhodují podle potřeby společně o povolení systémů a sítí IT, v nichž jsou zapojeny GSR, členské státy, decentralizované subjekty EU nebo třetí osoby (státy nebo mezinárodní organizace).

Decentralizované subjekty EU

8. Každý ředitel decentralizovaného subjektu EU odpovídá za dodržování bezpečnostních předpisů ve svém subjektu. Obvykle pověří některého ze svých pracovníků, který bude odpovídat za tuto oblast. Tato osoba je označena jako bezpečnostní úředník.

Členské státy

9. Každý členský stát určí vnitrostátní bezpečnostní orgán odpovědný za bezpečnost utajovaných skutečností EU ([1]).

10. V rámci správní struktury každého členského státu odpovídá příslušný vnitrostátní bezpečnostní orgán za:

    a) dodržování bezpečnosti utajovaných skutečností EU držených jakýmikoli veřejnými nebo soukromými vnitrostátními útvary, subjekty nebo zařízeními, doma nebo v cizině;

    b) povolení vytvoření spisoven TRÈS SECRET UE/EU TOP SECRET (tato pravomoc může být přenesena na kontrolního úředníka pro skutečnosti TRÈS SECRET UE/EU TOP SECRET ústřední spisovny);

    c) pravidelnou kontrolu bezpečnostních opatření na ochranu utajovaných skutečností EU;

    d) zajištění, aby všechen vnitrostátní personál i cizí příslušníci zaměstnaní ve vnitrostátních útvarech, subjektech nebo zařízeních, kteří mohou mít přístup k utajovaným skutečnostem EU se stupněm utajení TRÈS SECRET UE/EU TOP SECRET, SECRET UE a CONFIDENTIEL UE, prošli bezpečnostními prověrkami;

    e) sestavení nezbytných bezpečnostních plánů, aby se předešlo tomu, že se utajované skutečnosti EU dostanou do neoprávněných rukou.

Vzájemné bezpečnostní kontroly

11. Bezpečnostní kancelář GSR a příslušný vnitrostátní bezpečnostní orgán uskutečňují společně a na základě vzájemné dohody pravidelné kontroly předpisů přijatých pro ochranu utajovaných skutečností EU uvnitř GSR a stálých zastoupení členských států při Evropské unii a uvnitř objektů vyhrazených členským státům v budovách Rady ([2]).

12. Pravidelné kontroly ustanovení přijatých na ochranu utajovaných skutečností EU v decentralizovaných subjektech EU provádí bezpečnostní kancelář GSR nebo na žádost generálního tajemníka/vysokého představitele vnitrostátní bezpečnostní orgán hostitelského členského státu.

([1]) Seznam vnitrostátních bezpečnostních orgánů odpovědných za bezpečnost utajovaných skutečností EU je uveden v příloze 1.
([2]) Aniž je dotčena Vídeňská úmluva o diplomatických vztazích z roku 1961.

ODDÍL II

KLASIFIKACE A OZNAČENÍ

STUPNĚ KLASIFIKACE ([1])

Skutečnosti jsou klasifikovány podle těchto stupňů:

1. TRÈS SECRET UE/EU TOP SECRET: tento stupeň se použije výlučně pro informace a materiály, jejichž neoprávněné vyzrazení by mohlo výjimečně závažně poškodit základní zájmy Evropské unie nebo jednoho či více členských států.

2. 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.

3. 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.

4. 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.

OZNAČENÍ

5. K upřesnění oblasti, které se týká daný dokument, nebo k označení zvláštního rozšiřování na základě „potřeby vědět“ lze používat výstražné označení.

6. Označení ESDP/PESD 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.

7. Některé dokumenty, zejména ty, které se vztahují na systémy informačních technologií (IT), mohou nést další označení spojená s doplňujícími bezpečnostními opatřeními vymezenými v příslušných předpisech.

UVÁDĚNÍ KLASIFIKACE A OZNAČENÍ

8. Klasifikace a označení se uvádějí takto:

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

   b) na dokumentech se stupněm utajení CONFIDENTIEL UE mechanickými prostředky a ručně nebo vytištěním na předem orazítkovaný a registrovaný papír;

   c) na dokumentech se stupněm utajení SECRET UE a TRÈS SECRET UE/EU TOP SECRET mechanickými prostředky a ručně.

([1]) Srovnávací tabulka bezpečnostní klasifikace EU, NATO, ZEU a členských států je uvedena v příloze 2.

ODDÍL III

PRAVIDLA KLASIFIKACE

1. Skutečnosti se klasifikují pouze, je-li to nezbytné. Klasifikace je jasně a řádně vyznačena a trvá pouze po dobu, po kterou skutečnost vyžaduje ochranu.

2. Odpovědnost za klasifikaci skutečností a za jakékoli následné snížení klasifikace nebo za odtajnění [1] má výlučně původce dokumentu.

   Úředníci a jiní zaměstnanci GSR klasifikují skutečnosti, snižují jejich klasifikaci nebo je odtajňují na pokyn svého generálního ředitele nebo s jeho souhlasem.

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

4. Počet osob oprávněných vypracovat dokumenty TRÈS SECRET UE/EU TOP SECRET musí být omezen na přísné minimum a jména těchto osob musí být uvedena na seznamu vytvořeném GSR, jednotlivými členskými státy a případně jednotlivými decentralizovanými subjekty EU.

UPLATNĚNÍ KLASIFIKACÍ

5. Klasifikace dokumentu se stanoví podle úrovně citlivosti jeho obsahu v souladu s definicemi v bodech 1 až 4 oddílu II. Klasifikaci je nutno používat správně a střídmě. To se týká zvláště klasifikace TRÈS SECRET UE/EU TOP SECRET.

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

   Jestliže používání vysokého stupně utajení může na první pohled zdánlivě zajišťovat větší ochranu dokumentů, může pak systematické přidělování příliš vysokého stupně utajení vést ke ztrátě důvěry v platnost klasifikačního systému.

   Na druhé straně by přání vyhnout se omezením spojeným s ochranou nemělo vést ke stanovení příliš nízkého stupně utajení.

   Praktické vodítko pro stanovení stupně utajení je obsaženo v příloze 3.

7. Stránky, odstavce, oddíly, přílohy, dodatky a připojené části dokumentu mohou vyžadovat různou klasifikaci a musí být podle toho označeny. Klasifikace dokumentu jako celku je stanovena podle části s nejvyšší klasifikací.

8. Klasifikace průvodního dopisu nebo sdělení k připojeným částem musí být stejně vysoká jako nejvyšší klasifikace těchto částí. Původce jasně uvede jejich stupeň klasifikace, pokud budou odděleny od připojených částí.

SNÍŽENÍ KLASIFIKACE A ODTAJNĚNÍ

9. Klasifikace utajovaného dokumentu EU může být snížena a dokument lze odtajnit pouze se souhlasem jeho původce a, je-li to nezbytné, po konzultaci ostatních zúčastněných stran. Snížení klasifikace nebo odtajnění musí být potvrzeno písemně. Instituce, členský stát, kancelář, nástupnická organizace nebo nadřízený orgán, kteří jsou autoři dokumentu, musí uvědomit své příjemce o změně klasifikace a příjemci jsou povinni na to upozornit další příjemce, kterým předali originál dokumentu nebo jeho kopii.

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

---

[1] Snížením klasifikace se rozumí snížení stupně klasifikace; odtajněním se rozumí odstranění jakékoli klasifikace.

ODDÍL IV

FYZICKÁ BEZPEČNOST

OBECNĚ

1. Hlavním cílem fyzických bezpečnostních opatření je zabránit neoprávněným osobám získat přístup k utajovaným informacím nebo materiálům EU.

BEZPEČNOSTNÍ POŽADAVKY

2. 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.

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

   a) ke klasifikaci 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 nebo jiné instituce nebo třetí osoby, které disponují utajovanými skutečnostmi EU, zejména sabotáže, terorismu a jiné podvratné nebo trestné činnosti.

4. Cílem použitých fyzických bezpečnostních opatření je:

   a) zabránit lstivému nebo násilnému vniknutí;

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

   c) bránit úředníkům a jiným zaměstnancům GSR, úředních útvarů členských států nebo ostatních institucí nebo třetích osob, kteří nemají „potřebu vědět“, v přístupu k utajovaným skutečnostem EU.

FYZICKÁ BEZPEČNOSTNÍ OPATŘENÍ

Bezpečnostní oblasti

5. Oblasti, kde jsou zpracovávány a uloženy skutečnosti se stupněm utajení 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 uloženy skutečnosti se stupněm utajení 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;

      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 uloženy skutečnosti se stupněm utajení CONFIDENTIEL UE nebo vyšším takovým způsobem, že je možné chránit je před přístupem neoprávněných osob prostředky vnitřní kontroly, např. objekty, v nichž jsou umístěny kanceláře, kde jsou pravidelně zpracovávány a uloženy skutečnosti se stupněm utajení 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.

Administrativní oblast

6. 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 RESTREINT UE.

Kontroly vstupů a výstupů

7. Vstup do bezpečnostních oblastí kategorií I a II je kontrolován systémem propustek nebo osobní identifikace pro stálý personál. 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.

Pochůzky

8. 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 dvě hodiny.

Bezpečnostní schránky a trezory

9. Pro uchovávání utajovaných skutečností EU se používají tři kategorie schránek:

— kategorie A: schránky schválené vnitrostátními normami pro uchovávání skutečností se stupněm utajení TRÈS SECRET UE/EU TOP SECRET v bezpečnostní oblasti kategorie I nebo II,

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

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

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

Zámky

11. 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.

Kontrola klíčů a kombinací

12. Klíče od bezpečnostních schránek nesmějí být vynášeny mimo budovu. Kombinace se naučí zpaměti pouze osoby, které je potřebují znát. Bezpečnostní úředník zúčastněného subjektu 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.

13. 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.

Zařízení pro odhalování vniknutí

14. 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.

Schválené vybavení

15. Vnitrostátní bezpečnostní orgány musí samy nebo společně s orgány jiné země aktualizovat seznamy, vedené podle typu a modelu, bezpečnostního vybavení, které schválily k přímé nebo nepřímé ochraně utajovaných skutečností za různých okolností a podmínek, které budou upřesněny. Bezpečnostní kancelář GSR musí aktualizovat srovnatelný seznam založený mimo jiné na informacích poskytovaných vnitrostátními bezpečnostními orgány. Decentralizované subjekty EU konzultují před nákupem vybavení bezpečnostní kancelář GSR a případně vnitrostátní bezpečnostní orgány hostitelského členského státu.

Fyzická ochrana kopírovacích zařízení a faxů

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

OCHRANA PROTI NAHLÉDNUTÍ A ODPOSLECHU

Nahlédnutí

17. 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.

Odposlech

18. Kanceláře nebo oblasti, ve kterých se pravidelně projednávají utajované skutečnosti se stupněm utajení SECRET UE nebo vyšším, musí být, odůvodňuje-li to riziko, chráněny před pokusy o pasivní a aktivní odposlech. Hodnocení rizika odposlechů provádí příslušný bezpečnostní orgán případně po konzultaci vnitrostátního bezpečnostního orgánu.

19. Pro stanovení ochranných opatření, která mají být přijata v citlivých objektech proti pasivnímu odposlechu (např. izolace stěn, dveří, podlah a stropů, měření vycházejícího hluku) a aktivnímu odposlechu (např. pátrání po mikrofonech), může bezpečnostní kancelář GSR požádat o podporu odborníky z vnitrostátního bezpečnostního orgánu. Bezpečnostní úředníci decentralizovaných subjektů EU mohou požádat bezpečnostní kancelář GSR, aby prováděla technické kontroly, nebo požádat o podporu odborníky z vnitrostátního bezpečnostního orgánu.

20. Podobně mohou odborníci na bezpečnostní techniku vnitrostátních bezpečnostních orgánů na žádost příslušného bezpečnostního úředníka ověřovat telekomunikační zařízení a elektrická nebo elektronická kancelářská zařízení jakéhokoli druhu používaná při zasedáních se stupněm utajení SECRET UE a vyšším, vyžadují-li to okolnosti.

TECHNICKY CHRÁNĚNÉ OBLASTI

21. 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.

22. Musí se vést podrobný inventář 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 je třeba zamezit instalaci komunikačních linek do technicky chráněných oblastí.

ODDÍL V

OBECNÁ PRAVIDLA TÝKAJÍCÍ SE ZÁSADY „POTŘEBA VĚDĚT“ A BEZPEČNOSTNÍCH PROVĚREK

1. 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 TRÈS SECRET UE/EU TOP SECRET, SECRET UE a CONFIDENTIEL UE je povolen pouze osobám, které prošly příslušnou bezpečnostní prověrkou.

2. „Potřebu vědět“ určuje GSR, decentralizované subjekty EU a útvary členského státu, ve kterém osoba vykonává své funkce, s ohledem na požadavky těchto funkcí.

3. Za bezpečnostní prověrky personálu odpovídá zaměstnavatel úředníka postupy použitelnými v této oblasti. Postup prověrek úředníků a jiných zaměstnanců GSR je stanoven v oddíle VI.

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

   Bezpečnostní osvědčení daného stupně může držiteli umožnit přístup ke skutečnostem nižšího stupně.

4. Jiné osoby než úředníci nebo jiní zaměstnanci GSR nebo členských států (např. členové, úředníci nebo zaměstnanci orgánů EU), s nimiž může být nezbytné posuzovat nebo konzultovat utajované skutečnosti EU, musí mít bezpečnostní prověrku umožňující přístup k utajovaným skutečnostem EU a musí být poučeni o své odpovědnosti v oblasti bezpečnosti. Stejné pravidlo se uplatňuje za obdobných podmínek pro externí smluvní partnery, odborníky nebo konzultanty.

ZVLÁŠTNÍ PRAVIDLA PRO PŘÍSTUP KE SKUTEČNOSTEM SE STUPNĚM UTAJENÍ TRÈS SECRET UE/EU TOP SECRET

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

6. Všechny osoby, které potřebují získat přístup ke skutečnostem se stupněm utajení TRÈS SECRET UE/EU TOP SECRET, určí jmenovitě vedoucí jejich útvaru a jejich jména jsou vedena v příslušném rejstříku skutečností TRÈS SECRET UE/EU TOP SECRET.

7. Všechny osoby oprávněné k přístupu ke skutečnostem se stupněm utajení TRÈS SECRET UE/EU TOP SECRET musí nejprve podepsat potvrzení, že byly poučeny o bezpečnostních postupech Rady a že plně chápou svou zvláštní odpovědnost za ochranu skutečností TRÈS 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.

8. U osob, které mají přístup ke skutečnostem se stupněm utajení TRÈS 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 TRÈS SECRET UE/EU TOP SECRET.

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

ZVLÁŠTNÍ PRAVIDLA PRO PŘÍSTUP KE SKUTEČNOSTEM SE STUPNĚM UTAJENÍ SECRET UE A CONFIDENTIEL UE

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

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

12. V případě osob, které mají přístup ke skutečnostem se stupněm utajení SECRET UE nebo CONFIDENTIEL UE v průběhu zasedání atd., musí příslušný kontrolní úředník útvaru nebo subjektu, kde jsou zaměstnány, upozornit útvar, který zasedání pořádá, že jsou oprávněny k přístupu k těmto skutečnostem.

ZVLÁŠTNÍ PRAVIDLA PRO PŘÍSTUP K INFORMACÍM SE STUPNĚM UTAJENÍ RESTREINT UE

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

PŘEVODY

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

ZVLÁŠTNÍ POKYNY

15. 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;

    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.

16. 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.

17. Neexistují bezpečnostní předpisy Rady pro soukromé cesty, a to nezávisle na jejich cíli, personálu zmocněného pro přístupu k utajovaným skutečnostem EU. Příslušné bezpečnostní orgány však seznámí úředníky a jiné zaměstnance spadající do jejich pravomoci s předpisy platnými pro cestování, které by se jich mohly týkat. Bezpečnostní úředníci odpovídají za organizaci schůzek dotčeného personálu k osvěžení znalostí příslušných zvláštních pokynů.

ODDÍL VI

BEZPEČNOSTNÍ PROVĚRKY ÚŘEDNÍKŮ A JINÝCH ZAMĚSTNANCŮ GSR

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

2. Pro přístup k utajovaným skutečnostem se stupněm utajení „TRÈS SECRET UE/EU TOP SECRET, SECRET UE a CONFIDENTIEL UE“ musí všechny osoby uvedené v bodu 1 nejprve získat oprávnění pro tento účel postupem podle bodů 4 a 5.

3. Oprávnění se uděluje pouze osobám, které prošly bezpečnostní prověrkou příslušných vnitrostátních orgánů členských států postupem podle bodů 6 až 10.

4. Orgán oprávněný ke jmenování ve smyslu čl. 2 prvního pododstavce pracovního řádu odpovídá za udělování oprávnění podle odstavců 1, 2 a 3.

   Orgán oprávněný ke jmenování udělí oprávnění po převzetí stanoviska příslušných vnitrostátních orgánů členských států na základě bezpečnostní prověrky provedené v souladu s body 6 až 12.

5. Oprávnění, které má dobu platnosti pět let, nesmí být uděleno na dobu delší než je doba výkonu funkcí odůvodňujících jeho udělení. Orgán oprávněný ke jmenování může jeho platnost prodloužit postupem podle bodu 4.

   Orgán oprávněný ke jmenování 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 orgánem oprávněným ke jmenování, a rovněž příslušnému vnitrostátnímu orgánu.

6. Cílem bezpečnostních šetření je zjistit, zda neexistují námitky, aby daná osoba mohla mít přístup k utajovaným skutečnostem v držení Rady.

7. Bezpečnostní šetření provádí s pomocí dotčené osoby a na žádost orgánu oprávněného ke jmenování příslušné vnitrostátní orgány členského státu, jehož je osoba, které má být uděleno oprávnění, příslušníkem. Pokud má dotčená osoba bydliště na území jiného členského státu, mohou dotčené vnitrostátní orgány zajistit spolupráci orgánů státu místa bydliště.

8. V rámci šetření je dotčená osoba povinna vyplnit osobní prohlášení.

9. Orgán oprávněný ke jmenování 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.

10. 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.

11. Vydají-li příslušné vnitrostátní orgány členského státu kladné stanovisko, může orgán oprávněný ke jmenování udělit dotčené osobě oprávnění.

12. Vydají-li příslušné vnitrostátní orgány záporné stanovisko, oznámí se smysl tohoto stanoviska dotčené osobě, která může požádat orgán oprávněný ke jmenování o vyslechnutí. Považuje-li to orgán oprávněný ke jmenování za nezbytné, může požádat příslušné vnitrostátní orgány o doplňující vysvětlení, která tyto orgány mohou poskytnout. Je-li záporné stanovisko potvrzeno, nelze oprávnění udělit.

13. Všechny osoby oprávněné ve smyslu bodů 4 a 5 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.

14. Orgán oprávněný ke jmenování přijme všechna nezbytná opatření k provedení tohoto oddílu, zejména opatření týkající se úpravy přístupu k seznamu oprávněných osob.

15. Výjimečně a vyžaduje-li to útvar, může orgán oprávněný ke jmenování 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 7.

16. Takto udělená prozatímní a dočasná oprávnění neumožňují přístup ke skutečnostem se stupněm utajení TRÈS SECRET UE/EU TOP SECRET; přístup k nim je vyhrazen úředníkům, u nichž bylo účinně s pozitivními výsledky provedeno šetření v souladu s bodem 7. Do vydání výsledků šetření mohou úředníci, u kterých se požaduje prověrka pro stupeň TRÈS SECRET UE/EU TOP SECRET, dostat dočasné a prozatímní oprávnění pro přístup k utajovaným skutečnostem se stupněm utajení nejvýše SECRET UE včetně.

ODDÍL VII

PŘÍPRAVA, ŠÍŘENÍ, PŘENOS, ARCHIVACE A NIČENÍ UTAJOVANÝCH MATERIÁLŮ EU

Obsah

Obecná ustanovení

Tento oddíl upřesňuje opatření pro přípravu, šíření, přenos, archivaci a ničení utajovaných dokumentů EU, jak jsou vymezeny v bodu 3 písm. a) základních zásad a minimálních bezpečnostních norem v části I této přílohy. Používá se jako podklad pro přizpůsobení těchto opatření jiným utajovaným materiálům EU podle jejich typu a případ od případu.

Kapitola I

Příprava a šíření utajovaných dokumentů EU

PŘÍPRAVA

1. Jak je stanoveno v oddílu II, uvádějí se 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 TRÈS SECRET UE/EU TOP SECRET a 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 CONFIDENTIEL UE nebo vyšším musí být uveden seznam všech příloh a připojených částí.

2. Dokumenty se stupněm utajení 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 s výjimkou zvláštního případu popsaného v bodu 27 tohoto oddílu.

   Ustanovení pro zpracování utajovaných dokumentů s využitím výpočetní techniky jsou uvedena v oddílu XI.

ŠÍŘENÍ

3. Utajované skutečnosti EU lze rozšiřovat pouze osobám, které mají „potřebu vědět“ a prošly příslušnou bezpečnostní prověrkou. Počáteční šíření upřesní původce dokumentu.

4. Dokumenty se stupněm utajení TRÈS SECRET UE/EU TOP SECRET se rozšiřují prostřednictvím spisoven TRÈS SECRET UE/EU TOP SECRET (viz oddíl VIII). V případě sdělení se stupněm utajení TRÈS SECRET UE/EU TOP SECRET může příslušná spisovna pověřit vedoucího střediska komunikace, aby připravil počet kopií odpovídající seznamu příjemců.

5. Dokumenty se stupněm utajení 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.

6. Všechny dokumenty se stupněm utajení CONFIDENTIEL UE a vyšším zaznamenává při příchodu a při odchodu spisovna subjektu. Do knihy nebo na speciálně chráněné nosiče dat se zaznamenávají údaje (spisové číslo, datum a případně číslo výtisku), které umožňují dokumenty identifikovat.

Kapitola II

Přenos utajovaných dokumentů EU

BALENÍ

7. Dokumenty se stupněm utajení CONFIDENTIEL EU 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.

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

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

10. Vnitřní obálka je uzavřena do vnější obálky označené číslem zásilky pro účely převzetí. Za žádných okolností se na vnější obálce nesmí objevit bezpečnostní klasifikace.

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

PŘENOS UVNITŘ BUDOVY NEBO SKUPINY BUDOV

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

PŘENOS DOKUMENTŮ EU UVNITŘ ZEMĚ

13. Uvnitř jedné země jsou dokumenty se stupněm utajení TRÈS SECRET UE/EU TOP SECRET přenášeny výlučně prostřednictvím oficiální kurýrní služby nebo osobami oprávněnými k přístupu ke skutečnostem se stupněm utajení TRÈS SECRET UE/EU TOP SECRET.

14. Kdykoli se pro přenos dokumentu se stupněm utajení TRÈS SECRET UE/EU TOP SECRET mimo rámec budovy nebo skupiny budov použije kurýrní služba, uplatní se ustanovení o balení a potvrzování příjmu uvedená v této kapitole. Kurýrní služby mají takový personál, aby bylo zajištěno, že balíčky obsahující dokumenty TRÈS SECRET UE/EU TOP SECRET zůstanou pod přímým a stálým dohledem odpovědné osoby.

15. Výjimečně mohou dokumenty se stupněm utajení TRÈS 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 TRÈS SECRET UE/EU TOP SECRET;

    b) způsob dopravy vyhovuje vnitrostátním pravidlům, kterými se řídí přenos vnitrostátních dokumentů se stupněm utajení TOP SECRET;

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

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

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

17. Každý členský stát nebo decentralizovaný subjekt EU vypracuje na základě těchto předpisů 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 IV;

    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.

PŘENOS Z JEDNOHO ČLENSKÉHO STÁTU DO JINÉHO

18. Materiál se stupněm utajení CONFIDENTIEL UE a vyšším je přenášen z jednoho členského státu do jiného diplomatickou nebo vojenskou kurýrní službou.

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

20. Vnitrostátní bezpečnostní orgány mohou 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. Každý členský stát vypracuje pokyny pro mezinárodní přepravu materiálu se stupněm utajení SECRET UE včetně jinými osobami než jsou diplomatičtí a vojenští kurýři. Tyto pokyny vyžadují, aby:

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

b) všechny takto přenášené materiály byly zaznamenány v příslušné kanceláři 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 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 ustanovení týkající se cesty předpisům EU nebo, jsou-li přísnější, vnitrostátním předpisům;

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

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;

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

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.

PŘENOS DOKUMENTŮ SE STUPNĚM UTAJENÍ RESTREINT UE

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

BEZPEČNOST PERSONÁLU KURÝRNÍCH SLUŽEB

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

Kapitola III

Přenos elektrickými a jinými technickými prostředky

23. 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 XI.

24. Skutečnosti se stupněm utajení CONFIDENTIEL UE a SECRET UE mohou přenášet pouze schválená přenosová centra a sítě nebo terminály a systémy.

Kapitola IV

Doplňkové výtisky a překlady a výpisy z utajovaných dokumentů EU

25. Kopírování nebo překlady dokumentů se stupněm utajení TRÈS SECRET UE/EU TOP SECRET může povolit pouze původce dokumentu.

26. Jestliže osoby, které neprošly bezpečnostní prověrkou pro stupeň utajení TRÈS SECRET UE/EU TOP SECRET, potřebují informace obsažené v dokumentu se stupněm utajení TRÈS SECRET UE/EU TOP SECRET, které však samy takto klasifikovány nejsou, může být vedoucí spisovny TRÈS SECRET UE/EU TOP SECRET pověřen vytvořit potřebný počet výpisů z daného dokumentu. Vedoucí zároveň přijme potřebná opatření, aby těmto výpisům byl přidělen odpovídající stupeň utajení.

27. Dokumenty se stupněm utajení SECRET UE a nižším může rozmnožovat a překládat příjemce v souladu s vnitrostátními bezpečnostními předpisy a za podmínky, že přísně dodržuje zásadu „potřeba vědět". Bezpečnostní opatření použitelná pro původní dokument se rovněž uplatňují pro reprodukce nebo překlady dokumentu. Decentralizované subjekty EU rovněž dodržují tyto bezpečnostní předpisy.

Kapitola V

Inventury a kontroly, archivace a ničení utajovaných dokumentů EU

INVENTURY A KONTROLY

28. Každá spisovna TRÈS SECRET UE/EU TOP SECRET uvedená v oddíle VIII provádí každoročně podrobnou inventuru dokumentů se stupněm utajení TRÈS SECRET UE/EU TOP SECRET v souladu s předpisy uvedenými v oddíle VIII bodech 9 a 11. Utajované dokumenty EU se stupněm utajení nižším než TRÈS SECRET UE/EU TOP SECRET podléhají vnitřním kontrolám v souladu s vnitrostátními směrnicemi a v případě GSR a decentralizovaných subjektů EU v souladu s pokyny generálního tajemníka, vysokého představitele.

Cílem těchto činností je zjistit zejména stanovisko držitele:

a) ke snížení klasifikace některých dokumentů nebo k případnému odtajnění dokumentů;

b) ke zničení dokumentů.

ARCHIVACE UTAJOVANÝCH SKUTEČNOSTÍ EU

29. Aby byly obtíže s archivací co nejmenší, jsou všichni kontrolní úředníci všech spisoven oprávněni převádět dokumenty se stupněm utajení TRÈS SECRET UE/EU TOP SECRET, SECRET UE a 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 TRÈS 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 TRÈS SECRET UE/EU TOP SECRET, SECRET UE nebo CONFIDENTIEL UE;

e) převedení dokumentů se stupněm utajení TRÈS SECRET UE/EU TOP SECRET nebo 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 předpisy uvedenými v bodech 31 až 36.

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

PRAVIDELNÉ NIČENÍ UTAJOVANÝCH DOKUMENTŮ EU

31. 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 TRÈS SECRET UE/EU TOP SECRET ničí výlučně ústřední spisovna, která je tím pověřena. Každý zničený dokument je uveden v zápise o zničení podepsaném kontrolním úředníkem TRÈS SECRET UE/EU TOP SECRET a svědkem, který prošel bezpečnostní prověrkou stupně TRÈS 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 TRÈS SECRET UE/EU TOP SECRET včetně utajovaného odpadu, který vzniká při přípravě těchto dokumentů (např. poškozené výtisky, koncepty, na stroji psané poznámky a uhlový papír) se zničí pod dohledem úředníka prověřeného pro stupeň TRÈS SECRET UE/EU TOP SECRET spálením, rozdrcením, roztrháním nebo jiným způsobem tak, aby je nebylo možné identifikovat a znovu sestavit.

32. Dokumenty se stupněm utajení SECRET UE zničí spisovna, která je tím pověřená, pod dohledem osoby, jež prošla bezpečnostní prověrkou, a to jedním z postupů uvedených v bodu 31 písm. c). Zničení dokumentů se stupněm utajení SECRET UE je uvedeno v podepsaných zápisech, které spisovna archivuje spolu s doklady o rozdělení nejméně tři roky.

33. Dokumenty se stupněm utajení CONFIDENTIEL UE zničí spisovna, která je tím pověřena, pod dohledem osoby, jež prošla bezpečnostní prověrkou, jedním z postupů uvedených v bodu 31 písm. c). Jejich zničení se zaznamená v souladu s vnitrostátními předpisy a v případě GSR nebo decentralizovaných subjektů EU v souladu s pokyny generálního tajemníka, vysokého představitele.

34. Dokumenty se stupněm utajení RESTREINT UE zničí spisovna, která je tím pověřena, nebo uživatel v souladu s vnitrostátními předpisy a v případě GSR nebo decentralizovaných subjektů EU v souladu s pokyny generálního tajemníka, vysokého představitele.

ZNIČENÍ V NOUZOVÝCH SITUACÍCH

35. GSR, členské státy a decentralizované subjekty EU 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; ve svých organizacích vyhlásí pokyny, které považují za nezbytné pro zamezení tomu, aby se utajované skutečnosti EU dostaly do neoprávněných rukou.

36. Ustanovení přijatá pro zabezpečení nebo zničení materiálů se stupněm utajení SECRET UE a CONFIDENTIEL UE nesmí za žádných okolností ovlivnit zabezpečení ani zničení materiálů se stupněm utajení TRÈS SECRET UE/EU TOP SECRET, zejména kódovacího zařízení, jejichž opatrování má přednost před všemi ostatními úkoly. Opatření, která mají být přijata k zabezpečení a zničení kódovacího zařízení v případě nouze, se řídí podle pokynů vydaných pro jednotlivé případy.

KAPITOLA VI

Zvláštní pravidla pro dokumenty určené Radě

37. V rámci GSR sleduje „kancelář pro utajované skutečnosti" informace se stupněm utajení SECRET UE nebo CONFIDENTIEL UE obsažené v dokumentech Rady.

Za odpovědnosti generálního ředitele pro personální věci a administrativu tato kancelář

a) řídí operace, které se týkají záznamů, reprodukce, překladů, přenosu, odesílání a ničení takových skutečností;

b) aktualizuje rejstřík utajovaných skutečností;

c) pravidelně konzultuje původce o potřebě nadále zachovávat utajení skutečností;

d) ve spolupráci s kanceláří pro bezpečnost stanoví praktická opatření pro utajení a odtajnění skutečností.

38. Kancelář pro utajované skutečnosti vede rejstřík 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) vypracování inventářů utajovaných skutečností předložených Radě;

j) rejstřík, kde jsou zaznamenány operace odtajnění a snížení klasifikace utajovaných skutečností.

39. Na kancelář pro utajované skutečnosti GSR se vztahují obecná pravidla uvedená v kapitolách I až V tohoto oddílu, s výhradou změn vyplývajících ze zvláštních pravidel stanovených v této kapitole.

ODDÍL VIII

SPISOVNY TRÈS SECRET UE/EU TOP SECRET

1. Úlohou spisoven TRÈS SECRET UE/EU TOP SECRET je zajistit registraci dokumentů TRÈS SECRET UE/EU TOP SECRET, nakládání s nimi a jejich šíření v souladu s bezpečnostními předpisy. Vedoucí spisovny TRÈS SECRET UE/EU TOP SECRET je v jednotlivých členských státech, v GSR a v příslušných decentralizovaných subjektech EU kontrolním úředníkem TRÈS SECRET UE/EU TOP SECRET.

2. Ústřední spisovny působí jako hlavní orgán pro příjem a šíření pro členské státy, GSR a decentralizované subjekty EU, ve kterých byly tyto spisovny zřízeny, a případně rovněž pro ostatní orgány EU, mezinárodní organizace a třetí státy, s nimiž Rada 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 TRÈS SECRET UE/EU TOP SECRET; aktualizují záznamy o každém dokumentu, který mají na starosti.

4. Spisovny TRÈS SECRET UE/EU TOP SECRET nižší úrovně se zřizují, jak je uvedeno v oddílu I, aby se vyhovělo dlouhodobé potřebě, a jsou napojeny na ústřední spisovnu TRÈS SECRET UE/EU TOP SECRET. Je-li potřeba nahlížet do dokumentů se stupněm utajení TRÈS SECRET UE/EU TOP SECRET pouze dočasná a příležitostná, lze tyto dokumenty poskytnout, aniž je zřízena spisovna TRÈS SECRET UE/EU TOP SECRET nižší úrovně, pokud stanovená pravidla zajišťují, že tyto dokumenty zůstanou pod kontrolou příslušné spisovny TRÈS 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 TRÈS SECRET UE/EU TOP SECRET předávat dokumenty se stupněm utajení TRÈS SECRET UE/EU TOP SECRET přímo jiným spisovnám nižší úrovně podřízeným stejné ústřední spisovně TRÈS SECRET UE/EU TOP SECRET.

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

ÚSTŘEDNÍ SPISOVNY TRÈS SECRET UE/EU TOP SECRET

7. Jako kontrolní úředník odpovídá vedoucí spisovny TRÈS SECRET UE/EU TOP SECRET za:

   a) předávání dokumentů se stupněm utajení TRÈS SECRET UE/EU TOP SECRET v souladu s pravidly stanovenými v oddíle VII;

   b) aktualizaci seznamu všech podřízených spisoven TRÈS 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 TRÈS SECRET UE/EU TOP SECRET šířené ústřední spisovnou;

   d) vedení záznamů o držených a rozšiřovaných dokumentech se stupněm utajení TRÈS SECRET UE/EU TOP SECRET;

   e) aktualizaci seznamu všech ústředních spisoven TRÈS SECRET UE/EU TOP SECRET, s nimiž obvykle udržuje písemný styk, spolu se jmény a podpisy pověřených kontrolních úředníků a jejich oprávněných zástupců;

   f) zajištění hmotné bezpečnosti všech dokumentů se stupněm utajení TRÈS SECRET UE/EU TOP SECRET držených ve spisovně v souladu s pravidly uvedenými v oddíle IV.

SPISOVNY TRÈS SECRET UE/EU TOP SECRET NIŽŠÍ ÚROVNĚ

8. Jako kontrolní úředník odpovídá vedoucí spisovny TRÈS SECRET UE/EU TOP SECRET nižší úrovně za:

   a) zajištění předávání dokumentů se stupněm utajení TRÈS SECRET UE/EU TOP SECRET v souladu s pravidly vymezenými v oddíle VII a v bodech 5 a 6 oddílu VIII;

b) aktualizaci seznamu všech osob oprávněných k přístupu ke skutečnostem se stupněm utajení TRÈS SECRET UE/EU TOP SECRE, které kontroluje;

c) šíření dokumentů se stupněm utajení TRÈS 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;

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

e) aktualizaci seznamu spisoven TRÈS SECRET UE/EU TOP SECRET, se kterými je oprávněn vyměňovat dokumenty se stupněm utajení TRÈS SECRET UE/EU TOP SECRET spolu se jmény a podpisy pověřených kontrolních úředníků a jejich oprávněných zástupců;

f) zajištění hmotné bezpečnosti všech dokumentů se stupněm utajení TRÈS SECRET UE/EU TOP SECRET uložených ve spisovně nižší úrovně v souladu s pravidly uvedenými v oddíle IV.

INVENTURY

9. Každých dvanáct měsíců provede každá spisovna TRÈS SECRET UE/EU TOP SECRET podrobnou inventuru všech dokumentů se stupněm utajení TRÈS SECRET UE/EU TOP SECRET, za které odpovídá. Dokument se považuje za zkontrolovaný, jestliže spisovna dokument fyzicky zkontroluje nebo má potvrzení o převzetí od spisovny TRÈS SECRET UE/EU TOP SECRET, které byl dokument předán, nebo zápis o zničení dokumentu nebo pokyn ke snížení klasifikace daného dokumentu nebo k jeho odtajnění.

10. Spisovny nižší úrovně předávají výsledky své roční inventury ústřední spisovně, které jsou podřízeny, ke dni stanovenému ústřední spisovnou.

11. Vnitrostátní bezpečnostní orgány a orgány EU, mezinárodní organizace a decentralizované subjekty EU, ve kterých byla zřízena ústřední spisovna TRÈS SECRET UE/EU TOP SECRET, předají generálnímu tajemníkovi, vysokému představiteli nejpozději do 1. dubna každého roku výsledky ročních inventur provedených v ústředních spisovnách TRÈS SECRET UE/EU TOP SECRET.

ODDÍL IX

BEZPEČNOSTNÍ OPATŘENÍ, KTERÁ SE POUŽIJÍ PŘI ZVLÁŠTNÍCH ZASEDÁNÍCH TÝKAJÍCÍCH SE VELMI CITLIVÝCH ZÁLEŽITOSTÍ KONANÝCH MIMO OBJEKTY RADY

ÚVOD

1. Konají-li se zasedání Evropské rady, Rady, Rady ministrů nebo jiná významná zasedání mimo objekty Rady 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.

ODPOVĚDNOST

Hostitelské členské státy

2. Členský stát, na jehož území se zasedání koná (hostitelský členský stát), musí zajistit ve spolupráci s bezpečnostní kanceláří GSR bezpečnost zasedání Evropské rady, Rady, Rady ministrů nebo jiných významných zasedání a fyzickou bezpečnost hlavních delegátů a jejich spolupracovníků.

V oblasti ochrany bezpečnosti musí hostitelský členský stát zejména 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 v objektech;

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

Členské státy

3. Orgány členských států přijmou opatření nezbytná, aby:

a) buď bezpečnostní úředník zasedání přímo poskytl, v případě potřeby signálním přenosem nebo faxem, jejich delegátům příslušné potvrzení o bezpečnostní prověrce, nebo prostřednictvím bezpečnostní kanceláře GSR;

b) jakékoli zvláštní ohrožení bylo oznámeno orgánům hostitelského členského státu a případně bezpečnostní kanceláři GSR, aby mohla být přijata potřebná opatření.

Bezpečnostní úředník zasedání

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

a) i) 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;

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

iii) trvalé koordinace s příslušnými orgány hostitelského členského státu a s bezpečnostní kanceláří GSR;

b) zařazení bezpečnostních pokynů do dokumentace k zasedání s ohledem na požadavky stanovené v těchto bezpečnostních předpisech a v jakýchkoli jiných bezpečnostních pokynech považovaných za nezbytné.

Bezpečnostní kancelář GSR

5. Bezpečnostní kancelář GSR má úlohu poradce v otázkách bezpečnosti při přípravě zasedání; musí zde být zastoupena, aby případně pomáhala a radila bezpečnostnímu úředníkovi zasedání a delegacím.

6. Každá delegace na zasedání musí určit jednoho bezpečnostního úředníka, který bude řešit bezpečnostní otázky ve své delegaci a udržovat kontakt s bezpečnostním úředníkem zasedání a se zástupcem bezpečnostní kanceláře GSR.

BEZPEČNOSTNÍ OPATŘENÍ

Bezpečnostní oblasti

7. Vytvářejí se tyto bezpečnostní oblasti:

   a) bezpečnostní oblast kategorie II, zahrnující případně redakční místnost, kanceláře a reprografická zařízení GSR 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.

Propustky

8. Bezpečnostní úředník zasedání musí vydat visačky příslušného typu podle požadavků delegací. Podle potřeby lze odlišit povolení vstupu do jednotlivých bezpečnostních oblastí.

9. 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.

10. Kromě účastníků vybavených visačkou bude přístup na místo zasedání povolen co nejmenšímu počtu osob. Státní delegace, které chtějí během zasedání přijmout návštěvníky, o tom musí uvědomit bezpečnostního úředníka zasedání. 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.

Kontrola fotografických a záznamových zařízení

11. 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 bezpečnostního úředníka zasedání.

Kontrola aktovek, přenosných počítačů a zásilek

12. 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 bezpečnostní úředník zasedání za nezbytné, mohou být stanovena přísnější opatření pro kontroly aktovek a zásilek.

Technická bezpečnost

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

Dokumenty delegací

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

Bezpečné uložení dokumentů

15. Jestliže GSR, 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.

Kontrola kanceláří

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

Odstranění utajovaného odpadu EU

17. Veškerý odpad se považuje za utajovaný odpad EU a koše nebo pytle na papír se předávají GSR a delegacím ke zničení. GSR a delegace musí před odchodem z místností, které jim byly přiděleny, předat odpad bezpečnostnímu úředníkovi zasedání, který zajistí jejich zničení podle předpisů.

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

ODDÍL X

NARUŠENÍ BEZPEČNOSTI A VYZRAZENÍ UTAJOVANÝCH SKUTEČNOSTÍ EU

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

2. 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.

3. 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.

4. Je důležité, aby všechny osoby, které mají nakládat s utajovanými skutečnostmi EU, byly důkladně poučeny o bezpečnostních postupech, o nebezpečí neuvážených rozhovorů a o vztazích s tiskem. Musí si být vědomy toho, že je důležité okamžitě oznámit jakékoli narušení bezpečnosti, o němž se dozvědí, bezpečnostnímu orgánu členského státu, instituci nebo subjektu, ve kterém jsou zaměstnány.

5. Zjistí-li bezpečnostní orgán 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) zjistil skutečný stav;

   b) zhodnotil a snížil na minimum způsobenou škodu;

   c) zabránil opakování;

   d) uvědomil příslušné úřady o důsledcích narušení bezpečnosti.

   V této souvislosti jsou poskytovány tyto informace:

   i) popis dotčených skutečností, zejména s upřesněním jejich klasifikace, 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.

6. Každý bezpečnostní orgán, jakmile byl upozorněn, že mohlo dojít k narušení bezpečnosti, je povinen na tuto skutečnost okamžitě upozornit tímto postupem: spisovna EU TOP SECRET nižší úrovně oznámí věc bezpečnostní kanceláři GSR prostřednictvím ústřední spisovny EU TOP SECRET; v případě, že dojde k vyzrazení utajovaných skutečností EU v jurisdikci některého členského státu, musí být tato skutečnost sdělena bezpečnostní kanceláři GSR podle bodu 5 prostřednictvím odpovědného vnitrostátního bezpečnostního orgánu.

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

8. Jakmile je generální tajemník/vysoký představitele 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 klasifikace dotčených dokumentů. Rovněž je třeba uvést poškození zájmů EU nebo jednoho či více členských států a opatření přijatá s cílem zabránit jakémukoli opakování.

9. Původce uvědomí příjemce a dá jim potřebné pokyny.

10. V souladu s příslušnými pravidly a aniž je dotčena možnost soudního postihu, mohou být přijata kázeňská opatření proti jakékoli osobě, která je odpovědná za vyzrazení utajovaných skutečností EU.

ODDÍL XI

OCHRANA SKUTEČNOSTÍ ZPRACOVÁVANÝCH V SYSTÉMECH INFORMAČNÍCH TECHNOLOGIÍ A V KOMUNIKAČNÍCH SYSTÉMECH

Obsah

Kapitola I

Úvod

OBECNÉ ASPEKTY

1. Bezpečnostní politika a požadavky vymezené v tomto oddíle se uplatňují na všechny komunikační a informační systémy a sítě (dále jen „SYSTÉMY“), v nichž se zpracovávají skutečnosti se stupněm utajení CONFIDENTIEL UE a vyšším.

2. SYSTÉMY, které zpracovávají skutečnosti se stupněm utajení 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. Příslušný orgán pro schvalování z hlediska bezpečnosti (Security Accreditation Authority, SAA) rozhodne, jaká bezpečnostní opatření mají být pro tyto systémy použita; tato opatření jsou úměrná vyhodnocenému riziku a jsou slučitelná s politikou uvedenou v těchto bezpečnostních předpisech.

3. Ochrana detekčních systémů obsahujících zabudované IT SYSTÉMY je určena a uvedena v obecném rámci systémů, ke kterým patří, s využitím ustanovení tohoto oddílu v co největší možné míře.

OHROŽENÍ A SLABÁ MÍSTA SYSTÉMŮ

4. Obecně lze ohrožení 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. Slabá místa mohou rovněž vyplynout z opomenutí nebo mohou souviset s příliš slabou, neúplnou nebo nedůslednou kontrolou; mohou mít technickou, procedurální nebo provozní povahu.

5. Utajované či neutajované skutečnosti EU zpracovávané v SYSTÉMECH v koncentrované formě, 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. Existují rovněž rizika neoprávněného vyzrazení, poškození, úpravy nebo vymazání skutečností. Kromě toho složité a často choulostivé zařízení je nákladné a často je obtížné rychle jej opravit nebo nahradit. Tyto SYSTÉMY jsou proto lákavým cílem pro akce zaměřené na získávání informací a pro sabotáže, zejména tehdy, zdají-li se bezpečnostní opatření neúčinná.

BEZPEČNOSTNÍ OPATŘENÍ

6. Hlavním cílem bezpečnostních opatření uvedených v tomto oddíle je zajistit ochranu před neoprávněným vyzrazením skutečností (ztráta důvěrnosti) a před ztrátou celistvosti a dostupnosti skutečností. Aby bylo dosaženo náležité ochrany SYSTÉMŮ, které zpracovávají utajované skutečnosti EU, je nezbytné upřesnit vhodné normy klasické bezpečnosti a vhodné bezpečnostní postupy a techniky vytvořené zvlášť pro každý SYSTÉM.

7. Za účelem vytvoření bezpečného prostředí pro činnost SYSTÉMU je třeba vypracovat a zavést vyvážený soubor bezpečnostních opatření. Oblasti použití těchto opatření se týkají fyzických prvků, personálu, netechnických postupů, provozních postupů počítačů a komunikací.

8. Pro počítače je třeba stanovit bezpečnostní opatření (bezpečnostní vlastnosti hardwaru a softwaru), které umožní uplatňovat zásadu „potřeba vědět“ a vyhnout se neoprávněnému vyzrazení skutečností a nebo jej zjistit. Míra, v jaké lze spoléhat na bezpečnostní opatření platná pro počítače, je určena během procesu vymezení bezpečnostních požadavků. Schvalovací proces umožňuje zjistit, zda existuje dostatečná úroveň zajištění, která odůvodňuje důvěru v tato opatření.

STANOVENÍ BEZPEČNOSTNÍCH POŽADAVKŮ VLASTNÍCH DANÉMU SYSTÉMU

9. Pro všechny SYSTÉMY, které zpracovávají skutečnosti se stupněm utajení CONFIDENTIEL UE a vyšším, musí orgán pro provoz IT systému (IT System Operational Authority, ITSOA) případně s přispěním a za podpory osob odpovědných za projekt a orgánu INFOSEC vypracovat stanovení bezpečnostních požadavků pro daný SYSTÉM (SYSTEM-Specific Security Requirement Statement, SSRS), který schválí orgán pro schvalování z hlediska bezpečnosti. Stanovení bezpečnostních požadavků pro daný SYSTÉM se rovněž požaduje, považuje-li orgán pro schvalování z hlediska bezpečnosti dostupnost a celistvost skutečností se stupněm utajení RESTREINT UE nebo neutajovaných skutečností za podstatnou.

10. Stanovení bezpečnostních požadavků pro daný SYSTÉM 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.

11. Stanovení bezpečnostních požadavků pro daný SYSTÉM představuje závaznou dohodu mezi orgánem provozujícím systém a orgánem pro schvalování z hlediska bezpečnosti, na jejímž základě se SYSTÉM schvaluje.

12. Stanovení bezpečnostních požadavků pro daný SYSTÉM je úplným a jasným vyjádřením bezpečnostních zásad, které je třeba dodržovat, a podrobných bezpečnostních požadavků, které je třeba splnit. Je založené na bezpečnostní politice Rady a na hodnocení rizik nebo je určeno parametry, jako jsou provozní podmínky, nejnižší stupeň bezpečnostní prověrky personálu, nejvyšší stupeň utajení zpracovávaných skutečností, bezpečnostní režim provozu nebo požadavky uživatele. Stanovení bezpečnostních požadavků pro daný SYSTÉM je nedílnou součástí dokumentace projektu předkládané orgánům příslušným pro technické, rozpočtové a bezpečnostní schválení. Ve své konečné podobě představuje úplný popis požadavků, kterým musí SYSTÉM vyhovovat, má-li být bezpečný.

BEZPEČNOSTNÍ REŽIMY PROVOZU

13. Všechny SYSTÉMY, které zpracovávají skutečnosti se stupněm utajení 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 ekvivalent:

a) „dedicated“;

b) „system high“ a

c) „multi-level“.

Kapitola II

Definice

DOPLŇUJÍCÍ OZNAČENÍ

14. Doplňující označení, např. CRYPTO nebo jakékoli jiné označení vyžadující speciální nakládání uznávané EU, se používají, je-li potřeba zajistit omezené rozšíření a zvláštní zacházení s dokumentem, které se vyžaduje vedle požadavků bezpečnostní klasifikace.

15. 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.

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.

16. 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.

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.

17. 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.

18. 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. Opatření INFOSEC zahrnují bezpečnost počítačů, přenosu, emisí a šifrovací bezpečnost a odhalování ohrožení skutečností a SYSTÉMŮ a jeho předcházení.

19. 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.

20. 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.

21. BEZPEČNOSTÍ 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.

22. 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.

23. 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.

24. 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 prvků:

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 (SecOPs) 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;

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

25. IT SYSTÉMEM 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 orgánu provozujícího systém.

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

26. BEZPEČNOSTNÍ VLASTNOSTI IT SYSTÉMU 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 IT systému.

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

Poznámky:

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

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

28. BEZPEČNOSTNÍ VLASTNOSTI IT SÍTĚ zahrnují bezpečnostní vlastnosti každého IT systému, 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 v síti, mechanismy a postupy bezpečnostního označování a identifikace, kontroly přístupu, programy a kontrolní cesty).

29. OBLASTÍ IT se rozumí: oblast s jedním počítačem nebo více počítači, s jejich místními periferiemi a paměťovými jednotkami, s jejich řídicími 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.

30. 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.

31. Bezpečnostními opatřeními TEMPEST se rozumí: bezpečnostní opatření určená pro ochranu zařízení a komunikační infrastruktury před vyzrazením utajovaných skutečností neúmyslným elektromagnetickým vyzařováním.

Kapitola III

Odpovědnost v oblasti bezpečnosti

OBECNĚ

32. Odpovědnost Bezpečnostního výboru uvedená v oddíle 1 bodu 4 zahrnuje otázky INFOSEC. Bezpečnostní výbor organizuje svou činnost tak, aby mohl poskytovat odborné rady k výše uvedeným otázkám.

33. V případě obtíží spojených s bezpečností (incidenty, narušení atd.) přijme příslušný vnitrostátní orgán nebo bezpečnostní kancelář GSR neprodleně opatření. Všechny obtíže je třeba oznámit bezpečnostní kanceláři GSR.

34. Generální tajemník, vysoký představitel nebo případně vedoucí decentralizovaného subjektu EU zřídí kancelář INFOSEC, která bude pověřena vypracováním obecných zásad pro bezpečnostní orgán týkajících se zavádění a kontroly zvláštních bezpečnostních vlastností zahrnutých do SYSTÉMŮ.

ORGÁN PRO SCHVALOVÁNÍ Z HLEDISKA BEZPEČNOSTI (SAA)

35. Orgánem pro schvalování z hlediska bezpečnosti je:

— vnitrostátní bezpečnostní orgán,

— orgán pověřený generálním tajemníkem/vysokým představitelem,

— bezpečnostní orgán decentralizovaného subjektu EU nebo

— jejich delegovaní nebo jmenovaní zástupci v závislosti na SYSTÉMU, který má být schválen.

36. Orgán pro schvalování z hlediska bezpečnosti odpovídá za soulad SYSTÉMŮ s bezpečnostní politikou Rady. Je pověřen udělit schválení SYSTÉMU, který má ve svém provozním prostředí zpracovávat utajované skutečnosti EU určeného stupně utajení. Pokud jde o GSR a případně decentralizované subjekty EU, odpovídá orgán pro schvalování z hlediska bezpečnosti za bezpečnost jménem generálního tajemníka, vysokého představitele nebo vedoucích decentralizovaných subjektů.

Do jurisdikce orgánu pro schvalování z hlediska bezpečnosti GSR spadají všechny SYSTÉMY provozované v objektu GSR. SYSTÉMY a složky SYSTÉMŮ provozované v členském státě zůstávají v pravomoci tohoto členského státu. Spadají-li jednotlivé složky SYSTÉMU do pravomoci orgánu pro schvalování z hlediska bezpečnosti GSR a ostatních orgánů pro schvalování z hlediska bezpečnosti, určí všechny dotčené strany společný výbor pro schvalování, jeho koordinaci bude zajišťovat orgán pro schvalování z hlediska bezpečnosti GSR.

ORGÁN PRO BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ (INFOSEC)

37. Orgán pro bezpečnost informačních systémů (INFOSEC) odpovídá za činnost kanceláře INFOSEC. Pokud jde o GSR a případně o decentralizované subjekty EU, odpovídá orgán INFOSEC 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.

ORGÁN PRO PROVOZ IT SYSTÉMU (ITSOA)

38. Orgán INFOSEC přenese co nejrychleji odpovědnost za zavedení kontrol a fungování speciálních bezpečnostních vlastností SYSTÉMU na orgán ITSOA. Tato odpovědnost platí po celou dobu existence SYSTÉMU od vytvoření projektu až po závěrečnou likvidaci.

39. Orgán ITSOA odpovídá za všechna bezpečnostní opatření vytvořená jako součást celého SYSTÉMU. Je rovněž pověřen zpracováním provozních postupů pro zajištění bezpečnosti a rozhoduje o bezpečnostních normách a zvyklostech, kterým má vyhovět dodavatel SYSTÉMU.

40. Orgán ITSOA může podle potřeby přenést část své odpovědnosti například na bezpečnostní úředníky INFOSEC pověřené systémem a pracovištěm. Jedna osoba může vykonávat různé funkce INFOSEC.

UŽIVATELÉ

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

ŠKOLENÍ INFOSEC

42. V rámci GSR, decentralizovaných subjektů EU nebo úředních útvarů členských států je třeba zajistit vzdělávání a školení týkající se INFOSEC na různých úrovních a pro různé pracovníky.

Kapitola IV

Netechnická bezpečnostní opatření

BEZPEČNOSTNÍ OPATŘENÍ TÝKAJÍCÍ SE PERSONÁLU

43. Uživatelé SYSTÉMU musí projít bezpečnostní prověrkou odpovídající stupni utajení a obsahu zpracovávaných skutečností v jejich SYSTÉMU a musí mít „potřebu vědět“. Přístup k některým zařízením nebo informacím specifickým pro bezpečnost SYSTÉMŮ vyžaduje zvláštní povolení udělené podle postupů Rady.

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

45. 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. Záměrem je, aby jedna osoba nemohla změnit nebo úmyslně poškodit systém nebo síť bez spolupráce s další osobou nebo s více dalšími osobami.

FYZICKÁ BEZPEČNOST

46. Oblasti IT a oblasti vzdálených terminálů/pracovních stanic (jak jsou vymezeny v bodech 29 a 30), ve kterých jsou skutečnosti se stupněm utajení 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 nebo podle jejich vnitrostátní obdoby.

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

KONTROLA PŘÍSTUPU K SYSTÉMU

48. 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.

49. Informace a materiály umožňující kontrolu přístupu, které již nejsou k tomuto účelu používány, se zničí v souladu s body 61 až 63.

Kapitola V

Technická bezpečnostní opatření

BEZPEČNOST SKUTEČNOSTÍ

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

51. Subjekt 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.

52. 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 klasifikaci.

53. Při přenosu skutečností z jednoho SYSTÉMU do druhého musí být během přenosu a v přijímajícím SYSTÉMU chráněny způsobem odpovídajícím původní klasifikaci a kategorii skutečností.

54. Všechny nosiče dat musí být zpracovány v souladu s nejvyšší klasifikací archivovaných skutečností nebo označení nosiče dat a po celou dobu musí být přiměřeně chráněny.

55. Znovu použitelné nosiče dat použité pro záznam utajovaných skutečností EU mají zachován nejvyšší stupeň utajení přidělovaný datům, pro které byly použity, dokud není klasifikace těchto skutečností řádně snížena nebo odstraněna a takto překlasifikovaný nosič není odtajněn nebo zničen schváleným postupem GSR nebo vnitrostátního orgánu (viz body 61 až 63).

KONTROLA A ODPOVĚDNOST ZA SKUTEČNOSTI

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

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

58. 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 takto rozptýlených dat. Pro skutečnosti se stupněm utajení SECRET UE a vyšším tyto postupy zahrnují zvláštní pokyny pro odpovědnost za skutečnosti.

NAKLÁDÁNÍ S ODNÍMATELNÝMI NOSIČI DAT A JEJICH KONTROLA

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

60. Uživatelé se musí ujistit, že utajované skutečnosti EU jsou zaznamenány na nosičích dat s příslušným označením klasifikace 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.

ODTAJNĚNÍ A ZNIČENÍ NOSIČŮ DAT

61. Klasifikace nosičů dat používaných pro záznam utajovaných skutečností EU může být snížena nebo mohou být odtajněny, pokud se použijí schválené postupy GSR nebo schválené vnitrostátní postupy.

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

63. Nosiče dat, která nelze odtajnit ani použít znovu, se zničí schváleným postupem GSR nebo schváleným vnitrostátním postupem.

BEZPEČNOST KOMUNIKACÍ

64. 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 odposloucháváním. Skutečnosti přenášené prostřednictvím komunikačního systému jsou chráněny na základě požadavků nezbytných pro zajištění jejich důvěrnosti, celistvosti a dostupnosti.

65. 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.

66. Během přenosu je důvěrnost skutečností se stupněm utajení SECRET UE a vyšším chráněna šifrovacími metodami nebo produkty schválenými Radou na doporučení Bezpečnostního výboru Rady. Během přenosů je důvěrnost skutečností se stupněm utajení CONFIDENTIEL UE nebo RESTREINT UE chráněna šifrovacími metodami nebo produkty schválenými buď generálním tajemníkem/vysokým představitelem na doporučení Bezpečnostního výboru, nebo členským státem.

67. Podrobná pravidla uplatňovaná pro přenosy utajovaných skutečností EU musí být uvedena ve specifických bezpečnostních pokynech schválených Radou na doporučení Bezpečnostního výboru Rady.

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

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

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.

69. 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.

BEZPEČNOST INSTALACÍ A VYZAŘOVÁNÍ

70. 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 nejvyšší klasifikaci skutečností, které má SYSTÉM ukládat a zpracovávat.

71. Veškerá zařízení musí být instalována v souladu s platnými bezpečnostními předpisy Rady.

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

73. Protiopatření TEMPEST uplatňovaná pro instalace GSR a decentralizovaných subjektů EU jsou posuzovány a schvalovány schvalovacím orgánem TEMPEST pověřeným bezpečnostním orgánem GSR. Pro vnitrostátní instalace, které slouží ke zpracování utajovaných skutečností EU, je schvalujícím orgánem uznaný vnitrostátní schvalovací orgán TEMPEST.

Kapitola VI

Bezpečnost během zpracování

PROVOZNÍ POSTUPY TÝKAJÍCÍ SE BEZPEČNOSTI

74. Provozní postupy pro zajištění bezpečnosti vymezují zásady k přijetí v oblasti bezpečnosti, provozní postupy, které se mají používat, a odpovědnost personálu. Za vypracování provozních postupů pro zajištění bezpečnosti odpovídá orgán pro provoz IT systému.

OCHRANA SOFTWARU A SPRÁVA KONFIGURACE

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

76. Nové nebo pozměněné verze softwaru budou používány pro zpracování utajovaných skutečností EU, až po ověření orgánem pro provoz IT systému.

ZJIŠŤOVÁNÍ PŘÍTOMNOSTI SOFTWARU PŮSOBÍCÍHO ŠKODU A POČÍTAČOVÝCH VIRŮ

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

78. Všechny nosiče dat vstupující do GSR nebo do decentralizovaného subjektu EU nebo do orgánů členských států musí být před zavedením do jakéhokoli SYSTÉMU ověřeny, zda neobsahují software působící škodu nebo počítačové viry.

ÚDRŽBA

79. 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.

80. 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.

Kapitola VII

Nabývání

81. 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 15 408), nebo musí probíhat řízení o jejich hodnocení nebo osvědčení příslušným orgánem pro hodnocení nebo osvědčování.

82. 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 objekt, který mu zajišťuje požadovanou ochranu, aniž by nejprve bylo se schválením orgánu pro schvalování z hlediska bezpečnosti odtajněno, a že toto schválení nemusí být vždy možné.

SCHVALOVÁNÍ

83. 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. Subsystémy a vzdálené terminály/pracovní stanice musí být schváleny jako součást SYSTÉMŮ, ke kterým jsou připojeny. Pokud určitý SYSTÉM zajišťuje spojení Rady i jiných organizací, dohodne se GSR a dotčené bezpečnostní orgány na otázce schválení.

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

HODNOCENÍ A UDĚLENÍ OSVĚDČENÍ

85. 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.

86. Požadavky na hodnocení a vystavení osvědčení jsou zahrnuty do plánování systému a jsou jasně uvedeny ve stanovení bezpečnostních požadavků pro daný SYSTÉM.

87. Hodnocení a udělování osvědčení provádí v souladu se schválenými směrnicemi personál s nezbytnou technickou kvalifikací, který prošel příslušnými bezpečnostními prověrkami a jedná na účet orgánu pro provoz IT systému.

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

89. 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.

SYSTEMATICKÉ KONTROLY BEZPEČNOSTNÍCH VLASTNOSTÍ PŘI PRODLUŽOVÁNÍ SCHVÁLENÍ

90. Orgán pro provoz IT systému stanoví systematickou kontrolu, která zaručí, že všechny bezpečnostní vlastnosti SYSTÉMU jsou stále platné.

91. Stanovení bezpečnostních požadavků pro daný SYSTÉM 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 orgán pro provoz IT 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.

92. Orgán pro schvalování z hlediska bezpečnosti provádí pravidelně inspekce a přezkoušení všech SYSTÉMŮ, které mají bezpečnostní vlastnosti. U SYSTÉMŮ, které zpracovávají skutečnosti klasifikované jako TRÈS SECRET UE/EU TOP SECRET nebo zvláštní kategorie, se inspekce provádějí nejméně jednou ročně.

Kapitola VIII

Dočasné nebo příležitostné použití

BEZPEČNOST MIKROPOČÍTAČŮ A OSOBNÍCH POČÍTAČŮ

93. 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.

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

POUŽÍVÁNÍ SOUKROMÉHO POČÍTAČOVÉHO VYBAVENÍ IT K OFICIÁLNÍ PRÁCI RADY

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

96. Soukromý hardware, software a nosiče dat se nesmějí vnášet do bezpečnostních oblastí kategorie I nebo kategorie II, kde se zpracovávají utajované skutečnosti EU, bez povolení vedoucího bezpečnostní kanceláře GSR nebo příslušného úřadu členského státu či příslušného decentralizovaného subjektu EU.

POUŽÍVÁNÍ POČÍTAČOVÉHO VYBAVENÍ IT SMLUVNÍHO PARTNERA NEBO VYBAVENÍ DODANÉHO VNITROSTÁTNÍM DODAVATELEM K OFICIÁLNÍ PRÁCI RADY

97. Používání počítačového vybavení a softwaru smluvního partnera pro oficiální práci Rady v organizacích může povolit vedoucí bezpečnostní kanceláře GSR nebo příslušného úřadu členského státu nebo decentralizovaného subjektu EU. Používání počítačového vybavení IT a softwaru poskytnutého vnitrostátním dodavatelem zaměstnanci GSR nebo decentralizovaného subjektu EU může být rovněž povoleno; v tom případě podléhá IT vybavení inventuře GSR. 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.

ODDÍL XII

PŘEDÁVÁNÍ UTAJOVANÝCH SKUTEČNOSTÍ EU TŘETÍM STÁTŮM NEBO MEZINÁRODNÍM ORGANIZACÍM

ZÁSADY, KTERÝMI SE ŘÍDÍ PŘEDÁVÁNÍ UTAJOVANÝCH SKUTEČNOSTÍ EU

1. O předání utajovaných skutečností třetím státům nebo mezinárodním organizacím rozhoduje Rada na základě:

   — povahy a obsahu těchto skutečností,

   — „potřeby vědět“ příjemce,

   — výhodnosti pro EU.

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

2. 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; Bezpečnostní výbor Rady předá Radě technické stanovisko k tomuto bodu.

3. 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 Radou.

ÚROVNĚ

4. Jakmile Rada 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.

5. 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.

6. Každá úroveň spolupráce určuje bezpečnostní předpisy přizpůsobené v jednotlivých případech technickému stanovisku Bezpečnostního výboru Rady, které musí příjemci skutečností dodržovat při ochraně jim předávaných utajovaných skutečností. Tyto postupy a bezpečnostní předpisy jsou podrobně uvedeny v přílohách 4, 5 a 6.

DOHODY

7. Rozhodne-li Rada, 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.

8. V případě příležitostné spolupráce na úrovni 3, která je již ze své definice časově a účelově omezena, lze „dohodu o bezpečnostních postupech pro výměnu utajovaných skutečností“ nahradit jednoduchým 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 RESTREINT UE.

9. Návrhy dohod o bezpečnostních postupech nebo memorand o porozumění schvaluje před předložením k rozhodnutí Radě Bezpečnostní výbor.

10. Vnitrostátní bezpečnostní orgány poskytují generálnímu tajemníkovi/vysokému představiteli všechnu nezbytnou pomoc, aby bylo zajištěno, že jsou předávané skutečnosti použity a chráněny v souladu s dohodami o bezpečnostních postupech nebo o memorandech o porozumění.

Dodatek 1

Seznam vnitrostátních bezpečnostních orgánů

BELGIE

Ministère des Affaires Étrangères, du Commerce Extérieur et de la Coopération au Développement
Direction de la sécurité – A 01
Rue des Petits Carmes, 15
B-1000 Bruxelles
Telefon: (32-2) 501 85 14
Fax: (32-2) 501 80 58
Dálnopis: 21376
Telegrafická adresa: Direction de Sécurité A01 – MINAFET

DÁNSKO

Politiets Efterretningstjeneste
Borups Alle 266
DK-2400 Copenhagen NV
Telefon: (45-33) 14 88 88
Fax: (45-38) 19 07 05

Forsvarsministeriet
Forsvarets Efterretningstjeneste
Kastellet 30
DK-2100 Copenhagen Ø
Telefon; (45-33) 32 55 66
Fax: (45-33) 93 13 20

NĚMECKO

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101D
D-10559 Berlin
Telefon; (49-30) 39 81 15 28
Fax: (49-30) 39 81 16 10

ŘECKO

Γενικό Επιτελείο Εjνικής Άμυνας (ΓΕΕΘΑ)
Υπηρεσία Στρατιωτικών Πληροφοριών (ΥΣΠ – Β′ Κλάδος)
Γραφείο Ασφάλειας
ΣΤΓ 1020– Χολαργός (Αjήνα)
Ελλαδα
Τηλέφωνα: (30-1) 655 22 03 (ώρες γραφείου)
(30-1) 642 22 05 (εικοσιτετράωρο)
Φαξ: (30-1) 642 69 40

Hellenic National Defence
General Staff (HNDGS)
Intelligence Branch/Security
(INT. BR./SEC.)
STG 1020, Holargos – Athens
Řecko
Telefon; (30-1) 655 22 03 (v pracovní době)
(30-1) 655 22 05 (nepřetržitě)
Fax: (30-1) 642 69 40

ŠPANĚLSKO

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera Nacional Radial VI, km 8 500
E-28023 Madrid
Telefon; (34-91) 372 57 07
Fax: (34-91) 372 58 08
E-mail: nsa-sp@areatec.com

FRANCIE

Secrétariat général de la Défense Nationale
Service de Sécurité de Défense (SGDN/SSD)
51 Boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telefon; (33-0) 144 18 81 80
Fax: (33-0) 144 18 82 00
Dálnopis: SEGEDEFNAT 200019
Telegrafická adresa: SEGEDEFNAT PARIS

IRSKO

National Security Authority
Department of Foreign Affairs
80 St. Stephens Green
Dublin 2
Telefon; (353-1) 478 08 22
Fax: (353-1) 478 14 84

ITÁLIE

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Ufficio Centrale per la Sicurezza
Via della Pineta Sacchetti, 216
I-00168 Roma
Telefon; (39-06) 627 47 75
Fax: (39-06) 614 33 97
Dálnopis: 623876 AQUILA 1
Telegrafická adresa: ess: PCM-ANS-UCSI-ROMA

LUCEMBURSKO

Autorité Nationale de Sécurité
Ministère d'État
Boîte Postale 2379
L-1023 Luxembourg
Telefon; (352) 478 22 10 central
(352) 478 22 35 direct
Fax: (352) 478 22 43
(352) 478 22 71
Dálnopis: 3481 SERET LU
Telegrafická adresa: MIN D'ETAT – ANS

NIZOZEMSKO

Ministerie van Binnenlandse Zaken
Postbus 20010
NL-2500 EA Den Haag
Telefon; (31-70) 320 44 00
Fax: (31-70) 320 07 33
Dálnopis: 32166 SYTH NL

Ministerie van Defensie
Militaire Inlichtingendienst (MID)
Postbus 20701
NL-250 ES Den Haag
Telefon; (31-70) 318 70 60
Fax: (31-70) 318 79 51

RAKOUSKO

Bundesministerium für auswärtige Angelegenheiten
Abteilung I.9
Ballhausplatz 2
A-1014 Wien
Telefon; (43-1) 531 15 34 64
Fax: (43-1) 531 8 52 19

PORTUGALSKO

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1449-004 Lisboa
Telefon; (351-21) 301 55 10
(351-21) 301 00 01, extension 20 45 37
Fax: (351-21) 302 03 50

FINSKO

Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Ulkoasiainministeriö/Utrikesministeriet
Laivastokatu/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Telefon; (358-9) 13 41 53 38
Fax: (358-9) 13 41 53 03

ŠVÉDSKO

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telefon; (46-8) 405 54 44
Fax: (46-8) 723 11 76

SPOJENÉ KRÁLOVSTVÍ

The Secretary (for DIR/5)
PO Box 5656
London EC1A 1AH
Telefon; (44-20) 72 70 87 51
Fax: (44-20) 76 30 14 28
Telegrafická adresa: UK Delegation to Security Policy Dept FCO, s uvedením poznámky „in Box 5656 for DIR/5“.

Dodatek 2

Srovnávací tabulka vnitrostátních bezpečnostních klasifikací

KLASIFIKACE EU	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Klasifikace NATO (1)				
Klasifikace ZEU	Focal Top Secret	ZEU Secret	ZEU Confidential	ZEU Restricted
Belgie	Très secret Zeer Geheim	Secret Geheim	Confidentiel Vertouwelijk	Diffussion restreinte Beperkte Verspeiding
Dánsko	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Německo	Streng Geheim	Geheim	VS (2) — Vertraulich	VS — Nur für den Dienstgebrauch
Řecko	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης χρήσης
Španělsko	Secreto	Reservado	Confidencial	Difusion Limitada
Francie	Très secret Défense (3)	Secret Défense	Confidentiel Défense	Diffusion restreinte
Irsko	Top Secret	Secret	Confidentiel	Restricted
Itálie	Segretissimo	Segreto	Riservatissimo	Riservato
Lucembursko	Très secret	Secret	Confidentiel	Diffusion restreinte
Nizozemsko	STG Zeer Geheim	STG Geheim	STG Confidentieel	
Rakousko	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Portugalsko	Muito Secreto	Secreto	Confidencial	Reservado
Finsko	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Švédsko	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Spojené království	Top Secret	Secret	Confidentiel	Restricted

(1) Srovnávací tabulka vnitrostátních bezpečnostních klasifikací: NATO: shoda se stupni klasifikace NATO bude stanovena při projednávání dohody o bezpečnosti mezi Evropskou unií a NATO.

(2) Německo: VS = Verschlusssache.

(3) Francie: Klasifikaci „Très Secret Défense“, která se týká vládních prioritních záležitostí, lze změnit pouze s povolením premiéra.

Dodatek 3

Praktický průvodce ke klasifikaci

Tento průvodce je pouze informativní a nelze jej vykládat, jako by měnil základní ustanovení oddílů II a III.

Klasifikace	Kdy	Kdo	Označení	Snížení klasifikace/odtajnění/zničení	
				Kdo	Kdy
TRÈS 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 (oddíl II bod 1).	Vyzrazení informací nebo materiálu označených TRÈS 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.	Členské státy: řádně zmocněné osoby (původci) (oddíl III bod 4); GSR: řádně zmocněné osoby (původci) (oddíl III bod 4), generální tajemník, vysoký představitel a náměstek generálního tajemníka. Původci stanoví datum nebo lhůtu, od kdy lze snížit klasifikaci nebo odtajnit skutečnosti obsažené v dokumentu. Jinak posuzují tuto otázku nejpozději každých pět let, aby zjistili, zda je původní klasifikace nadále nezbytná (oddíl III bod 10).	Klasifikace TRÈS SECRET UE/EU TOP SECRET se přiděluje dokumentům TRÈS SECRET UE/EU TOP SECRET a případně souvisí s označením ESDP pořízeným mechanickými prostředky a ručně (oddíl II bod 8). Klasifikace EU 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 (oddíl VII bod 1).	Rozhodnutí o odtajnění nebo snížení klasifikace může přijmout výlučně původce nebo generální tajemník, vysoký představitel nebo náměstek generálního tajemníka, kteří jsou povinni uvědomit o změně klasifikace následné příjemce, kterým předložili originál nebo jeho kopie (oddíl VIII bod 9). Dokumenty TRÈS 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 TRÈS SECRET UE/EU TOP SECRET, úředníkem, který byl svědkem zničení a který musí projít prověrkou stupně TRÈS 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 (oddíl VI bod 31).	Nadbytečné výtisky a dokumenty, které již nejsou potřeba, je nutné zničit. (oddíl VII bod 31). Dokumenty TRÈS SECRET UE/EU TOP SECRET včetně všeho utajovaného odpadu, který vzniká při přípravě těchto dokumentů TRÈS 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 TRÈS SECRET UE/EU TOP SECRET spálením, rozdrcením, roztrháním nebo jiným způsobem tak, aby je nebylo možné identifikovat a znovu sestavit (oddíl VII bod 31).

Klasifikace	Kdy	Kdo	Označení	Snížení klasifikace/odtajnění/zničení	
				Kdo	Kdy
SECRET EU: 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 (oddíl II bod 1).	Vyzrazení skutečností nebo materiálu označených SECRET UE by mohlo: — vyvolat mezinárodní napětí, — vážně poškodit vztahy se spřátelenými vládami, — přímo ohrozit lidské životy nebo váždně 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, hodpodářským nebo obchodním zájmům EU nebo některého členského státu.	Členské státy: zmocněné osoby (původci) (oddíl III bod 2); GSR a decentralizované subjekty EU: zmocněné osoby (původci) (oddíl III bod 2), generální ředitelé, generální tajemník, vysoký představitel a náměstek generálního tajemníka. Původci uvedou datum nebo lhůtu, od kdy lze snížit klasifikaci nebo odtajnit skutečnosti obsažené v dokumentu. Jinak posuzují tuto otázku nejpozději každých pět let, aby zjistili, zda je původní klasifikace nadále nezbytná (oddíl VII bod 1).	Klasifikace SECRET UE se přiděluje dokumentům SECRET UE a případně souvisí s označením ESDP pořízeným mechanickými prostředky a ručně (oddíl III bod 8). Klasifikace EU 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 (oddíl VII bod 1).	Rozhodnutí o odtajnění nebo snížení klasifikace může přijmout výlučně původce nebo generální tajemník, vysoký představitel nebo náměstek generálního tajemníka, kteří jsou povinni uvědomit o změně klasifikace následné příjemce, kterým předložili originál nebo jeho kopie (odd. VII odst. 9). Dokumenty 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 (oddíl VII bod 32).	Nadbytečné výtisky a dokumenty, které již nejsou potřeba, je nutné zničit (oddíl VII bod 31). Dokumenty SECRET UE včetně všeho utajovaného odpadu, který vzniká při přípravě těchto dokumentů TRÈS 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 (oddíl VII bod 31 a 33).

Klasifikace	Kdy	Kdo	Označení	Snížení klasifikace/odtajnění/zničení	
				Kdo	Kdy
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 (oddíl II bod 3).	Vyzrazení skutečností nebo materiálu označených 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.	Členské státy: zmocněné osoby (původci) (oddíl III bod 2); GSR a decentralizované subjekty EU: zmocněné osoby (původci) (oddíl III bod 2), generální ředitelé, generální tajemník/vysoký představitel a náměstek generálního tajemníka. Původci uvedou datum nebo lhůtu, od kdy lze snížit klasifikaci nebo odtajnit skutečnosti obsažené v dokumentu. Jinak posuzují tuto otázku nejpozději každých pět let, aby zjistili, zda je původní klasifikace nadále nezbytná (oddíl III bod 10).	Klasifikace CONFIDENTIEL UE se přiděluje dokumentům CONFIDENTIEL UE a případně souvisí s označením ESDP pořízeným mechanickými prostředky a ručně nebo vytištěním na předem orazítkovaný registrovaný papír (oddíl II bod 8). Klasifikace EU musí být uvedena 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 (oddíl VII bod 1).	Rozhodnutí o odtajnění nebo snížení klasifikace může přijmout výlučně původce nebo generální tajemník, vysoký představitel nebo náměstek generálního tajemníka, kteří jsou povinni uvědomit o změně klasifikace následující příjemce, kterým předložili originál nebo jeho kopie (oddíl VII bod 31). Dokumenty CONFIDENTIEL UE ničí spisovna, která je za ně odpovědná, pod dohledem osoby, která prošla bezpečnostní prověrkou. Zničení se zaznamenává v souladu s vnitrostátními předpisy a v případě GSR nebo decentralizovaných subjektů EU podle pokynů generálního tajemníka, vysokého představitele nebo náměstka generálního tajemníka (oddíl VII bod 33).	Nadbytečné výtisky a dokumenty, které již nejsou potřeba, je nutné zničit (oddíl VII bod 31).

Klasifikace	Kdy	Kdo	Označení	Snížení klasifikace/odtajnění/zničení	
				Kdo	Kdy
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 (oddíl II bod 4).	Vyzrazení skutečností nebo materiálu označených 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.	Členské státy: zmocněné osoby (původci) (oddíl III bod 2); GSR a decentralizované subjekty EU: zmocněné osoby (původci) (oddíl III bod 2), generální ředitelé, generální tajemník, vysoký představitel a náměstek generálního tajemníka. Původci uvedou datum nebo lhůtu, od kdy lze snížit klasifikaci nebo odtajnit skutečnosti obsažené v dokumentu. Jinak posuzují tuto otázku nejpozději každých pět let, aby zjistili, zda je původní klasifikace nadále nezbytná (oddíl III bod 10).	Klasifikace RESTREINT UE se přiděluje dokumentům RESTREINT UE a podle potřeby nese navíc označení ESDP pořízené mechanickými prostředky a ručně (oddíl II bod 8) Klasifikace EU musí být uvedena nahoře a dole uprostřed každé stránky a každá stránka musí být očíslovaná. Každý dokument musí obsahovat spisové číslo a datum (oddíl VII bod 1).	Rozhodnutí o odtajnění nebo snížení klasifikace může přijmout pouze původce, generální tajemník, vysoký představitel nebo náměstek generálního tajemníka, kteří jsou povinni uvědomit o změně klasifikace následné příjemce, kterým předložili originál nebo jeho kopie (oddíl III bod 9). Dokumenty RESTREINT UE ničí spisovna, která je za ně odpovědná, v souladu s vnitrostátními předpisy a v případě GSR nebo decentralizovaných subjektů EU podle pokynů generálního tajemníka, vysokého představitele nebo náměstka generálního tajemníka (oddíl VII bod 34).	Nadbytečné výtisky a dokumenty, které již nejsou potřeba, je nutné zničit (oddíl VII bod 31).

Dodatek 4

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 signatáři Smlouvy o Evropské unii, nebo jiným mezinárodním organizacím, jejichž bezpečnostní politika a předpisy jsou srovnatelné s bezpečnostní politikou a předpisy EU, odpovídá Rada.

2. Rada může rozhodování o předávání utajovaných skutečností přenést. Při přenesení odpovědnosti upřesní povahu skutečností, které lze předávat, a jejich stupeň utajení, který obvykle nebude vyšší než CONFIDENTIEL UE.

3. S výhradou uzavření bezpečnostní dohody podávají bezpečnostní orgány dotčených států nebo mezinárodních organizací žádosti o předání utajovaných skutečností EU generálnímu tajemníkovi/vysokému představiteli, ve kterých upřesní účel předání skutečností a povahu a stupeň utajení požadovaných utajovaných skutečností.

   Žádosti mohou podat rovněž členské státy nebo decentralizované subjekty EU, které považují předání utajovaných skutečností EU za žádoucí; žadatelé upřesní cíle a výhody takového předání pro EU a povahu a stupeň utajení skutečností, jež mají být předány.

4. Žádost posoudí GSR, který:

   — získá stanovisko členského státu nebo případně decentralizovaného subjektu EU, kteří jsou původci předávaných skutečností,

   — 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 předpisy,

   — získá od bezpečnostních orgánů členských států technické stanovisko týkající se důvěry, kterou lze věnovat přijímajícím státům nebo mezinárodním orgánům.

5. GSR předá žádost a doporučení bezpečnostní kanceláře k rozhodnutí Radě.

BEZPEČNOSTNÍ PŘEDPISY, KTERÉ MUSÍ DODRŽOVAT PŘÍJEMCI

6. Generální tajemník/vysoký představitel oznámí přijímajícím státům nebo mezinárodním organizacím rozhodnutí Rady povolit předání utajovaných skutečností EU a předá jim tolik výtisků těchto bezpečnostních předpisů, kolik považuje za nezbytné. Podal-li žádost některý členský stát, oznámí příjemci povolení předání tento stát.

   Rozhodnutí předat skutečnosti bude vykonatelné, pouze pokud příjemci přijmou písemný závazek, že:

   — budou používat skutečnosti pouze ke stanoveným účelům,

   — budou chránit skutečnosti v souladu s těmito bezpečnostními předpisy, 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 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 společnou dohodou na základě ustanovení oddílu VII těchto bezpečnostních předpisů. Tyto postupy zejména upřesní, kterým spisovnám jsou utajované skutečnosti EU předávány.

b) Jestliže utajované skutečnosti, jejichž předání bylo Radou povoleno, zahrnují skutečnosti se stupněm utajení TRÈS SECRET UE/EU TOP SECRET, musí přijímající země nebo mezinárodní organizace vytvořit ústřední spisovnu EU, a je-li potřeba spisovny nižší úrovně. Na tyto spisovny se vztahuje oddíl VIII těchto bezpečnostních předpisů.

9. *Registrace*

Jakmile některá spisovna přijme dokument EU se stupněm utajení 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), klasifikaci 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 VI těchto bezpečnostních předpisů. Kopie zápisů o zničení dokumentů SECRET UE a TRÈS SECRET UE/EU TOP SECRET se zasílají spisovně EU, která dokumenty zaslala.

b) Utajované dokumenty EU je třeba zahrnout 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 CONFIDENTIEL UE nebo SECRET UE, překládat je a pořizovat z nich výpisy bez povolení vedoucího dotčené bezpečnostní organizace, která kopie, překlady a výpisy registruje a zkontroluje a připojí k nim nezbytná označení.

Reprodukování nebo překlad dokumentu se stupněm utajení TRÈS SECRET UE/EU TOP SECRET může povolit pouze původce, přičemž v povolení uvede počet povolených kopií; jestliže původce nelze určit, je dotaz zaslán bezpečnostní kanceláři GSR.

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 bezpečnostní kancelář GSR, 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 bezpečnostní kanceláře GSR, která zamezí opakování.

14. *Kontroly*

Bezpečnostní kancelář GSR 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 bezpečnostních předpisů.

Dodatek 5

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 Rada. V zásadě se toto předávání omezuje na skutečnosti klasifikované do stupně SECRET UE včetně; vylučují se vnitrostátní skutečnosti předávané pouze členským státům a kategorie utajovaných skutečností EU chráněné zvláštními označeními.

2. Rada může rozhodování o předávání utajovaných skutečností přenést; při přenesení, v rámci omezení uvedených v odstavci 1, upřesní povahu skutečností, které lze předávat, a jejich stupeň utajení omezený nejvýše na RESTREINT UE.

3. S výhradou uzavření bezpečnostní dohody podávají bezpečnostní orgány dotčených států nebo mezinárodních organizací žádosti o předání utajovaných skutečností EU generálnímu tajemníkovi, vysokému představiteli, ve kterých upřesní účel předání skutečností a povahu a stupeň utajení požadovaných utajovaných skutečností.

   Žádosti mohou podat rovněž členské státy nebo decentralizované subjekty EU, které považují předání utajovaných skutečností EU za žádoucí; žadatelé upřesní cíle a výhody takového předání pro EU a povahu a stupeň utajení skutečností, jež mají být předány.

4. Žádost posoudí GSR, který:

   — získá stanovisko členského státu nebo případně decentralizovaného subjektu EU, kteří jsou původci předávaných skutečností,

   — vytvoří předběžné 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 Bezpečnostního výboru Rady nebo požádá, případně zjednodušeným písemným postupem, vnitrostátní bezpečnostní orgány členských států o přezkoumání s cílem získat technické stanovisko Bezpečnostního výboru.

5. Technický posudek Bezpečnostního výboru Rady 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 klasifikace nebo odtajnění skutečnosti původcem před předáním skutečnosti přijímající zemi nebo mezinárodní organizaci ([1]).

([1]) Orgán, který vydal dokument, uplatňuje postup vymezený v bodě 9 ve oddíle III pro všechny výtisky šířené v EU.

6. Generální tajemník, vysoký představitel předá Radě k rozhodnutí žádost a technické stanovisko Bezpečnostního výboru Rady, které získala bezpečnostní kancelář GSR.

BEZPEČNOSTNÍ PŘEDPISY, KTERÉ MUSÍ DODRŽOVAT PŘÍJEMCI

7. Generální tajemník/vysoký představitel oznámí přijímajícím státům nebo mezinárodním organizacím rozhodnutí Rady povolit předání utajovaných skutečností EU a předá jim srovnávací tabulku stupňů utajení platných v EU a v dotčených státech nebo organizacích. Podá-li žádost členský stát, oznámí příjemci povolení předání tento stát.

Rozhodnutí předat skutečnosti bude vykonatelné, pouze pokud příjemci přijmou písemný závazek, že:

— budou používat skutečnosti pouze ke stanoveným účelům,

— budou chránit skutečnosti v souladu s předpisy stanovenými Radou.

8. Nepřijme-li Rada na základě technického stanoviska Bezpečnostního výboru Rady rozhodnutí o zvláštním postupu pro nakládání s utajovanými dokumenty EU (odstranění poznámky o utajení EU, specifická označení atd.), budou stanovena následující pravidla ochrany.

V opačném případě se pravidla upraví.

9. *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 EU, 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 generálnímu tajemníkovi/vysokému představiteli.

10. *Předávání dokumentů*

a) Praktický postup při předávání dokumentů je přijat společnou dohodou bezpečnostní kanceláře GSR s bezpečnostními orgány přijímajících států nebo mezinárodních organizací na základě pravidel stanovených v oddílu VII těchto bezpečnostních předpisů. Tyto postupy uvedou zejména přesné adresy, na které mají být dokumenty zaslány, a kurýrní nebo poštovní služby používané pro předávání utajovaných skutečností EU.

b) Dokumenty se stupněm utajení CONFIDENTIEL UE a vyšším se předávají ve dvojité obálce. Vnitřní obálka se označí „EU“ 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 potom vloží do vnější obálky, na niž 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.

11. *Registrace*

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

12. *Vracení dokumentů*

Při vracení utajovaného dokumentu Radě nebo členskému státu, který jej předal, postupuje příjemce podle bodu 10.

13. *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 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 bezpečnostní kanceláře GSR je zakázáno pořizovat fotokopie dokumentu se stupněm utajení CONFIDENTIEL UE nebo vyšším nebo z něj pořizovat výpisy.

d) Je třeba vymezit a potvrdit společně s bezpečnostní kanceláří GSR postup pro rychlé a úplné zničení dokumentů v případě nouze.

14. *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.

15. *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 bezpečnostní kanceláři GSR nebo vnitrostátnímu bezpečnostnímu orgánu členského státu, který převzal iniciativu při přepravě dokumentů (s kopií pro bezpečnostní kancelář GSR);

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.

16. *Kontroly*

Bezpečnostní kancelář GSR je oprávněna po dohodě s dotčenými státy nebo mezinárodními organizacemi provádět ověření účinnosti opatření na ochranu předávaných utajovaných skutečností EU.

17. *Zprávy*

Má-li stát nebo organizace v držení utajované skutečnosti EU, předkládá každý rok ke dni stanovenému při udělení oprávnění k přijímání skutečností zprávu potvrzující dodržování bezpečnostních předpisů.

Dodatek 6

Obecné zásady pro předávání utajovaných skutečností EU třetím státům nebo mezinárodním organizacím

Spolupráce na úrovni 3

POSTUPY

1. Může dojít k tomu, že se Rada rozhodne za určitých zvláštních okolností spolupracovat se státy nebo organizacemi, které nemohou poskytnout záruky požadované těmito bezpečnostními předpisy, přestože tato spolupráce může vyžadovat předání utajovaných skutečností EU. Takto předávány nesmí být vnitrostátní skutečnosti speciálně vyhrazené členským státům.

2. Za těchto zvláštních okolností nejprve posoudí Rada z hlediska obsahu žádosti o spolupráci s EU podané třetími státy nebo mezinárodními organizacemi nebo navržené členskými státy nebo decentralizovanými subjekty EU a případně si vyžádá stanovisko členského státu nebo decentralizovaného subjektu, které jsou původci skutečnosti. Rada zváží vhodnost předání utajovaných skutečností, zhodnotí „potřebu vědět" příjemce a stanoví povahu utajovaných skutečností, které lze předávat.

3. Vysloví-li se Rada pro předání skutečností, svolá generální tajemník/vysoký představitel Bezpečnostní výbor Rady nebo požádá, případně zjednodušeným písemným postupem, vnitrostátní bezpečnostní orgány členských států o přezkoumání s cílem získat technické stanovisko Bezpečnostního výboru

4. Technické stanovisko Bezpečnostního výboru Rady 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 klasifikace nebo odtajnění skutečností původcem před jejich předáním dotčeným zemím nebo mezinárodním organizacím ([1]);

   d) postupů pro nakládání s dokumenty, které mají být předány (viz bod 5 níže);

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

5. Dokumenty předávané státům nebo organizacím podle této přílohy jsou v zásadě připraveny bez uvedení zdroje a stupně utajení EU. Bezpečnostní výbor Rady může doporučit:

   — přijetí zvláštního označení nebo kódovaného jména,

   — přijetí zvláštního systému klasifikace, který vytvoří vazbu mezi jednotlivými stupni citlivosti předávaných skutečností a kontrolními opatřeními, jež jsou potřebná na základě metod předávání dokumentů požadovaných od příjemce (viz příklady v bodu 14).

6. Bezpečnostní kancelář GSR předloží Radě technické stanovisko Bezpečnostního výboru a případně k němu přiloží návrhy na přenesení pravomocí nezbytných pro výkon úkolu, zejména v případech nouze.

7. Jakmile Rada schválí předání utajovaných skutečností EU a praktické prováděcí postupy, naváže bezpečnostní kancelář GSR nezbytné kontakty s bezpečnostní službou dotčeného státu nebo organizace, aby usnadnila uplatňování předpokládaných bezpečnostních opatření.

([1]) Orgán, který vydal dokument, uplatňuje postup vymezený v bodě 9 ve oddíle III pro všechny výtisky šířené v EU.

8. Bezpečnostní kancelář GSR předá pro informaci všem členským státům a případně decentralizovaným subjektům EU tabulku, v níž je uvedena povaha, stupeň utajení skutečností a organizace a země, do kterých mohou být na základě rozhodnutí Rady předány.

9. Vnitrostátní bezpečnostní orgán členského státu, který informace předává, nebo bezpečnostní kancelář GSR přijmou všechna nezbytná opatření, aby usnadnily zhodnocení škody a případné následné přepracování postupů.

10. Při každé změně podmínek spolupráce je třeba věc znovu předložit Radě.

BEZPEČNOSTNÍ PŘEDPISY, KTERÉ MUSÍ PŘÍJEMCI DODRŽOVAT

11. Generální tajemník, vysoký představitel oznámí přijímajícím státům nebo mezinárodním organizacím rozhodnutí Rady povolit předávání utajovaných skutečností EU a předá jim podrobná pravidla ochrany navržená Bezpečnostním výborem Rady a schválená Radou. Podá-li žádost členský stát, oznámí příjemci povolení předání tento stát.

Rozhodnutí předat skutečnosti bude vykonatelné, pouze pokud příjemci přijmou písemný závazek, že:

— budou používat skutečnosti pouze za účelem spolupráce schválené Radou,

— chránit skutečnosti podle požadavků Rady.

12. *Předávání dokumentů*

a) Praktický postup při předávání dokumentů je přijat společnou dohodou bezpečnostní kanceláře GSR 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 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.

13. *Registrace při převzetí*

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

14. *Používání a ochrana vyměňovaných utajovaných skutečností*

a) Skutečnosti se stupněm utajení 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 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 SECRET UE jsou zasílány diplomatickou poštou, bezpečnou poštovní službou a bezpečnými telekomunikačními prostředky. Dokument se stupněm utajení SECRET UE lze kopírovat pouze s písemným souhlasem původce. Všechny kopie jsou registrovány a kontrolovány. Pro všechny operace týkající se dokumentů stupně SECRET UE se vydávají potvrzení.

b) Skutečnosti se stupněm utajení 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 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 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.

15. *Zničení*

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

16. *Porušení bezpečnosti*

Dojde-li k vyzrazení skutečností se stupněm utajení CONFIDENTIEL UE nebo SECRET UE nebo vznikne-li podezření z vyzrazení, provede vnitrostátní bezpečnostní orgán státu nebo vedoucí bezpečnosti organizace šetření okolností vyzrazení. Je-li vyzrazení šetřením potvrzeno, je třeba upozornit původce. Přijmou se nezbytná opatření pro nápravu nevhodných postupů nebo způsobů uložení, pokud způsobily vyzrazení. Generální tajemník Rady/vysoký představitel nebo vnitrostátní bezpečnostní orgán členského státu, který předal vyzrazené skutečnosti, může požádat příjemce o upřesnění týkající se šetření.