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

►**B**

ROZHODNUTIE RADY

z 19. marca 2001

prijímajúce bezpečnostné nariadenia Rady

(2001/264/ES)

(Ú. v. ES L 101, 11.4.2001, s. 1)

Zmenené a doplnené:

		Úradný vestník		
		Č.	Strana	Dátum
►**M1**	Rozhodnutie Rady 2004/194/ES z 10. februára 2004	L 63	48	28.2.2004
►**M2**	Rozhodnutie Rady 2005/571/ES z 12. júla 2005	L 193	31	23.7.2005
►**M3**	Rozhodnutie Rady 2005/952/ES z 20. decembra 2005	L 346	18	29.12.2005

▼B

ROZHODNUTIE RADY

z 19. marca 2001

prijímajúce bezpečnostné nariadenia Rady

(2001/264/ES)

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o založení Európskeho spoločenstva a najmä na jej článok 207 ods. 3,

so zreteľom na rozhodnutie Rady 2000/396/ES, ESUO, Euratom z 5. júna 2000 prijímajúce rokovací poriadok Rady [1], a najmä na jeho článok 24,

keďže:

(1) S cieľom rozvoja aktivít Rady v oblastiach, ktoré vyžadujú určitú mieru dôvernosti, je vhodné ustanoviť jednotný bezpečnostný systém vzťahujúci sa na Radu, jej Generálny sekretariát a členské štáty.

(2) Takýto systém by mal v jednotnom texte spájať tento predmet, na ktorý sa vzťahujú všetky predchádzajúce rozhodnutia a ustanovenia v tej istej oblasti.

(3) V praxi podstatná časť informácií EÚ, ktoré sú utajené ako CONFIDENTIEL UE a vo vyššej kategórii, sa týka Spoločnej bezpečnostnej a obrannej politiky.

(4) S cieľom zaistenia účinnosti takto ustanoveného bezpečnostného systému, členské štáty by sa mali stotožňovať s jeho fungovaním prijímaním národných opatrení, pokiaľ ide o ustanovenia tohto rozhodnutia, ak ich príslušné orgány a zamestnanci pracujú s tajnými informáciami EÚ.

(5) Rada víta úmysel Komisie zaviesť do dátumu uplatňovania tohto rozhodnutia jednotný systém, ktorý je v súlade s prílohami tohto dokumentu, s cieľom zaistenia hladkého fungovania rozhodovacieho procesu v únii.

(6) Rada vyzdvihuje význam stotožnenia sa Európskeho parlamentu a Komisie s pravidlami a normami dôvernosti, ktoré sú potrebné na ochranu záujmov únie a jej členských štátov.

(7) Toto rozhodnutie sa prijíma bez vplyvu na článok 255 zmluvy a nástroje jeho vykonávania.

(8) Toto rozhodnutie sa prijíma bez toho, aby bola dotknutá prax existujúca v členských štátoch, pokiaľ ide o informovanie ich národných parlamentov o aktivitách únie,

ROZHODLA TAKTO:

Článok 1

Týmto sa schvaľujú bezpečnostné nariadenia Rady uvedené v prílohe.

Článok 2

1. Generálny tajomník/vysoký predstaviteľ prijíma vhodné opatrenia na zaistenie rešpektovania nariadení uvedených v článku 1 v rámci Generálneho sekretariátu Rady (ďalej uvádzaný ako GSC) v prípade práce s tajnými informáciami EÚ úradníkmi a inými zamestnancami GSC, externými dodávateľmi GSC a pracovníkmi dočasne pridelenými GSC, ako aj v rámci komplexu budov Rady a decentralizovaných úradov EÚ [2].

---

[1] Ú. v. ES L 149, 23.6.2000, s. 21.

[2] Pozri Závery Rady z 10. novembra 2000.

▼B

2. Členské štáty majú prijímať vhodné opatrenia v súlade s národnými dojednaniami na zaistenie rešpektovania nariadení uvedených v článku 1 v prípade práce s tajnými informáciami EÚ v rámci svojich štátnych služieb a prevádzkových kancelárií:

a) príslušníkmi stálych zastupiteľstiev členských štátov v Európskej únii, ako aj príslušníkmi národných delegácií, ktorí sa zúčastňujú na zasadnutiach Rady alebo jej orgánov alebo zúčastňujú sa na iných aktivitách Rady;

b) inými príslušníkmi národných administratív členských štátov, ktorí pracujú s tajnými informáciami EÚ pri výkone svojej funkcie na území členského štátu alebo v zahraničí a

c) externými dodávateľmi členských štátov a dočasne pridelenými pracovníkmi, ktorí pracujú s tajnými informáciami EÚ.

Členské štáty majú o prijatých opatreniach okamžite informovať GSC.

3. Opatrenia, ktoré sú uvedené v odsekoch 1 a 2, sa majú prijímať do 30. novembra 2001.

Článok 3

S cieľom dodržiavania základných princípov a minimálnych noriem bezpečnosti uvedených v časti 1 prílohy, generálny tajomník/vysoký predstaviteľ môže prijímať opatrenia v súlade s časťou II oddiel I(1) a (2) prílohy.

Článok 4

Toto rozhodnutie od dátumu jeho uplatňovania nahrádza:

a) rozhodnutie Rady 98/319/ES z 27. apríla 1998 týkajúce sa postupov, na základe ktorých môžu mať úradníci a zamestnanci Generálneho sekretariátu Rady prístup k tajným informáciám uchovávaným Radou ([1]);

b) rozhodnutie generálneho tajomníka/vysokého predstaviteľa z 27. júla 2000 o opatreniach na ochranu tajných informácií uplatniteľných na Generálny sekretariát Rady ([2]);

c) rozhodnutie 433/97 generálneho tajomníka Rady z 22. mája 1997 o postupe, pokiaľ ide o povolenie mať tajné informácie úradníkov zodpovedných za fungovanie parlamentnej siete.

Článok 5

1. Toto rozhodnutie nadobúda účinnosť dňom jeho uverejnenia.

2. Uplatňuje sa od 1. decembra 2001.

([1]) Ú. v. ES L 140, 12.5.1998, s. 12.
([2]) Ú. v. ES C 239, 23.8.2000, s. 1.

▼B

PRÍLOHA

BEZPEČNOSTNÉ NARIADENIA RADY EURÓPSKEJ ÚNIE

▼B

OBSAH

ČASŤ I

Základné princípy a minimálne normy bezpečnosti

ČASŤ II

ODDIEL I

Organizácia bezpečnosti v Rade Európskej únie

ODDIEL II

Utajenia a označovania

ODDIEL III

Riadenie utajenia

ODDIEL IV

Fyzická bezpečnosť

ODDIEL V

Všeobecné pravidlá pre princíp „potreby poznať“ a povolenie mať tajné informácie

ODDIEL VI

Postup na získanie povolenia mať tajné informácie pre úradníkov a iných zamestnancov GSC

ODDIEL VII

Príprava, distribúcia, prenos, uchovávanie a zničenie tajného materiálu EÚ

ODDIEL VIII

Trés secret UE/prísne tajné registre EÚ

ODDIEL IX

Bezpečnostné opatrenia, ktoré sa majú uplatňovať v čase určitých zasadnutí, ktoré sa konajú mimo komplexu budov Rady a ktoré zahŕňajú veľmi citlivé problémy

ODDIEL X

Porušenia bezpečnosti a ohrozenie tajných informácií EÚ

ODDIEL XI

Ochrana informácií spracovávaných v systémoch informačnej technológie a komunikačných systémoch

ODDIEL XII

Sprístupnenie tajných informácií EÚ tretím štátom alebo medzinárodným organizáciám

Dodatky

Dodatok 1

Zoznam orgánov národnej bezpečnosti

Dodatok 2

Porovnanie národných bezpečnostných utajení

Dodatok 3

Návod na praktické uskutočnenie utajenia

Dodatok 4

Usmernenia pre sprístupňovanie tajných informácií EÚ tretím štátom alebo medzinárodným organizáciám

▼B

— Spolupráca na úrovni 1

Dodatok 5

Usmernenia pre sprístupňovanie tajných informácií EÚ tretím štátom alebo medzinárodným organizáciám

— Spolupráca na úrovni 2

Dodatok 6

Usmernenia pre sprístupňovanie tajných informácií EÚ tretím štátom alebo medzinárodným organizáciám

— Spolupráca na úrovni 3

▼B

ČASŤ I

ZÁKLADNÉ PRINCÍPY A MINIMÁLNE NORMY BEZPEČNOSTI

ÚVOD

1. Tieto ustanovenia stanovujú základné princípy a minimálne normy bezpečnosti, ktoré má primeraným spôsobom dodržiavať Rada, Generálny sekretariát Rady (ďalej uvádzaný ako „GSC“), členské štáty a decentralizované orgány Európskej únie (ďalej uvádzané ako „decentralizované orgány EÚ“) kvôli ochrane bezpečnosti a uisteniu, že bola vytvorená spoločná norma ochrany.

2. Termín „tajné informácie EÚ“ znamená akékoľvek informácie a materiál, ktorých neoprávnené prezradenie by mohlo spôsobiť rôzne stupne poškodenia záujmov EÚ alebo jedného alebo viacerých jej členských štátov bez ohľadu na to, či takéto informácie pochádzajú z EÚ alebo sú získané z členských štátov, od tretích krajín alebo medzinárodných organizácií.

3. V týchto nariadeniach:

   a) „dokument“ znamená akúkoľvek listinu, poznámku, zápis, správu, memorandum, telegram/správu, náčrt, fotografiu, diapozitív, film, mapu, graf, plán, zápisník, šablónu, uhlíkovú pásku, pásku na písacom stroji alebo pásku tlačiarne, pásku, kazetu, počítačový disk, CD ROM alebo iné fyzické médium, na ktoré boli zaznamenané informácie;

   b) „materiál“ znamená „dokument“, ako je definovaný v a) vyššie a tiež akúkoľvek položku zariadenia alebo vybavenia, tiež spracovanú alebo ktorej spracovanie prebieha.

4. Bezpečnosť má nasledovné hlavné ciele:

   a) chrániť tajné informácie EÚ pred špionážou, ohrozením alebo neoprávneným prezradením;

   b) chrániť tajné informácie EÚ spracovávané v komunikačných a informačných systémoch a sieťach pred ohrozením ich celistvosti a dostupnosti;

   c) chrániť zariadenia, v ktorých sa nachádzajú informácie EÚ, pred sabotážou a svojvoľným zámerným poškodením;

   d) v prípade výskytu poruchy zhodnotiť spôsobené poškodenie, obmedziť jeho následky a prijať potrebné nápravné opatrenia.

5. Základmi správnej bezpečnosti sú:

   a) v každom členskom štáte organizácia národnej bezpečnosti zodpovedná za:

      i) zber a zaznamenávanie správ o špionáži, sabotáži, terorizme a iných podvratných činnostiach a

      ii) informácie a poskytovanie Rady svojej vláde a prostredníctvom nej Rade o povahe ohrození bezpečnosti a prostriedkoch ochrany pred nimi;

   b) v každom členskom štáte a v rámci GSC, technický orgán INFOSEC zodpovedný za spoluprácu s príslušným orgánom bezpečnosti s cieľom poskytovania informácií a Rady týkajúcej sa technických ohrození bezpečnosti a prostriedkov ochrany pred nimi;

   c) pravidelná spolupráca medzi oddeleniami vlády, orgánmi a príslušnými službami GSC kvôli stanoveniu a odporúčaniu, ak je to vhodné:

      i) ktoré informácie, zdroje a inštalácie sa majú chrániť a

      ii) stanoveniu spoločných noriem ochrany.

6. Ak ide o dôvernosť, potrebná je starostlivosť a skúsenosti pri výbere informácií a materiálu, ktoré sa majú chrániť, a stanovenie stupňa ochrany, ktorú požadujú. Podstatné je, aby stupeň ochrany odpovedal bezpečnostnému kritickému stavu jednotlivej informácie a materiálu, ktorý sa má chrániť.

▼B

S cieľom zaistenia hladkého toku informácií sa majú podniknúť kroky, aby sa zabránilo nadmernému utajovaniu. Systém utajenia je nástroj na realizovanie týchto princípov; podobný systém utajenia sa má dodržiavať pri spôsoboch plánovania a organizovania s cieľom reagovania na špionáž, sabotáž, terorizmus a iné ohrozenia tak, aby sa poskytovala najvyššia miera ochrany najdôležitejším budovám, v ktorých sú tajné informácie, a najcitlivejším miestam, ktoré sú v nich.

ZÁKLADNÉ PRINCÍPY

7. Bezpečnostné opatrenia:

a) sa majú vzťahovať na všetky osoby, ktoré majú prístup k tajným informáciám, médiám prenášajúcim tajné informácie, všetkým budovám, v ktorých sa nachádzajú takéto informácie, a dôležitým zariadeniam;

b) sa majú navrhovať tak, aby odhalili osoby, ktorých postoj by mohol ohroziť bezpečnosť tajných informácií a významných zariadení, v ktorých sa nachádzajú tajné informácie, a zabezpečiť ich vylúčenie alebo odstránenie;

c) majú zabrániť neoprávnenej osobe prístup k tajným informáciám alebo zariadeniam, v ktorých sa nachádzajú;

d) majú zaisťovať, aby sa tajné informácie rozširovali iba na základe princípu potreby poznať, ktorý je základný pre všetky stránky bezpečnosti;

e) majú zaisťovať integritu (t. j. predchádzanie korupcii alebo neoprávnenej zmene alebo neoprávnenému vymazaniu) a dostupnosť (t. j. nie je odmietnutý prístup pre tých, ktorí ho potrebujú a sú oprávnení mať tento prístup) všetkých informácií, tiež tajných alebo neutajených, a najmä takých informácií, ktoré sa uchovávajú, spracovávajú alebo prenášajú elektromagnetickou formou.

ORGANIZÁCIA BEZPEČNOSTI

Spoločné minimálne normy

8. Rada a každý členský štát má zaistiť dodržiavanie spoločných minimálnych noriem bezpečnosti vo všetkých administratívnych a/alebo vládnych oddeleniach, iných inštitúciách EÚ, orgánoch a u dodávateľov tak, aby sa mohli tajné informácie EÚ odovzdávať v dôvere, že sa s nimi bude pracovať s rovnakou starostlivosťou. Takéto minimálne normy majú obsahovať kritériá pre povolenie mať tajné informácie pre pracovníkov a postupy na ochranu tajných informácií EÚ. ►M3 Takéto minimálne normy takisto zahŕňajú minimálne normy, ktoré sa majú uplatniť v prípade, že GSR zmluvne zverí úlohy zahŕňajúce, predpokladajúce a/alebo obsahujúce utajované skutočnosti EÚ priemyselným alebo iným subjektom: tieto spoločné minimálne normy sú uvedené v oddiele XIII časti II. ◄

BEZPEČNOSŤ PRACOVNÍKOV

Povolenie pracovníkov mať tajné informácie

9. Všetky osoby, ktoré požadujú prístup k informáciám utajeným ako CONFIDENTIEL UE alebo vo vyššej kategórii, majú byť riadne preverené pred povolením takéhoto prístupu. Podobné preverenie sa požaduje v prípade osôb, ktorých povinnosti zahŕňajú technickú prevádzku alebo údržbu komunikačných a informačných systémov obsahujúcich tajné informácie. Toto preverenie sa má navrhovať tak, aby stanovilo, či takíto jednotlivci:

a) sú absolútne lojálni;

b) majú taký charakter a sú takí rozvážni, pokiaľ ide o povahu, že niet pochýb o ich bezúhonnosti pri práci s tajnými informáciami, alebo

c) môžu byť zraniteľní nátlakom z cudzích alebo iných zdrojov, napríklad kvôli bývalému miestu bydliska alebo minulým spojeniam, ktoré by mohli predstavovať riziko pre bezpečnosť.

Pri postupoch s cieľom poskytnutia povolenia mať tajné informácie treba venovať zvlášť dôkladné preskúmanie osobám:

▼B

d) ktorým sa má poskytnúť prístup k TRÉS SECRET UE/PRÍSNE TAJNÝM informáciám EÚ;

e) zastávajúcim funkcie vyžadujúce pravidelný prístup k značnému množstvu SECRET UE informácií;

f) ktorých povinnosti im poskytujú prístup ku komunikačným systémom s kritickým významom pre úlohu alebo informačným systémom a tým príležitosť získať neoprávnený prístup k rozsiahlym množstvám tajných informácií EÚ alebo možnosť uštedriť vážnu škodu, pokiaľ ide o poslanie úlohy prostredníctvom skutkov technickej sabotáže.

Za okolností uvedených v pododsekoch d), e) a f), najpraktickejšie je použitie techniky preskúmania predpokladov.

10. Ak sa majú použiť osoby, ktoré nemajú stanovenú „potrebu poznať“ za okolností, za ktorých môžu mať prístup k tajným informáciám EÚ (napríklad, kuriéri, bezpečnostní agenti, pracovníci údržby a upratovači atď.), majú najprv riadne získať povolenie mať tajné informácie.

Záznamy o osobných povoleniach mať tajné informácie

11. Všetky služby, orgány alebo inštitúcie pracujúce s tajnými informáciami EÚ alebo v ktorých sa nachádzajú komunikačné alebo informačné systémy mimoriadne dôležité pre úlohu majú udržiavať záznam o udelených povoleniach mať tajné informácie prideleným pracovníkom. Každé povolenie mať tajné informácie sa má overovať, ako vyžadujú okolnosti, aby sa zaistila jeho primeranosť pre aktuálnu úlohu danej osoby; treba ho znovu preverovať ako prioritnú záležitosť vždy, keď je prijatá nová informácia naznačujúca, že ďalšie pridelenie pre tajnú prácu už nie je viac v zhode so záujmami bezpečnosti. Záznam o povoleniach mať tajné informácie sa má uchovávať u vedúceho bezpečnosti pre príslušné služby, orgán alebo inštitúciu.

Bezpečnostné poučenie pracovníkov

12. Všetci pracovníci zamestnaní vo funkciách, kde by mohli mať prístup k tajným informáciám, majú byť dôkladne inštruovaní o potrebe bezpečnosti pri prevzatí úlohy a v pravidelných intervaloch a o postupoch na jej dosiahnutie. Vhodným postupom je požadovať, aby všetci takíto pracovníci písomne potvrdili, že plne porozumeli bezpečnostným predpisom príslušným pre ich zaradenie.

Zodpovednosti manažmentu

13. Vedúci sú povinní poznať svojich pracovníkov, ktorí sú zapojení do tajnej práce alebo ktorí majú prístup ku komunikačným systémom mimoriadne významným pre úlohu alebo informačným systémom a zaznamenávať a podávať správu o akýchkoľvek incidentoch alebo očividných zraniteľnostiach, ktoré by pravdepodobne mali vplyv na bezpečnosť.

Bezpečnostný status pracovníkov

14. Majú sa ustanoviť postupy na zaistenie, aby sa v prípade dozvedenia sa nepriaznivých informácií týkajúcich sa jednotlivca mohlo určiť, či tento jednotlivec je použitý pre tajnú prácu alebo má prístup ku komunikačným alebo informačným systémom s mimoriadnym významom pre úlohu a či bol informovaný príslušný orgán. Ak sa preukáže, že takýto jednotlivec predstavuje bezpečnostné riziko, treba ho vylúčiť alebo odstrániť z úloh, kde by mohol ohrozovať bezpečnosť.

FYZICKÁ BEZPEČNOSŤ

Potreba ochrany

15. Stupeň opatrení fyzickej bezpečnosti, ktoré sa majú uplatňovať na zaistenie ochrany tajných informácií EÚ, má byť úmerný utajeniu, rozsahu ohrozenia uchovávaných informácií a materiálu. Preto treba dbať na to, aby sa zabránilo prílišnému alebo nedostatočnému utajeniu, utajenie má podliehať pravidelnému revidovaniu. Všetci držitelia tajných informácií EÚ majú dodržiavať jednotné praktiky týkajúce sa utajenia týchto informácií a majú

▼B

spĺňať spoločné normy ochrany týkajúce sa úschovy, prenosu a nakladania s informáciami a materiálom vyžadujúcim ochranu.

Kontrola

16. Skôr ako priestory, v ktorých sa nachádzajú tajné informácie EÚ, zostanú bez dozoru, osoby, ktoré ich majú na starosti, majú zaistiť, aby boli bezpečne uschované a aby boli aktivované všetky bezpečnostné zariadenia (zámky, poplašné zariadenia atď.). Po pracovnom čase sa majú vykonávať ďalšie nezávislé kontroly.

Bezpečnosť budov

17. Budovy, v ktorých sa nachádzajú tajné informácie EÚ alebo komunikačné a informačné systémy, ktoré majú mimoriadny význam pre úlohu, majú byť chránené pred neoprávneným vstupom. Povaha ochrany, ktorá sa poskytuje tajným informáciám EÚ, napríklad uzavretie okien na závoru, zámky dverí, stráže pri vstupoch, automatizované systémy kontroly vstupu, bezpečnostné kontroly a hliadky, poplašné systémy, systémy na zisťovanie vstupu a strážne psy, závisí od:

a) utajenia, rozsahu a umiestnenia v budove informácií a materiálu, ktorý sa má chrániť;

b) kvality bezpečnostných kontajnerov pre tieto informácie a materiál;

c) fyzickej povahy a umiestnenia budovy.

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

Plány pre prípad výnimočných situácií

19. Vopred sa majú pripraviť podrobné plány na ochranu tajných informácií počas miestnych alebo národných výnimočných situácií

BEZPEČNOSŤ INFORMÁCIÍ (INFOSEC)

20. INFOSEC sa vzťahuje na identifikáciu a uplatňovanie bezpečnostných opatrení na ochranu informácií, spracovávaných, uchovávaných alebo prenášaných v komunikačných, informačných a iných elektronických systémoch pred stratou dôvernosti, celistvosti alebo dostupnosti, tiež náhodnou alebo zámernou. Majú sa prijať primerané protiopatrenia s cieľom zabránenia prístupu k informáciám EÚ neoprávneným osobám, aby sa predišlo odmietnutiu prístupu k informáciám EÚ oprávneným užívateľom a aby sa zabránilo korupcii alebo neoprávnenej zmene alebo vymazaniu informácií EÚ.

RUŠIACA SABOTÁŽ A INÉ FORMY ZÁKERNÉHO ÚMYSELNÉHO POŠKODENIA

21. Fyzické opatrenia na ochranu dôležitých zariadení, v ktorých sa nachádzajú tajné informácie, sú najlepšou bezpečnostnou ochranou proti sabotáži a zákernému úmyselnému poškodeniu a samotné povolenie mať tajné informácie nie je účinnou náhradou. Príslušný národný orgán má zhromažďovať informácie týkajúce sa špionáže, sabotáže, terorizmu a iných podvratných aktivít.

PRÍSTUPNENIE TAJNÝCH INFORMÁCIÍ TRETÍM ŠTÁTOM ALEBO MEDZINÁRODNÝM ORGANIZÁCIÁM

22. Rada má prijímať rozhodnutie o sprístupnení tajných informácií EÚ pochádzajúcich z Rady tretiemu štátu alebo medzinárodnej organizácii. Ak pôvodca informácií, ktorých sprístupnenie sa požaduje, nie je Rada, Rada sa snaží najprv získať súhlas pôvodcu na ich sprístupnenie. Ak nie je možné stanoviť pôvodcu, Rada má prevziať zodpovednosť pôvodcu.

23. Ak Rada dostane tajné informácie od tretích štátov, od medzinárodných organizácií alebo od tretích strán, týmto informáciám sa má poskytnúť ochrana primeraná ich utajeniu a ekvivalentná normám stanoveným

▼B

v týchto predpisoch pre tajné informácie EÚ alebo také vyššie normy, ako môže požadovať tretia strana sprístupňujúca informácie. Môžu sa dohodnúť spoločné kontroly.

24. Vyššie uvedené princípy sa majú vykonávať v súlade s podrobnými ustanoveniami uvedenými v časti II.

▼B

ČASŤ II

ODDIEL I

ORGANIZÁCIA BEZPEČNOSTI V RADE EURÓPSKEJ ÚNIE

Generálny tajomník/vysoký predstaviteľ

1. Generálny tajomník/vysoký predstaviteľ má:

   a) vykonávať bezpečnostnú politiku Rady;

   b) hodnotiť problémy bezpečnosti, ktoré mu predložila Rada alebo jej príslušné orgány;

   c) preskúmať otázky vyžadujúce zmeny v bezpečnostnej politike Rady, v úzkej spolupráci s orgánmi národnej bezpečnosti (alebo inými príslušnými) orgánmi členských štátov (ďalej „NSA“). Dodatok 1 obsahuje zoznam týchto orgánov.

2. Generálny tajomník/vysoký predstaviteľ je zodpovedný najmä za:

   a) koordinovanie všetkých záležitostí týkajúcich sa aktivít Rady;

   b) požadovanie, aby každý členský štát zriadil centrálny TRÉS SECRET UE/PRÍSNE TAJNÝ EÚ register, a požadovanie, aby takýto register bol zriadený v decentralizovaných orgánoch EÚ, ak je to vhodné;

   c) adresovanie označeným orgánom členských štátov požiadavky na orgány národnej bezpečnosti (NSA), aby zabezpečili povolenia mať tajné informácie pre pracovníkov zamestnaných v GSC v súlade s oddielom VI;

   d) prešetrenie alebo nariadenie prešetrenia akéhokoľvek úniku tajných informácií EÚ, ktorý sa vyskytol v GSC alebo akýchkoľvek decentralizovaných orgánoch EÚ na základe evidentného dôkazu;

   e) požadovanie od príslušných bezpečnostných orgánov, aby začali vyšetrovanie, ak sa zdá, že sa vyskytol únik tajných informácií EÚ mimo GSC alebo decentralizovaných orgánov EÚ a je zodpovedný za koordinovanie vyšetrovaní, ak je zaangažovaný viac ako jeden bezpečnostný orgán;

   f) vykonávanie, spolu s príslušnými orgánmi národnej bezpečnosti a s ich súhlasom, periodických kontrol bezpečnostných dojednaní na ochranu tajných informácií EÚ v členských štátoch;

   g) udržiavanie úzkej spolupráce so všetkými príslušnými bezpečnostnými orgánmi s cieľom dosiahnutia koordinácie bezpečnosti;

   h) dôsledné sledovanie bezpečnostnej politiky a postupov Rady a, ak sa tak požaduje, pripravovanie primeraného odporúčania. V tomto ohľade má predložiť Rade ročný plán kontroly pripravený bezpečnostným úradom Generálneho sekretariátu Rady.

Bezpečnostný výbor Rady

3. Potrebné je zriadiť bezpečnostný výbor. Výbor má pozostávať z predstaviteľov orgánov národnej bezpečnosti každého členského štátu. Predsedá mu generálny tajomník/vysoký predstaviteľ alebo jeho zástupca. Tiež predstavitelia decentralizovaných orgánov EÚ môžu byť prizvaní, aby sa zúčastnili, ak sa plánuje prediskutovanie otázok, ktoré sa ich týkajú.

4. Bezpečnostný výbor má zasadať podľa pokynov Rady na požiadanie generálneho tajomníka/vysokého predstaviteľa alebo orgánu národnej bezpečnosti. Výbor má právomoc prešetriť a hodnotiť všetky problémy bezpečnosti týkajúce sa konaní Rady a, ak je to vhodné, predkladať odporúčania Rade. Pokiaľ ide o aktivitu Generálneho sekretariátu Rady, výbor má právomoc predkladať odporúčania týkajúce sa problémov bezpečnosti generálnemu tajomníkovi/vysokému predstaviteľovi.

▼B

Bezpečnostný úrad Generálneho sekretariátu Rady

5. Na splnenie povinností, ktoré sú uvedené v odsekoch 1 a 2, generálny tajomník/vysoký predstaviteľ má mať k dispozícii bezpečnostný úrad Generálneho sekretariátu Rady s cieľom koordinácie, kontroly a vykonávania bezpečnostných opatrení.

6. Vedúci bezpečnostného úradu Generálneho sekretariátu Rady má byť hlavným poradcom generálnemu tajomníkovi/vysokému predstaviteľovi, pokiaľ ide o bezpečnostné otázky, a pôsobí ako tajomník pre bezpečnostný výbor. V tomto ohľade má viesť aktualizáciu bezpečnostných nariadení a koordinovať bezpečnostné opatrenia s príslušnými orgánmi členských štátov a, ak je to vhodné, s medzinárodnými organizáciami spojenými s Radou prostredníctvom bezpečnostných dohôd. V tomto zmysle pôsobí ako styčný úradník.

7. Vedúci bezpečnostného úradu Generálneho sekretariátu Rady má byť zodpovedný za akreditáciu systémov a sietí informačnej technológie (IT systémy a siete) v rámci Generálneho sekretariátu Rady. Vedúci bezpečnostného úradu Generálneho sekretariátu Rady a príslušný orgán národnej bezpečnosti majú spoločne rozhodovať, ak je to vhodné, o akreditácii IT systémov a sietí týkajúcich sa Generálneho sekretariátu Rady, členských štátov, decentralizovaných orgánov EÚ a/alebo tretích strán (štátov alebo medzinárodných organizácií).

Decentralizované orgány EÚ

8. Každý riaditeľ decentralizovaného orgánu EÚ má byť zodpovedný za vykonávanie bezpečnosti v rámci svojej inštitúcie. Zvyčajne menuje člena zo svojho pracovného kolektívu, ktorý je mu v tejto oblasti zodpovedný. Tento člen pracovného kolektívu sa označuje ako bezpečnostný úradník.

Členské štáty

9. Každý členský štát má stanoviť orgán národnej bezpečnosti (NSA) zodpovedný za bezpečnosť tajných informácií ([1]).

10. V rámci administratívy každého členského štátu, príslušný orgán národnej bezpečnosti má byť zodpovedný za:

    a) zachovanie bezpečnosti tajných informácií EÚ, ktoré uchováva akékoľvek národné oddelenie, orgán alebo úrad, štátny alebo súkromný, doma alebo v zahraničí;

    b) povoľovanie zriadenia TRÈS SECRET UE/PRÍNE TAJNÝCH EÚ registrov (toto oprávnenie sa môže previesť na kontrolného úradníka TRÈS SECRET UE/PRÍSNE TAJNÉHO EÚ centrálneho registra);

    c) pravidelnú kontrolu bezpečnostných dojednaní na ochranu tajných informácií EÚ;

    d) zaistenie, aby všetci štátni príslušníci, ako aj cudzinci zamestnaní v rámci národného oddelenia, orgánu alebo úradu, ktorí môžu mať prístup k informáciám EÚ utajeným ako TRÉS SECRET UE/PRÍSNE TAJNÉ INFORMÁCIE EÚ, SECRET UE a CONFIDENTIEL UE, mali povolenia mať tajné informácie;

    e) zostavovanie takých plánov bezpečnosti, ako považujú za potrebné, aby sa predišlo tomu, aby sa tajné informácie EÚ dostali do neoprávnených rúk.

Spoločné kontroly bezpečnosti

11. Bezpečnostný úrad Generálneho sekretariátu Rady a príslušný orgán národnej bezpečnosti majú spoločne a na základe vzájomnej dohody vykonávať pravidelné kontroly bezpečnostných dojednaní na ochranu tajných informácií EÚ na Generálnom sekretariáte Rady a v stálych zastupiteľstvách členských štátov v Európskej únii ([2]).

([1]) Pozrite si dodatok 1, v ktorom je uvedený zoznam orgánov národnej bezpečnosti zodpovedných za bezpečnosť tajných informácií EÚ.

([2]) Bez dosahu na Viedenský dohovor z roku 1961 o diplomatických vzťahoch.

▼B

12. Bezpečnostný úrad Generálneho sekretariátu Rady alebo na požiadanie generálneho tajomníka orgán národnej bezpečnosti hostiteľského členského štátu má vykonávať pravidelné kontroly bezpečnostných dojednaní na ochranu tajných informácií EÚ v decentralizovaných orgánoch EÚ.

▼B

ODDIEL II

UTAJENIA A OZNAČOVANIA

ÚROVNE UTAJENIA ([1])

Informácie sú utajované na nasledovných úrovniach:

1. TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ: toto utajenie sa má uplatňovať na informácie a materiál, ktorého neoprávnené prezradenie by mohlo spôsobiť mimoriadne vážne poškodenie hlavných záujmov Európskej únie alebo jedného alebo viacerých jej členských štátov.

2. SECRET UE: toto utajenie sa má uplatňovať iba na informácie a materiál, ktorého neoprávnené prezradenie by mohlo vážne poškodiť hlavné záujmy Európskej únie a jedného alebo viacerých jej členských štátov.

3. CONFIDENTIEL UE: toto utajenie sa má uplatňovať na informácie a materiál, ktorého neoprávnené prezradenie by mohlo poškodiť hlavné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov.

4. RESTREINT UE: toto utajenie sa má uplatňovať na informácie a materiál, ktorého prezradenie by mohlo byť nevýhodné pre záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov.

OZNAČENIA

5. Môže sa použiť označenie zachovávania opatrnosti na špecifikovanie oblasti, na ktorú sa vzťahuje dokument, alebo určitej distribúcie na základe potreby poznať.

6. Na dokumenty a ich kópie týkajúce sa bezpečnosti a obrany únie alebo jedného alebo viacerých jej členských štátov alebo týkajúce sa riadenia vojenskej alebo nevojenskej krízy sa má uplatňovať označenie ESDP/PESD.

7. Určité dokumenty, najmä týkajúce sa systémov informačnej technológie (IT), môžu mať ďalšie označenie doplňujúce bezpečnostné opatrenia, ako je definované v príslušných nariadeniach.

PRIPOJENIE UTAJENIA A OZNAČENÍ

8. Utajenie a označenia sa majú uplatňovať nasledovne:

   a) na dokumenty RESTREINT UE, mechanickými alebo elektronickými prostriedkami;

   b) na dokumenty CONFIDENTIEL UE, mechanickými prostriedkami a ručne alebo vytlačením na vopred opečiatkovaný zaregistrovaný dokument;

   c) na dokumenty SECRET UE a TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ, mechanickými prostriedkami a ručne.

([1]) V dodatku 2 môžete nájsť komparatívnu tabuľku stupňov bezpečnosti EÚ, NATO, WEU a členských štátov.

▼B

ODDIEL III

RIADENIE UTAJENIA

1. Informácie sa majú utajovať, iba ak je to potrebné. Utajenie má byť jasne a správne uvedené a má sa ponechať iba dovtedy, pokiaľ informácie požadujú ochranu.

2. Iba pôvodca informácií nesie zodpovednosť za utajenie informácií a za akékoľvek následné zaradenie do nižšej kategórie alebo odtajenie ([1]).

   Úradníci a iní zamestnanci Generálneho sekretariátu Rady majú utajovať informácie, zaraďovať do nižšej kategórie alebo odtajňovať informácie na základe pokynu od generálneho tajomníka alebo s jeho súhlasom.

3. Podrobné postupy na zaobchádzanie s tajnými dokumentmi boli tak rámcované, aby sa zaistila ochrana primeraná informáciám, ktoré obsahujú.

4. Treba zachovať minimálne množstvo osôb, ktoré sú oprávnené vytvárať TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ dokumenty a ich mená majú byť uvedené na zozname pripravenom Generálnym sekretariátom Rady, každým členským štátom a, ak je to vhodné, každým decentralizovaným orgánom EÚ.

UPLATŇOVANIE UTAJENÍ

5. Utajenie dokumentu má určovať úroveň citlivosti jeho obsahu v súlade s definíciou v oddiele II, odseky 1 až 4. Dôležité je, aby sa utajenie používalo správne a striedmo. Vzťahuje sa to najmä na utajenie TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ.

6. Pôvodca dokumentu, ktorý má uskutočniť utajenie, má mať pri tom na mysli nariadenia, ktoré boli uvedené vyššie a má potlačiť akúkoľvek tendenciu k nadmernému utajeniu alebo nedostatočnému utajeniu.

   Aj keď sa na prvý pohľad môže zdať, že vysoká miera utajenia je zárukou väčšej ochrany, rutinné nadmerné utajovanie môže viesť k strate dôvery, pokiaľ ide o platnosť systému utajovania.

   Na druhej strane, dokumenty sa nemajú nedostatočne utajovať s cieľom vyhýbať sa obmedzeniam spojeným s ochranou.

   Praktický návod na utajovanie je uvedený v dodatku 3.

7. Jednotlivé stránky, odseky, oddiely, prílohy, dodatky, pripojenia a vložky daného dokumentu môžu vyžadovať rôzne utajenia a majú sa podľa toho označovať. Utajenie dokumentu ako celok má takú mieru utajenia, ako má jeho najtajnejšia časť.

8. Utajenie dokumentu alebo zápisu obsahujúceho prílohy má mať takú mieru utajenia, ako je najvyššie utajenie jeho príloh. Pôvodca dokumentu má jasne uvádzať úroveň jeho utajenia v prípade jeho oddelenia sa od príloh.

ZARADENIE DO NIŽŠEJ KATEGÓRIE

9. Tajné dokumenty EÚ sa môžu zaradiť do nižšej kategórie alebo odtajiť iba s povolením ich pôvodcu a, ak je to potrebné, po prediskutovaní s ostatnými zainteresovanými stranami. Zaradenie do nižšej kategórie alebo odtajenie sa má potvrdiť písomne. Inštitúcia, členský štát, úrad, nástupnícka organizácia alebo vyšší orgán, od ktorého pochádza dokument, je zodpovedný za informovanie svojich adresátov o zmene a títo sú zasa zodpovední za informovanie o zmene dokumentu akýchkoľvek následných adresátov, ktorým poslali alebo skopírovali tento dokument.

10. Ak je to možné, pôvodcovia majú v utajených dokumentoch špecifikovať dátum alebo obdobie, kedy sa obsah môže zaradiť do nižšej kategórie alebo odtajiť. V opačnom prípade majú dokumenty revidovať aspoň každých päť rokov, aby sa presvedčili, že je potrebné pôvodné utajenie.

([1]) Zaradenie do nižšej kategórie (déclassement) znamená zníženie úrovne utajenia; odtajenie (déclassification) znamená odstránenie akéhokoľvek utajenia.

▼B

▼B

ODDIEL IV

FYZICKÁ BEZPEČNOSŤ

VŠEOBECNE

1. Hlavným cieľom opatrení fyzickej bezpečnosti je zabrániť neoprávnenej osobe získať prístup k tajným informáciám a/alebo materiálu EÚ.

BEZPEČNOSTNÉ POŽIADAVKY

2. Všetky prevádzky, priestory, budovy, úrady, miestnosti, komunikačné a informačné systémy atď., v ktorých sa uchovávajú a/alebo spracovávajú tajné informácie, a materiál EÚ sa majú chrániť prostredníctvom primeraných opatrení fyzickej bezpečnosti.

3. Pri rozhodovaní, do akej miery je potrebná ochrana fyzickej bezpečnosti, treba vziať do úvahy všetky dôležité faktory, ako sú:

   a) utajenie informácií a/alebo materiálu;

   b) množstvo a forma (napríklad vytlačená kópia, počítačové pamäťové médium) udržiavaných informácií;

   c) miestne stanovené ohrozenie spravodajskými službami, ktoré sa zameriavajú na EÚ, členské štáty a/alebo iné inštitúcie alebo tretie strany, ktoré majú tajné informácie EÚ, najmä pokiaľ ide o sabotáž, terorizmus a iné podvratné a/alebo kriminálne aktivity.

4. Uplatňované opatrenia fyzickej bezpečnosti majú byť určené tak, aby:

   a) odopreli nedovolený alebo vynútený vstup votrelca;

   b) zabránili, zadržali alebo zistili kroky nelojálnych pracovníkov (vlastný špión);

   c) zabránili tým úradníkom a iným zamestnancom Generálneho sekretariátu Rady, vládnych úradov členských štátov a/alebo iných inštitúcií alebo tretích strán, ktorí nepotrebujú poznať tieto informácie, aby mali prístup k tajným informáciám EÚ.

OPATRENIA FYZICKEJ BEZPEČNOSTI

Oblasti bezpečnosti

5. Oblasti, kde sa pracuje s informáciami utajenými ako CONFIDENTIEL UE alebo vo vyššej kategórii alebo sa tam uchovávajú, majú byť tak organizované a štruktúrované, aby odpovedali jednému z nasledovného:

   a) Oblasť bezpečnosti triedy I: oblasť, kde sa pracuje s informáciami CONFIDENTIEL UE alebo vo vyššej kategórii alebo sa tam uchovávajú takým spôsobom, že vstup do tejto oblasti predstavuje pre všetky praktické účely prístup k tajným informáciám. Takáto oblasť vyžaduje:

      i) jasne definovaný a chránený perimeter, prostredníctvom ktorého sa kontroluje každý vstup alebo výstup;

      ii) systém kontroly vstupu, ktorý vpustí iba tých, ktorí riadne prešli kontrolou a sú osobitne oprávnení vstúpiť do tejto oblasti;

      iii) špecifikáciu utajenia informácií, ktoré sa zvyčajne udržiavajú v tejto oblasti, t. j. informácií, ku ktorým bol poskytnutý prístup.

   b) Oblasť bezpečnosti triedy II: oblasť, kde sa spracovávajú alebo uchovávajú informácie CONFIDENTIEL UE alebo vo vyššej kategórii takým spôsobom, aby sa chránili pred prístupom neoprávnených osôb prostredníctvom interne stanovených kontrol, napríklad prevádzky obsahujúce kancelárie, v ktorých sa pravidelne spracovávajú a uchovávajú informácie CONFIDENTIEL UE alebo vo vyššej kategórii. Takáto oblasť vyžaduje:

      i) jasne definovaný a chránený perimeter, prostredníctvom ktorého sa kontroluje každý vstup alebo výstup;

▼B

ii) systém kontroly vstupu, ktorý vpustí bez doprovodu iba tých, ktorí prešli riadnou kontrolou a sú špeciálne oprávnení vstúpiť do tejto oblasti. Pre všetky ostatné osoby sa zabezpečia doprovody alebo ekvivalentné kontroly, aby sa zabránilo neoprávnenému prístupu k tajným informáciám EÚ a nekontrolovanému vstupu do oblasti podliehajúcej kontrolám technickej bezpečnosti

Tieto oblasti, na ktorých nie sú 24 hodín služobní pracovníci, sa majú skontrolovať okamžite po zvyčajnom pracovnom čase kvôli uisteniu, že tajné informácie EÚ sú riadne zabezpečené.

Administratívna oblasť

6. Môže sa vytvoriť administratívna oblasť nižšej bezpečnosti, ktorá je okolo oblasti bezpečnosti triedy I alebo triedy II, alebo vedie k tejto oblasti. Takáto oblasť vyžaduje jasne definovaný perimeter umožňujúci kontrolu pracovníkov a vozidiel. V administratívnych oblastiach sa majú spracovávať a uchovávať iba informácie RESTREINT UE.

Kontroly vstupu a výstupu

7. Vstup do bezpečnostných oblastí triedy I a triedy II sa má kontrolovať systémom preukazov alebo na základe osobného poznania uplatniteľného na stálych pracovníkov. Treba zriadiť tiež systém kontroly návštevníkov, ktorý je určený na zamietnutie neoprávneného prístupu k tajným informáciám EÚ. Systémy preukazov môže podporovať automatizovaná identifikácia, ktorú treba považovať za doplnok, ale nie za úplné nahradenie stráže. Zmena v hodnotení ohrozenia môže vyžadovať posilnenie kontrolných opatrení vstupu a výstupu, napríklad počas návštevy prominentných osôb.

Strážne hliadky

8. Po zvyčajnom pracovnom čase majú zaujať svoje miesto hliadky pre oblasti bezpečnosti triedy I a triedy II, aby chránili majetok EÚ proti ohrozeniu, poškodeniu alebo strate. Frekvenciu hliadok majú stanoviť miestne okolnosti ako odporúčajúca rada je, aby sa vykonávali každé štyri hodiny.

Bezpečnostné kontajnery a pancierové komory

9. Na uchovávanie tajných informácií EÚ sa majú používať tri triedy kontajnerov:

— trieda A: kontajnery národne schválené na uchovávanie TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ informácií v oblastiach bezpečnosti triedy I alebo triedy II,

— trieda B: kontajnery národne schválené na uchovávanie SECRET UE a CONFIDENTIEL UE informácií v rámci oblasti bezpečnosti triedy I alebo triedy II,

— trieda C: kancelársky nábytok vhodný na uchovávanie iba RESTREINT UE informácií.

10. Pre pancierové komory vyhotovené v rámci oblasti bezpečnosti triedy I alebo triedy II a pre všetky oblasti bezpečnosti triedy I, kde sa uchovávajú informácie utajené ako CONFIDENTIEL UE a vo vyššej kategórii na otvorených policiach alebo zobrazené na grafoch, mapách atď., majú byť steny, podlahy a stropy, dvere so zámkami certifikované orgánom národnej bezpečnosti ako poskytujúce ochranu ekvivalentnú triede bezpečnostného kontajnera schváleného na uchovávanie informácií rovnakého utajenia.

Zámky

11. Zámky použité v bezpečnostných kontajneroch a pancierových komorách, v ktorých sa uchovávajú tajné informácie EÚ, majú spĺňať nasledovné normy:

— skupina A: národne schválené pre kontajnery triedy A,

— skupina B: národne schválené pre kontajnery triedy B,

— skupina C: vhodné iba pre kancelársky nábytok triedy C.

▼B

Kontrola kľúčov a kombinácií

12. Kľúče od bezpečnostných kontajnerov sa nemajú brať z budovy úradu. Nastavenia kombinácie bezpečnostných kontajnerov si majú zapamätať osoby, ktoré ich potrebujú poznať. Kvôli použitiu v prípade núdze, bezpečnostný úradník príslušnej inštitúcie má byť zodpovedný za úschovu náhradných kľúčov a písomný záznam každého nastavenia kombinácie; majú sa držať v osobitne zapečatených nepriesvitných obálkach. Pracovné kľúče, náhradné bezpečnostné kľúče a nastavenia kombinácie sa majú držať v osobitných bezpečnostných kontajneroch. Týmto kľúčom a nastaveniam kombinácie treba venovať bezpečnostnú ochranu, ktorá nemá byť menej prísna ako je tá, ktorú má materiál, ku ktorému poskytujú prístup.

13. Poznanie nastavení kombinácie bezpečnostných kontajnerov sa má obmedziť na čo najmenší počet ľudí. Kombinácie sa majú prestavovať:

a) pri príjme nového kontajnera;

b) vždy, keď sa udeje zmena pracovníkov;

c) vždy, ak sa vyskytne ohrozenie alebo je podozrenie, že sa vyskytne;

d) v intervaloch najlepšie šesť mesiacov a aspoň každých 12 mesiacov.

Zariadenia na zistenie vniknutia

14. Ak sú použité poplašné systémy, uzavretý okruh televíznych a iných elektrických zariadení na ochranu tajných informácií EÚ, má byť k dispozícii núdzový elektrický zdroj na zaistenie neprerušenej prevádzky systému v prípade prerušenia hlavného energetického zdroja. Ďalšou základnou požiadavkou je, aby zlyhanie alebo poškodenie takýchto systémov malo za následok poplach alebo iné spoľahlivé upozornenie pracovníkov dozoru.

Schválené zariadenie

15. Orgány národnej bezpečnosti majú udržiavať aktuálne zoznamy podľa typu a modelu bezpečnostného zariadenia, ktoré sú z ich vlastných alebo z bilaterálnych zdrojov, schválených na priamu alebo nepriamu ochranu tajných informácií za rôznych presne stanovených okolností a podmienok. Bezpečnostný úrad Generálneho sekretariátu Rady má uchovávať podobný zoznam, ktorý sa okrem iného opiera o informácie z orgánov národnej bezpečnosti. Decentralizované orgány EÚ sa majú poradiť s bezpečnostným úradom Generálneho sekretariátu Rady a, ak je to vhodné, s orgánom národnej bezpečnosti svojho hostiteľského členského štátu pred nákupom takéhoto zariadenia.

Fyzická ochrana kopírovacích a telefaxových prístrojov

16. Kopírovacie a telefaxové prístroje sa majú fyzicky chrániť do toho rozsahu, ktorý je potrebný, aby ich mohli používať iba oprávnené osoby a aby všetky tajné produkty podliehali riadnym kontrolám.

OCHRANA PROTI PREHLIADANIU A NAČÚVANIU

Prehliadanie

17. Majú sa prijať všetky primerané opatrenia cez deň aj v noci, aby si žiadna neoprávnená osoba nemohla prezrieť tajné informácie EÚ, ani neúmyselne.

Načúvanie

18. Kancelárie alebo priestory, v ktorých sa pravidelne diskutuje o tajných informáciách SECRET UE alebo patriacich do vyššej kategórie, sa majú chrániť pred pokusom o pasívne a aktívne načúvanie, ak to riziko vyžaduje. Zhodnotenie rizika takýchto pokusov má byť povinnosťou príslušného bezpečnostného orgánu, ak je to potrebné, po porade s orgánmi národnej bezpečnosti.

19. Bezpečnostný úrad Generálneho sekretariátu Rady môže požiadať o pomoc odborníkov z orgánov národnej bezpečnosti pri stanovovaní ochranných opatrení, ktoré sa majú prijať v prevádzkach citlivých na pasívne načúvanie (napríklad izolácia stien, dverí, podlahy a stropov, miera ohrozujúcich

▼B

emanácií) a na aktívne načúvanie (napríklad hľadanie mikrofónov). Bezpečnostní úradníci z decentralizovaných orgánov EÚ môžu požiadať o technické kontroly, ktoré má vykonať bezpečnostný úrad Generálneho sekretariátu Rady a/alebo o pomoc odborníkov s orgánov národnej bezpečnosti.

20. Podobne, ak tak vyžadujú okolnosti, môžu na požiadanie príslušného bezpečnostného úradníka odborníci z orgánov národnej bezpečnosti pre technickú bezpečnosť skontrolovať telekomunikačné zariadenie a elektrické alebo elektronické kancelárske zariadenie akéhokoľvek druhu počas stretnutí na úrovni SECRET UE alebo na vyššej úrovni.

TECHNICKY BEZPEČNÉ OBLASTI

21. Určité oblasti sa môžu označiť ako technicky bezpečné oblasti. Treba vykonať zvláštnu vstupnú kontrolu. Takéto oblasti, ak nie sú obsadené, majú sa udržiavať uzavreté schválenou metódou a všetky kľúče sa majú považovať za bezpečnostné kľúče. Tieto oblasti podliehajú pravidelným fyzickým kontrolám, ktoré sa majú vykonávať tiež po akomkoľvek neoprávnenom vstupe alebo podozrení takéto vstupu.

22. Treba udržiavať podrobný súpis zariadenia a nábytku, aby sa mohol monitorovať jeho pohyb. Žiaden predmet nábytku alebo zariadenia sa nemá priniesť do takejto oblasti, pokiaľ sa nepodrobil dôkladnej kontrole špeciálne vyškolenými bezpečnostnými pracovníkmi, ktorí sú určení na zisťovanie akýchkoľvek odpočúvacích zariadení. Spravidla je potrebné vyhnúť sa inštalácii komunikačných liniek v technicky bezpečných oblastiach.

▼B

ODDIEL V

VŠEOBECNÉ PRAVIDLÁ PRE PRINCÍP POTREBY POZNAŤ A POVOLENIE MAŤ TAJNÉ INFORMÁCIE

1. Prístup k tajným informáciám EÚ sa má povoliť iba osobám, ktoré majú „potrebu poznať“ na vykonávanie svojich povinností alebo úloh. Prístup k informáciám TRÉS SECRET UE/PRÍSNE TAJNÝM EÚ, SECRET UE a CONFIDENTIEL UE sa má povoliť iba osobám, ktoré majú príslušné povolenie mať tajné informácie.

2. Zodpovednosť za stanovenie „potreby poznať“ majú v rámci Generálneho sekretariátu Rady, decentralizované orgány EÚ a služby alebo oddelenie členského štátu, v ktorom má byť príslušná osoba zamestnaná, podľa požiadaviek úlohy.

3. Prekontrolovanie pracovníkov je povinnosťou zamestnávateľa úradníka na základe príslušných uplatniteľných postupov. Pokiaľ ide o úradníkov a iných zamestnancov Generálneho sekretariátu Rady, postup na získanie povolenia mať tajné informácie je uvedený v oddiele VI.

   Tento postup bude viesť k vydaniu „povolenia mať tajné informácie“ uvádzajúceho úroveň tajných informácií, ku ktorým môže mať preverená osoba prístup, a dátum jeho uplynutia.

   Povolenie mať tajné informácie pre dané utajenie môže poskytovať jeho držiteľovi prístup k informáciám s nižším utajením.

4. Osoby, iné ako úradníci alebo iní zamestnanci Generálneho sekretariátu Rady alebo členských štátov, napríklad príslušníci, úradníci alebo zamestnanci inštitúcií EÚ, s ktorými môže byť potrebné prediskutovať alebo ktorým môže byť potrebné ukázať tajné informácie EÚ, musia mať povolenie, pokiaľ ide o tajné informácie EÚ, a musia byť informované, čo sa týka o ich zodpovednosti za bezpečnosť. To isté pravidlo sa má uplatňovať za podobných okolností na externých dodávateľov, odborníkov alebo konzultantov.

ZVLÁŠTNE PRAVIDLÁ PRE PRÍSTUP K TRÉS SECRET UE/PRÍSNE TAJNÝM INFORMÁCIÁM EÚ

5. Všetky osoby, ktoré majú mať prístup k TRÉS SECRET UE/PRÍSNE TAJNÝM informáciám EÚ, sa majú najprv preveriť pre prístup k takýmto informáciám.

6. Všetky osoby, od ktorých sa vyžaduje, aby mali prístup k TRÉS SECRET UE/PRÍSNE TAJNÝM informáciám EÚ, majú byť označené vedúcim ich oddelenia a ich mená sa majú uchovávať v príslušnom TRÉS SECRET/PRÍSNE TAJNOM EÚ registri.

7. Skôr, ako majú mať prístup k TRÉS SECRET UE/PRÍSNE TAJNÝM informáciám EÚ, všetky osoby majú podpísať potvrdenie v tom zmysle, že boli inštruované o bezpečnostných postupoch Rady a že plne porozumeli svojej zvláštnej zodpovednosti za ochranu TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ informácií a chápu následky, ktoré ustanovujú pravidlá EÚ a národné právo alebo administratívne pravidlá, ak sa tajné informácie dostanú do neoprávnených rúk zámerne alebo v dôsledku hrubej nedbalosti.

8. V prípade osôb, ktoré majú prístup k TRÉS SECRET UE/PRÍSNE TAJNÝM EÚ informáciám na zasadnutiach atď., príslušný pracovník kontroly služieb alebo orgánu, v ktorom je táto osoba zamestnaná, má informovať orgán organizujúci zasadnutie, že dané osoby majú takéto povolenie.

9. Mená všetkých osôb, ktorých povinnosti už viac nevyžadujú prístup k TRÉS SECRET UE/PRÍSNE TAJNÝM informáciám EÚ, sa majú odstrániť z TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ zoznamu. Okrem toho, všetky takéto osoby treba upozorniť na ich zvláštnu zodpovednosť za ochranu TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ informácií. Majú tiež podpísať vyhlásenie uvádzajúce, že nikdy nepoužijú ani neodovzdajú TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ informácie, ktoré majú.

▼B

ZVLÁŠTNE PRAVIDLÁ PRE PRÍSTUP K INFORMÁCIÁM SECRET UE A CONFIDENTIEL UE

10. Všetky osoby, ktoré majú mať prístup k informáciám SECRET UE alebo CONFIDENTIEL UE, sa majú najprv do vhodnej miery prekádrovať.

11. Všetky osoby, ktoré majú mať prístup k informáciám SECRET UE alebo CONFIDENTIEL UE, sa majú oboznámiť s príslušnými bezpečnostnými nariadeniami a majú byť informované o dôsledkoch nedbalosti.

12. V prípade osôb, ktoré majú prístup k informáciám SECRET UE alebo CONFIDENTIEL UE na zasadnutiach atď., bezpečnostný úradník orgánu, v ktorom je táto osoba zamestnaná, má informovať orgán organizujúci zasadnutie, že príslušné osoby majú takéto povolenie.

ZVLÁŠTNE PRAVIDLÁ PRE PRÍSTUP K INFORMÁCIÁM RESTREINT UE

13. Osoby s prístupom k informáciám RESTREINT UE majú byť oboznámené s bezpečnostnými nariadeniami a s dôsledkami nedbalosti.

PREVODY

14. Ak je príslušník pracovného kolektívu preložený z miesta, ktoré vyžaduje prácu s tajným materiálom EÚ, registračný úrad má dohliadať na správne odovzdanie tohto materiálu odchádzajúcim úradníkom prichádzajúcemu úradníkovi.

ZVLÁŠTNE POKYNY

15. Osoby, od ktorých sa vyžaduje práca s tajnými informáciami EÚ, by mali byť pri prvom prevzatí svojich povinností a pravidelne potom oboznámené s:

    a) nebezpečenstvami pre bezpečnosť vznikajúcimi z nediskrétneho rozhovoru;

    b) opatreniami, ktoré treba prijať vo vzťahu s tlačou;

    c) ohrozeniami, ktoré predstavujú aktivity spravodajských služieb, ktoré sa zameriavajú na EÚ a členské štáty, pokiaľ ide o tajné informácie a aktivity EÚ;

    d) povinnosťou okamžite informovať príslušné bezpečnostné orgány o akomkoľvek prístupe alebo manévri, ktorý vedie k podozreniam zo špionážnej aktivity alebo o akýchkoľvek nezvyčajných okolnostiach týkajúcich sa bezpečnosti.

16. Všetky osoby, ktoré často prichádzajú do styku s predstaviteľmi krajín, ktorých spravodajské služby sa zameriavajú na EÚ a členské štáty, pokiaľ ide o tajné informácie a aktivity EÚ, majú byť inštruované o technikách, ktoré sú známe, že ich používajú rôzne spravodajské služby.

17. Neexistujú žiadne bezpečnostné nariadenia Rady týkajúce sa súkromnej cesty na akékoľvek miesto pracovníkmi, ktorí boli preverení s cieľom prístupu k tajným informáciám EÚ. Ale príslušné bezpečnostné orgány by mali oboznámiť úradníkov a iných zamestnancov, ktorí spadajú pod ich zodpovednosť, s cestovnými nariadeniami, ktorým môžu podliehať. Povinnosťou bezpečnostných úradníkov má byť zorganizovať doplňujúce stretnutia pre príslušníkov pracovného kolektívu týkajúce sa týchto zvláštnych pokynov.

▼B

ODDIEL VI

POSTUP NA ZÍSKANIE POVOLENIA MAŤ TAJNÉ INFORMÁCIE PRE PRACOVNÍKOV A INÝCH ZAMESTNANCOV GENERÁLNEHO SEKRETARIÁTU RADY

1. Prístup k informáciám majú mať iba úradníci a iní pracovníci generálneho sekretariátu Rady alebo osoby pracujúce v rámci Generálneho sekretariátu Rady, ktoré z dôvodu svojich povinností a kvôli požiadavkám funkcie potrebujú poznať alebo používať tajné informácie, ktorých držiteľom je Rada.

2. Aby mohli mať osoby uvedené v odseku 1 prístup k informáciám utajeným ako „TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ“, „SECRET UE“ a „CONFIDENTIEL UE“, musia byť oprávnené v súlade s postupom uvedeným v odsekoch 4 a 5.

3. Povolenie sa má poskytovať iba osobám, ktoré sa podrobili bezpečnostnej kontrole vykonanej príslušnými národnými orgánmi členských štátov (NSA) v súlade s postupom uvedeným v odsekoch 6 až 10.

4. Menovací orgán v zmysle článku 2 prvý pododsek personálneho poriadku je zodpovedný za poskytovanie povolení uvedených v odsekoch 1, 2 a 3.

   Menovací orgán má udeliť povolenie po získaní stanoviska príslušných národných orgánov členských štátov na základe bezpečnostného prekádrovania vykonaného v súlade s odsekom 6 až 12.

5. Povolenie, ktoré je platné počas obdobia piatich rokov, nesmie prekročiť dobu trvania úloh, na základe ktorých bolo udelené. Menovací orgán ho môže obnovovať v súlade s postupom uvedeným v odseku 4.

   Menovací orgán má stiahnuť povolenie, ak sa domnieva, že existujú k tomu opodstatnené dôvody. Akékoľvek rozhodnutie stiahnuť povolenie treba oznámiť príslušnej osobe, ktorá môže požadovať, aby ju vypočul menovací orgán a príslušný národný orgán.

6. Cieľom bezpečnostného prekádrovania má byť stanoviť, že neexistujú žiadne námietky, pokiaľ ide o dovolenie, aby osoba mala prístup k tajným informáciám uchovávaným Radou.

7. Bezpečnostné prekádrovanie majú vykonať za pomoci príslušnej osoby a na požiadanie menovacieho orgánu príslušné národné orgány členského štátu, ktorého štátnym príslušníkom je osoba, ktorá je subjektom povolenia. Ak by príslušná osoba mala trvalé bydlisko na území iného členského štátu, príslušné národné orgány môžu zabezpečiť spoluprácu s orgánmi štátu trvalého bydliska.

8. Ako súčasť procesu prekádrovania možno požiadať príslušnú osobu o vyplnenie osobného informačného formulára.

9. Menovací orgán špecifikuje vo svojej žiadosti typ a úroveň tajných informácií, ktoré majú byť sprístupnené príslušnej osobe tak, aby mohli príslušné národné orgány vykonať proces prekádrovania a poskytnúť svoje stanovisko, pokiaľ ide o úroveň povolenia, ktorá by bola vhodná, aby sa poskytla tejto osobe.

10. Celý proces bezpečnostného kádrovania spolu so získanými výsledkami podlieha príslušným pravidlám a nariadeniam platným v danom členskom štáte, vrátane tých, ktoré sa týkajú odvolaní.

11. Ak príslušné národné orgány členského štátu poskytnú kladné stanovisko, menovací orgán môže udeliť povolenie príslušnej osobe.

12. Negatívne stanovisko majú príslušné národné orgány oznámiť danej osobe, ktorá môže požiadať, aby bola vypočutá menovacím orgánom. Ak sa domnieva, že je to potrebné, menovací orgán môže požiadať príslušné národné orgány o akékoľvek ďalšie objasnenie, ktoré môžu poskytnúť. Ak sa potvrdí negatívne stanovisko, povolenie sa neudelí.

13. Všetky osoby, ktorým sa udeľuje povolenie v zmysle odsekov 4 a 5, majú v čase udelenia tohto povolenia a potom v pravidelných intervaloch dostať

▼B

akékoľvek potrebné pokyny týkajúce sa ochrany tajných informácií a prostriedkov na zaistenie takejto ochrany. Takéto osoby podpíšu vyhlásenie potvrdzujúce prijatie týchto pokynov, v ktorom súhlasia s ich dodržiavaním.

14. Menovací orgán má prijímať akékoľvek opatrenia na vykonávanie tohto oddielu, najmä pokiaľ ide o pravidlá upravujúce prístup k zoznamu oprávnených osôb.

15. Výnimočne, ak to vyžaduje výkon služby, menovací orgán môže po poskytnutí oznámenia príslušných národných orgánov a za predpokladu, že do jedného mesiaca nie je od nich žiadna reakcia, udeliť dočasné oprávnenie na obdobie nepresahujúce šesť mesiacov, až do výsledku kádrovania uvedeného v odseku 7.

16. Predbežné a dočasné oprávnenia, ktoré sú takto udelené, nemajú poskytovať prístup k TRÉS SECRET UE/PRÍSNE TAJNÝM EÚ informáciám; takýto prístup sa má obmedziť na úradníkov, ktorí skutočne prešli prekádrovaním s kladnými výsledkami v súlade s odsekom 7. Až do výsledku kádrovania môže sa úradníkom, ktorí sú požiadaní, aby prešli kontrolou na úrovni TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ, povoliť dočasne a predbežne prístup k informáciám utajeným až do úrovne SECRET UE vrátane tejto úrovne.

▼B

ODDIEL VII

PRÍPRAVA, DISTRIBÚCIA, PRENOS, UCHOVÁVANIE A ZNIČENIE TAJNÉHO MATERIÁLU EÚ

Obsah

Všeobecné ustanovenia	
Kapitola I	Príprava a distribúcia tajných dokumentov EÚ
Kapitola II	Prenos tajných dokumentov EÚ
Kapitola III	Elektrické a iné prostriedky technického prenosu
Kapitola IV	Zvláštne kópie a preklady a výňatky z tajných dokumentov EÚ
Kapitola V	Inventárne zoznamy a kontroly, uchovávanie a zničenie tajných dokumentov EÚ
Kapitola VI	Osobitné pravidlá uplatniteľné na dokumenty určené Rade

▼B

Všeobecné ustanovenia

Tento oddiel podrobne uvádza opatrenia na prípravu, distribúciu, prenos, uchovávanie a zničenie tajných dokumentov EÚ, ako je definované v odseku 3a) základných princípov a minimálnych noriem bezpečnosti vysvetlených v časti I tejto prílohy. Má sa používať ako odvolávka na prispôsobovanie týchto pravidiel pre iný tajný materiál EÚ, podľa jeho typu a na základe prípadu za prípadom.

Kapitola I

Príprava a distribúcia tajných dokumentov EÚ

PRÍPRAVA

1. Utajenia a označenia EÚ sa majú uplatňovať, ako je ustanovené v oddiele II a majú byť uvedené hore a dole v strede každej strany a každá strana má byť očíslovaná. Každý tajný dokument EÚ má uvádzať referenčné číslo a dátum. V prípade TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov a dokumentov SECRET UE sa toto referenčné číslo uvádza na každej strane. Ak sa majú distribuovať v niekoľkých kópiách, každá má mať číslo kópie, ktoré je uvedené na prvej strane, spolu s celkovým počtom strán. Všetky prílohy a dodatky majú byť uvedené v zozname na prvej strane dokumentu utajeného ako CONFIDENTIEL UE alebo vo vyššej kategórii.

2. Dokumenty utajené ako CONFIDENTIEL UE a vo vyššej kategórii majú písať, prekladať, uchovávať, vytvárať fotokópie z nich, reprodukovať magneticky alebo pomocou mikrofilmu iba osoby, ktoré boli preverené s cieľom prístupu k tajným informáciám EÚ aspoň do príslušného bezpečnostného utajenia daného dokumentu, okrem zvláštneho prípadu opísaného v odseku 27 tohto oddielu.

   Ustanovenia upravujúce vytváranie tajných dokumentov na počítači sú vysvetlené v oddiele XI.

DISTRIBÚCIA

3. Tajné informácie EÚ sa majú distribuovať iba osobám, ktoré ich potrebujú poznať a majú príslušné povolenie mať tajné informácie. Počiatočnú distribúciu špecifikuje ich pôvodca.

4. TRÉS SECRET UE/PRÍSNE TAJNÉ dokumenty EÚ sa majú dávať do obehu prostredníctvom TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ registrov (pozri oddiel VIII). V prípade TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ správ môže príslušný register povoliť vedúcemu komunikačného strediska vytvorenie množstva kópií, ktoré je uvedené v zozname adresátov.

5. Dokumenty, ktoré sú utajené ako SECRET UE a v nižšej kategórii, môže ďalej distribuovať pôvodný adresát iným adresátom na základe potreby poznať. Orgány, od ktorých pochádzajú, majú však jasne stanoviť akékoľvek upozornenia, ktoré chcú uložiť. Ak sú uložené takéto upozornenia, príjemcovia môžu ďalej distribuovať dokumenty iba s povolením orgánov, od ktorých pochádzajú.

6. Každý dokument, ktorý je utajený ako CONFIDENTIEL UE alebo vo vyššej kategórii, sa má zaznamenať pri príchode alebo opustení inštitúcie do registra tejto inštitúcie. Údaje, ktoré sa majú zadávať (odvolávky, dátum a, ak je to uplatniteľné, počet kópií), majú byť také, aby sa umožnila identifikácia dokumentov a zápis do denníka alebo na špeciálne chránené počítačové médium.

Kapitola II

Prenos tajných dokumentov EÚ

BALENIE

7. Dokumenty utajené ako CONFIDENTIEL UE alebo vo vyššej kategórii sa majú prenášať v neporušených nepriesvitných dvojitých obálkach. Vnútorná obálka má byť označená príslušným bezpečnostným utajením EÚ a, ak je to

▼B

možné, má tiež uvádzať úplné údaje týkajúce sa názvu pracoviska príjemcu a adresy.

8. Iba kontrolný úradník registračného úradu alebo jeho zástupca môže otvoriť vnútornú obálku a potvrdiť príjem priložených dokumentov, pokiaľ obálka nie je adresovaná jednotlivcovi. V takomto prípade registračný úrad má zaprotokolovať príchod obálky a iba jednotlivec, ktorému je adresovaná, môže otvoriť vnútornú obálku a potvrdiť príjem dokumentov, ktoré obsahuje.

9. Vo vnútornej obálke sa má nachádzať príjmový formulár. Príjem, ktorý nie je tajný, má uvádzať referenčné číslo, dátum a číslo kópie dokumentu, ale nikdy nie predmet.

10. Vnútorná obálka má byť vložená do vonkajšej obálky, na ktorej je číslo zásielky pre účely prijatia. Za žiadnych okolností sa bezpečnostné utajenie neuvádza na vonkajšej obálke.

11. Pre dokumenty utajené ako CONFIDENTIEL EU alebo vo vyššej kategórii si kuriéri alebo doručovatelia majú nechať potvrdiť príjem odpovedajúci číslam zásielok.

PRENOS V RÁMCI BUDOVY ALEBO SKUPINY BUDOV

12. V rámci danej budovy alebo skupiny budov môžu sa prenášať tajné dokumenty v zapečatenej obálke uvádzajúcej iba meno adresáta pod podmienkou, že ich prenáša osoba, ktorá prešla skúškou, pokiaľ ide o úroveň utajenia dokumentov.

PRENOS DOKUMENTOV EÚ V RÁMCI KRAJINY

13. TRÉS SECRET UE/PRÍSNE TAJNÉ dokumenty EÚ by sa mali posielať prostredníctvom oficiálnych kuriérskych služieb alebo osôb oprávnených mať prístup k TRÉS SECRET UE/PRÍSNE TAJNÝM EÚ informáciám.

14. Vždy, keď sa použijú kuriérske služby na odovzdanie TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ dokumentu mimo hraníc budovy alebo skupiny budov, treba sa prispôsobiť ustanoveniam týkajúcim sa balenia a prevzatia uvedeným v tejto kapitole. Doručovacie služby majú byť tak vybavené personálom, aby sa zaistilo, aby zásielky obsahujúce TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ dokumenty zostali celý čas pod priamym dohľadom zodpovedného úradníka.

15. Výnimočne TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ dokumenty môžu prijať úradníci, iní ako kuriéri, mimo hraníc budovy alebo skupiny budov pre miestne použitie na stretnutiach a diskusiách pod podmienkou, že:

    a) doručovateľ je oprávnený mať prístup k týmto TRÉS SECRET UE/PRÍSNE TAJNÝM EÚ dokumentom;

    b) spôsob prepravy vyhovuje národným pravidlám upravujúcim prenos národných PRÍSNE TAJNÝCH dokumentov;

    c) za žiadnych okolností úradník nenechá TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ dokumenty bez dozoru;

    d) uskutočnené sú dojednania týkajúce sa zoznamu dokumentov takto prepravovaných, ktoré sa majú držať v TRÉS SECRET UE/PRÍSNE TAJNOM EÚ registri uchovávajúcom dokumenty a ktoré sú zaznamenané do denníka a kontrolované voči tomuto záznamu pri ich vrátení.

16. V rámci danej krajiny SECRET UE a CONFIDENTIEL UE dokumenty sa môžu posielať poštou, ak je takýto spôsob prenosu povolený podľa národných nariadení a je v súlade s ustanoveniami týchto nariadení alebo kuriérskou službou alebo osobami, ktoré prešli skúškou, pokiaľ ide o prístup k tajným informáciám EÚ.

17. Každý členský štát alebo decentralizovaný orgán EÚ by mal pripraviť pokyny pre osobné odovzdávanie tajných dokumentov EÚ založené na týchto nariadeniach. Doručovateľ má byť požiadaný, aby si prečítal a podpísal tieto pokyny. Tieto pokyny majú vysvetľovať najmä, že za žiadnych okolností dokumenty:

▼B

a) sa nemajú dostať z držby doručovateľa, pokiaľ nie sú v bezpečnej úschove v súlade s ustanoveniami uvedenými v oddiele IV;

b) nemajú zostať bez dozoru pri verejnej preprave alebo v súkromných vozidlách alebo na miestach ako sú reštaurácie alebo hotely. Nesmú sa uložiť v hotelových trezoroch alebo nechať bez dozoru v hotelových izbách;

c) sa nesmú čítať na verejných miestach, ako je letisko alebo vlaky.

PRENOS Z JEDNÉHO ČLENSKÉHO ŠTÁTU DO DRUHÉHO

18. Materiál utajený ako CONFIDENTIEL UE alebo vo vyššej kategórii sa má prepravovať z jedného členského štátu do druhého diplomatickými alebo vojenskými kuriérskymi službami.

19. Avšak, môže sa povoliť osobná preprava materiálu utajeného ako SECRET UE a CONFIDENTIEL UE, ak je preprava tak zabezpečená, aby sa zaistilo, že sa nemôže dostať do rúk žiadnych neoprávnených osôb.

20. Orgány národnej bezpečnosti môžu povoliť osobnú prepravu, ak nie sú k dispozícii diplomatickí a vojenskí kuriéri alebo použitie takýchto kuriérov by malo za následok oneskorenie, ktoré by bolo škodlivé pre operácie EÚ a určený príjemca urýchlene požaduje daný materiál. Každý členský štát by mal pripraviť pokyny vzťahujúce sa na medzinárodnú osobnú prepravu materiálu, utajeného až do kategórie SECRET UE vrátane, osobami inými ako diplomatickí a vojenskí kuriéri. Tieto pokyny by mali požadovať, aby:

a) doručovateľ mal príslušné povolenie mať tajné informácie poskytnuté členskými štátmi;

b) sa v príslušnom úrade alebo registri uchovával záznam o každom takto prepravovanom materiále;

c) zásielky alebo vrecia, ktoré obsahujú materiál EÚ, mali úradnú pečať preto, aby sa predišlo alebo zabránilo colnej kontrole, a nálepky s identifikáciou a pokynmi pre nálezcu;

d) doručovateľ mal kuriérske osvedčenie a/alebo poverenie uznávané všetkými štátmi EÚ oprávňujúce ho na prepravu zásielky, ako je určené;

e) neprechádzal žiadnym nečlenským štátom EÚ alebo jeho hranicou pri pozemnej preprave, pokiaľ odosielajúci štát nemá výslovnú záruku od tohto štátu;

f) dojednania cesty doručovateľa, pokiaľ ide o miesta určenia, trasy, ktoré sa majú zvoliť, a dopravné prostriedky, ktoré sa majú použiť, boli v súlade s nariadeniami EÚ alebo, ak sú národné nariadenia, pokiaľ ide o takéto záležitosti prísnejšie – v súlade s takýmito nariadeniami;

g) sa materiál neponechal v držbe doručovateľa, pokiaľ nie je uložený do bezpečnej úschovy v súlade s ustanoveniami uvedenými v oddiele IV;

h) sa materiál nenechal bez dozoru vo verejných alebo súkromných vozidlách ani na miestach, ako sú reštaurácie alebo hotely. Nesmie sa ukladať do hotelových trezorov alebo ponechávať bez dozoru v hotelových izbách;

i) ak materiál, ktorý sa prepravuje, obsahuje dokumenty, tieto sa nesmú čítať na verejných miestach (napríklad v lietadle, vlakoch atď.).

Osoba, ktorá je určená na prepravu tajného materiálu, musí prečítať a podpísať bezpečnostnú inštruktáž, ktorá obsahuje minimálne pokyny uvedené vyššie a postupy, ktoré sa majú dodržiavať v prípade núdze alebo v prípade vyžiadania zásielky obsahujúcej tajný materiál colnými alebo letiskovými bezpečnostnými úradníkmi.

PRENOS RESTREINT UE DOKUMENTOV

21. Nie sú stanovené žiadne osobitné ustanovenia na prepravu RESTREINT UE dokumentov okrem toho, že treba zaistiť, aby sa nemohli dostať do rúk neoprávnených osôb.

▼B

BEZPEČNOSŤ PRACOVNÍKOV KURIÉRA

22. Všetci kuriéri a doručovatelia, ktorí sú použití na prepravu SECRET UE a CONFIDENTIEL UE dokumentov, majú prejsť kontrolou, pokiaľ ide o bezpečnosť.

Kapitola III

Elektrické a iné prostriedky technického prenosu

23. Komunikačné bezpečnostné opatrenia sú navrhnuté tak, aby zaisťovali bezpečný prenos tajných informácií EÚ. Oddiel XI sa zaoberá podrobnými pravidlami uplatniteľnými na prenos tajných informácií EÚ.

24. Iba akreditované komunikačné strediská a siete a/alebo terminály a systémy môžu prenášať informácie utajené ako CONFIDENTIEL UE a SECRET UE.

Kapitola IV

Zvláštne kópie a preklady a výňatky z tajných dokumentov EÚ

25. Iba pôvodca môže povoľovať kópiu alebo preklad TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov.

26. Ak osoby bez povolenia mať TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ informácie požadujú informácie, ktoré, aj keď sú obsiahnuté v TRÉS SECRET UE/PRÍSNE TAJNOM EÚ dokumente, nemajú toto utajenie, vedúci TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ registra môže povoliť vytvorenie potrebného množstva výňatkov z tohto dokumentu. Zároveň má podniknúť kroky na zaistenie, aby tieto výňatky dostali príslušné bezpečnostné utajenie.

27. Dokumenty utajené ako SECRET UE a v nižšej kategórii môže príjemca reprodukovať a prekladať v rámci národných bezpečnostných nariadení a pod podmienkou, že sa striktne dodržiava princíp potreby poznať. Bezpečnostné opatrenia uplatniteľné na pôvodný dokument majú byť uplatniteľné tiež na reprodukcie a/alebo jeho preklady. Decentralizované orgány EÚ majú dodržiavať tieto bezpečnostné nariadenia.

Kapitola V

Inventárne zoznamy a kontroly, uchovávanie a zničenie tajných dokumentov EÚ

INVENTÁRNE ZOZNAMY A KONTROLY

28. Každý rok TRÉS SECRET UE/PRÍSNE TAJNÝ EÚ register, ako je uvedený v oddiele VIII, má uskutočniť na položky rozpísaný inventárny zoznam TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov v súlade s nariadeniami uvedenými v oddiele VIII (9) až (11). Tajné dokumenty EÚ pod úrovňou TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ majú podliehať interným kontrolám v súlade s národnými usmerneniami a v prípade Generálneho sekretariátu Rady alebo decentralizovaných orgánov EÚ sa uskutočňujú podľa pokynov od generálneho tajomníka/vysokého predstaviteľa.

Tieto operácie majú poskytovať príležitosť zaistiť stanoviská držiteľov, pokiaľ ide o:

a) možnosť zaradenia určitých dokumentov do nižšej kategórie alebo odtajenie;

b) dokumenty, ktoré sa majú zničiť.

ARCHÍVNE UCHOVÁVANIE TAJNÝCH INFORMÁCIÍ EÚ

29. S cieľom minimalizovania problémov uchovávania, úradníci kontroly všetkých registrov majú byť oprávnení, aby dokumenty TRÉS SECRET UE/PŘISNE TAJNÉ EÚ dokumenty, dokumenty SECRET UE a CONFIDENTIEL UE boli uchované na mikrofilme alebo inak

▼B

na magnetickom alebo optickom médiu na archívne účely pod podmienkou, že:

a) proces mikrofilmovania/uchovávania vykonávajú pracovníci, ktorí prešli kontrolou pre odpovedajúcu príslušnú úroveň utajenia;

b) médium mikrofilmu/pamäťové médium poskytuje rovnakú bezpečnosť ako originálne dokumenty;

c) vytváranie mikrofilmov/uchovávanie akéhokoľvek TRÉS SECRET UE/ PRÍSNE TAJNÉHO EÚ dokumentu sa oznamuje pôvodcovi;

d) zvitky filmu alebo iný typ podpory obsahujú iba dokument rovnakého utajenia TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ, SECRET UE alebo CONFIDENTIEL EU;

e) vytváranie mikrofilmu/uchovávanie TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ dokumentu alebo dokumentu SECRET UE je jasne uvedené v zázname používanom pre ročný inventárny súpis;

f) pôvodné dokumenty, ktoré boli dané na mikrofilm alebo inak uchované, sa zničia v súlade s nariadeniami vysvetlenými v odsekoch 31 až 36.

30. Tieto pravidlá sa tiež uplatňujú na akúkoľvek inú formu uchovávania povolenú orgánom národnej bezpečnosti, ako je elektromagnetické médium a optický disk.

OBVYKLÉ ZNIČENIE TAJNÝCH DOKUMENTOV EÚ

31. S cieľom zabránenia nepotrebnému hromadeniu tajných dokumentov EÚ tie, ktoré vedúci inštitúcie, ktorá ich uchováva, považuje za zastaralé a nadbytočné, pokiaľ ide o počet, sa majú zničiť, akonáhle je to možné, nasledovným spôsobom:

a) TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ dokumenty má zničiť iba centrálny registračný úrad, ktorý je za ne zodpovedný. Každý zničený dokument má byť uvedený v osvedčení o zničení, ktoré je podpísané úradníkom kontroly TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov a úradníkom, ktorý je svedkom zničenia, ktorí majú prejsť kontrolou, pokiaľ ide o úroveň TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ. V tomto zmysle sa má urobiť zápis do denníka;

b) registračný úrad má uchovávať osvedčenia o zničení spolu s distribučnými hárkami počas obdobia desiatich rokov. Kópie sa majú doručiť pôvodcovi alebo príslušnému centrálnemu registračnému úradu, iba ak sa to výslovne požaduje;

c) TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ dokumenty, vrátane všetkého tajného odpadu vyplývajúceho z prípravy TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov, ako sú pokazené kópie, pracovné náčrty, napísané poznámky a kópie na prieklepovom papieri, sa majú zničiť pod dohľadom úradníka pre úroveň TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ spálením, rozdrvením, rozsekaním na kúsky alebo inak zničením na nerozoznateľnú formu, ktorú nie je možné znovu dať dokopy.

32. Dokumenty SECRET UE má zničiť registračný úrad zodpovedný za tieto dokumenty pod dohľadom osoby s povolením mať tajné informácie, použitím jedného z postupov uvedených v odseku 31 c). SECRET UE dokumenty, ktoré sú zničené, majú byť uvedené na podpísaných osvedčeniach o zničení, ktoré sa uchovávajú v registračnom úrade, spolu s distribučnými formulármi, aspoň počas troch rokov.

33. Dokumenty CONFIDENTIEL UE má zničiť registračný úrad zodpovedný za tieto dokumenty pod dohľadom osoby s povolením mať tajné informácie, jedným z postupov uvedených v odseku 31 c). Ich zničenie sa má zaznamenať v súlade s národnými nariadeniami a v prípade Generálneho sekretariátu Rady alebo decentralizovaných orgánov EÚ podľa pokynov generálneho tajomníka/vysokého predstaviteľa.

34. Dokumenty RESTREINT UE má zničiť registračný úrad zodpovedný za tieto dokumenty alebo užívateľ v súlade s národnými nariadeniami

▼B

a v prípade Generálneho sekretariátu Rady alebo decentralizovaných orgánov EÚ podľa pokynov generálneho tajomníka/vysokého predstaviteľa.

ZNIČENIE V PRÍPADOCH NÚDZE

35. Generálny sekretariát Rady, členské štáty a decentralizované orgány EÚ majú pripraviť plány, ktoré vychádzajú z miestnych podmienok, na ochranu tajného materiálu EÚ v čase krízy, vrátane potrebných plánov výnimočného zničenia a evakuácie; v rámci svojich príslušných organizácií majú oznámiť pokyny považované za potrebné na zabránenie, aby sa tajné informácie EÚ dostali do neoprávnených rúk.

36. Dojednania na ochranu a/alebo zničenie SECRET UE a CONFIDENTIEL UE materiálu v čase krízy nemajú za žiadnych okolností nepriaznivo ovplyvňovať ochranu alebo zničenie TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ materiálu, vrátane kódovacieho zariadenia, ktorého riešenie bude mať prioritu pred všetkými ostatnými úlohami. Opatrenia, ktoré sa majú prijať na ochranu a zničenie kódovacieho zariadenia za nepredvídaných okolností, majú byť uvedené v pokynoch na konkrétny účel.

KAPITOLA VI

Osobitné pravidlá uplatniteľné na dokumenty určené Rade

37. V rámci Generálneho sekretariátu Rady má Úrad pre tajné informácie monitorovať informácie utajené ako SECRET UE alebo CONFIDENTIEL UE, ktoré sa nachádzajú v dokumentoch pre Radu.

Do právomoci generálneho riaditeľa pre personál a administratívu spadá:

a) riadiť operácie týkajúce sa registrácie, reprodukcie, prekladu, prenosu, odoslania a zničenia takýchto informácií;

b) aktualizovať zoznam údajov o tajných informáciách;

c) pravidelne preskúmať otázky potreby zachovať utajenie informácií;

d) stanovovať, s spolupráci s bezpečnostným úradom, praktické dojednania pre utajovanie a odtajenie informácií.

38. Úrad pre tajné informácie má udržiavať register nasledovných údajov:

a) dátum prípravy tajných informácií;

b) úroveň utajenia;

c) dátum uplynutia utajenia;

d) názov a oddelenie vydávajúceho;

e) príjemca alebo príjemcovia s poradovým číslom;

f) predmet;

g) množstvo;

h) počet kópií daných do obehu;

i) príprava súpisov tajných informácií predložených Rade;

j) register odtajenia a zníženia kategórie tajných informácií.

39. Všeobecné pravidlá, ustanovené v kapitolách I až V tohto oddielu sa uplatňujú na úrad pre tajné informácie Generálneho sekretariátu Rady, pokiaľ neboli zmenené osobitnými pravidlami uvedenými v tejto kapitole.

▼B

ODDIEL VIII

TRÉS SECRET UE/PRÍSNE TAJNÉ REGISTRE EÚ

1. Účelom TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ registrov je zaistiť zaznamenávanie, spracovanie a distribúciu TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov v súlade s bezpečnostnými nariadeniami. Vedúci TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ registra, respektíve v každom členskom štáte, na Generálnom sekretariáte Rady a, ak je to vhodné, v decentralizovaných orgánoch EÚ je úradník kontroly pre TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ dokumenty.

2. Centrálne registre pôsobia ako hlavný prijímajúci a odosielajúci orgán v členských štátoch, na Generálnom sekretariáte Rady a v decentralizovaných orgánoch EÚ, v ktorých boli zriadené takéto registre, ako aj, ak je to vhodné, v iných inštitúciách EÚ, medzinárodných organizáciách a tretích štátoch, s ktorými má Rada dohody o bezpečnostných postupoch pre výmenu tajných informácií.

3. Ak je to potrebné, zriaďujú sa podregistre, ktoré majú byť zodpovedné za internú správu TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov; majú udržiavať aktuálne záznamy o obehu každého dokumentu, ktorý uchováva podregister.

4. TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ podregistre sa majú zriaďovať tak, ako je uvedené v oddiele I ako odozva na dlhodobé potreby a majú byť pripojené k centrálnemu TRÉS SECRET UE/PRÍSNE TAJNÉMU EÚ registru. Ak je potrebné iba dočasne a príležitostne nazrieť do TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov, tieto dokumenty je možné uvoľniť bez zriaďovania TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ podregistra za predpokladu, že sú stanovené pravidlá na zaistenie, aby zostali pod kontrolou príslušného TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ registra a za predpokladu, že sa dodržiavajú všetky fyzické a personálne bezpečnostné opatrenia.

5. Podregistre nesmú prenášať TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ dokumenty do iných podregistrov toho istého centrálneho TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ registra bez jeho výslovného súhlasu.

6. Všetky výmeny TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov medzi podregistrami, ktoré nie sú pripojené k tomu istému centrálnemu registru, majú ísť cez centrálne TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ registre.

CENTRÁLNE TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ REGISTRE

7. Ako kontrolný úradník, vedúci centrálneho TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ registra, má byť zodpovedný za:

   a) prenos TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov v súlade s nariadeniami definovanými v oddiele VII;

   b) uchovávanie zoznamu všetkých svojich závislých TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ podregistrov spolu s menami a podpismi menovaných kontrolných úradníkov a ich oprávnených zástupcov;

   c) udržiavanie potvrdení o príjme z registrov pre všetky TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ dokumenty distribuované centrálnym registrom;

   d) uchovávanie záznamu o TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentoch, ktoré uchovával a distribuoval;

   e) udržiavanie aktuálneho zoznamu všetkých centrálnych TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ registrov, s ktorými zvyčajne korešponduje, spolu s menami a podpismi menovaných kontrolných úradníkov a ich oprávnených zástupcov;

   f) fyzickú ochranu všetkých TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov, ktoré sa držia v registri v súlade s nariadeniami uvedenými v oddiele IV.

▼B

TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ PODREGISTRE

8. Ako kontrolný úradník, vedúci TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ podregistra má byť zodpovedný za:

   a) prenos TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov v súlade s nariadeniami uvedenými v oddiele VII a odseku 5 a 6 oddielu VIII;

   b) uchovávanie aktuálneho zoznamu všetkých osôb oprávnených mať prístup k TRÉS SECRET UE/PRÍSNE TAJNÝM EÚ informáciám, ktoré má pod svojou kontrolou;

   c) distribúciu TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov v súlade s pokynmi pôvodcu alebo na základe potreby poznať, pričom sa najprv preverí, či adresát má požadované povolenie mať tajné informácie;

   d) uchovávanie aktuálneho záznamu o TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentoch, ktoré uchovával alebo ktoré sa dávajú do obehu pod jeho kontrolou alebo ktoré boli odovzdané do iných TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ registrov a udržiavanie všetkých príslušných potvrdení o príjme;

   e) udržiavanie aktuálneho zoznamu TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ registrov, s ktorými je oprávnený vymieňať si TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ dokumenty, spolu s menami a podpismi kontrolných úradníkov a ich oprávnených zástupcov;

   f) fyzickú ochranu všetkých TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov, ktoré sa držia v podregistri v súlade s nariadeniami uvedenými v oddiele IV.

INVENTÁRNE SÚPISY

9. Každých dvanásť mesiacov každý TRÉS SECRET UE/PRÍSNE TAJNÝ EÚ register má vyhotoviť na položky rozpísaný súpis všetkých TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov, za ktoré je zodpovedný. Dokument sa považuje za spadajúci do zodpovednosti registra, ak register fyzicky získa dokument alebo uchováva doklad o príjme z TRÉS SECRET UE/PRÍSNE TAJNÉHO EÚ registra, do ktorého bol dokument prevedený, uchováva osvedčenie o zničení pre dokument alebo pokyn na zaradenie do nižšej kategórie alebo odtajenie tohto dokumentu.

10. Podregistre majú zaslať zistenia svojho každoročného inventárneho súpisu do centrálneho registra, ktorému sú zodpovedné k dátumu, ktorý špecifikoval centrálny register.

11. Národné bezpečnostné orgány, ako aj tie inštitúcie EÚ, medzinárodné organizácie a decentralizované orgány EÚ, v ktorých boli zriadené centrálne TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ registre, majú odoslať zistenia každoročných inventárnych súpisov vykonaných v centrálnych TRÉS SECRET UE/PRÍSNE TAJNÝCH EÚ registroch generálnemu tajomníkovi/vysokému predstaviteľovi každý rok najneskôr do 1. apríla.

▼B

ODDIEL IX

BEZPEČNOSTNÉ OPATRENIA, KTORÉ SA MAJÚ UPLATŇOVAŤ V ČASE URČITÝCH ZASADNUTÍ, KTORÉ SA KONAJÚ MIMO KOMPLEXU BUDOV RADY A KTORÉ ZAHŔŇAJÚ VEĽMI CITLIVÉ PROBLÉMY

VŠEOBECNE

1. Ak sa konajú zasadnutia Európskej rady, Rady, ministerské alebo iné významné stretnutia mimo komplexu budov Rady v Bruseli a Luxemburgu a ak je to zdôvodnené konkrétnymi bezpečnostnými požiadavkami týkajúcimi sa vysokej citlivosti otázok alebo informácií, ktorými sa zaoberajú, mali by sa prijať bezpečnostné opatrenia opísané nižšie. Tieto opatrenia sa týkajú iba ochrany tajných informácií EÚ; môžu sa navrhnúť aj iné bezpečnostné opatrenia.

ZODPOVEDNOSTI

Hostiteľské členské štáty

2. Členský štát, na ktorého území sa koná stretnutie (hostiteľský členský štát) by mal byť zodpovedný, v spolupráci s bezpečnostným úradom Generálneho sekretariátu Rady, za bezpečnosť stretnutí Európskej rady, Rady, ministerských alebo iných významných stretnutí a za fyzickú bezpečnosť hlavných delegátov a ich pracovníkov.

   Pokiaľ ide o ochranu bezpečnosti, mal by hlavne zaistiť, aby:

   a) sa zostavili plány, ktoré sa zaoberajú ohrozeniami bezpečnosti a incidentmi týkajúcimi sa bezpečnosti, príslušnými opatreniami vzťahujúcimi sa najmä na bezpečnú úschovu tajných dokumentov EÚ v úradoch;

   b) sa prijali opatrenia na umožnenie prístupu do komunikačného systému Rady s cieľom prijatia a prenosu tajných správ EÚ. Hostiteľský členský štát má zabezpečiť tiež prístup k bezpečným telefónnym systémom, ak sa tak požaduje.

Členské štáty

3. Orgány členských štátov by mali podniknúť potrebné kroky na zaistenie, aby:

   a) sa zabezpečilo príslušné potvrdenie mať tajné informácie pre ich národných delegátov, ak je to potrebné, prostredníctvom signálu alebo faxu, priamo bezpečnostnému úradníkovi stretnutia alebo cez bezpečnostný úrad Generálneho sekretariátu Rady;

   b) orgány hostiteľského členského štátu boli informované o akomkoľvek konkrétnom ohrození a, ak je to vhodné, bezpečnostný úrad Generálneho sekretariátu Rady tak, aby mohli podniknúť potrebné kroky.

Bezpečnostný úradník stretnutia

4. Mal by byť menovaný bezpečnostný úradník stretnutia, ktorý je zodpovedný za celkovú prípravu a kontrolu všeobecných interných bezpečnostných opatrení a za koordináciu s ostatnými príslušnými bezpečnostnými orgánmi. Opatrenia, ktoré prijíma, by sa mali v podstate týkať:

   a) i) ochranných opatrení v mieste stretnutia na zaistenie, aby sa stretnutie uskutočnilo bez incidentu, ktorý by mohol ohroziť bezpečnosť akýchkoľvek tajných informácií EÚ, ktoré sa tam môžu použiť;

   ii) kontroly pracovníkov, ktorí majú dovolený prístup na miesto stretnutia, priestorov delegácií a konferenčných miestností a skontrolovania akéhokoľvek zariadenia;

   iii) neustálej koordinácie s príslušnými orgánmi hostiteľského členského štátu a s bezpečnostným úradom Generálneho sekretariátu Rady;

▼B

b) začlenenia bezpečnostných pokynov do materiálu stretnutia s náležitým zreteľom na požiadavky uvedené v týchto bezpečnostných nariadeniach alebo akékoľvek iné potrebné bezpečnostné pokyny.

Bezpečnostný úrad Generálneho sekretariátu Rady

5. Bezpečnostný úrad generálneho sekretariátu Rady by mal pôsobiť ako poradca pre bezpečnosť pri príprave stretnutia; mal by tam byť zastúpený, aby v prípade potreby pomohol a poradil bezpečnostnému úradníkovi stretnutia a delegáciám.

6. Každá delegácia stretnutia by mala označiť bezpečnostného úradníka, ktorý je zodpovedný za riešenie bezpečnostných záležitostí v rámci svojej delegácie a za zachovanie spojenia s bezpečnostným úradníkom stretnutia, ako aj so zástupcom bezpečnostného úradu Generálneho sekretariátu Rady, ako sa požaduje.

BEZPEČNOSTNÉ OPATRENIA

Oblasti bezpečnosti

7. Mali by sa stanoviť nasledovné oblasti bezpečnosti:

a) oblasť bezpečnosti triedy II pozostávajúca z miestnosti na vytváranie návrhov, kancelárií Generálneho sekretariátu Rady a reprografického zariadenia, ako aj kancelárií delegácií, ak je to vhodné;

b) oblasť bezpečnosti triedy I, ktorá pozostáva z konferenčnej miestnosti a tlmočníckych kabíniek a kabíniek pre zvukových technikov;

c) administratívne oblasti pozostávajúce z priestoru pre tlač a tých častí v mieste stretnutia, ktoré sa používajú na administratívu, stravovanie a ubytovanie, ako aj priestoru, ktorý bezprostredne susedí s tlačovým centrom a miestom stretnutia.

Priepustky

8. Bezpečnostný úradník stretnutia by mal vystaviť vhodné menovky, ako požadujú delegácie podľa ich potrieb. Ak sa tak požaduje, môže sa rozlišovať prístup do rôznych oblastí bezpečnosti.

9. Bezpečnostné pokyny stretnutia by mali požadovať od všetkých zúčastnených osôb, aby nosili vždy svoje menovky v rámci miesta stretnutia a to tak, aby ich bolo vidieť, aby ich mohli v prípade potreby skontrolovať bezpečnostní pracovníci.

10. Okrem účastníkov, ktorí majú menovky, na miesto stretnutia treba vpustiť čo najmenší počet ľudí. Národné delegácie, ktoré chcú počas stretnutia prijať návštevníkov, by mali o tom informovať bezpečnostného úradníka stretnutia. Návštevníci majú dostať odznak návštevníka. Mal by sa vyplniť formulár priepustky návštevníka uvádzajúci jeho/jej meno a meno navštívenej osoby. Návštevníkov by mala vždy doprevádzať stráž objektu alebo osoba, ktorá je navštívená. Sprevádzajúca osoba má mať formulár návštevníkovej priepustky a vráti ho, spolu s odznakom návštevníka, bezpečnostným pracovníkom, keď návštevník opúšťa miesto stretnutia.

Kontrola fotografického a audio-zariadenia

11. Do oblasti bezpečnosti triedy I nie je možné priniesť žiadnu kameru alebo zariadenie na záznam, okrem zariadenia, ktoré priniesli fotografi a zvukoví technici riadne povoleného bezpečnostným úradníkom stretnutia.

Kontrola kufríkov, prenosných počítačov a balíkov

12. Držitelia priepustky, ktorí majú dovolený prístup do bezpečnostnej oblasti, si môžu zvyčajne priniesť svoje kufríky na dokumenty a prenosné počítače (iba s vlastným napájaním) bez vykonania kontroly. V prípade balíkov pre delegácie, delegácie môžu prevziať doručenie balíkov, ktoré skontroluje bezpečnostný úradník delegácie, prešli kontrolou zvláštnym zariadením alebo ktoré otvorili bezpečnostní pracovníci s cieľom kontroly. Ak sa bezpečnostný úradník stretnutia domnieva, že je to potrebné, môžu sa stanoviť prísnejšie opatrenia na kontrolu kufríkov na dokumenty a balíkov.

▼B

Technická bezpečnosť

13. Skupina pre technickú bezpečnosť môže zabezpečiť, aby bola zasadacia miestnosť technicky bezpečná a môže tiež vykonávať elektronický dohľad počas stretnutia.

Dokumenty delegácií

14. Delegácie by mali byť zodpovedné za prevzatie tajných dokumentov EÚ na stretnutia a zo stretnutí. Mali by byť tiež zodpovedné za overenie a bezpečnosť týchto dokumentov počas ich používania v priestoroch, ktoré im boli pridelené. Môžu požiadať hostiteľské členské štáty o pomoc pri preprave tajných dokumentov na miesto stretnutia a z tohto miesta.

Bezpečná úschova dokumentov

15. Ak Generálny sekretariát Rady, Komisia alebo delegácie nie sú schopné uchovávať svoje tajné dokumenty v súlade so schválenými normami, môžu uložiť tieto dokumenty v zapečatenej obálke u bezpečnostného úradníka stretnutia, oproti dokladu o ich prevzatí, aby tento bezpečnostný úradník mohol potom uložiť dokumenty v súlade so schválenými normami.

Kontrola úradov

16. Bezpečnostný úradník stretnutia by mal zariadiť, aby sa kancelárie Generálneho sekretariátu Rady a delegácií skontrolovali na konci každého pracovného dňa s cieľom zaistenia, aby sa všetky tajné dokumenty EÚ držali na bezpečnom mieste; v opačnom prípade by mal prijať potrebné opatrenia.

Zničenie tajného odpadu EÚ

17. Každý odpad by sa mal považovať za tajný EÚ odpad a koše alebo vrecia s odpadovým papierom sa majú dať na likvidáciu Generálnemu sekretariátu Rady a delegáciám. Pred opustením priestorov, ktoré im boli pridelené, Generálny sekretariát Rady a delegácie by mali vziať svoj odpad bezpečnostnému úradníkovi stretnutia, ktorý má zariadiť jeho zničenie podľa nariadení.

18. Na konci stretnutia sa majú všetky dokumenty, ktoré už viac Generálny sekretariát Rady alebo delegácie nepotrebujú považovať za odpad. Predtým, ako sa zrušia bezpečnostné opatrenia prijaté pre stretnutie, mala by sa vykonať dôkladná prehliadka priestorov Generálneho sekretariátu Rady a delegácií. Dokumenty, pre ktoré bol podpísaný doklad o prevzatí, ak je to uplatniteľné, sa majú zničiť, ako je predpísané v oddiele VII.

▼B

ODDIEL X

PORUŠENIE BEZPEČNOSTI A OHROZENIE TAJNÝCH INFORMÁCIÍ EÚ

1. Porušenie bezpečnosti sa vyskytuje ako dôsledok aktu alebo opomenutia, ktoré je v rozpore s bezpečnostným nariadením Rady alebo národným bezpečnostným nariadením, ktoré môže znamenať nebezpečenstvo alebo ohrozenie pre tajné informácie EÚ.

2. Ohrozenie tajných informácií EÚ sa vyskytuje, ak sa úplne alebo čiastočne dostanú do rúk neoprávnených osôb, t. j. osôb, ktoré nemajú povolenie mať tajné informácie alebo nemajú požadovanú potrebu ich poznať, alebo ak je pravdepodobnosť výskytu takéto prípadu.

3. Tajné informácie EÚ môžu byť ohrozené v dôsledku nepozornosti, nedbalosti alebo nediskrétnosti, ako aj aktivitami služieb, ktoré sa zameriavajú na EÚ alebo jej členské štáty, pokiaľ ide o tajné informácie EÚ a aktivity, alebo podvratnými organizáciami.

4. Dôležité je, aby všetky osoby, od ktorých sa požaduje, aby pracovali s tajnými informáciami, boli dôkladne inštruované o bezpečnostných postupoch, nebezpečenstvách nediskrétneho rozhovoru a ich vzťahov s tlačou. Mali by si byť vedomé dôležitosti okamžitého oznámenia akéhokoľvek porušenia bezpečnosti, ktoré si mohli všimnúť, bezpečnostnému orgánu členského štátu, inštitúcii alebo orgánu, v ktorom sú zamestnané.

5. Ak bezpečnostný orgán zistí alebo je informovaný o porušení bezpečnosti týkajúcej sa tajných informácií EÚ alebo o strate alebo zmiznutí tajného materiálu EÚ, podnikne včasné kroky na:

   a) zistenie skutočností;

   b) zhodnotenie a minimalizovanie danej škody;

   c) zabránenie opätovnému výskytu;

   d) informovanie príslušných orgánov o vplyvoch porušenia bezpečnosti.

   V tejto súvislosti majú sa poskytnúť nasledovné informácie:

   i) popis príslušných informácií vrátane ich utajenia, referenčného čísla a čísla kópie, dátumu, pôvodcu, predmetu a rozsahu;

   ii) stručný popis okolností porušenia bezpečnosti vrátane dátumu a obdobia, počas ktorého boli informácie vystavené ohrozeniu;

   iii) údaj o tom, či bol informovaný pôvodca.

6. Povinnosťou každého bezpečnostného orgánu je čo možno najskôr informovať, že sa vyskytlo takéto porušenie bezpečnosti, túto skutočnosť oznámiť okamžite použitím nasledovného postupu: PRÍSNE TAJNÝ EÚ podregister má informovať o tejto záležitosti bezpečnostný úrad Generálneho sekretariátu Rady cez svoj centrálny PRÍSNE TAJNÝ EÚ register; v prípade ohrozenia tajných informácií EÚ vyskytujúceho sa v rámci jurisdikcie členského štátu treba o tom informovať bezpečnostný úrad Generálneho sekretariátu Rady, ako je uvedené v odseku 5, prostredníctvom zodpovedného orgánu národnej bezpečnosti.

7. Prípady týkajúce sa RESTREINT UE informácií treba oznamovať iba vtedy, ak predstavujú nezvyčajné udalosti.

8. Po informovaní o tom, že sa vyskytlo porušenie bezpečnosti, generálny tajomník/vysoký predstaviteľ má:

   a) informovať orgán, od ktorého pochádzajú príslušné tajné informácie;

   b) požiadať príslušné bezpečnostné orgány o začatie vyšetrovania;

   c) koordinovať vyšetrovania, ak pôsobí viac ako jeden bezpečnostný orgán;

   d) získať správu o okolnostiach porušovania, dátume a období, počas ktorého sa mohlo vyskytovať a bolo zistené, s podrobným opisom obsahu a utajenia príslušného materiálu. Treba informovať tiež

▼B

o poškodení, ktoré sa vyskytlo, pokiaľ ide o záujmy EÚ alebo jedného alebo viacerých jej členských štátov a o krokoch podniknutých na zabránenie opakovaného výskytu.

9. Orgán, od ktorého pochádzajú informácie, má informovať adresátov a poskytnúť im príslušné pokyny.

10. Akýkoľvek jednotlivec zodpovedný za ohrozovanie tajných informácií EÚ podlieha disciplinárnemu postihu podľa príslušných nariadení a predpisov. Takéto kroky nemajú mať žiaden vplyv na akékoľvek právne konanie.

▼B

ODDIEL XI

OCHRANA INFORMÁCIÍ SPRACOVÁVANÝCH V SYSTÉMOCH INFORMAČNEJ TECHNOLÓGIE A KOMUNIKAČNÝCH SYSTÉMOCH

Podrobný obsah

Kapitola I	Úvod
Kapitola II	Definície
Kapitola III	Povinnosti týkajúce sa bezpečnosti
Kapitola IV	Netechnické bezpečnostné opatrenia
Kapitola V	Technické bezpečnostné opatrenia
Kapitola VI	Bezpečnosť počas spracovania
Kapitola VII	Obstarávanie
Kapitola VIII	Dočasné alebo príležitostné použitie

▼B

Kapitola I

Úvod

VŠEOBECNÉ ASPEKTY

1. Bezpečnostná politika a požiadavky v tomto oddiele sa uplatňujú na všetky komunikačné a informačné systémy a siete (ďalej SYSTÉMY) spracovávajúce informácie utajené ako CONFIDENTIEL UE alebo vo vyššej kategórii.

2. SYSTÉMY spracovávajúce RESTREINT UE informácie vyžadujú tiež bezpečnostné opatrenia na ochranu dôvernosti týchto informácií. Všetky SYSTÉMY požadujú bezpečnostné opatrenia na ochranu celistvosti a dostupnosti týchto systémov a informácií, ktoré obsahujú. Bezpečnostné opatrenia, ktoré sa majú uplatňovať na tieto systémy, stanovuje označený orgán na schvaľovanie bezpečnosti (SAA) a odpovedajú zhodnotenému riziku a sú v zhode s postupom stanoveným v týchto bezpečnostných nariadeniach.

3. Ochrana senzorových systémov obsahujúcich vložené IT SYSTÉMY sa má určovať a špecifikovať v celkovom kontexte systémov, ku ktorým patria použitím uplatniteľných ustanovení tohto oddielu do tej miery, ako je to možné.

OHROZENIA A ZRANITEĽNOSTI SYSTÉMOV

4. Podľa všeobecných termínov možno ohrozenie definovať ako možnosť náhodného alebo zámerného ohrozenia bezpečnosti. V prípade SYSTÉMOV takéto ohrozenie zahŕňa stratu jednej alebo viacerých vlastností dôvernosti, celistvosti a dostupnosti. Zraniteľnosť možno definovať ako miernosť alebo nedostatočnosť kontrol, ktorá by uľahčovala alebo poskytovala podnet k ohrozeniu určitého majetku alebo cieľa. Zraniteľnosť môže byť opomenutie alebo sa môže týkať nedostatočnosti pevnosti, úplnosti alebo dôslednosti kontroly; táto môže byť technického, procedurálneho alebo prevádzkového charakteru.

5. Tajné a netajné informácie EÚ spracovávané v SYSTÉMOCH v koncentrovanej forme, ktoré sú určené na rýchle získanie, komunikáciu a použitie, sú vystavené mnohým rizikám. Tieto zahŕňajú prístup neoprávnených užívateľov k informáciám alebo, naopak, odmietnutie prístupu oprávneným užívateľom. Ide tiež o riziká nepovoleného odhalenia, korupcie, zmeny alebo vymazania informácií. Okrem toho, zložité a niekedy krehké zariadenie je drahé a často je ťažké rýchlo ho opraviť alebo vymeniť. Tieto SYSTÉMY sú preto aktraktívnymi terčmi pre operácie zberu informácií a sabotáž, najmä ak sa bezpečnostné opatrenia považujú za neúčinné.

BEZPEČNOSTNÉ OPATRENIA

6. Hlavným účelom bezpečnostných opatrení uvedených v tomto oddiele je poskytovať ochranu pred neoprávneným odhalením informácií (strata dôvernosti) a voči strate celistvosti a dostupnosti informácií. Na dosiahnutie primeranej ochrany bezpečnosti SYSTÉMU spracovávajúceho tajné informácie EÚ by sa mali ustanoviť vhodné normy dohodnutej bezpečnosti spolu s primeranými presne definovanými bezpečnostnými postupmi a technikami konkrétne určenými pre každý SYSTÉM.

7. Treba identifikovať a vykonávať vyváženú sústavu bezpečnostných opatrení s cieľom vytvorenia bezpečného prostredia, v ktorom funguje SYSTÉM. Oblasti uplatňovania týchto opatrení sa týkajú fyzických prvkov, pracovníkov, netechnických postupov, počítačových a komunikačných prevádzkových postupov.

8. Potrebné sú počítačové bezpečnostné opatrenia (hardvérové a softvérové bezpečnostné charakteristiky) na vykonávanie princípu potreby poznať a zabránenie alebo odhalenie neoprávneného prezradenia informácií. Počas procesu stanovovania bezpečnostnej požiadavky sa určí miera, do ktorej treba počítať s počítačovými bezpečnostnými opatreniami. Proces akreditácie má určiť, aby existovala primeraná miera istoty ako dôkaz tejto dôvery týkajúcej sa počítačových bezpečnostných opatrení.

▼B

FORMULÁCIA BEZPEČNOSTNEJ POŽIADAVKY ŠPECIFICKEJ PRE SYSTÉM (SSRS)

9. Pre všetky SYSTÉMY spracovávajúce informácie utajené ako CONFIDENTIEL UE a vo vyššej kategórii sa požaduje, aby orgán prevádzkujúci IT systém (ITSOA) predložil formuláciu bezpečnostnej požiadavky špecifickej pre systém (SSRS) v spolupráci so vstupom a, ak je to potrebné, za pomoci pracovníkov projektu a orgánu INFOSEC a schváleného SAA. Formulovanie bezpečnostnej požiadavky špecifickej pre systém sa požaduje tiež, ak orgán na schvaľovanie bezpečnosti (SAA) považuje za kritickú dostupnosť a celistvosť informácií RESTREINT UE alebo netajných informácií.

10. SSRS sa má formulovať v skorej etape začiatku projektu a má sa rozvíjať a vylepšovať ako sa vyvíja projekt, plniac rôzne úlohy v rôznych etapách projektu a životného cyklu SYSTÉMU.

11. Formulácia bezpečnostnej požiadavky špecifickej pre systém (SSRS) predstavuje záväznú dohodu medzi orgánom prevádzkujúcim IT systém a orgánom na schvaľovanie bezpečnosti, oproti ktorej sa má schvaľovať systém.

12. SSRS je kompletné a jednoznačné vyjadrenie bezpečnostných princípov, ktoré sa majú dodržiavať, a podrobných bezpečnostných požiadaviek, ktoré sa majú splniť. Vychádza z bezpečnostnej politiky a hodnotenia rizika Rady alebo je uložené prostredníctvom parametrov vzťahujúcich sa na prevádzkové prostredie, najnižšiu úroveň povolenia mať tajné informácie pre pracovníkov, najvyššie utajenie spracovávaných informácií, bezpečnostný spôsob prevádzky alebo požiadavky užívateľa. Formulácia bezpečnostnej požiadavky špecifickej pre systém je nedeliteľnou súčasťou projektovej dokumentácie predloženej príslušným orgánom na účely technického, rozpočtového a bezpečnostného schválenia. Vo svojej konečnej podobe formulácia bezpečnostnej požiadavky špecifickej pre systém predstavuje kompletné vyjadrenie toho, čo je potrebné pre SYSTÉM, aby bol bezpečný.

BEZPEČNOSTNÉ REŽIMY PREVÁDZKY

13. Všetky SYSTÉMY, ktoré spracovávajú informácie utajené ako CONFIDENTIEL UE a vo vyššej kategórii, sa majú schvaľovať na prevádzku v jednom alebo, ak tak oprávňujú požiadavky počas rôznych časových období, viac ako v jednom z nasledovných režimov prevádzky alebo ich národnom ekvivalente:

    a) vyhradená;

    b) prevádzka systému s vysokou bezpečnosťou a

    c) viacúrovňová prevádzka.

Kapitola II

Definície

ĎALŠIE OZNAČENIA

14. Ďalšie označenia ako CRYPTO alebo akékoľvek iné zvláštne označenie manipulácie uznávané v EÚ sa majú uplatňovať, ak je potrebná obmedzená distribúcia a zvláštne spracovanie okrem toho, ktoré je určené bezpečnostným utajením.

15. „VYHRADENÝ“ BEZPEČNOSTNÝ REŽIM PREVÁDZKY znamená: režim prevádzky, v ktorom majú prejsť kontrolou VŠETCI jednotlivci s prístupom k SYSTÉMU, pokiaľ ide o najvyššiu úroveň utajenia informácií spracovávaných v SYSTÉME, a jednotlivci s prirodzenou potrebou poznať pre VŠETKY informácie spracovávané v SYSTÉME.

    Poznámky:

    (1) Prirodzená potreba poznať znamená, že nie je povinnou požiadavkou počítačových bezpečnostných charakteristík zaistiť separáciu informácií v rámci SYSTÉMU.

▼B

(2) Iné bezpečnostné charakteristiky (napríklad fyzické, personálne a procedurálne) majú vyhovovať požiadavkám pre najvyššiu úroveň utajenia a všetkým označeniam kategórie informácií spracovávaných v SYSTÉME.

16. REŽIM PREVÁDKY S „VYSOKOU BEZPEČNOSŤOU SYSTÉMU“ znamená režim prevádzky, v ktorom VŠETCI jednotlivci s prístupom k SYSTÉMU majú prejsť kontrolou, pokiaľ ide o najvyššiu úroveň utajenia informácií spracovávaných v SYSTÉME, ale NIE VŠETCI jednotlivci s prístupom k SYSTÉMU majú prirodzenú potrebu poznať pre informácie spracovávané v SYSTÉME.

Poznámky:

(1) Neexistencia prirodzenej potreby poznať znamená, že požiadavkou, pokiaľ ide o počítačové bezpečnostné charakteristiky, je zabezpečiť selektívny prístup k informáciám a separáciu informácií v rámci SYSTÉMU.

(2) Iné bezpečnostné charakteristiky (napríklad fyzické, personálne a procedurálne) majú vyhovovať požiadavkám pre najvyššiu úroveň utajenia a všetkým označeniam kategórie informácií spracovávaných v SYSTÉME.

(3) Všetky informácie, ktoré sa spracovávajú alebo sú dostupné pre SYSTÉM pod týmto režimom prevádzky, spolu s vytvoreným výstupom sa majú chrániť eventuálne ako informácie s označením kategórie a informácie s najvyššou úrovňou utajenia, ktoré sú spracovávané, pokiaľ sa neustanoví inak, s jedinou výnimkou, ak existuje akceptovateľná úroveň dôvery, ktorá môže nahradiť akúkoľvek existujúcu charakterizujúcu funkčnosť.

17. „VIACÚROVŇOVÝ“ BEZPEČNOSTNÝ REŽIM PREVÁDZKY znamená: režim prevádzky, v ktorom neprechádzajú kontrolou VŠETCI jednotlivci s prístupom k SYSTÉMU, pokiaľ ide o najvyššiu úroveň utajenia informácií spracovávaných v SYSTÉME, a NIE VŠETCI jednotlivci s prístupom k SYSTÉMU majú prirodzenú potrebu poznať pre informácie spracovávané v rámci SYSTÉMU.

Poznámky:

(1) Tento režim dovoľuje súčasne spracovávanie informácií s rôznymi úrovňami utajenia a zmiešaných označení kategórie informácií.

(2) Skutočnosť, že nie všetci jednotlivci prechádzajú kontrolou, pokiaľ ide o najvyššie úrovne, spojená s neexistenciou prirodzenej potreby poznať, naznačuje, že požiadavkou, pokiaľ ide o počítačové bezpečnostné charakteristiky, je zaistiť selektívny prístup k informáciám a separáciu informácií v rámci SYSTÉMU.

18. INFOSEC znamená: uplatňovanie bezpečnostných opatrení na ochranu informácií, ktoré sú spracovávané, uchovávané alebo prenášané v komunikačných, informačných a iných elektronických systémoch pred stratou dôvernosti, celistvosti alebo dostupnosti, tiež náhodnou alebo zámernou, a zabrániť strate celistvosti a dostupnosti samotných systémov. Opatrenia INFOSEC obsahujú tie, ktoré sa týkajú počítačovej bezpečnosti, bezpečnosti prenosu, vysielania a kryptografickej bezpečnosti a zisťovania, dokumentácie a reagovania na ohrozenia informácií a SYSTÉMOV.

19. POČÍTAČOVÁ BEZPEČNOSŤ (COMPUSEC) znamená: uplatňovanie hardvérových, mikroprogramových a softvérových bezpečnostných charakteristík na počítačový systém s cieľom ochrany alebo zabránenia neoprávnenému prezradeniu, manipulácii, modifikácii/vymazaniu informácií alebo odmietnutia služieb.

20. POČÍTAČOVÝ BEZPEČNOSTNÝ PRODUKT znamená: produkt generickej počítačovej bezpečnosti, ktorý je určený na začlenenie do IT systému na použitie pri zvyšovaní alebo zabezpečovaní dôvernosti, celistvosti alebo dostupnosti spracovávaných informácií.

▼B

21. BEZPEČNOSŤ KOMUNIKÁCIÍ (COMSEC) znamená: uplatňovanie bezpečnostných opatrení na telekomunikácie s cieľom odmietnutia prístupu neoprávneným osobám k informáciám hodnoty, ktorá môže vyplývať z vlastnenia a študovania takýchto telekomunikácií alebo s cieľom zaistenia hodnovernosti takýchto telekomunikácií.

Poznámka:

Takéto opatrenia zahŕňajú kryptografickú bezpečnosť, bezpečnosť prenosu a vysielania; a tiež obsahujú procedurálnu, fyzickú, personálnu bezpečnosť, bezpečnosť dokumentu a počítačovú bezpečnosť.

22. HODNOTENIE znamená: podrobné technické preskúmanie bezpečnostných stránok SYSTÉMU alebo šifrovacieho alebo počítačového bezpečnostného produktu príslušným orgánom.

Poznámky:

(1) Hodnotenie skúma, či existuje požadovaná funkčnosť bezpečnosti a zisťuje prítomnosť ohrozujúcich vedľajších efektov vyplývajúcich z takejto funkčnosti a hodnotí nepodplatiteľnosť tejto funkčnosti.

(2) Hodnotenie určuje mieru, do ktorej sú splnené bezpečnostné požiadavky SYSTÉMU alebo bezpečnostné nároky počítačového bezpečnostného produktu a ustanovuje úroveň istoty SYSTÉMU alebo funkcie zverenej kryptografickému alebo počítačovému bezpečnostnému produktu.

23. CERTIFIKÁCIA znamená: vydanie formálneho vyhlásenia, podloženého nezávislým preskúmaním výkonu a výsledkov hodnotenia, miery, do ktorej SYSTÉM spĺňa bezpečnostnú požiadavku alebo počítačový bezpečnostný produkt spĺňa vopred definované bezpečnostné nároky.

24. AKREDITÁCIA znamená: oprávnenie a schválenie udelené SYSTÉMU spracovávať tajné informácie EÚ vo svojom prevádzkovom prostredí.

Poznámka:

Takáto akreditácia sa má uskutočniť po vykonávaní všetkých bezpečnostných postupov a dosiahnutí dostatočnej úrovne ochrany zdrojov systému. Akreditácia sa má zvyčajne robiť na základe formulácie bezpečnostnej požiadavky špecifickej pre systém, vrátane nasledovného:

a) formulácia cieľa akreditácie pre systém: najmä aká úroveň (aké úrovne) informácií sa majú spracovávať a aký režim (aké režimy) prevádzky systému alebo bezpečnosti siete sa navrhujú;

b) vykonanie kontroly riadenia rizika s cieľom identifikovania ohrození a zraniteľností a opatrení reakcie na ne;

c) bezpečnostné prevádzkové postupy (SecOPs) s podrobným popisom navrhovaných operácií (napríklad režimy, služby, ktoré sa majú poskytovať) vrátane popisu bezpečnostných charakteristík SYSTÉMU, ktoré majú tvoriť základ akreditácie;

d) plán na vykonávanie a zachovanie bezpečnostných charakteristík;

e) plán na počiatočné a následné testovanie, hodnotenie a certifikáciu bezpečnosti systému alebo bezpečnosti siete a

f) certifikácia, ak sa požaduje, spolu s ostatnými prvkami akreditácie.

25. IT SYSTÉM znamená: sústavu zariadenia, metód a postupov a, ak je potrebné, pracovníkov, ktorí tvoria organizáciu s cieľom vykonávania funkcií spracovávania informácií.

Poznámky:

(1) Bolo prijaté, že znamená súpravu vybavenia konfigurovaného na spracovávanie informácií v rámci systému.

(2) Takéto systémy môžu slúžiť v prospech konzultačných, príkazových, kontrolných, komunikačných, vedeckých alebo administratívnych aplikácií vrátane spracovania textov.

▼B

(3) Ohraničenia systému sa spravidla určia ako prvky, ktoré sú pod kontrolou samostatného orgánu prevádzkujúceho IT systém (ITSOA).

(4) IT systém môže obsahovať podsystémy, z ktorých niektoré sú samotné IT systémy.

26. BEZPEČNOSTNÉ CHARAKTERISTIKY IT SYSTÉMU obsahujú všetky hardvérové/mikroprogramové/softvérové funkcie, charakteristiky a vlastnosti; prevádzkové postupy, postupy týkajúce sa zodpovednosti a kontroly prístupu, oblasť IT, oblasť dislokovaného terminálu/pracovnej stanice a obmedzenia riadenia, fyzickú štruktúru a zariadenia, kontroly pracovníkov a komunikácií potrebné na zabezpečenie akceptovateľnej úrovne ochrany pre tajné informácie, ktoré sa majú spracovávať v IT systéme.

27. IT SIEŤ znamená: geograficky rozšírenú organizáciu IT systémov, ktoré sú vzájomne prepojené na výmenu dát a obsahujúcu komponenty vzájomne spojených IT systémov a ich prepojenie s podpornými údajmi alebo komunikačnými sieťami.

Poznámky:

(1) IT sieť môže využívať služby jednej alebo niekoľkých komunikačných sietí, ktoré sú vzájomne spojené na výmenu dát; niekoľko IT sietí môže využívať služby spoločnej komunikačnej siete.

(2) IT sieť sa nazýva „lokálna“, ak spája spolu niekoľko počítačov v tom istom mieste.

28. BEZPEČNOSTNÉ CHARAKTERISTIKY IT SIETE zahŕňajú bezpečnostné charakteristiky IT systému jednotlivých IT systémov, ktoré tvoria sieť spolu s ďalšími komponentmi a charakteristikami spojenými so sieťou ako takou (napríklad sieťové komunikácie, bezpečnostná identifikácia a mechanizmy a postupy označovania, kontroly prístupu, programy a preverovacie záznamy) potrebné na zaistenie akceptovateľnej úrovne ochrany pre tajné informácie.

29. IT OBLASŤ znamená: oblasť, ktorá obsahuje jeden alebo viac počítačov, ich miestne periférne a pamäťové jednotky, riadiace jednotky a vyhradenú sieť a komunikačné zariadenie.

Poznámka:

Nezahŕňa osobitnú oblasť, v ktorej sa nachádzajú dislokované periférne zariadenia alebo terminály/pracovné stanice, aj keď tieto zariadenia sú pripojené na zariadenie v IT oblasti.

30. OBLASŤ DISLOKOVANÉHO TERMINÁLU/PRACOVNEJ STANICE znamená: oblasť obsahujúcu nejaké počítačové zariadenie, jeho lokálne periférne zariadenia alebo terminály/pracovné stanice a akékoľvek priradené komunikačné zariadenie, oddelené od IT oblasti.

31. Protiopatrenia TEMPEST: bezpečnostné opatrenia určené na ochranu zariadenia a komunikačných infraštruktúr pred ohrozením tajných informácií prostredníctvom nezámerných elektromagnetických emisií.

Kapitola III

Povinnosti týkajúce sa bezpečnosti

VŠEOBECNÉ ZÁLEŽITOSTI

32. Povinnosti bezpečnostného výboru, ktoré sú definované v oddiele I odsek 4, zahŕňajú otázky INFOSEC. Bezpečnostný výbor má organizovať svoje aktivity takým spôsobom, aby mohol poskytovať odbornú Radu, pokiaľ ide o vyššie uvedené problémy.

33. V prípade problémov týkajúcich sa bezpečnosti (incidenty, porušenia atď.) zodpovedný národný orgán a/alebo bezpečnostný úrad Generálneho sekretariátu Rady má podniknúť okamžité kroky. Všetky problémy sa majú predkladať bezpečnostnému úradu Generálneho sekretariátu Rady.

▼B

34. Generálny tajomník/vysoký predstaviteľ alebo, ak je to vhodné, vedúci decentralizovaného orgánu EÚ zriadi úrad INFOSEC, ktorý bude zabezpečovať usmerňovanie bezpečnostného orgánu pri vykonávaní a kontrole zvláštnych bezpečnostných charakteristík označených ako súčasť SYSTÉMOV.

ORGÁN NA SCHVAĽOVANIE BEZPEČNOSTI (SAA)

35. Orgánom na schvaľovanie bezpečnosti má byť buď:

— orgán národnej bezpečnosti,

— orgán označený generálnym tajomníkom/vysokým predstaviteľom,

— bezpečnostný orgán decentralizovaného orgánu EÚ, alebo

— ich delegovaní/menovaní zástupcovia v závislosti od SYSTÉMU, ktorý sa má schvaľovať.

36. Orgán na schvaľovanie bezpečnosti je zodpovedný za zaisťovanie zhody SYSTÉMOV s bezpečnostnou politikou Rady. Jednou z jeho úloh má byť udeľovanie schválenia SYSTÉMU na spracovávanie tajných informácií EÚ pre definovanú úroveň utajenia v jeho prevádzkovom prostredí. Pokiaľ ide o Generálny sekretariát Rady a, ak je to vhodné, decentralizované orgány EÚ, orgán na schvaľovanie bezpečnosti má uplatňovať zodpovednosť za bezpečnosť v mene generálneho tajomníka/vysokého predstaviteľa alebo vedúcich decentralizovaných orgánov.

Jurisdikcia orgánu na schvaľovanie bezpečnosti Generálneho sekretariátu Rady má zahŕňať všetky SYSTÉMY, ktoré sú v prevádzke v komplexe budov Generálneho sekretariátu Rady. SYSTÉMY a komponenty SYSTÉMOV, ktoré sú v prevádzke v členskom štáte, spadajú pod jurisdikciu orgánu na schvaľovanie bezpečnosti Generálneho sekretariátu Rady a iných orgánov na schvaľovanie bezpečnosti, všetky strany majú menovať spoločnú schvaľovaciu Radu, ktorú koordinuje orgán na schvaľovanie bezpečnosti Generálneho sekretariátu Rady.

ORGÁN INFOSEC (IA)

37. Orgán INFOSEC je zodpovedný za aktivity úradu INFOSEC. Pokiaľ ide o Generálny sekretariát Rady a, ak je to vhodné, decentralizované orgány EÚ, orgán INFOSEC je zodpovedný za:

— poskytovanie technickej rady a pomoci orgánu na schvaľovanie bezpečnosti,

— poskytovanie pomoci pri vytváraní formulácie bezpečnostnej požiadavky špecifickej pre systém,

— kontrolovanie formulácie bezpečnostnej požiadavky špecifickej pre systém na zaistenie zhody s týmito bezpečnostnými nariadeniami a politikou INFOSEC a dokumentmi týkajúcimi sa architektúry,

— účasť v schvaľovacích výboroch/radách tak, ako sa požaduje, a poskytovanie INFOSEC odporúčania orgánu na schvaľovanie bezpečnosti, pokiaľ ide o schvaľovanie,

— poskytovanie podpory pre školiace a vzdelávacie aktivity INFOSEC,

— poskytovanie technickej pomoci pri prešetrovaní incidentov spojených s INFOSEC,

— vytvorenie usmernenia pre technický postup na zaistenie používania iba oprávneného softvéru.

ORGÁN PREVÁDZKUJÚCI IT SYSTÉM (ITSOA)

38. Orgán INFOSEC má čo možno v najskoršej možnej etape previesť zodpovednosť za vykonávanie a fungovanie kontrol a zvláštne bezpečnostné charakteristiky SYSTÉMU na orgán prevádzkujúci IT systém. Táto zodpovednosť má trvať počas celého životného cyklu SYSTÉMU od etapy pojmu projektu až po konečné použitie.

▼B

39. Orgán prevádzkujúci IT systém má byť zodpovedný za všetky bezpečnostné opatrenia navrhnuté ako súčasť celkového systému. Táto povinnosť zahŕňa prípravu bezpečnostných prevádzkových postupov (SecOPs). Orgán prevádzkujúci IT systém má stanoviť bezpečnostné normy a praktiky, ktoré má spĺňať dodávateľ SYSTÉMU.

40. Ak je to vhodné, orgán prevádzkujúci IT systém môže poveriť časťou svojich zodpovedností napríklad bezpečnostného technika INFOSEC a bezpečnostného technika na pracovisku INFOSEC. Rôzne funkcie INFOSEC môže vykonávať jedna osoba.

UŽÍVATELIA

41. Všetci užívatelia majú byť zodpovední za to, aby ich činnosti nemali nepriaznivý vplyv na bezpečnosť SYSTÉMU, ktorý používajú.

ŠKOLENIE INFOSEC

42. Na Generálnom sekretariáte Rady, v decentralizovaných orgánoch EÚ alebo vládnych oddeleniach členského štátu má byť zabezpečené vzdelávanie a školenie INFOSEC na rôznych úrovniach a pre rôznych pracovníkov tak, ako je to vhodné.

Kapitola IV

Netechnické bezpečnostné opatrenia

BEZPEČNOSŤ PRACOVNÍKOV

43. Užívatelia SYSTÉMU majú prejsť kontrolou a majú mať potrebu poznať, ako je vhodné pre utajenie a obsah informácií spracovávaných v ich konkrétnom SYSTÉME. Prístup k určitému zariadeniu alebo informáciám špecifickým pre bezpečnosť SYSTÉMOV bude vyžadovať zvláštne povolenie mať tajné informácie vydané podľa postupov Rady.

44. Orgán na schvaľovanie bezpečnosti má označiť všetky citlivé funkcie a špecifikovať úroveň povolenia mať tajné informácie a kontroly, ktorú vyžadujú všetci pracovníci, ktorí ich zastávajú.

45. SYSTÉMY sa majú špecifikovať a navrhovať tak, aby uľahčovali rozdelenie povinností a zodpovedností pracovníkom, aby sa zabránilo, aby jedna osoba mala úplné vedomosti alebo kontrolu hlavných miest bezpečnosti systému. Cieľom by malo byť, aby tajná dohoda medzi dvoma alebo viacerými jednotlivcami nepostačovala na uskutočnenie zmeny alebo zámernej degradácie systému alebo siete.

FYZICKÁ BEZPEČNOSŤ

46. Oblasti IT a oblasti dislokovaného terminálu/pracovnej stanice (ako je definované v odsekoch 29 a 30), v ktorých sa spracovávajú informácie utajené ako CONFIDENTIEL EU alebo vo vyššej kategórii prostriedkami IT, alebo kde je možný potenciálny prístup k takýmto informáciám, sa majú stanoviť ako bezpečnostné oblasti triedy I alebo triedy II alebo národný ekvivalent, ako je to vhodné.

47. Oblasti IT a oblasti dislokovaného terminálu/pracovnej stanice, v ktorých sa môže modifikovať bezpečnosť SYSTÉMU, nemá zastávať iba jeden oprávnený úradník/iný zamestnanec.

KONTROLA PRÍSTUPU K SYSTÉMU

48. Všetky informácie a materiál, ktorý umožňuje kontrolu prístupu do SYSTÉMU, majú byť chránené dohodami odpovedajúcimi najvyššiemu utajeniu a označeniu kategórie informácií, ku ktorým môžu poskytovať prístup.

49. Ak sa už viac nepoužívajú na tento účel, informácie a materiál o kontrole prístupu sa majú zničiť podľa odsekov 61 až 63.

▼B

Kapitola V

Technické bezpečnostné opatrenia

BEZPEČNOSŤ INFORMÁCIÍ

50. Povinnosťou pôvodcu informácií má byť identifikovať a utajiť všetky dokumenty obsahujúce informácie bez ohľadu na to, či sú vo forme výstupu na tlačiarni, alebo na počítačovom pamäťovom médiu. Každá stránka výstupu na tlačiarni má byť vo vrchnej časti a dolu označená utajením. Výstup, či už vo forme výstupu na tlačiarni, alebo počítačového pamäťového média, má mať rovnaké utajenie ako najvyššie utajenie informácií použitých na jeho vytvorenie. Spôsob, ktorým funguje SYSTÉM, môže mať tiež vplyv na utajenie výstupov daného systému.

51. Organizácia a držitelia jej informácií sú povinné zvažovať problémy agregácie jednotlivých prvkov informácií a prekážky, ktoré vznikli z príslušných prvkov, a určiť, či je alebo nie je vhodné vyššie utajenie pre informácie ako celok.

52. Skutočnosť, že informácie môžu mať stručný kód, kód prenosu alebo môžu byť v akejkoľvek forme binárneho vyjadrenia, nepredstavuje žiadnu bezpečnostnú ochranu a nemala by preto ovplyvňovať utajenie informácií.

53. Ak sa informácie prenášajú z jedného SYSTÉMU do druhého, informácie majú byť chránené počas prenosu a v prijímajúcom SYSTÉME spôsobom odpovedajúcim pôvodnému utajeniu a kategórii informácií.

54. Všetky počítačové pamäťové médiá sa majú spracovávať spôsobom odpovedajúcim najvyššiemu utajeniu uchovávaných informácií alebo označeniu média a majú sa vždy primerane chrániť.

55. Opätovne použiteľné pamäťové médiá používané na záznam tajných informácií EÚ si majú zachovať najvyššie utajenie, na aké boli kedy použité, až kým tieto informácie nie sú riadne zaradené do nižšej kategórie alebo odtajené a podľa toho je preutajené médium alebo odtajené médium alebo zničené postupom schváleným Generálnym sekretariátom Rady alebo národným postupom (pozri odseky 61 až 63).

KONTROLA A ZODPOVEDNOSŤ ZA INFORMÁCIE

56. Majú sa udržiavať automatické (revízne záznamy) alebo manuálne protokoly ako záznam o prístupe k informáciám utajeným ako SECRET UE alebo vo vyššej kategórii. Tieto záznamy sa majú udržiavať v súlade s týmito bezpečnostnými nariadeniami.

57. Tajné EÚ výstupy uchovávané v oblasti IT sa môžu považovať za jednu tajnú položku a nemusia byť zaregistrované pod podmienkou, že materiál je primeraným spôsobom identifikovaný, označený jeho utajením a kontrolovaný.

58. Ak sa vytvára výstup zo SYSTÉMU spracovávajúceho tajné informácie EÚ a prenáša sa do oblasti dislokovaného terminálu/pracovnej stanice z IT oblasti, majú sa ustanoviť postupy, ktoré sú schválené orgánom na schvaľovanie bezpečnosti (SAA), na kontrolovanie vzdialeného výstupu. Pre SECRET UE a vyššiu kategóriu takéto postupy majú obsahovať presne definované pokyny, pokiaľ ide o zodpovednosť za informácie.

ZAOBCHÁDZANIE S VYBERATEĽNÝM POČÍTAČOVÝM MÉDIOM A JEHO KONTROLA

59. So všetkými vyberateľnými počítačovými médiami utajenými ako CONFIDENTIEL UE a vo vyššej kategórii sa má zaobchádzať ako s materiálom a uplatňujú sa všeobecné pravidlá. Príslušná identifikácia a označenia utajenia sa majú prispôsobiť konkrétnemu fyzickému zovňajšku média, aby ich bolo možné jasne rozoznať.

60. Užívatelia nesú zodpovednosť za zaistenie, aby sa tajné informácie EÚ uložili na médium s primeraným označením utajenia a ochranou. Majú sa stanoviť postupy na zaistenie, aby sa uchovávanie informácií

▼B

na počítačovom pamäťovom médiu pre všetky úrovne informácií EÚ vykonávalo v súlade s týmito bezpečnostnými pravidlami.

ODTAJENIE A ZNIČENIE POČITAČOVÉHO PAMÄŤOVÉHO MÉDIA

61. Počítačové pamäťové médium, ktoré je použité na záznam tajných informácií EÚ, sa môže zaradiť do nižšej kategórie alebo odtajiť, ak sa uplatnia schválené postupy Generálneho sekretariátu Rady alebo národné postupy.

62. Počítačové pamäťové médium, na ktorom sú TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ informácie alebo zvláštna kategória informácií, sa nemá odtajňovať a znovu používať.

63. Ak sa počítačové pamäťové médium nemôže odtajiť alebo nie je znovu použiteľné, má sa zničiť postupom schváleným Generálnym sekretariátom Rady alebo národným postupom.

BEZPEČNOSŤ KOMUNIKÁCIÍ

64. Ak sa tajné informácie EÚ prenášajú elektromagneticky, vykonávajú sa zvláštne opatrenia na ochranu dôvernosti, celistvosti a použiteľnosti takýchto prenosov. Orgán na schvaľovanie bezpečnosti má určiť požiadavky na ochranu prenosov pred odhalením a zachytením. Informácie, ktoré sa prenášajú v komunikačnom systéme, sa majú chrániť na základe požiadaviek týkajúcich sa dôvernosti, celistvosti a použiteľnosti.

65. Ak sa požadujú kryptografické metódy na zabezpečenie dôvernosti, integrity a dostupnosti ochrany, takéto metódy alebo s nimi spojené produkty majú byť na tento účel výslovne schválené orgánom na schvaľovanie bezpečnosti.

66. Počas prenosu sa má dôvernosť informácií utajených ako SECRET UE a vo vyššej kategórii chrániť kryptografickými metódami alebo produktmi schválenými Radou na základe odporúčania bezpečnostného výboru Rady. Počas prenosu sa má dôvernosť informácií utajených ako CONFIDENTIEL UE alebo RESTREINT UE chrániť kryptografickými metódami alebo produktmi schválenými generálnym tajomníkom/vysokým predstaviteľom na základe odporúčania bezpečnostného výboru Rady alebo schválenými členským štátom.

67. Podrobné pravidlá uplatniteľné na prenos tajných informácií EÚ sú uvedené v zvláštnych bezpečnostných pokynoch schválených Radou na odporúčanie bezpečnostného výboru Rady.

68. Za výnimočných prevádzkových okolností, informácie utajené ako RESTREINT UE, CONFIDENTIEL UE a SECRET UE sa môžu prenášať ako nešifrovaný text pod podmienkou, že každý prípad je výslovne povolený. Takéto výnimočné okolnosti sú nasledovné:

a) počas hrozby alebo skutočnej krízy, konfliktu alebo vojnových situácií a

b) ak má rozhodujúci význam rýchlosť doručenia a nie sú k dispozícii prostriedky šifrovania a bolo stanovené, že prenesené informácie v tejto dobe nemôžu byť použité na nepriaznivé ovplyvnenie operácií.

69. SYSTÉM má mať schopnosť rozhodne odmietnuť prístup k tajným informáciám EÚ alebo všetkým jeho dislokovaným pracovným staniciam alebo terminálom, ak sa prístup požaduje, a to fyzickým odpojením alebo zvláštnymi softvérovými vlastnosťami schválenými orgánom na schvaľovanie bezpečnosti.

BEZPEČNOSŤ INŠTALÁCIE A VYSIELANIA

70. Počiatočná inštalácia SYSTÉMOV a jej akákoľvek zmena má byť tak špecifikovaná, aby inštaláciu vykonali montážni technici, ktorí majú povolenie mať tajné informácie pod neustálym dozorom technicky kvalifikovaných pracovníkov, ktorí prešli kontrolou, pokiaľ ide o prístup k tajným informáciám EÚ na úrovni rovnajúcej sa najvyššiemu utajeniu informácií, o ktorých sa predpokladá, že sa budú uchovávať a spracovávať v SYSTÉME.

71. Každé zariadenie sa má inštalovať v súlade s aktuálnou bezpečnostnou politikou Rady.

▼B

72. SYSTÉMY spracovávajúce informácie utajené ako CONFIDENTIEL UE a vo vyššej kategórii sa majú chrániť takým spôsobom, aby ich bezpečnosť nemohla byť ohrozená nebezpečnými vyžarovaniami, ktorých preskúmanie a kontrola je uvedená ako „TEMPEST“.

73. Protiopatrenia TEMPEST pre zariadenia Generálneho sekretariátu Rady a decentralizovaných orgánov EÚ má kontrolovať a schvaľovať orgán TEMPEST označený Generálnym sekretariátom Rady. Pre národné zariadenia, ktoré spracovávajú tajné informácie EÚ, má byť schvaľovací orgán uznávaný národný schvaľovací orgán TEMPEST.

Kapitola VI

Bezpečnosť počas spracovania

BEZPEČNOSTNÉ PREVÁDZKOVÉ POSTUPY

74. Bezpečnostné prevádzkové postupy (SecOPs) definujú princípy, ktoré sa majú prijať v bezpečnostných záležitostiach, prevádzkové postupy, ktoré sa majú dodržiavať, a zodpovednosti pracovníkov. Bezpečnostné prevádzkové postupy sa pripravujú pod zodpovednosťou orgánu prevádzkujúceho IT systém (ITSOA).

SOFTVÉROVÁ OCHRANA/RIADENIE KONFIGURÁCIE

75. Bezpečnostná ochrana aplikačných programov sa určuje na základe stanovenia bezpečnostného utajenia programu samotného skôr než utajenia informácií, ktoré sa majú spracovávať. Softvérové verzie, ktoré sú v používaní, by sa mali v pravidelných intervaloch overovať, aby sa zaistila ich integrita a správne fungovanie.

76. Nové alebo modifikované verzie softvéru by sa nemali používať na spracovávanie tajných informácií EÚ, pokiaľ nie sú preverené orgánom prevádzkujúcim IT systém.

KONTROLA PRÍTOMNOSTI ŠKODLIVÉHO SOFTVÉRU/POČITAČOVÝCH VÍRUSOV

77. Pravidelne sa má vykonávať kontrola prítomnosti škodlivého softvéru/počítačových vírusov v súlade s požiadavkami orgánu na schvaľovanie bezpečnosti (SAA).

78. Každé počítačové pamäťové médium prichádzajúce na Generálny sekretariát Rady alebo do decentralizovaných orgánov EÚ sa má pred zavedením do akéhokoľvek SYSTÉMU skontrolovať na prítomnosť akéhokoľvek škodlivého softvéru alebo počítačových vírusov.

ÚDRŽBA

79. Zmluvy a postupy pre plánovanú údržbu a údržbu SYSTÉMOV na zavolanie, pre ktoré bola vytvorená formulácia bezpečnostnej požiadavky špecifickej pre systém (SSRS), majú uvádzať požiadavky a dojednania pre pracovníkov údržby a ich príslušné zariadenie vstupujúce do IT oblasti.

80. Požiadavky sa majú jasne uviesť vo formulácii bezpečnostnej požiadavky špecifickej pre systém a postupy sa jasne uvedú v bezpečnostných prevádzkových postupoch. Poskytovateľ údržby, ktorý vyžaduje diagnostické postupy pre vzdialený prístup, sa má povoliť iba za výnimočných okolností, pod najprísnejšou bezpečnostnou kontrolou a iba so súhlasom orgánu na schvaľovanie bezpečnosti (SAA).

Kapitola VII

Obstarávanie

81. Akýkoľvek bezpečnostný produkt, ktorý sa má použiť so SYSTÉMOM, ktorý sa má obstarávať, by mal byť zhodnotený a certifikovaný alebo súčasne by malo prebiehať jeho hodnotenie a certifikácia príslušným hodnotiacim a certifikačným orgánom oproti medzinárodne uznávaným kritériám (ako sú Spoločné kritériá pre hodnotenie bezpečnosti informačnej technológie, pozri ISO 15 408).

▼B

82. Pri rozhodovaní o tom, či sa má zariadenie, najmä počítačové pamäťové médium, prenajať alebo skôr kúpiť, treba mať na mysli, že takéto zariadenie, akonáhle je používané na spracovávanie tajných informácií EÚ, sa nemôže uvoľniť mimo primerane bezpečného prostredia bez toho, aby bolo najprv odtajené so súhlasom orgánu na schvaľovanie bezpečnosti a že takýto súhlas nie je vždy možný.

SCHVAĽOVANIE

83. Všetky systémy, pre ktoré treba predložiť formuláciu bezpečnostnej požiadavky špecifickej pre systém pred spracovávaním tajných informácií EÚ, majú byť schválené na základe informácií poskytnutých vo formulácii bezpečnostnej požiadavky špecifickej pre systém, bezpečnostných prevádzkových postupoch a akejkoľvek inej príslušnej dokumentácii orgánom na schvaľovanie bezpečnosti. Podsystémy a dislokované terminály/pracovné stanice sa majú schvaľovať ako súčasť všetkých SYSTÉMOV, s ktorými sú spojené. Ak SYSTÉM slúži Rade, ako aj iným organizáciám, Generálny sekretariát Rady a príslušné bezpečnostné orgány majú spoločne súhlasiť s akreditáciou.

84. Proces schvaľovania sa môže vykonať v súlade so stratégiou schvaľovania vhodnou pre konkrétny SYSTÉM a definovanou orgánom na schvaľovanie bezpečnosti.

HODNOTENIE A CERTIFIKÁCIA

85. V určitých prípadoch sa pred schválením majú zhodnotiť a certifikovať bezpečnostné charakteristiky hardvéru, mikroprogramového vybavenia a softvéru SYSTÉMU ako schopné ochrany informácií na určenej úrovni utajenia.

86. Požiadavky na hodnotenie a certifikáciu sa majú zahrnúť do plánovania systému a jasne uviesť vo formulácii bezpečnostnej požiadavky špecifickej pre systém.

87. Procesy hodnotenia a certifikácie sa vykonávajú v súlade so schválenými usmerneniami, a to technicky kvalifikovanými a náležite bezpečnostne preverenými pracovníkmi, ktorí konajú v mene orgánu prevádzkujúceho IT systém.

88. Môžu sa zabezpečiť tímy z menovaného hodnotiaceho alebo certifikačného orgánu členského štátu alebo jeho menovaných zástupcov, napríklad príslušný a bezpečnostne preverený dodávateľ.

89. Stupeň príslušných hodnotiacich a certifikačných procesov môže byť nižší (napríklad zahŕňajúci iba integračné aspekty) tam, kde sa SYSTÉMY opierajú o existujúce národne hodnotené a certifikované produkty počítačovej bezpečnosti.

RUTINNÁ KONTROLA BEZPEČNOSTNÝCH CHARAKTERISTÍK PRE ĎALŠIE SCHVAĽOVANIE

90. Orgán prevádzkujúci IT systém má stanoviť rutinné kontrolné postupy, ktoré majú zaistiť stálu platnosť všetkých bezpečnostných charakteristík SYSTÉMU.

91. Typy zmeny, ktoré by viedli k opätovnému schvaľovaniu alebo ktoré vyžadujú vopred súhlas orgánu na schvaľovanie bezpečnosti, sa majú jasne identifikovať a stanoviť vo formulácii bezpečnostnej požiadavky špecifickej pre systém. Po akejkoľvek zmene, oprave alebo poruche, ktorá by mohla ovplyvniť bezpečnostné charakteristiky SYSTÉMU, orgán prevádzkujúci IT systém zaistí, aby sa urobila kontrola na zaistenie správnej funkcie bezpečnostných charakteristík. Ďalšie schválenie SYSTÉMU bude zvyčajne závisieť od uspokojivého vykonania kontrol.

92. Všetky SYSTÉMY, kde boli vykonávané bezpečnostné charakteristiky, bude pravidelne kontrolovať alebo revidovať orgán na schvaľovanie bezpečnosti. Pokiaľ ide o systémy spracovávajúce TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ alebo informácie s ďalšími označeniami, kontroly sa vykonávajú aspoň raz ročne.

▼B

Kapitola VIII

Dočasné alebo príležitostné použitie

BEZPEČNOSŤ MIKROPOČÍTAČOV/OSOBNÝCH POČÍTAČOV

93. Mikropočítače/osobné počítače (PC) s pevnými diskami (alebo iným energeticky nezávislým pamäťovým médiom) pracujúce v samostatnom režime alebo ako sieťové konfigurácie a prenosné počítačové zariadenia (napríklad prenosné PC a elektronické „notebooky“) s pevnými diskami sa považujú za informačné pamäťové médium v tom istom zmysle ako pružné disky alebo iné vyberateľné počítačové pamäťové médium.

94. Týmto zariadeniam sa poskytuje úroveň ochrany, pokiaľ ide o prístup, spracovávanie, uchovávanie a prepravu, odpovedajúca najvyššej úrovni utajenia informácií, aké boli kedy uchované alebo spracované (pokiaľ neboli zaradené do nižšej kategórie alebo odtajené v súlade so schválenými postupmi).

POUŽITIE IT ZARIADENIA V SÚKROMNOM VLASTNÍCTVE PRE OFICIÁLNU PRÁCU RADY

95. Na spracovávanie tajných informácií EÚ je zakázané používanie vyberateľného počítačového pamäťového média, softvéru a IT hardvéru (napríklad PC a prenosných výpočtových zariadení) s pamäťovou kapacitou, ktoré sú v súkromnom vlastníctve.

96. Hardvér, softvér a média v súkromnom vlastníctve sa nemajú uvádzať do oblasti triedy I alebo triedy II, kde sa spracovávajú tajné informácie EÚ bez povolenia vedúceho bezpečnostného orgánu Generálneho sekretariátu Rady alebo oddelenia členského štátu alebo príslušného decentralizovaného orgánu EÚ.

POUŽITIE IT ZARIADENIA, KTORÉ VLASTNÍ DODÁVATEĽ, ALEBO NÁRODNE DODANÉHO IT ZARIADENIA PRE OFICIÁLNU PRÁCU RADY

97. Použitie IT zariadenia a softvéru, ktoré vlastní dodávateľ v organizáciách pre oficiálnu prácu Rady, môže povoliť iba vedúci bezpečnostného úradu Generálneho sekretariátu Rady alebo oddelenia členského štátu alebo príslušného decentralizovaného orgánu EÚ. Môže sa povoliť tiež použitie národne dodaného IT zariadenia a softvéru zamestnancami na Generálnom sekretariáte Rady alebo v decentralizovanom orgáne EÚ; v tomto prípade zariadenie IT je podchytené v inventári Generálneho sekretariátu Rady. V jednom i druhom prípade, ak sa má zariadenie IT používať na spracovávanie tajných informácií EÚ, je potrebná konzultácia s orgánom na schvaľovanie bezpečnosti, či boli náležite zohľadnené a vykonávané prvky INFOSEC, ktoré sú uplatniteľné na použitie tohto zariadenia.

▼B

ODDIEL XII

SPRÍSTUPNENIE TAJNÝCH INFORMÁCIÍ EÚ TRETÍM STRANÁM ALEBO MEDZINÁRODNÝM ORGANIZÁCIÁM

PRINCÍPY UPRAVUJÚCE SPRÍSTUPNENIE TAJNÝCH INFORMÁCIÍ EÚ

1. O sprístupnení tajných informácií EÚ tretím štátom alebo medzinárodným organizáciám rozhoduje Rada na základe:

   — povahy a obsahu takýchto informácií,

   — potreby poznať pokiaľ ide o príjemcov informácií,

   — miery výhod pre EÚ.

   Členský štát, ktorý je pôvodcom tajných informácií EÚ, ktoré sa majú sprístupniť, je požiadaný o súhlas.

2. Tieto rozhodnutia sa prijímajú na základe prípadu za prípadom v závislosti od:

   — požadovanej miery spolupráce s príslušnými tretími štátmi alebo medzinárodnými organizáciami,

   — dôvery, ktorú požívajú, ktorá vyplýva z úrovne bezpečnosti, ktorá by sa mala uplatňovať na tajné informácie EÚ zverené týmito štátom alebo organizáciám a zo zhody medzi bezpečnostnými pravidlami, ktoré sa tam uplatňujú, a tými, ktoré sú uplatňované v EÚ; bezpečnostný výbor Rady poskytne Rade svoje technické stanovisko k tejto záležitosti.

3. Prijatie tajných informácií EÚ tretím štátmi alebo medzinárodnými organizáciami znamená ako samozrejmosť uistenie, že informácie sa nepoužijú na iné účely, ako sú tie, ktoré sú dôvodom na sprístupnenie alebo výmenu informácií, a že im bude poskytnutá ochrana, ktorú požaduje Rada.

ÚROVNE

4. Akonáhle sa Rada rozhodla, že sa tajné informácie môžu sprístupniť alebo vymeniť s daným členským štátom alebo medzinárodnou organizáciou, rozhodne o úrovni spolupráce, ktorá je možná. Závisí to najmä od bezpečnostnej politiky a nariadení uplatňovaných týmto štátom alebo organizáciou.

5. Ide o tri úrovne spolupráce:

   Úroveň 1 Spolupráca s tretími štátmi alebo s medzinárodnými organizáciami, ktorých bezpečnostná politika a nariadenia sú veľmi blízke tým, ktoré sú v EÚ.

   Úroveň 2 Spolupráca s tretími štátmi alebo medzinárodnými organizáciami, ktorých bezpečnostná politika a nariadenia sú výrazne odlišné od tých, ktoré sú v EÚ.

   Úroveň 3 Príležitostná spolupráca s tretími štátmi alebo medzinárodnými organizáciami, ktorých bezpečnostnú politiku a bezpečnostné nariadenia nie je možné zhodnotiť.

6. Každá úroveň spolupráce má určovať bezpečnostné nariadenia, v jednotlivých prípadoch preformulované vzhľadom k technickému stanovisku bezpečnostného výboru Rady, ktorých uplatňovanie sa požaduje od príjemcov na ochranu tajných informácií, ktoré im boli sprístupnené. Tieto postupy a bezpečnostné opatrenia sú podrobne uvedené v dodatkoch 4, 5 a 6.

DOHODY

7. Akonáhle Rada rozhodla, že existuje trvalá alebo dlhodobá potreba výmeny tajných informácií medzi EÚ a tretími štátmi alebo inými medzinárodnými organizáciami, navrhne s nimi „dohody o bezpečnostných postupoch pre výmenu tajných informácií“, ktoré definujú účel spolupráce a recipročné pravidlá na ochranu vymenených tajných informácií.

▼B

8. V prípade príležitostnej spolupráce úrovne 3, ktorá je definíciou obmedzená, pokiaľ ide o čas a účel, jednoduché memorandum dohody definujúce povahu tajných informácií, ktoré sa majú vymieňať, a recipročné záväzky týkajúce sa informácií môže nahrádzať dohodu o postupoch pre výmenu tajných informácií pod podmienkou, nie sú utajené vo vyššej kategórii ako RESTREINT UE.

9. Návrhy dohôd o bezpečnostných postupoch alebo memoranda dohody schvaľuje bezpečnostný výbor pred ich predložením Rade na jej rozhodnutie.

10. Orgány národnej bezpečnosti (NSAs) budú poskytovať generálnemu tajomníkovi/vysokému predstaviteľovi všetku potrebnú pomoc na zaistenie, aby sa informácie, ktoré majú byť sprístupnené, používali a chránili v súlade s ustanoveniami dohôd o bezpečnostných postupoch alebo memoranda dohody.

▼M3

ODDIEL XIII

SPOLOČNÉ MINIMÁLNE NORMY PRE PRIEMYSELNÚ BEZPEČNOSŤ

1. Tento oddiel sa zaoberá bezpečnostnými aspektmi priemyselnej činnosti špecifickými pre rokovanie o zmluvách a zadávanie zmlúv, ktoré zverujú úlohy zahŕňajúce, predpokladajúce a/alebo obsahujúce utajované skutočnosti EÚ, a pre vykonávanie týchto zmlúv priemyselnými alebo inými subjektmi, vrátane poskytnutia alebo sprístupnenia utajovaných skutočností EÚ v rámci procesu verejného obstarávania (obdobie predkladania ponúk a rokovania pred udelením zmluvy).

VYMEDZENIE POJMOV

2. Na účely týchto spoločných minimálnych noriem sa uplatňujú tieto definície:

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

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

   c) „dodávateľ“: fyzická alebo právnická osoba právne spôsobilá uzatvárať zmluvy;

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

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

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

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

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

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

   j) „kniha bezpečnostných aspektov (SAL)“: súbor osobitných zmluvných podmienok vydaných zmluvným orgánom, ktorý identifikuje bezpečnostné požiadavky alebo prvky vyžadujúce bezpečnostnú ochranu

▼M3

a ktorý tvorí neoddeliteľnú súčasť zmluvy podliehajúcej utajeniu zahŕňajúcej vytvorenie utajovaných skutočností EÚ alebo prístup k nim;

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

ORGANIZÁCIA

3. Generálny sekretariát Rady (GSR) môže zmluvne zveriť úlohy zahŕňajúce, predpokladajúce a/alebo obsahujúce utajované skutočnosti EÚ priemyselným alebo iným subjektom registrovaným v členskom štáte.

4. GSR zabezpečí, že pri zadávaní zmluvy podliehajúcej utajeniu sú splnené všetky požiadavky vyplývajúce z uvedených minimálnych noriem.

5. Každý členský štát zabezpečí, aby jeho NBÚ mal vhodné štruktúry na uplatňovanie týchto minimálnych noriem na priemyselnú bezpečnosť. Tieto štruktúry môžu zahŕňať jeden alebo viacero UBÚ.

6. Konečnú zodpovednosť za ochranu utajovaných skutočností EÚ v rámci priemyselných alebo iných subjektov má ich vedenie.

7. Keď je zadaná zmluva alebo subdodávateľská zmluva, ktorá spadá do pôsobnosti týchto minimálnych noriem, GSR a/alebo prípadne NBÚ/UBÚ bezodkladne informuje NBÚ/UBÚ členského štátu, v ktorom je dodávateľ alebo subdodávateľ registrovaný.

ZMLUVY PODLIEHAJÚCE UTAJENIU

8. Bezpečnostné utajenie zmlúv podliehajúcich utajeniu musí zohľadňovať tieto zásady:

a) GSR určí podľa potreby aspekty zmluvy, ktoré vyžadujú ochranu a následné bezpečnostné utajenie; musí pri tom zohľadniť pôvodné bezpečnostné utajenie, ktoré pôvodca pridelil informáciám vytvoreným pred udelením zmluvy;

b) celkový stupeň utajenia zmluvy nesmie byť nižší ako najvyššia úroveň utajenia ktoréhokoľvek z jej prvkov;

c) utajované skutočnosti EÚ, ktoré vznikli počas zmluvných činností, sú utajované v súlade s SCG;

d) GSR je, ak je to vhodné, zodpovedný za zmenu celkového stupňa utajenia zmluvy alebo bezpečnostného utajenia ktoréhokoľvek z jej prvkov, pričom spolupracuje s pôvodcom a informuje všetky zainteresované strany;

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

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

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

▼M3

11. NBÚ/UBÚ je zodpovedný za vydanie osobnej bezpečnostnej previerky (OBP) v súlade s vnútroštátnymi právnymi predpismi pre všetky osoby, ktoré sú zamestnané v priemyselných alebo iných subjektoch registrovaných v danom členskom štáte a ktorých funkcia vyžaduje prístup k skutočnostiam EÚ so stupňom utajenia CONFIDENTIEL UE alebo SECRET UE v prípade zmluvy podliehajúcej utajeniu.

12. Zmluvy podliehajúce utajeniu musia zahŕňať SAL, ako je vymedzená v bode 2 písm. j). SAL musí obsahovať SCG.

13. Pred začatím rokovaní o zmluve podliehajúcej utajeniu sa GSR spojí s NBÚ/UBÚ členských štátov, v ktorých sú dotknuté priemyselné alebo iné subjekty registrované, s cieľom získať potvrdenie, že sú držiteľmi platnej FSC zodpovedajúcej stupňu bezpečnostného utajenia zmluvy.

14. Verejný obstarávateľ nesmie uzavrieť zmluvu podliehajúcu utajeniu s víťazom verejnej súťaže predtým, ako tento získa platné osvedčenie FSC.

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

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

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

18. Podmienky, za ktorých môže dodávateľ uzatvárať subdodávateľské vzťahy, musia byť definované vo verejnej súťaži a v zmluve. So subjektami registrovanými v štáte, ktorý nie je členským štátom EÚ, sa nemôže uzavierať žiadna subdodávateľská zmluva bez výslovného písomného povolenia GSR.

19. Počas celého trvania zmluvy bude príslušný NBÚ/UBÚ v spolupráci s GSR sledovať súlad so všetkými jej bezpečnostnými ustanoveniami. Oznamovanie bezpečnostných udalostí sa vykonáva v súlade s ustanoveniami uvedenými v oddieli X časti II týchto bezpečnostných nariadení. Zmena alebo odobratie FSC sa bezodkladne oznamuje GSR a všetkým ostatným NBÚ/UBÚ, ktorým bola oznámená.

20. Skončenie zmluvy podliehajúcej utajeniu alebo subdodávateľskej zmluvy podliehajúcej utajeniu oznámi GSR a/alebo prípadne NBÚ/UBÚ bezodkladne NBÚ/UBÚ členského štátu, v ktorom je dodávateľ alebo subdodávateľ registrovaný.

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

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

NÁVŠTEVY

23. Návštevy zamestnancov GSR priemyselných alebo iných subjektov, ktoré sú zmluvnou stranou zmlúv podliehajúcich utajeniu EÚ, v členských štátoch sa musia pripraviť v spolupráci s dotknutým NBÚ/UBÚ. Návštevy zamestnancov priemyselných alebo iných subjektov v rámci zmlúv podliehajúcich utajeniu EÚ sa musia pripraviť v spolupráci medzi dotknutými NBÚ/UBÚ. NBÚ/UBÚ, ktorých sa zmluva podliehajúca utajeniu EÚ týka, sa však môžu dohodnúť na postupe, pri ktorom sa návštevy zamestnancov priemyselných alebo iných subjektov môžu pripravovať priamo.

▼M3

ODOVZDÁVANIE A PREPRAVA UTAJOVANÝCH SKUTOČNOSTÍ EÚ

24. Pokiaľ ide o odovzdávanie utajovaných skutočností EÚ, uplatňujú sa ustanovenia kapitoly II oddielu VII časti II a prípadne oddielu XI bezpečnostných nariadení. S cieľom doplniť tieto ustanovenia sa budú uplatňovať akékoľvek existujúce platné postupy medzi členskými štátmi.

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

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

b) úroveň ochrany zásielky je stanovená najvyšším stupňom utajenia materiálu v nej obsiahnutého;

c) pre spoločnosti realizujúce prepravu sa v prípade potreby vykoná FSC. V takýchto prípadoch sa zamestnanci pracujúci so zásielkou podrobia previerke v súlade so spoločnými minimálnymi normami stanovenými v tomto oddiele;

d) cesty sa vykonávajú priamo z miesta pôvodu do miesta určenia a uskutočňujú sa v čo najkratšom možnom čase;

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

f) pred akýmkoľvek presunom utajovaného materiálu EÚ odosielateľ vypracuje plán prepravy a schváli ho dotknutý NBÚ/UBÚ.

▼B

Dodatok 1

Zoznam vnútroštátnych bezpečnostných orgánov

BELGICKO

Service public fédéral des affaires étrangères, du commerce extérieur et de la coopération au développement
Autorité nationale de sécurité (ANS)
Direction du protocole et de la sécurité
Service de la sécurité P&S 6
Rue des Petits Carmes 15
B-1000 Bruxelles
Telephone Secretariat: + 32/2/519 05 74
Telephone Presidency: + 32/2/501 82 20
+ 32/2/501 87 10
Fax: + 32/2/519 05 96

ČESKÁ REPUBLIKA

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56
Tel.: (420) 257 28 33 35
Fax: (420) 257 28 31 10

DÁNSKO

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg
Telephone: (45) 33 14 88 88
Fax: (45) 33 43 01 90

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 København Ø
Telephone: (45) 33 32 55 66
Fax: (45) 33 93 13 20

NEMECKO

Bundesministerium des Innern
Referat IS 4
Alt-Moabit 101 D
D-11014 Berlin
Telefon: + 49-1-888 681 15 26
Fax: + 49-1-888 681 558 06

ESTÓNSKO

Eesti Vabariigi Kaitseministeerium
(Ministry of Defence, Republic of Estonia, Department of Security National Security Authority)
Sakala 1
EE-15094 Tallinn
Telephone: + 372/717 00 30
+ 372/717 00 31
+ 372/717 00 77
Fax: + 372/717 00 01

GRÉCKO

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)

▼**M2**

Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
GR-ΣΤΓ 1020 Χολαργός (Αθήνα)
Τηλέφωνα: (30-210) 657 20 09 (ώρες γραφείου)
(30-210) 657 20 10 (ώρες γραφείου)
Φαξ: (30-210) 642 64 32
(30-210) 652 76 12

[Hellenic National Defence General Staff (HNDGS)]
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Holargos — Athens
Telephone: (30-210) 657 20 09 (office hours)
(30-210) 657 20 10 (office hours)
Fax: (30-210) 642 64 32
(30-210) 652 76 12

ŠPANIELSKO

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
Carretera nacional radial VI, km 8,5
E-28023 Madrid
Telephone: + 34/913 72 57 07
+ 34/913 72 50 27
Fax: + 34/913 72 58 08

FRANCÚZSKO

Secrétariat général de la défense nationale
Service de sécurité de défense (SGDN/SSD)
51, boulevard de la Tour-Maubourg
F-75700 Paris 07 SP
Telephone: + 33/1/71 75 81 77
Fax: + 33/1/71 75 82 00

ÍRSKO

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

TALIANSKO

Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
Cesis III Reparto (UCSi)
Via di Santa Susanna, 15
I-00187 Roma
Telephone: + 39/06/611 742 66
Fax: + 39/06/488 52 73

CYPRUS

Υπουργείο Άμυνας
Στρατιωτικό επιτελείο του υπουργού
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
CY-1432 Λευκωσία
Τηλέφωνα: (357-22) 80 75 69
(357-22) 80 75 19

▼M2

(357-22) 80 77 64
Φαξ: (357-22) 30 23 51

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi Street
CY-1432 Nicosia
Telephone: (357-22) 80 75 69
(357-22) 80 75 19
(357-22) 80 77 64
Fax: (357-22) 30 23 51

LOTYŠSKO

National Security Authority of Constitution Protection
Bureau of the Republic of Latvia
Miera iela 85 A
LV-1013 Riga
Telephone: + 371/702 54 18
Fax: + 371/702 54 54

LITVA

Lithuanian National Security Authority
Gedimino ave. 40/1
LT-01110 Vilnius
Telephone: + 370/5/266 32 01
Fax: + 370/5/266 32 00

LUXEMBURSKO

Autorité nationale de sécurité
Ministère d'État
Boîte postale 23 79
L-1023 Luxembourg
Telephone: + 352/478 22 10 central
+ 352/478 22 35 direct
Fax: + 352/478 22 43
+ 352/478 22 71

MAĎARSKO

National Security Authority Republic of Hungary
Nemzeti Biztonsági Felügyelet
Pf.: 2
HU-1352 Budapest
Telephone: + 361/346 96 52
Fax: + 361/346 96 58

MALTA

Ministry of Justice and Home Affairs
P.O. Box 146
MT-Valletta
Telephone: + 356/21 24 98 44
Fax: + 356/21 23 53 00

HOLANDSKO

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag
Nederland
Telephone: (31-70) 320 44 00
Fax: (31-70) 320 07 33

Ministerie van Defensie

▼M2

Beveiligingsautoriteit (BA)
Postbus 20701
2500 ES Den Haag
Nederland
Telephone: (31-70) 318 70 60
Fax: (31-70) 318 75 22

RAKÚSKO

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien
Telefon: + 43-1-531 15 23 96
Fax: + 43-1-531 15 25 08

POĽSKO

Wojskowe Służby Informacyjne (Military Information Services
National Security Authority – Military Sphere)
PL-00-909 Warszawa 60
Telephone: + 48/22/684 13 62
Fax: + 48/22/684 10 76

Agencja Bezpieczeństwa Wewnętrznego – ABW (Internal Security Agency
National Security Authority – Civilian Sphere
Department for the Protection of Classified Information)
ul. Rakowiecka 2A
PL-00-993 Warszawa
Telephone: + 48/22/585 73 60
Fax: + 48/22/585 85 09

PORTUGALSKO

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Avenida Ilha da Madeira, 1
P-1400-204 Lisboa
Tel.: (351) 21 301 17 10
Fax: (351) 21 303 17 11

SLOVINSKO

Office of the Government of the Republic of Slovenia
For the Protection of Classified Information – NSA
Slovenska cesta 5
SI-1000 Ljubljana
Tel.: (386-1) 426 91 20
Faks: (386-1) 426 91 21

SLOVENSKO

Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
SK-851 05 Bratislava
Telephone: + 421/2/68 69 23 14
Fax: + 421/2/68 69 17 00

FÍNSKO

Ulkoasiainministeriö/Utrikesministeriet
Alivaltiosihteeri (Hallinto)/Understatssekreteraren (Administration)
Laivastokatu 22/Maringatan 22
PL/PB 176
FIN-00161 Helsinki/Helsingfors
Telephone: (358-9) 16 05 53 38

▼**M2**

Fax: (358-9) 16 05 53 03

ŠVÉDSKO

Utrikesdepartementet
SSSB
S-103 39 Stockholm
Telephone: + 46/8/405 54 44
Fax: + 46/8/723 11 76

SPOJENÉ KRÁĽOVSTVO

UK National Security Authority
PO Box 49359
London, SW1P 1LU
United Kingdom
Telephone (44-207) 930 87 68
Fax (44-207) 821 86 04

▼M2

Dodatok 2

Porovnanie bezpečnostných klasifikácií

Klasifikácia EÚ a členských štátov EÚ	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Euratom	*Eura — Top Secret*	*Eura — Secret*	*Eura — Confidential*	*Eura — Restricted*
Belgicko	Très Secret Zeer geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte verspreiding
Česká republika	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dánsko	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Nemecko	Streng geheim	Geheim	VS (9) — Vertraulich	VS — Nur für den Dienstgebrauch
Estónsko	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Grécko	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Španielsko	Secreto	Reservado	Confidencial	Difusión Limitada
Francúzsko	Très Secret Défense (10)	Secret Défense	Confidentiel Défense	nota (11)
Írsko	Top Secret	Secret	Confidential	Restricted
Taliansko	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Lotyšsko	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembursko	Très Secret	Secret	Confidentiel	Diffusion restreinte

▼M2

Klasifikácia EÚ a členských štátov EÚ	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Maďarsko	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Holandsko	Zeer geheim	Geheim	Confidentieel	Vertrouwelijk
Rakúsko	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poľsko	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalsko	Muito Secreto	Secreto	Confidencial	Reservado
Slovinsko	Strogo tajno	Tajno	Zaupno	Interno
Slovensko	Prísne tajné	Tajné	Dôverné	Vyhradené
Fínsko	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Švédsko	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Spojené kráľovstvo	Top Secret	Secret	Confidential	Restricted
Klasifikácia medzinárodných organizácií	TRÈS SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
Klasifikácia NATO	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
Klasifikácia WEU	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted

([9]) Nemecko: VS = Verschlusssache.
([10]) Francúzsko: klasifikáciu Trés Secret Défense, ktorá sa vzťahuje na najdôležitejšie štátne záležitosti, je možné zmeniť len po odsúhlasení predsedom vlády.
([11]) Francúzsko nepoužíva vo svojom vnútroštátnom systéme pri zatriedení kategóriu „DIFFUSION RESTREINTE“. Francúzsko sa zaoberá dokumentmi a chráni dokumenty, ktoré majú označenie „RESTREINT EU“ podľa svojich vnútroštátnych zákonov a platných právnych predpisov, ktoré nie sú menej prísne ako ustanovenia bezpečnostných nariadení Rady.

Dodatok 3

Praktický návod pre utajenie

Tento návod je doporučujúci a nemá sa vysvetľovať ako zmena základných ustanovení uvedených v oddieloch II a III.

Utajenie	Kedy	Kto	Označenia	Zaradenie do nižšej kategórie/odtajenie/zničenie	
				Kto	Kedy
TRÈS SECRET UE/PRÍSNE TAJNÉ EÚ: Toto utajenie sa má používať iba na informácie a materiál, ktorého neoprávnené prezradenie by mohlo spôsobiť mimoriadne vážne poškodenie hlavných záujmov Európskej únie alebo jedného alebo viacerých jej členských štátov [SII (1)].	Ohrozenie majetku označeného TRÈS SECRET UE/PRÍSNE TAJNÝ EÚ by pravdepodobne: — ohrozovalo priamo stabilitu EÚ alebo jedného z jej členských štátov alebo spriatelených krajín — spôsobovalo mimoriadne vážne poškodenie vzťahov so spriatelenými vládami — viedlo priamo k rozsiahlym stratám na životoch — spôsobovalo mimoriadne vážne poškodenie operačnej efektívnosti alebo bezpečnosti členských štátov alebo ozbrojených síl iných spolupracovníkov alebo plynulej efektívnosti mimoriadne dôležitej bezpečnosti alebo činností spravodajských služieb — spôsobovalo vážne dlhodobé poškodenie ekonomiky EÚ alebo členských štátov	Členské štáty: náležite oprávnené osoby (pôvodcovia) [SIII(4)]; Generálny sekretariát Rady: náležite oprávnené osoby (pôvodcovia) [SIII(4)], generálny tajomník/vysoký predstaviteľ a DSG. Pôvodcovia majú uvádzať dátum alebo obdobie, kedy sa môže obsah zaradiť do nižšej kategórie alebo odtajiť. V opačnom prípade sa dokumenty majú znovu preveriť aspoň každých päť rokov, aby sa zistilo, či je potrebné pôvodné utajenie [SIII(10)].	Utajenie TRÈS SECRET UE/PRÍSNE TAJNÉ EÚ sa uplatňuje na dokumenty TRÈS SECRET UE/PRÍSNE TAJNÉ EÚ a, kde je to uplatniteľné, uvedie sa ochranné označenie ESDP mechanickými prostriedkami alebo ručne [SII(8)]. Utajenia EÚ sa majú uvádzať hore a dolu v strede každej strany a každá strana má byť očíslovaná. Každý dokument má mať referenčné číslo a dátum; toto referenčné číslo má byť na každej strane. Ak sa majú distribuovať v niekoľkých kópiách, každá kópia má mať číslo kópie, ktoré je uvedené na prvej strane, spolu s celkovým počtom strán. Všetky prílohy a dodatky majú byť uvedené v zozname na prvej strane [SVII(1)].	Odtajenie alebo zaradenie do nižšej kategórie je výhradne povinnosťou generálneho tajomníka/vysokého úradníka alebo DSG, ktorý má informovať o zmene akýchkoľvek ďalších adresátov, ktorým bol poslaný alebo skopírovaný dokument [SVIII(9)]. Dokumenty TRÈS SECRET UE/PRÍSNE TAJNÉ EÚ má zničiť centrálny register alebo podregister, ktorý je za ne zodpovedný. Každý zničený dokument má byť uvedený na osvedčení o zničení, ktoré je podpísané úradníkom kontroly pre dokumenty TRÈS SECRET UE/PRÍSNE TAJNÉ EÚ dokumenty a úradníkom, ktorý je svedkom tohto zničenia, ktorý má prejsť kontrolou, pokiaľ ide o utajenie TRÈS SECRET UE/PRÍSNE TAJNÉ EÚ. V tomto zmysle treba urobiť záznam do denníka. Register má uchovávať osvedčenia o zničení, spolu s distribučnou listinou počas obdobia desiatich rokov [SVII(31)].	Nadbytočné kópie a dokumenty, ktoré už viac nie sú potrebné, sa musia zničiť [SVII(31)]. Dokumenty TRÈS SECRET UE/PRÍSNE TAJNÉ EÚ, vrátane všetkého tajného odpadu vyplývajúceho z prípravy TRÈS SECRET UE/PRÍSNE TAJNÝCH EÚ dokumentov, ako sú pokazené kópie, pracovné náčrty, napísané poznámky a kópie cez kopírovací papier, sa majú zničiť pod dohľadom úradníka pre TRÈS SECRET UE/PRÍSNE TAJNÉ EÚ spálením, rozdrvením, rozsekaním na kúsky alebo inak rozkúskovaním na nerozoznateľnú a nezložiteľnú podobu [SVII (31)].

▼B

Utajenie	Kedy	Kto	Označenia	Zaradenie do nižšej kategórie/odtajenie/zničenie	
				Kto	Kedy
SECRET: Toto utajenie sa má uplatňovať iba na informácie a materiál, ktorých neoprávnené prezradenie by mohlo vážne poškodiť hlavné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov [SII(2)].	Ohrozenie majetku označeného SECRET UE by pravdepodobne: — zvýšilo medzinárodné napätia — vážne poškodilo vzťahy so spriatelenými vládami — priamo ohrozovalo život alebo vážne poškodzovalo verejný poriadok alebo individuálnu bezpečnosť alebo slobodu — spôsobovalo vážne poškodenie operačnej efektívnosti alebo bezpečnosti členských štátov alebo ozbrojených síl iných spolupracovníkov alebo plynulej efektívnosti mimoriadne dôležitej bezpečnosti alebo činností spravodajských služieb — spôsobovalo značné materiálne poškodenie finančných, menových, ekonomických a obchodných záujmov EÚ alebo jedného z jej členských štátov.	Členské štáty: náležite oprávnené osoby (pôvodcovia) [SIII(2)]; Generálny sekretariát Rady a decentralizované orgány EÚ: oprávnené osoby (pôvodcovia) [SIII(2)], generálni riaditelia, generálny tajomník/vysoký predstaviteľ a DSG. Pôvodcovia majú uvádzať dátum alebo obdobie, kedy sa môže obsah zaradiť do nižšej kategórie alebo odtajiť. V opačnom prípade sa dokumenty majú znovu preveriť aspoň každých päť rokov, aby sa zistilo, či je potrebné pôvodné utajenie [SVII(1)].	Utajenie SECRET UE sa uplatňuje na dokumenty SECRET UE a, kde je to uplatniteľné, uvedie sa ochranné označenie ESDP mechanickými prostriedkami alebo ručne [SIII(8)]. Utajenia EÚ sa majú uvádzať hore a dolu v strede každej strany a každá strana má byť očíslovaná. Každý dokument má mať referenčné číslo a dátum; toto referenčné číslo má byť na každej strane. Ak sa majú distribuovať v niekoľkých kópiách, každá kópia má mať číslo kópie, ktoré je uvedené na prvej strane, spolu s celkovým počtom strán. Všetky prílohy a dodatky majú byť uvedené v zozname na prvej strane [SVII(1)].	Odtajenie alebo zaradenie do nižšej kategórie je výhradne povinnosťou pôvodcu alebo generálneho tajomníka/vysokého úradníka alebo DSG, ktorý má informovať o zmene akýchkoľvek ďalších adresátov, ktorým bol poslaný alebo skopírovaný dokument [SVII(9)]. Dokumenty SECRET UE má zničiť register, ktorý je zodpovedný za tieto dokumenty, pod dohľadom osoby, ktorá má povolenie mať tajné informácie. SECRET UE dokumenty, ktoré sa majú zničiť, majú byť uvedené v podpísaných osvedčeniach o zničení, ktoré má register uchovávať spolu s formulármi zničenia aspoň tri roky [SVII(32)].	Nadbytočné kópie a dokumenty, ktoré už viac nie sú potrebné, sa musia zničiť [SVII(31)]. Dokumenty SECRET UE, vrátane všetkého tajného odpadu vyplývajúceho z prípravy SECRET UE dokumentov, ako sú pokazené kópie, pracovné náčrty, napísané poznámky a kópie cez kopírovací papier, sa majú zničiť spálením, rozdrvením, rozsekaním na kúsky alebo inak rozkúskovaním na nerozoznateľnú a nezložiteľnú podobu [SVII(31),(32)].

Utajenie	Kedy	Kto	Označenia	Zaradenie do nižšej kategórie/odtajenie/zničenie	
				Kto	Kedy
CONFIDENTIEL UE: Toto utajenie sa má uplatňovať na informácie a materiál, ktorých neoprávnené prezradenie by mohlo poškodiť hlavné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov [SII(3)].	Ohrozenie majetku označeného CONFIDENTIEL UE by pravdepodobne: — vážne poškodilo diplomatické vzťahy, čo by vyvolalo oficiálny protest alebo iné sankcie — nepriaznivo ovplyvnilo individuálnu bezpečnosť alebo slobodu — spôsobovalo poškodenie operačnej elektívnosti alebo bezpečnosti členských štátov alebo ozbrojených síl iných spolupracovníkov alebo plynulej efektívnosti mimoriadne dôležitej bezpečnosti alebo činností spravodajských služieb — do značnej miery podkopávalo finančnú životaschopnosť významných organizácií — bránilo vyšetrovaniu alebo uľahčovalo páchanie vážneho trestného činu — pôsobilo podstatnou mierou proti finančným, menovým, ekonomickým a obchodným záujmom EÚ alebo členských štátov. — vážne znemožňovalo rozvoj alebo fungovanie hlavnej politiky EÚ — ukončovalo alebo inak vážne narušovalo dôležité aktivity EÚ	Členské štáty: oprávnené osoby (pôvodcovia) [SIII(2)]; Generálny sekretariát Rady a decentralizované orgány EÚ: oprávnené osoby (pôvodcovia) [SIII(2)], generálni riaditelia, generálny tajomník/vysoký predstaviteľ a DSG; Pôvodcovia majú uvádzať dátum alebo obdobie, kedy sa môže obsah zaradiť do nižšej kategórie alebo odtajiť. V opačnom prípade sa dokumenty majú znovu preveriť aspoň každých päť rokov, aby sa zistilo, či je potrebné pôvodné utajenie [SIII(10)].	Utajenie CONFIDENTIEL UE sa uplatňuje na dokumenty CONFIDENTIEL UE a, kde je to uplatniteľné, uvádza sa ochranné označenie ESDP mechanickými prostriedkami alebo ručne alebo vytlačením na vopred opečiatkovaný zaregistrovaný dokument [SII(8)]. Utajenia EÚ sa majú uvádzať hore a dolu v strede každej strany a každá strana má byť očíslovaná. Každý dokument má mať referenčné číslo a dátum. Všetky prílohy a dodatky majú byť uvedené v zozname na prvej strane [SVII(1)].	Odtajenie alebo zaradenie do nižšej kategórie je výhradne povinnosťou pôvodcu alebo generálneho tajomníka/vysokého úradníka alebo DSG, ktorý má informovať o zmene akýchkoľvek ďalších adresátov, ktorým bol poslaný alebo skopírovaný dokument [SVII(31)]. Dokumenty CONFIDENTIEL UE má zničiť register, ktorý je zodpovedný za tieto dokumenty pod dohľadom osoby, ktorá má povolenie mať tajné informácie. Ich zničenie sa má zaznamenávať v súlade s národnými nariadeniami a v prípade Generálneho sekretariátu Rady alebo decentralizovaných orgánov EÚ podľa pokynov od generálneho tajomníka/vysokého predstaviteľa alebo DSG [SVII(33)].	Nadbytočné kópie a dokumenty, ktoré už viac nie sú potrebné, sa musia zničiť [SVII(31)]. Dokumenty CONFIDENTIEL UE, vrátane všetkého tajného odpadu vyplývajúceho z prípravy CONFIDENTIEL UE dokumentov, ako sú pokazené kópie, pracovné náčrty, napísané poznámky a kópie cez kopírovací papier, sa majú zničiť spálením, rozdrvením, rozsekaním na kúsky alebo inak rozkúskovaním na nerozoznateľnú a nezložiteľnú podobu [SVII (31),(33)].

▼B

Utajenie	Kedy	Kto	Označenia	Zaradenie do nižšej kategórie/odtajenie/zničenie	
				Kto	Kedy
RESTREINT EU: Toto utajenie sa má uplatňovať na informácie a materiál, ktorých neoprávnené prezradenie by mohlo byť nevýhodné pre záujmy EÚ alebo jedného alebo viacerých jej členských štátov [SII (4)].	Ak ohrozenie majetku označeného RESTREINT UE by pravdepodobne: — malo nepriaznivý vplyv na diplomatické vzťahy — spôsobilo značné nebezpečenstvo pre jednotlivcov — spôsobovalo, že by bolo ťažké zachovať operačnú elektívnosť alebo bezpečnosť členských štátov alebo ozbrojených síl iných spolupracovníkov — spôsobovalo finančnú stratu alebo uľahčovalo nesprávny príjem alebo výhodu pre jednotlivcov alebo spoločnosti — porušovalo príslušné záväzky zachovávať dôvernosť informácií poskytnutých tretími stranami — porušovalo obmedzenia vyplývajúce zo zákona o prezradení informácií — nepriaznivo ovplyvňovalo vyšetrovanie alebo uľahčovalo by páchanie trestného činu — znevýhodňovalo EÚ alebo členské štáty pri obchodných alebo politických rokovaniach s inými — znemožňovalo efektívny rozvoj alebo fungovanie politiky EÚ — podkopávalo správne riadenie EÚ a jej činnosti	Členské štáty: oprávnené osoby (pôvodcovia) [SIII(2)]; Generálny sekretariát Rady a decentralizované orgány EÚ: oprávnené osoby (pôvodcovia) [SIII(2)], generálni riaditelia, generálny tajomník/vysoký predstaviteľ a DSG; Pôvodcovia majú uvádzať dátum alebo obdobie, kedy sa môže obsah zaradiť do nižšej kategórie alebo odtajiť. V opačnom prípade sa dokumenty majú znova preveriť aspoň každých päť rokov, aby sa zistilo, či je potrebné pôvodné utajenie [SIII(10)].	Utajenie RESTREINT UE sa uplatňuje na dokumenty RESTREINT UE a, kde je to uplatniteľné, uvádza sa ochranné označenie ESDP mechanickými prostriedkami alebo ručne [SII(8)]. Utajenia EÚ sa majú uvádzať hore a dolu v strede každej strany a každá strana má byť očíslovaná. Každý dokument má mať referenčné číslo a dátum [SVII(1)].	Odtajenie alebo zaradenie do nižšej kategórie je výhradne povinnosťou pôvodcu alebo generálneho tajomníka/vysokého úradníka alebo DSG, ktorý má informovať o zmene akýchkoľvek ďalších adresátov, ktorým bol poslaný alebo skopírovaný dokument [SIII(9)]. Dokumenty RESTREINT UE má zničiť register, ktorý je zodpovedný za tieto dokumenty v súlade s národnými nariadeniami a v prípade Generálneho sekretariátu Rady alebo decentralizovaných orgánov EÚ, podľa pokynov generálneho tajomníka/vysokého predstaviteľa alebo DSG [SVII(34)].	Nadbytočné kópie a dokumenty, ktoré už viac nie sú potrebné, sa musia zničiť [SVII(31)].

▼B

Dodatok 4

Usmernenia pre sprístupňovanie tajných informácií EÚ tretím štátom alebo medzinárodným organizáciám

Spolupráca na úrovni 1

POSTUPY

1. Povolenie na sprístupnenie tajných informácií EÚ krajinám, ktoré nie sú signatármi Zmluvy o Európskej únii alebo iným medzinárodných organizáciám, ktorých bezpečnostná politika a nariadenia sú porovnateľné s tými, ktoré sú v EÚ, poskytuje Rada.

2. Rada môže previesť právomoc rozhodovať o sprístupnení tajných informácií. Jej prenesenie právomoci uvádza povahu informácií, ktoré sa môžu sprístupniť, a ich úroveň utajenia, ktorá spravidla nebude vyššia ako CONFIDENTIEL UE.

3. Podľa záveru bezpečnostnej dohody, požiadavky na sprístupnenie tajných informácií EÚ predkladajú bezpečnostné orgány príslušných štátov alebo medzinárodných organizácií generálnemu tajomníkovi/vysokému predstaviteľovi, pričom tieto majú uvádzať účel, na ktorý je určené toto sprístupnenie, a povahu tajných informácií, ktoré sa majú sprístupniť.

   Ak je to žiaduce, tiež členský štát alebo decentralizovaný orgán EÚ môže predložiť žiadosti, pokiaľ ide o sprístupnenie tajných informácií EÚ; majú uvádzať účely a výhodu takéhoto zverejnenia pre EÚ, špecifikujúc povahu a utajenie informácií, ktoré sa majú sprístupniť.

4. Žiadosť bude hodnotiť Generálny sekretariát Rady, ktorý:

   — požiada o stanovisko členský štát alebo, ak je to vhodné, decentralizovaný orgán EÚ, ktorý je pôvodcom informácií, ktoré sa majú sprístupniť,

   — nadviaže potrebné kontakty s bezpečnostnými orgánmi krajín alebo medzinárodných organizácií, ktoré sú ich oprávnenými užívateľmi s cieľom overenia, či ich bezpečnostná politika a nariadenia sú také, aby zaručili ochranu sprístupnených tajných informácií v súlade s týmito bezpečnostnými nariadeniami,

   — požiada o technické stanoviská orgány národnej bezpečnosti členských štátov, pokiaľ ide o dôveru, ktorú požívajú štáty alebo medzinárodné organizácie, ktoré sú ich oprávnenými užívateľmi.

5. Generálny sekretariát Rady doručí žiadosť a odporúčanie bezpečnostného úradu Rade na jej rozhodnutie.

BEZPEČNOSTNÉ NARIADENIA, KTORÉ MAJÚ UPLATŇOVAŤ OPRÁVNENÍ UŽÍVATELIA INFORMÁCIÍ

6. Generálny tajomník/vysoký predstaviteľ má informovať štáty alebo medzinárodné organizácie, ktoré sú oprávnenými užívateľmi informácií, o rozhodnutí Rady povoliť sprístupnenie tajných informácií EÚ, pričom im odošle toľko kópií týchto bezpečnostných nariadení, ako sa môže považovať za potrebné. Ak požiadavku uskutočnil členský štát, tento štát má informovať užívateľa informácií o povolenom sprístupnení.

   Rozhodnutie o sprístupnení nadobudne účinnosť, iba ak oprávnení užívatelia informácií poskytnú písomné uistenie, že:

   — nebudú používať informácie na žiadne iné účely než sú dohodnuté účely,

   — budú chrániť informácie v súlade s týmito bezpečnostnými nariadeniami a najmä so zvláštnymi ustanoveniami uvedenými nižšie.

7. *Pracovníci*

▼B

a) Množstvo úradníkov, ktorí majú prístup k tajným informáciám EÚ, má byť striktne obmedzené, na základe princípu potreby poznať, na tie osoby, ktorých povinnosti vyžadujú takýto prístup.

b) Všetci úradníci a štátni príslušníci, ktorí sú oprávnení mať prístup k informáciám utajeným ako CONFIDENTIEL UE alebo vo vyššej kategórii, majú byť držiteľmi povolenia mať tajné informácie na príslušnej úrovni alebo ekvivalentného povolenia mať tajné informácie, alebo povolenia vydaného vládou ich vlastného štátu.

8. *Prenos dokumentov*

a) Treba rozhodnúť o praktických postupoch na prenos dokumentov dohodou na základe ustanovení oddielu VII bezpečnostných nariadení Rady. Majú špecifikovať najmä registre, do ktorých sa majú odosielať tajné informácie EÚ.

b) Ak tajné informácie, ktorých sprístupnenie Rada povolila, obsahujú TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ informácie, štát alebo medzinárodná organizácia, ktorá je ich oprávneným užívateľom, má zriadiť centrálny register EÚ a, ak je to potrebné, podriadené registre EÚ. Tieto registre upravujú ustanovenia oddielu VIII týchto bezpečnostných nariadení.

9. *Registrácia*

Akonáhle registračný úrad obdrží dokument EÚ utajený ako CONFIDENTIEL UE alebo vo vyššej kategórii, zaznamená dokument do zvláštneho registra, ktorý vedie táto organizácia, so stĺpcami pre dátum prijatia, údajmi o dokumente (dátum, odkaz a počet kópií), utajením, názvom, menom alebo názvom príjemcu, dátumom prijatia a dátumom, kedy je dokument vrátený oprávnenému užívateľovi alebo zničený.

10. *Zničenie*

a) Tajné dokumenty EÚ sa zničia v súlade s pokynmi uvedenými v oddiele VI týchto bezpečnostných nariadení. Kópie osvedčení o zničení pre dokumenty SECRET UE a TRÉS SECRET UE/PRÍSNE TAJNÉ EÚ sa zasielajú registračnému úradu EÚ, ktorý odoslal dokumenty.

b) Tajné dokumenty EÚ sa majú zahrnúť do plánov núdzového zničenia, ktoré majú orgány oprávnených užívateľov pre svoje vlastné tajné dokumenty.

11. *Ochrana dokumentov*

Treba podniknúť všetky kroky na zabránenie prístupu neoprávnených osôb k tajným informáciám EÚ.

12. *Kópie, preklady a výňatky*

Nesmú sa robiť žiadne fotokópie alebo preklad z dokumentu utajeného ako CONFIDENTIEL UE alebo SECRET UE alebo výňatky bez povolenia vedúceho príslušnej bezpečnostnej organizácie, ktorá zaregistruje a skontroluje tieto kópie, preklady a výňatky a opečiatkuje ich, ak je to potrebné.

Reprodukciu alebo preklad TRÉS SECRET UE/PRÍSNE TAJNÉHO dokumentu EÚ môže povoliť iba orgán, ktorý je jeho pôvodcom, ktorý má uviesť počet povolených kópií; ak nie je možné určiť orgán, ktorý je ich pôvodcom, požiadavka sa predloží bezpečnostnému orgánu Generálneho sekretariátu Rady.

13. *Porušenia bezpečnosti*

Ak sa udeje porušenie bezpečnosti týkajúce sa tajného dokumentu EÚ alebo je takéto podozrenie, treba okamžite podniknúť nasledovné kroky podľa záveru bezpečnostnej dohody:

a) vykonať prešetrenie, aby sa stanovili okolnosti porušenia bezpečnosti;

b) informovať bezpečnostný úrad Generálneho sekretariátu Rady, orgán národnej bezpečnosti a orgán, ktorý je pôvodcom dokumentu, alebo

▼B

jasne uviesť, že tieto orgány by neboli informované, ak by k tomu nebolo došlo;

c) podniknúť kroky na minimalizovanie vplyvov porušenia bezpečnosti;

d) prehodnotiť a vykonávať opatrenia na zabránenie opätovného výskytu;

e) vykonávať akékoľvek opatrenia odporúčané bezpečnostným úradom Generálneho sekretariátu Rady na zabránenie opätovného výskytu.

14. *Kontroly*

Bezpečnostný úrad Generálneho sekretariátu Rady má povolené na základe dohody s príslušnými štátmi alebo medzinárodnými organizáciami vykonať zhodnotenie efektívnosti opatrení na ochranu sprístupnených tajných informácií EÚ.

15. *Podávanie správy*

Podľa záveru bezpečnostnej dohody, pokiaľ príslušný štát alebo medzinárodná organizácia má tajné informácie EÚ, mali by predkladať ročnú správu do dátumu, ktorý je špecifikovaný v čase poskytnutia povolenia sprístupniť informácie, potvrdzujúcu, že sa zabezpečil súlad s týmito bezpečnostnými nariadeniami.

▼B

Dodatok 5

Usmernenia pre sprístupňovanie tajných informácií EÚ tretím krajinám alebo medzinárodným organizáciám

Spolupráca na úrovni 2

POSTUPY

1. Rada poskytuje povolenie sprístupniť tajné informácie EÚ tretím štátom alebo medzinárodným organizáciám, ktorých bezpečnostná politika a nariadenia sa značne odlišujú od tých, ktoré sú v EÚ. Väčšinou sa obmedzuje na informácie utajené až do SECRET UE vrátane; vylučuje národné informácie osobitne vyhradené členským štátom a kategórie tajných informácií chránené zvláštnymi označeniami.

2. Rada môže previesť svoju právomoc rozhodovať: pri takomto prenesení právomoci, v rámci obmedzení definovaných v odseku 1, uvádza povahu informácií, ktoré sa môžu sprístupniť, a ich úroveň utajenia, ktorá nie je vyššia ako RESTREINT UE.

3. Podľa záveru bezpečnostnej dohody, požiadavky na sprístupnenie tajných informácií EÚ predkladajú bezpečnostné orgány príslušných štátov alebo medzinárodných organizácií generálnemu tajomníkovi/vysokému predstaviteľovi, pričom tieto majú uvádzať účel, na ktorý je určené toto sprístupnenie, a povahu tajných informácií, ktoré sa majú sprístupniť.

   Ak je to žiaduce, tiež členský štát alebo decentralizovaný orgán EÚ môže predložiť žiadosti, pokiaľ ide o sprístupnenie tajných informácií EÚ; majú uvádzať účely a výhodu takéhoto zverejnenia pre EÚ, špecifikujúc povahu a utajenie informácií, ktoré sa majú sprístupniť.

4. Žiadosť bude hodnotiť Generálny sekretariát Rady, ktorý:

   — požiada o stanoviská členský štát alebo, ak je to vhodné, decentralizovaný orgán EÚ, ktorý je pôvodcom informácií, ktoré sa majú sprístupniť,

   — nadviaže predbežné kontakty s bezpečnostnými orgánmi štátov alebo medzinárodných organizácií, ktoré sú ich oprávnenými užívateľmi, s cieľom zistenia informácií o ich bezpečnostnej politike a nariadeniach a najmä kvôli zostaveniu tabuľky porovnávajúcej utajenia uplatniteľné v EÚ a v príslušnom štáte alebo organizácii,

   — zariadi stretnutie s bezpečnostným výborom Rady alebo, ak je to potrebné, použije tichý postup informovania sa u orgánov národnej bezpečnosti s cieľom získania technického stanoviska bezpečnostného výboru.

5. Technické stanovisko bezpečnostného výboru Rady sa má týkať nasledovného:

   — dôvery, ktorú môžu užívať štáty alebo medzinárodné organizácie, ktoré sú oprávnenými užívateľmi informácií vzhľadom na zhodnotenie bezpečnostných rizík, ktorým je vystavená EÚ alebo jej členské štáty,

   — zhodnotenia schopnosti oprávnených užívateľov chrániť tajné informácie, ktoré sprístupnila EÚ,

   — návrhov, pokiaľ ide o praktické postupy na spracovávanie odovzdaných tajných informácií EÚ (napríklad poskytnutie cenzurovaných verzií textu) a dokumentov (zachovanie alebo vymazanie záhlaví utajenia EÚ, osobitných označení atď.),

---

▼B

— zaradenia do nižšej kategórie alebo odtajenia orgánom, ktorý je pôvodcom informácií predtým, ako sú informácie sprístupnené krajinám alebo medzinárodným organizáciám, ktoré sú ich príjemcami ([1]).

6. Generálny tajomník/vysoký predstaviteľ doručí Rade na rozhodnutie požiadavku a technické stanovisko bezpečnostného výboru Rady, ktoré získal bezpečnostný úrad Generálneho sekretariátu Rady.

BEZPEČNOSTNÉ NARIADENIA, KTORÉ MAJÚ UPLATŇOVAŤ OPRÁVNENÍ UŽÍVATELIA INFORMÁCIÍ

7. Generálny tajomník/vysoký predstaviteľ má upozorniť štáty alebo medzinárodné organizácie, ktoré sú oprávnenými užívateľmi informácií, na rozhodnutie Rady povoliť sprístupnenie tajných informácií EÚ, spolu s tabuľkou porovnávajúcou utajenia uplatniteľné v rámci EÚ a príslušných štátoch alebo organizáciách. Ak požiadavku uskutočnil členský štát, tento štát má informovať užívateľa informácií o povolenom sprístupnení.

   Rozhodnutie o sprístupnení nadobudne účinnosť, iba ak oprávnení užívatelia informácií poskytnú písomné uistenie, že:

   — nebudú používať informácie na žiadne iné účely, než sú dohodnuté účely,

   — budú chrániť informácie v súlade s nariadeniami ustanovenými Radou.

8. Pokiaľ Rada nerozhodne o konkrétnom postupe na spracovávanie tajných dokumentov EÚ po získaní technického stanoviska bezpečnostného výboru Rady, ustanovia sa nasledovné pravidlá (vymazanie údaja utajenia EÚ, zvláštneho označenia atď.).

   V tom prípade sa pravidlá prispôsobia.

9. *Pracovníci*

   a) Množstvo úradníkov, ktorí majú prístup k tajným informáciám EÚ, má byť striktne obmedzené, na základe princípu potreby poznať, na tie osoby, ktorých povinnosti vyžadujú takýto prístup.

   b) Všetci úradníci a štátni príslušníci, ktorí sú oprávnení mať prístup k tajným informáciám, ktoré sprístupnila EÚ, majú byť držiteľmi národného povolenia mať tajné informácie v prípade národných tajných informácií, pre príslušnú úroveň ekvivalentnú tej, ktorá je v EÚ, ako je definované v komparatívnej tabuľke.

   c) Tieto národné povolenia alebo oprávnenia mať tajné informácie sa majú doručiť generálnemu tajomníkovi/vysokému predstaviteľovi kvôli informácii.

10. *Prenos dokumentov*

   a) Majú sa dohodnúť praktické postupy na prenos dokumentov medzi bezpečnostným úradom Generálneho sekretariátu Rady a bezpečnostnými orgánmi štátov alebo medzinárodných organizácií príjemcu založené na pravidlách uvedených v oddiele VII týchto nariadení. Tieto majú špecifikovať najmä presné adresy, na ktoré sa majú dokumenty doručiť, ako aj kuriérske alebo poštové služby používané na prenos tajných informácií EÚ.

   b) Dokumenty utajené ako CONFIDENTIEL UE a vo vyššej kategórii sa majú prenášať v dvojitej obálke. Vnútorná obálka je označená „UE“ spolu s bezpečnostným utajením. Pre každý tajný dokument je priložený formulár potvrdenia o príjme. Formulár potvrdenia o príjme, ktorý samotný nie je tajný, uvádza iba údaje o dokumente (jeho odkaz, dátum, číslo kópie) a jeho jazyk, ale nie názov.

([1]) Vyžaduje to, aby orgán, ktorý je pôvodcom informácií, uplatňoval postup definovaný v odseku 9 oddiel III v prípade všetkých kópií daných do obehu v EÚ.

▼B

c) Vnútorná obálka sa potom vloží do vonkajšej obálky, ktorá má mať číslo zásielky na účely potvrdenia príjmu. Vonkajšia obálka nemá uvádzať bezpečnostné utajenie.

d) Kuriéri majú vždy dostať potvrdenie o príjme uvádzajúce číslo zásielky.

11. *Registrácia pri príchode*

Orgán národnej bezpečnosti štátu adresáta alebo jeho ekvivalent v štáte, ktorý prijíma v mene vlády tajné informácie doručené Európskou úniou alebo bezpečnostný úrad medzinárodnej organizácie príjemcu, otvorí zvláštny register na zaznamenanie tajných informácií EÚ po ich prijatí. Register obsahuje stĺpce uvádzajúce dátum obdržania, údaje o dokumente (dátum, odkaz a číslo kópie), jeho utajenie, názov, meno alebo názov príjemcu, dátum vrátenia príjmového dokladu a dátum vrátenia dokumentu do EÚ alebo jeho zničenia.

12. *Vrátenie dokumentov*

Ak príjemca vracia tajný dokument Rade alebo členskému štátu, ktorý ho sprístupnil, postupuje tak, ako je uvedené v odseku 10.

13. *Ochrana*

a) Ak sa dokumenty nepoužívajú, uložia sa do bezpečnostného kontajnera, ktorý je schválený na úschovu národného tajného materiálu rovnakého utajenia. Kontajner neuvádza jeho obsah a má byť prístupný iba osobám oprávneným na prácu s tajnými informáciami EÚ. Ak sa použijú zámky na číselnú kombináciu, kombináciu majú poznať iba tí úradníci v štáte alebo organizácii, ktorí majú povolený prístup k tajným informáciám EÚ uchovávaným v kontajneri, a má sa meniť každých šesť mesiacov alebo skôr pri premiestnení úradníka, pri stiahnutí potvrdenia mať tajné informácie jednému z úradníkov, ktorí poznajú kombináciu alebo ak je riziko ohrozenia.

b) Tajné dokumenty EÚ odstraňujú z bezpečnostného kontajnera iba tí úradníci, ktorí prešli kontrolou, pokiaľ ide o prístup k tajným dokumentom EÚ a majú potrebu poznať. Zostávajú zodpovední za bezpečnú úschovu týchto dokumentov, pokiaľ sú v ich držbe, a najmä za zaistenie, aby neoprávnená osoba nemala prístup k dokumentom. Zaisťujú tiež, aby sa dokumenty uložili do bezpečnostného kontajnera, ak sa skončí práca s nimi a mimo pracovného času.

c) Bez povolenie bezpečnostného úradu Generálneho sekretariátu Rady sa nesmú robiť žiadne fotokópie dokumentu utajeného ako CONFIDENTIEL UE alebo vo vyššej kategórii a nesmú sa vyberať ani výňatky.

d) Treba definovať postup na rýchle a úplné zničenie dokumentov v zvláštnom prípade a potvrdiť ho s bezpečnostným úradom Generálneho sekretariátu Rady.

14. *Fyzická bezpečnosť*

a) Ak bezpečnostné kontajnery používané na uchovávanie tajných dokumentov EÚ nie sú v použití, majú sa vždy držať uzamknuté.

b) Ak pracovníci vykonávajúci údržbu alebo upratovanie potrebujú vojsť alebo pracovať v miestnosti, v ktorej sú takéto bezpečnostné kontajnery, majú byť vždy doprevádzaní príslušníkom bezpečnostnej služby štátu alebo organizácie alebo úradníkom, ktorý je konkrétne zodpovedný za dohľad nad bezpečnosťou miestnosti.

c) Mimo zvyčajného pracovného času (v noci, cez víkendy a štátne sviatky) bezpečnostné kontajnery obsahujúce tajné informácie EÚ má chrániť stráž alebo automatický poplašný systém.

15. *Porušenia bezpečnosti*

Ak sa udeje porušenie bezpečnosti týkajúce sa tajného dokumentu EÚ alebo je takéto podozrenie, treba okamžite podniknúť nasledovné kroky:

a) okamžite doručiť správu bezpečnostnému úradu Generálneho sekretariátu Rady alebo orgánu národnej bezpečnosti členského štátu, že boli podnik-

▼B

nuté kroky uvedené v zasielaných dokumentoch (s kópiou bezpečnostnému úradu Generálneho sekretariátu Rady);

b) vykonať prieskum, na konci ktorého sa predloží úplná správa bezpečnostnému orgánu (pozri a) vyššie). Potom by sa mali prijať nevyhnutné opatrenia na nápravu situácie.

16. *Kontroly*

Bezpečnostný úrad Generálneho sekretariátu Rady má povolené na základe dohody s príslušnými štátmi alebo medzinárodnými organizáciami vykonať zhodnotenie efektívnosti opatrení na ochranu sprístupnených tajných informácií EÚ.

17. *Podávanie správy*

Pokiaľ príslušný štát alebo medzinárodná organizácia má tajné informácie EÚ, mali by predkladať ročnú správu do dátumu, ktorý je špecifikovaný v čase poskytnutia povolenia na sprístupnenie informácií, potvrdzujúcu, že sa zabezpečil súlad s týmito bezpečnostnými nariadeniami.

▼B

Dodatok 6.

Usmernenia pre sprístupňovanie tajných informácií EÚ tretím štátom alebo medzinárodným organizáciám

Spolupráca na úrovni 3

POSTUPY

1. Niekedy Rada môže chcieť uskutočniť spoluprácu za určitých zvláštnych okolností so štátmi alebo organizáciami, ktoré nemôžu poskytnúť uistenia požadované týmito bezpečnostnými nariadeniami, avšak táto spolupráca môže vyžadovať sprístupnenie tajných informácií EÚ. Takéto sprístupnenie sa nevzťahuje na národné informácie osobitne vyhradené členským štátom.

2. Za takýchto zvláštnych okolností, požiadavky na spoluprácu s EÚ, či už z tretích štátov alebo medzinárodných organizácií, alebo navrhované členskými štátmi alebo, kde je to uplatniteľné, decentralizovanými orgánmi EÚ, má najprv zvážiť Rada, pokiaľ ide o ich obsah, ktorá, ak je to potrebné, požiada o stanoviská členský štát alebo decentralizovaný orgán, ktorý je pôvodcom informácií. Rada zváži, či je múdre sprístupniť tajné informácie, prístup užívateľov informácií s potrebou poznať a rozhodne o povahe tajných informácie, ktoré sa môžu odovzdávať.

3. Ak tak neurobí Rada, je povinnosťou generálneho tajomníka/vysokého predstaviteľa zvolať bezpečnostný výbor Rady alebo požiadať orgány národnej bezpečnosti členských štátov, ak je to vhodné použitím tichého postupu, s cieľom získania technického stanoviska bezpečnostného výboru.

4. Technické stanovisko bezpečnostného výboru Rady sa má týkať nasledovného:

   a) hodnotenia rizík bezpečnosti, ktorým je vystavená EÚ alebo jej členské štáty;

   b) utajenia informácií, ktoré sa môžu sprístupniť, ak je to vhodné, vzhľadom na ich povahu;

   c) zaradenia do nižšej kategórie alebo odtajenia informácií orgánom, ktorý je ich pôvodcom pred ich sprístupnením príslušným krajinám alebo medzinárodným organizáciám ([1]);

   d) postupov na prácu s dokumentmi, ktoré sa majú sprístupniť (pozri odsek 5 nižšie);

   e) možných metód prenosu (použitie verejných poštových služieb, verejných alebo bezpečných komunikácií, diplomatickej obálky, preverených kuriérov atď.).

5. Dokumenty, ktoré sú sprístupnené štátom alebo organizáciám, ktoré sú obsiahnuté v tomto dodatku, sa majú v podstate pripraviť s odvolávkou na zdroj alebo utajenie EÚ. Bezpečnostný výbor Rady môže odporúčať:

   — použitie osobitného označenia alebo kódovaného mena,

   — použitie zvláštneho systému utajenia spájajúceho citlivosť informácií na kontrolné opatrenia požadované metódami prenosu informácií príjemcu (pozri príklady v odseku 14).

6. Bezpečnostný úrad Generálneho sekretariátu Rady predloží technické stanovisko bezpečnostného výboru Rade, ak je potrebné s pripojením navrhovaných prenesení právomocí požadovaných na výkon úlohy, najmä za naliehavých okolností.

7. Akonáhle Rada schválila sprístupnenie tajných informácií EÚ a praktické vykonávacie postupy, bezpečnostný výbor Generálneho sekretariátu Rady nadviaže potrebný kontakt s príslušným bezpečnostným orgánom štátu

([1]) To znamená, že orgán, od ktorého pochádzajú informácie, uplatní postup definovaný v odseku 9 oddiel III na všetky kópie dané do obehu v rámci EÚ.

▼B

alebo organizáciou s cieľom uľahčenia uplatňovania plánovaných bezpečnostných opatrení.

8. Bezpečnostný úrad Generálneho sekretariátu Rady rozšíri medzi všetkými členskými štátmi a tam, kde je to vhodné, medzi príslušnými decentralizovanými orgánmi EÚ tabuľku slúžiacu ako odkaz, ktorá sumarizuje povahu a utajenie informácií a uvádza zoznam organizácií a krajín, ktorým môžu byť sprístupnené, ak tak rozhodla Rada.

9. Orgán národnej bezpečnosti členského štátu, ktorý uskutočňuje sprístupnenie, alebo bezpečnostný úrad Generálneho sekretariátu Rady prijme všetky potrebné opatrenia na uľahčenie zhodnotenia akéhokoľvek ďalšieho poškodenia a revidovania postupov.

10. Vždy, ak sa menia podmienky spolupráce, má byť o tom informovaná Rada.

BEZPEČNOSTNÉ NARIADENIA, KTORÉ MAJÚ UPLATŇOVAŤ OPRÁVNENÍ UŽÍVATELIA INFORMÁCIÍ

11. Generálny tajomník/vysoký predstaviteľ má upozorniť štáty alebo medzinárodné organizácie, ktoré sú oprávnenými užívateľmi informácií, na rozhodnutie Rady povoliť sprístupnenie tajných informácií EÚ, spolu s podrobnými pravidlami ochrany navrhovanými bezpečnostným výborom Rady a schválenými Radou. Ak požiadavku uskutočnil členský štát, tento štát má informovať užívateľa o povolenom sprístupnení.

    Rozhodnutie nadobudne účinnosť, iba ak oprávnení užívatelia informácií poskytnú písomné uistenie, že:

    — nebudú používať informácie na žiadne iné účely než sú dohodnuté účely,

    — poskytnú informáciám ochranu požadovanú Radou.

12. *Prenos dokumentov*

    a) Majú sa dohodnúť praktické postupy na prenos dokumentov medzi bezpečnostným úradom Generálneho sekretariátu Rady a bezpečnostnými orgánmi štátov alebo medzinárodných organizácií príjemcu. Tieto majú špecifikovať najmä presné adresy, na ktoré sa majú dokumenty doručiť.

    b) Dokumenty utajené ako CONFIDENTIEL UE a vo vyššej kategórii sa majú prenášať v dvojitej obálke. Vnútorná obálka má mať zvláštnu pečiatku alebo kódované meno, ako bolo rozhodnuté, a údaj o osobitnom utajení schválenom pre dokument. Pre každý tajný dokument bude priložený formulár potvrdenia o príjme. Formulár potvrdenia o príjme, ktorý samotný nie je tajný, uvádza iba údaje o dokumente (jeho odkaz, dátum, číslo kópie) a jeho jazyk, ale nie názov.

    c) Vnútorná obálka sa potom vloží do vonkajšej obálky, ktorá má mať číslo zásielky pre účely prijatia. Vonkajšia obálka nemá uvádzať bezpečnostné utajenie.

    d) Kuriéri majú vždy dostať potvrdenie o príjme uvádzajúce číslo zásielky.

13. *Registrácia pri príchode*

    Orgán národnej bezpečnosti štátu adresáta alebo jeho ekvivalent v štáte, ktorý prijíma v mene vlády tajné informácie doručené Európskou úniou alebo bezpečnostný úrad medzinárodnej organizácie príjemcu, otvorí zvláštny register na zaznamenanie tajných informácií EÚ po ich prijatí. Register obsahuje stĺpce uvádzajúce dátum obdržania, údaje o dokumente (dátum, odkaz a číslo kópie), jeho utajenie, názov, meno alebo titul príjemcu, dátum vrátenia príjmového dokladu do EÚ a dátum zničenia dokumentu.

15. *Použitie a ochrana vymenených tajných informácií*

    a) S informáciami na úrovni SECRET UE majú pracovať osobitne určení úradníci oprávnení mať prístup k informáciám s týmto utajením. Majú sa uchovávať v bezpečnostných skrinkách dobrej kvality, ktoré môžu otvoriť iba osoby oprávnené mať prístup k informáciám, ktoré obsahujú. Priestory, v ktorých sú umiestnené tieto skrinky, majú byť stále strážené

▼B

a má byť vytvorený systém overovania s cieľom zaistenia dovolenia vstupu iba oprávneným osobám. Informácie na úrovni SECRET UE sa prepravujú pomocou diplomatických obálok, bezpečných poštových služieb a bezpečných telekomunikácií. Dokument na úrovni SECRET UE sa smie kopírovať iba s písomným súhlasom orgánu, od ktorého pochádza. Všetky kópie sa majú zaregistrovať a monitorovať. Pre všetky operácie týkajúce sa dokumentov SECRET UE sa majú vystavovať potvrdenia o príjme.

b) S informáciami na úrovni CONFIDENTIEL UE majú pracovať náležite určení úradníci oprávnení, aby boli informovaní o danom predmete. Dokumenty sú uzamknuté v bezpečnostných skrinkách v kontrolovaných priestoroch.

Informácie na úrovni CONFIDENTIEL UE sa prepravujú v diplomatickej obálke, vojenskými poštovými službami a bezpečnými komunikáciami. Orgán príjemcu si môže urobiť kópie, pričom ich počet a distribúcia sa zaznamenáva do osobitných registrov.

c) S informáciami na úrovni RESTREIT UE sa pracuje v priestoroch, ktoré nie sú prístupné neoprávneným pracovníkom, a uchovávajú sa v uzamknutých kontajneroch. Dokumenty sa môžu prepravovať verejnými poštovými službami ako doporučenou poštou v dvojitej obálke a vo výnimočných situáciách počas operácií nechránenými verejnými komunikačnými systémami. Príjemca si môže urobiť kópie.

d) Informácie, ktoré nie sú tajné, nepožadujú osobitné ochranné opatrenia a môžu sa prepravovať poštou a verejnými komunikačnými systémami. Adresáti si môžu urobiť kópie.

15. *Zničenie*

Dokumenty, ktoré už viac nie sú potrebné, sa musia zničiť. V prípade dokumentov na úrovni RESTREINT UE a CONDIDENTIEL UE sa zapíše príslušná poznámka do osobitných registrov. V prípade dokumentov na úrovni SECRET UE sa vystavia osvedčenia o zničení, ktoré sú podpísané dvoma osobami dosvedčujúcimi ich zničenie.

16. *Porušenia bezpečnosti*

Ak sú ohrozené informácie na úrovni CONFIDENTIEL UE alebo SECRET UE alebo existuje podozrenie týkajúce sa ohrozenia, orgán národnej bezpečnosti štátu alebo vedúci bezpečnosti v organizácii prešetrí okolnosti tohto ohrozenia. Ak vyšetrenie prinesie potvrdzujúce výsledky, informuje sa orgán, od ktorého pochádzajú informácie. Treba podniknúť potrebné kroky na nápravu neprimeraných postupov alebo metód úschovy, ak tieto viedli k ohrozeniu. Generálny tajomník Rady/vysoký predstaviteľ alebo orgán národnej bezpečnosti členského štátu, ktorý sprístupnil ohrozené informácie, môže požiadať príjemcu o podrobné údaje o tomto prešetrovaní.