II

(Nelegislatívne akty)

ROZHODNUTIA

ROZHODNUTIE RADY

z 31. marca 2011

o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ

(2011/292/EÚ)

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 240 ods. 3,

so zreteľom na rozhodnutie Rady 2009/937/EÚ z 1. decembra 2009, ktorým sa mení a dopĺňa rokovací poriadok Rady [1], a najmä na jeho článok 24,

keďže:

(1) S cieľom rozvíjať aktivity Rady vo všetkých oblastiach, ktoré si vyžadujú manipuláciu s utajovanými skutočnosťami, je vhodné ustanoviť komplexný bezpečnostný systém na ochranu utajovaných skutočností vzťahujúci sa na Radu, jej generálny sekretariát a členské štáty.

(2) Toto rozhodnutie by sa malo uplatňovať, keď Rada, jej prípravné orgány a Generálny sekretariát Rady (ďalej len „GSR") manipulujú s utajovanými skutočnosťami EÚ.

(3) Členské štáty by v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi a v rozsahu potrebnom pre fungovanie Rady mali dodržiavať toto rozhodnutie, keď ich príslušné orgány, personál alebo dodávatelia manipulujú s utajovanými skutočnosťami EÚ, aby sa každému poskytlo ubezpečenie o tom, že pre utajované skutočnosti EÚ je zabezpečená rovnaká úroveň ochrany.

(4) Rada a Komisia sa zaviazali, že budú uplatňovať rovnaké bezpečnostné normy na ochranu utajovaných skutočností EÚ.

(5) Rada vyzdvihuje význam vhodného zapojenia Európskeho parlamentu a ostatných inštitúcií, agentúr, orgánov alebo úradov EÚ do uplatňovania zásad, noriem a predpisov týkajúcich sa ochrany utajovaných skutočností, ktoré sú potrebné na ochranu záujmov Únie a jej členských štátov.

(6) Agentúry a orgány EÚ zriadené na základe hlavy V kapitoly 2 Zmluvy o EÚ, Europol a Eurojust uplatňujú v rámci svojej vnútornej organizácie podľa ustanovení svojich zakladajúcich aktov základné zásady a minimálne štandardy ustanovené v tomto rozhodnutí na ochranu utajovaných skutočností EÚ.

(7) Bezpečnostné predpisy, ktoré Rada prijala na ochranu utajovaných skutočností EÚ, sa uplatňujú aj na operácie krízového riadenia vykonávané na základe hlavy V kapitoly 2 Zmluvy o EÚ a na ich personál.

(8) Bezpečnostné predpisy, ktoré Rada prijala na ochranu utajovaných skutočností EÚ, sa uplatňujú na osobitných zástupcov EÚ a členov ich tímu.

(9) Toto rozhodnutie sa prijíma bez toho, aby boli dotknuté články 15 a 16 Zmluvy o fungovaní Európskej únie (ZFEÚ) a nástroje, ktorými sa vykonávajú.

(10) Toto rozhodnutie sa prijíma bez toho, aby boli dotknuté postupy uplatňované v členských štátoch na informovanie národných parlamentov o činnostiach Únie,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Cieľ, rozsah pôsobnosti a vymedzenie pojmov

1. Týmto rozhodnutím sa ustanovujú základné zásady a minimálne štandardy bezpečnosti na ochranu utajovaných skutočností EÚ.

[1] Ú. v. EÚ L 325, 11.12.2009, s. 35.

2. Tieto základné zásady a minimálne štandardy sa vzťahujú na Radu a GSR a členské štáty ich dodržiavajú v súlade so svojimi príslušnými vnútroštátnymi zákonmi a inými právnymi predpismi, aby sa každému poskytlo ubezpečenie o tom, že pre utajované skutočnosti EÚ je zabezpečená rovnaká úroveň ochrany.

3. Na účely tohto rozhodnutia sa uplatňujú vymedzenia pojmov uvedené v dodatku A.

Článok 2

Vymedzenie utajovanej skutočnosti EÚ, stupne utajenia a označenia

1. „Utajovaná skutočnosť Európskej únie" (ďalej len „utajovaná skutočnosť EÚ") je každá informácia alebo vec označená označením stupňa utajenia EÚ, neoprávnená manipulácia s ktorou by mohla v rôznej miere poškodiť záujmy Európskej únie alebo jedného alebo viacerých členských štátov.

2. Utajované skutočnosti EÚ sa utajujú na jednom z týchto stupňov:

a) TRÉS SECRET UE/EU TOP SECRET: informácia alebo vec, neoprávnená manipulácia s ktorou by mohla mimoriadne vážne poškodiť základné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov;

b) SECRET UE/EU SECRET: informácia alebo vec, neoprávnená manipulácia s ktorou by mohla vážne poškodiť základné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informácia alebo vec, neoprávnená manipulácia s ktorou by mohla poškodiť základné záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov;

d) RESTREINT UE/EU RESTRICTED: informácia alebo vec, neoprávnená manipulácia s ktorou by mohla byť nevýhodná pre záujmy Európskej únie alebo jedného alebo viacerých jej členských štátov.

3. Utajované skutočnosti EÚ sa označujú stupňami utajenia uvedenými v odseku 2. Okrem toho môžu byť označené aj označeniami, ktoré určujú príslušnú oblasť činnosti, identifikujú pôvodcu, obmedzujú distribúciu, obmedzujú použitie alebo stanovujú rozsah možnej prístupnosti.

Článok 3

Riadenie utajovania

1. Príslušné orgány zabezpečujú, že utajovaná skutočnosť EÚ je náležite utajovaná, jasne označená ako utajovaná skutočnosť a že podlieha príslušnému stupňu utajenia, len pokiaľ je to nevyhnutné.

2. Stupeň utajenia utajovanej skutočnosti EÚ sa neznižuje, nezrušuje, ani sa nijaké označenia uvedené v článku 2 ods. 3 neupravujú ani neodstraňujú bez predchádzajúceho písomného súhlasu pôvodcu.

3. Rada schváli bezpečnostnú politiku pre oblasť vytvárania utajovaných skutočností EÚ, ktorá obsahuje praktické usmernenia pre určovanie stupňa utajenia.

Článok 4

Ochrana utajovaných skutočností

1. Utajované skutočnosti EÚ sa chránia v súlade s týmto rozhodnutím.

2. Držiteľ každej položky utajovanej skutočnosti EÚ je zodpovedný za jej ochranu v súlade s týmto rozhodnutím.

3. Keď členské štáty poskytnú štruktúram alebo sieťam Európskej únie utajované skutočnosti, ktoré sú označené národným označením stupňa utajenia, Rada a GSR ich chráni v súlade s požiadavkami uplatňovanými na utajované skutočnosti EÚ s rovnocenným stupňom utajenia stanoveným podľa ekvivalenčnej tabuľky stupňov utajenia, ktorá je uvedená v dodatku B.

4. Veľké množstvo utajovaných skutočností EÚ alebo ich spojenie si môže vyžadovať ochranu na úrovni, ktorá zodpovedá vyššiemu stupňu utajenia.

Článok 5

Riadenie bezpečnostných rizík

1. Riadenie rizík týkajúcich sa utajovaných skutočností EÚ sa uskutočňuje ako proces. Tento proces sa zameriava na určenie známych bezpečnostných rizík, stanovenie bezpečnostných opatrení na zníženie týchto rizík na prijateľnú úroveň v súlade so základnými zásadami a minimálnymi štandardmi stanovenými v tomto rozhodnutí a na uplatňovanie týchto opatrení v súlade s koncepciou hĺbkovej ochrany, ako je vymedzená v dodatku A. Účinnosť týchto opatrení sa neustále vyhodnocuje.

2. Bezpečnostné opatrenia na ochranu utajovaných skutočností EÚ počas celého ich životného cyklu zodpovedajú najmä ich stupňu utajenia, podobe a množstvu informácií alebo vecí, miestu, kde sa nachádzajú objekty, v ktorých sa utajované skutočnosti EÚ uchovávajú, a ich konštrukcii, stanovenej lokálnej úrovni ohrozenia zákernými a/alebo trestnými činnosťami vrátane špionáže, sabotáže a terorizmu.

3. V núdzových plánoch sa prihliada na potrebu chrániť utajované skutočnosti EÚ počas výnimočných situácií s cieľom predísť neoprávnenému prístupu k nim, neoprávnenej manipulácii s nimi alebo strate ich integrity alebo dostupnosti.

4. Preventívne a nápravné opatrenia zamerané na minimalizáciu dôsledkov významného zlyhania alebo významných incidentov pri manipulácii s utajovanými skutočnosťami EÚ a ich uchovávaní sú uvedené v plánoch na zabezpečenie kontinuity činností.

Článok 6

Vykonávanie tohto rozhodnutia

1. V prípade potreby Rada na základe odporúčania Bezpečnostného výboru schvaľuje bezpečnostné politiky, ktorými sa ustanovujú opatrenia na vykonanie tohto rozhodnutia.

2. Bezpečnostný výbor môže na svojej úrovni odsúhlasiť bezpečnostné usmernenia, ktorými sa dopĺňa alebo podporuje toto rozhodnutie a všetky bezpečnostné politiky schválené Radou.

Článok 7

Personálna bezpečnosť

1. Personálna bezpečnosť je uplatňovanie opatrení na zabezpečenie toho, že prístup k utajovaným skutočnostiam EÚ sa udeľuje len osobám, ktoré:

— majú potrebu poznať (zásada „need-to-know“),

— boli v prípade potreby bezpečnostne preverené pre príslušný stupeň a

— boli poučené o svojich povinnostiach.

2. Stanovia sa postupy na vykonanie previerky personálnej bezpečnosti, ktorou sa určuje, či osoba pri zohľadnení jej lojality, dôveryhodnosti a spoľahlivosti môže byť oprávnená na prístup k utajovaným skutočnostiam EÚ.

3. Všetky osoby pracujúce v GSR, ktoré môžu potrebovať na plnenie svojich úloh prístup k utajovaným skutočnostiam EÚ so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, musia byť pred udelením prístupu k takýmto utajovaným skutočnostiam EÚ bezpečnostne preverené pre príslušný stupeň. Postup pre vykonanie previerky personálnej bezpečnosti úradníkov a iných zamestnancov GSR je upravený v prílohe I.

4. Členovia personálu členských štátov uvedení v článku 14 ods. 3, ktorí môžu potrebovať na plnenie svojich úloh prístup k utajovaným skutočnostiam EÚ so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, musia byť pred udelením prístupu k takýmto utajovaným skutočnostiam EÚ bezpečnostne preverení pre príslušný stupeň alebo musia mať iné náležité oprávnenie, ktoré vyplýva z povahy ich funkcie, v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi.

5. Všetky osoby sú pred udelením prístupu k utajovaným skutočnostiam EÚ a pravidelne po ňom poučené o povinnostiach chrániť utajované skutočnosti EÚ podľa tohto rozhodnutia a tieto povinnosti akceptujú.

6. Vykonávacie ustanovenia k tomuto článku sa uvádzajú v prílohe I.

Článok 8

Fyzická bezpečnosť

1. Fyzická bezpečnosť je uplatňovanie fyzických a technických ochranných opatrení na zamedzenie neoprávneného prístupu k utajovaným skutočnostiam EÚ.

2. Opatrenia fyzickej bezpečnosti sa vytvárajú na zabránenie utajenému alebo násilnému vstupu narušiteľa, odradenie od neoprávnených činností, ich zamedzenie a odhalenie a na umožnenie rozdelenia pracovníkov na účely prístupu k utajovaným skutočnostiam EÚ podľa zásady „need-to-know“. Tieto opatrenia sa určujú na základe procesu riadenia rizík.

3. Opatrenia fyzickej bezpečnosti sa zavedú vo všetkých objektoch, budovách, kanceláriách, miestnostiach a iných priestoroch, v ktorých sa manipuluje s utajovanými skutočnosťami EÚ alebo sa takéto utajované skutočnosti uchovávajú, vrátane priestorov, v ktorých sú umiestnené komunikačné a informačné systémy vymedzené v článku 10 ods. 2.

4. Priestory, v ktorých sa uchovávajú utajované skutočnosti EÚ so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším sa zriaďujú ako zabezpečené priestory podľa prílohy II a schvaľuje ich príslušný bezpečnostný orgán.

5. Na ochranu utajovaných skutočností EÚ so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším sa používajú iba schválené zariadenia a prostriedky.

6. Vykonávacie ustanovenia k tomuto článku sa uvádzajú v prílohe II.

Článok 9

Správa utajovaných skutočností

1. Správa utajovaných skutočností znamená uplatňovanie administratívnych opatrení pri riadení utajovaných skutočností EÚ počas ich životného cyklu s cieľom doplniť opatrenia ustanovené v článkoch 7, 8 a 10, a tým pomôcť pri odradení od úmyselného alebo náhodného vyzradenia alebo straty takýchto utajovaných skutočností, pri zistení tohto vyzradenia alebo straty a pri obnove bezpečnosti. Takéto opatrenia sa týkajú najmä vytvárania, evidencie, rozmnožovania, prekladu, prenášania a ničenia utajovaných skutočností EÚ.

2. Pred poskytnutím utajovaných skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším a po ich prijatí sa utajované skutočnosti evidujú na bezpečnostné účely. Príslušné orgány v GSR a členských štátoch zriaďujú na tento účel systém registrov. Utajované skutočnosti so stupňom utajenia TRÈS SECRET UE/EU TOP SECRET sa evidujú v osobitných registroch.

3. Útvary a objekty, v ktorých sa s utajovanými skutočnosťami EÚ manipuluje a v ktorých sa tieto utajované skutočnosti uchovávajú, podliehajú pravidelným inšpekciám, ktoré vykonáva príslušný bezpečnostný orgán.

4. Utajované skutočnosti EÚ sa prenášajú medzi útvarmi alebo objektmi mimo fyzicky chránených priestorov takto:

a) vo všeobecnosti sa utajované skutočnosti EÚ prenášajú elektronickými prostriedkami, ktoré sú chránené kryptografickými produktmi schválenými v súlade s článkom 10 ods. 6;

b) keď sa prostriedky uvedené v písmene a) nepoužívajú, utajované skutočnosti EÚ sa prenášajú buď:

i) na elektronických médiách (napr. USB kľúčoch, CD, pevných diskoch), ktoré sú chránené kryptografickými produktmi schválenými v súlade s článkom 10 ods. 6, alebo

ii) v ostatných prípadoch podľa pokynov príslušného bezpečnostného orgánu a v súlade s príslušnými ochrannými opatreniami ustanovenými v prílohe III.

5. Vykonávacie ustanovenia k tomuto článku sa uvádzajú v prílohe III.

Článok 10

Ochrana utajovaných skutočností EÚ, s ktorými sa manipuluje v komunikačných a informačných systémoch

1. Informačná bezpečnosť (ďalej len „IA“ – Information Assurance) v oblasti komunikačných a informačných systémov je presvedčenie, že takéto systémy ochránia informácie, s ktorými sa v nich manipuluje, a budú fungovať vtedy a tak, ako majú, pod dohľadom oprávnených používateľov. Efektívna IA zabezpečuje primeranú úroveň dôvernosti, integrity, dostupnosti, nespochybniteľnosti a hodnovernosti. IA sa zakladá na procese riadenia rizík.

2. Komunikačný a informačný systém (ďalej len „CIS“ – Communication and Information System) je každý systém, ktorý umožňuje manipuláciu s informáciami v elektronickej podobe. Komunikačný a informačný systém zahŕňa všetky prostriedky potrebné na jeho prevádzku vrátane infraštruktúry, organizácie, ľudských a informačných zdrojov. Toto rozhodnutie sa uplatňuje na komunikačné a informačné systémy, ktorými sa manipuluje s utajovanými skutočnosťami EÚ.

3. Prostredníctvom CIS sa s utajovanými skutočnosťami EÚ manipuluje v súlade s koncepciou IA.

4. Všetky CIS podliehajú certifikácii. Cieľom certifikácie je dosiahnuť uistenie o tom, že sa zaviedli všetky vhodné bezpečnostné opatrenia a že sa dosiahla dostatočná úroveň ochrany utajovaných skutočností EÚ a CIS v súlade s týmto rozhodnutím. V potvrdení o certifikácii sa stanoví najvyšší stupeň utajenia utajovaných skutočností, s ktorými sa môže v CIS manipulovať, ako aj príslušné podmienky a požiadavky.

5. CIS, v ktorom sa manipuluje s utajovanými skutočnosťami so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a vyšším, musí byť chránený tak, aby nemohlo dôjsť k neúmyselnému vyzradeniu utajovaných skutočností prostredníctvom elektromagnetického vyžarovania (ďalej len „bezpečnostné opatrenia TEMPEST“).

6. Ak ochranu utajovaných skutočností EÚ zabezpečujú kryptografické produkty, tieto produkty sa schvaľujú takto:

a) Dôvernosť utajovaných skutočností so stupňom utajenia SECRET UE/EU SECRET a vyšším sa chráni kryptografickými produktmi schválenými Radou ako kryptografickým schvaľovacím orgánom (Crypto Approval Authority – ďalej len „CAA“) na základe odporúčania Bezpečnostného výboru.

b) Dôvernosť utajovaných skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo RESTREINT UE/EU RESTRICTED sa chráni kryptografickými produktmi schválenými generálnym tajomníkom Rady(ďalej len „generálny tajomník“) ako CAA na základe odporúčania Bezpečnostného výboru.

Bez ohľadu na písmeno b) sa dôvernosť utajovaných skutočností EÚ so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo RESTREINT UE/EU RESTRICTED môže v rámci vnútroštátnych systémov členských štátov chrániť kryptografickými produktmi schválenými CAA členského štátu.

7. Počas prenosu utajovaných skutočností EÚ elektronickými prostriedkami sa použijú schválené kryptografické produkty. Bez ohľadu na túto požiadavky možno v núdzových situáciách alebo pri špecifických technických konfiguráciách uvedených v prílohe IV použiť špecifické postupy.

8. Príslušné orgány GSR a členských štátov zriadia na účely informačnej bezpečnosti tieto orgány:

a) orgán pre IA (ďalej len „IAA“ – Information Assurance Authority);

b) orgán pre TEMPEST (ďalej len „TA“ – TEMPTEST Authority);

c) kryptografický schvaľovací orgán (ďalej len „CAA“ – Crypto Approval Authority);

d) kryptografický distribučný orgán (ďalej len „CDA“ – Crypto Distribution Authority).

9. Pre každý systém zriadia príslušné orgány GSR a členských štátov:

a) orgán bezpečnostnej certifikácie (ďalej len „SAA“ – Security Accreditation Authority);

b) operačný orgán pre IA.

10. Vykonávacie ustanovenia k tomuto článku sa uvádzajú v prílohe IV.

Článok 11

Priemyselná bezpečnosť

1. Priemyselná bezpečnosť je uplatňovanie opatrení na zabezpečenie ochrany utajovaných skutočností EÚ zo strany dodávateľov a subdodávateľov počas rokovaní pred uzavretím zmluvy a počas celého životného cyklu utajovanej zmluvy. Takéto zmluvy nezahŕňajú prístup k utajovaným skutočnostiam so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET.

2. GSR môže priemyselným alebo iným subjektom so sídlom v členskom štáte alebo v treťom štáte, ktorý uzavrel dohodu alebo administratívne dojednanie v súlade s článkom 12 ods. 2 písm. a) alebo b), zmluvou zveriť vykonanie úloh, ktoré zahŕňajú alebo si vyžadujú prístup k utajovaným skutočnostiam EÚ alebo manipuláciu s nimi, alebo ich uchovávanie uvedenými subjektmi.

3. GSR ako obstarávateľ zabezpečuje, že pri uzatváraní utajovaných zmlúv priemyselným alebo iným subjektom sú splnené minimálne normy priemyselnej bezpečnosti stanovené v tomto rozhodnutí a uvedené v zmluve.

4. Národný bezpečnostný orgán (ďalej len „NSA“ – National Security Authority), určený bezpečnostný orgán (ďalej len „DSA“ – Designated Security Authority) alebo akýkoľvek iný príslušný orgán každého členského štátu zabezpečuje v rámci možností, ktoré vyplývajú z vnútroštátnych zákonov a iných právnych predpisov, že dodávatelia a subdodávatelia so sídlom na jeho území prijmú všetky vhodné opatrenia na ochranu utajovaných skutočností EÚ pri rokovaní o zmluve alebo pri plnení utajovanej zmluvy.

5. NSA, DSA alebo akýkoľvek iný príslušný orgán každého členského štátu v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi zabezpečí, aby dodávatelia a subdodávatelia so sídlom v danom členskom štáte, ktorí sú zapojení do utajovaných zmlúv alebo subdodávateľských zmlúv, v dôsledku čoho potrebujú pri plnení týchto zmlúv alebo počas fázy pred uzavretím zmluvy prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET v rámci svojich zariadení, boli držiteľmi previerky bezpečnosti zariadenia (ďalej len „FSC“ – Facility Security Clearance) pre požadovaný stupeň utajenia.

6. Príslušný NSA, DSA alebo akýkoľvek iný príslušný bezpečnostný orgán udeľuje v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi a minimálnymi bezpečnostnými normami ustanovenými v prílohe I personálu dodávateľa alebo subdodávateľa, ktorý v rámci plnenia utajovanej zmluvy potrebuje prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET, previerku personálnej bezpečnosti (ďalej len „PSC“ – Personnel Security Clearance).

7. Vykonávacie ustanovenia k tomuto článku sa uvádzajú v prílohe V.

Článok 12

Výmena utajovaných skutočností s tretími štátmi a medzinárodnými organizáciami

1. Ak Rada rozhodne o potrebe výmeny utajovaných skutočností EÚ s tretím štátom alebo medzinárodnou organizáciou, vytvorí sa na tento účel príslušný rámec.

2. Na účely vytvorenia takéhoto rámca a vymedzenia recipročných pravidiel o ochrane vymieňaných utajovaných skutočností:

a) Rada uzatvorí dohody o bezpečnostných postupoch pri výmene a na ochranu utajovaných skutočností (ďalej len „dohody o bezpečnosti utajovaných skutočností“) alebo

b) generálny tajomník môže v súlade s bodom 17 prílohy VI uzatvoriť správne dojednania, pokiaľ stupeň utajenia utajovaných skutočností EÚ, ktoré sa majú poskytnúť, spravidla nebýva vyšší ako RESTREINT UE/EU RESTRICTED.

3. Dohody o bezpečnosti utajovaných skutočností alebo správne dojednania uvedené v odseku 2 obsahujú ustanovenia, ktorými sa zabezpečuje, že tretie štáty alebo medzinárodné organizácie, ktoré prijmú utajované skutočnosti EÚ, chránia takéto utajované skutočnosti na úrovni, ktorá zodpovedá ich stupňu utajenia, a v súlade s minimálnymi normami, ktoré nie sú menej prísne, ako normy ustanovené v tomto rozhodnutí.

4. Rozhodnutie o poskytnutí utajovaných skutočností, ktorých pôvodcom je Rada, tretiemu štátu alebo medzinárodnej organizácii prijíma pre každý jednotlivý prípad Rada na základe charakteru a obsahu týchto utajovaných skutočností, príjemcovej potreby poznať a miery výhod, ktoré z toho pre EÚ vyplývajú. Ak Rada nie je pôvodcom utajovaných skutočností, ktoré sa majú poskytnúť, GSR najprv získa od ich pôvodcu písomný súhlas na poskytnutie. Ak nie je možné pôvodcu zistiť, prevezme zodpovednosť pôvodcu Rada.

5. Dohodnú sa hodnotiace návštevy, ktorých cieľom je stanoviť účinnosť bezpečnostných opatrení uplatňovaných v treťom štáte alebo medzinárodnej organizácii na ochranu utajovaných skutočností EÚ, ktoré sa poskytli alebo vymenili.

6. Vykonávacie ustanovenia k tomuto článku sa uvádzajú v prílohe VI.

Článok 13

Narušenie bezpečnosti a vyzradenie utajovaných skutočností EÚ

1. Narušenie bezpečnosti nastáva v dôsledku konania alebo opomenutia zo strany osoby, ktoré je v rozpore s bezpečnostnými predpismi ustanovenými v tomto rozhodnutí.

2. Vyzradenie utajovaných skutočností EÚ nastáva, keď k nim v dôsledku narušenia bezpečnosti úplne alebo čiastočne získala prístup neoprávnená osoba.

3. Každé narušenie alebo podozrenie z narušenia bezpečnosti utajovaných skutočností EÚ sa ihneď oznamuje príslušnému bezpečnostnému orgánu.

4. Keď sa zistí vyzradenie alebo strata utajovaných skutočností EÚ alebo keď existuje dostatočný dôvod domnievať sa, že k vyzradeniu alebo strate došlo, príslušný bezpečnostný orgán prijme všetky vhodné opatrenia podľa príslušných zákonov a iných právnych predpisov, aby:

a) informoval pôvodcu;

b) zabezpečil, že na účely zistenia skutočností prípad vyšetria členovia personálu, ktorých sa narušenie bezpečnosti netýka bezprostredne;

c) vyhodnotil možné poškodenie záujmov EÚ alebo členských štátov;

d) prijal vhodné opatrenia na predchádzanie opätovnému výskytu a

e) informoval príslušné orgány o prijatých opatreniach.

5. Každá osoba, ktorá je zodpovedná za porušenie bezpečnostných predpisov ustanovených v tomto rozhodnutí, môže byť disciplinárne stíhaná podľa príslušných pravidiel a predpisov. Každá osoba, ktorá je zodpovedná za vyzradenie alebo stratu utajovaných skutočností EÚ, podlieha disciplinárnemu a/alebo súdnemu konaniu podľa príslušných zákonov, pravidiel a iných právnych predpisov.

Článok 14

Zodpovednosť za vykonávanie

1. Rada prijíma všetky potrebné opatrenia na zabezpečenie celkovej jednotnosti uplatňovania tohto rozhodnutia.

2. Generálny tajomník prijme všetky opatrenia potrebné na to, aby sa toto rozhodnutie uplatňovalo pri manipulácii s utajovanými skutočnosťami EÚ alebo akýmikoľvek inými utajovanými skutočnosťami alebo pri ich uchovávaní v objektoch používaných Radou a v rámci GSR vrátane jeho styčných úradov v tretích štátoch a pri manipulácii s týmito utajovanými skutočnosťami úradníkmi a inými zamestnancami GSR, vyslanými pracovníkmi na GSR, ako aj dodávateľmi GSR.

3. Členské štáty prijímajú všetky vhodné opatrenia v súlade so svojimi príslušnými vnútroštátnymi zákonmi a inými právnymi predpismi, aby pri manipulácii s utajovanými skutočnosťami EÚ a ich uchovávaní dodržiavali toto rozhodnutie tieto osoby:

a) personál stálych zastupiteľstiev členských štátov pri Európskej únii, ako aj národní delegáti, ktorí sa zúčastňujú na zasadnutiach Rady alebo jej prípravných orgánov alebo na iných činnostiach Rady;

b) ostatný personál verejnej správy členských štátov vrátane personálu, ktorý bol vyslaný, aby vo verejnej správe pracoval, bez ohľadu na to, či pracuje na území členského štátu alebo v zahraničí;

c) iné osoby v členských štátoch, ktoré majú náležité povolenie na prístup k utajovaným skutočnostiam EÚ na základe povahy svojich úloh, a

d) dodávatelia členských štátov na území členských štátov aj v zahraničí.

Článok 15

Organizácia bezpečnosti v Rade

1. V rámci svojej úlohy pri zabezpečovaní celkovej jednotnosti uplatňovania tohto rozhodnutia Rada schvaľuje:

a) dohody uvedené v článku 12 ods. 2 písm. a);

b) rozhodnutia, ktorými sa povoľuje poskytnúť utajované skutočnosti EÚ tretím štátom a medzinárodným organizáciám;

c) ročný inšpekčný program, ktorý navrhuje generálny tajomník a odporúča Bezpečnostný výbor, na vykonanie inšpekcií v útvaroch a objektoch členských štátov a agentúrach a orgánoch EÚ zriadených na základe hlavy V kapitoly 2 Zmluvy o EÚ, ako aj v Europole a Eurojuste a hodnotiacich návštev v tretích štátoch a medzinárodných organizáciách s cieľom posúdiť účinnosť opatrení prijatých na ochranu utajovaných skutočností EÚ a

d) bezpečnostné politiky v zmysle článku 6 ods. 1.

2. Bezpečnostným orgánom GSR je generálny tajomník. Generálny tajomník v tejto funkcii:

a) vykonáva a preveruje bezpečnostnú politiku Rady;

b) koordinuje všetky bezpečnostné veci týkajúce sa ochrany utajovaných skutočností súvisiacich s činnosťou Rady s NSA členských štátov;

c) úradníkom a iným zamestnancom GSR udeľuje PSC EÚ v zmysle článku 7 ods. 3 skôr, ako im možno udeliť prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším;

d) podľa potreby nariaďuje vyšetrovanie každého skutočného vyzradenia alebo straty utajovaných skutočností, ktoré Rada uchováva alebo ktoré sa v Rade vytvorili, alebo podozrenia z takéhoto vyzradenia alebo straty a predkladá príslušným bezpečnostným orgánom žiadosť o spoluprácu pri takomto vyšetrovaní;

e) vykonáva pravidelné inšpekcie bezpečnostných mechanizmov ochrany utajovaných skutočností v objektoch GSR;

f) vykonáva pravidelné inšpekcie bezpečnostných mechanizmov ochrany utajovaných skutočností EÚ v agentúrach a orgánoch EÚ zriadených na základe hlavy V kapitoly 2 Zmluvy o EÚ, ako aj v Europole a Eurojuste, pri operáciách krízového riadenia vykonávaných na základe hlavy V kapitoly 2 Zmluvy o EÚ a u osobitných zástupcov EÚ (ďalej len „OZEÚ") a členov ich tímu;

g) vykonáva v spolupráci s dotknutým NSA a po dohode s ním pravidelné inšpekcie bezpečnostných mechanizmov ochrany utajovaných skutočností EÚ v útvaroch a objektoch členských štátov;

h) koordinuje bezpečnostné opatrenia s príslušnými orgánmi členských štátov, ktoré sú zodpovedné za ochranu utajovaných skutočností, a prípadne tretích štátov alebo medzinárodných organizácií, okrem iného v súvislosti s povahou ohrození bezpečnosti utajovaných skutočností EÚ a prostriedkami ochrany proti nim;

i) uzatvára správne dojednania v zmysle 12 ods. 2 písm. b) a

j) vykonáva prvú a pravidelné hodnotiace návštevy v tretích štátoch a medzinárodných organizáciách s cieľom zistiť účinnosť opatrení prijatých na ochranu utajovaných skutočností EÚ, ktoré sa im poskytujú alebo s nimi vymieňajú.

Pri plnení týchto úloh je generálny tajomník k dispozícii Bezpečnostný úrad GSR.

3. Na účely vykonávania článku 14 ods. 3 by členské štáty mali:

a) určiť NSA zodpovedný za bezpečnostné mechanizmy ochrany utajovaných skutočností EÚ, aby sa zabezpečilo, že:

i) utajované skutočnosti EÚ, ktoré uchovávajú akékoľvek ministerstvá, orgány alebo agentúry bez ohľadu na to, či sú verejné alebo súkromné, doma alebo v zahraničí, sú chránené v súlade s týmto rozhodnutím;

ii) bezpečnostné mechanizmy na ochranu utajovaných skutočností EÚ sa podrobujú pravidelnej inšpekcii;

iii) všetky osoby, ktoré sú zamestnané vo verejnej správe alebo u dodávateľa a ktorým sa môže udeliť prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, sú náležite bezpečnostne preverené alebo na základe svojich úloh získali iné náležité povolenie v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi;

iv) vytvoria sa potrebné bezpečnostné programy na minimalizáciu rizika vyzradenia alebo straty utajovaných skutočností EÚ;

v) bezpečnostné záležitosti týkajúce sa ochrany utajovaných skutočností EÚ sa koordinujú s ostatnými príslušnými vnútroštátnymi orgánmi vrátane orgánov uvedených v tomto rozhodnutí a

vi) odpovedá sa na opodstatnené žiadosti o bezpečnostnú previerku od agentúr a orgánov EÚ zriadených na základe hlavy V kapitoly 2 Zmluvy o EÚ, ako aj od Europolu a Eurojustu, operácií krízového riadenia vykonávaných na základe hlavy V kapitoly 2 Zmluvy o EÚ a OZEÚ a ich tímov.

NSA sa uvádzajú v dodatku C;

b) zabezpečia, aby ich príslušné orgány poskytovali svojej vláde a prostredníctvom nej Rade informácie a rady o povahe ohrození bezpečnosti utajovaných skutočností EÚ a o prostriedkoch ochrany pred nimi.

Článok 16

Bezpečnostný výbor

1. Týmto sa zriaďuje Bezpečnostný výbor. Bezpečnostný výbor vykonáva preskúmanie a hodnotenie každej bezpečnostnej záležitosti, ktorá je v rozsahu pôsobnosti tohto rozhodnutia, a podľa potreby poskytuje Rade odporúčania.

2. Skladá sa zo zástupcov NSA členských štátov a na jeho zasadnutiach je prítomný zástupca Komisie a Európskej služby pre vonkajšiu činnosť. Výboru predsedá generálny tajomník alebo ním určený zástupca. Bezpečnostný výbor zasadá podľa pokynov Rady alebo na žiadosť generálneho tajomníka alebo NSA.

Na zasadnutia môžu byť prizvaní aj zástupcovia agentúr a orgánov EÚ zriadených na základe hlavy V kapitoly 2 Zmluvy o EÚ, ako aj Europolu a Eurojustu, keď sa rokuje o otázkach, ktoré sa ich týkajú.

3. Bezpečnostný výbor organizuje svoju činnosť tak, aby mohol poskytovať odporúčania ku konkrétnym oblastiam bezpečnosti. Vytvorí odbornú podskupinu pre otázky IA a podľa potreby iné odborné podskupiny. Stanoví mandát pre tieto odborné podskupiny, ktoré mu odovzdávajú správy o svojej činnosti a v prípade potreby akékoľvek odporúčania pre Radu.

Článok 17

Nahradenie predchádzajúcich rozhodnutí

1. Týmto rozhodnutím sa zrušuje a nahrádza rozhodnutie 2001/264/ES z 19. marca 2001 prijímajúce bezpečnostné nariadenia Rady ([1]).

2. Všetky utajované skutočnosti EÚ utajované v súlade s rozhodnutím Rady 2001/264/ES sú naďalej chránené v súlade s príslušnými ustanoveniami tohto rozhodnutia.

Článok 18

Nadobudnutie účinnosti

Toto rozhodnutie nadobúda účinnosť dňom jeho uverejnenia v *Úradnom vestníku Európskej únie*.

V Bruseli 31. marca 2011

Za Radu

predseda

VÖLNER P.

([1]) Ú. v. ES L 101, 11.4.2001, s. 1.

PRÍLOHY

PRÍLOHA I

Personálna bezpečnosť

PRÍLOHA II

Fyzická bezpečnosť

PRÍLOHA III

Správa utajovaných skutočností

PRÍLOHA IV

Ochrana utajovaných skutočností EÚ, s ktorými sa manipuluje v komunikačných a informačných systémoch

PRÍLOHA V

Priemyselná bezpečnosť

PRÍLOHA VI

Výmena utajovaných skutočností s tretími štátmi a medzinárodnými organizáciami

PRÍLOHA I

PERSONÁLNA BEZPEČNOSŤ

I. ÚVOD

1. V tejto prílohe sa uvádzajú vykonávacie ustanovenia k článku 7. Stanovujú sa v nej predovšetkým kritériá, na základe ktorých sa určuje, či osobe pri zohľadnení jej lojality, dôveryhodnosti a spoľahlivosti možno povoliť prístup k utajovaným skutočnostiam EÚ, a preverovacie a správne postupy, ktoré sa majú v tejto súvislosti dodržiavať.

2. V celej tejto prílohe pojem previerka personálnej bezpečnosti znamená národnú previerku personálnej bezpečnosti (ďalej len „národná PSC") a/alebo previerku personálnej bezpečnosti EÚ (ďalej len „PSC EÚ") v zmysle definícií v dodatku A okrem prípadov, keď je dôležité medzi týmito dvoma pojmami rozlišovať.

II. POVOLENIE PRÍSTUPU K UTAJOVANÝM SKUTOČNOSTIAM EÚ

3. Osobe sa môže povoliť prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším len potom, ako:

   a) sa určila jej potreba poznať;

   b) udelilo sa jej PSC pre príslušný stupeň alebo sa jej v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi na základe jej úloh udelilo iné náležité povolenie a

   c) bola poučená o bezpečnostných pravidlách a postupoch ochrany utajovaných skutočností EÚ a akceptovala svoje povinnosti v súvislosti s ochranou takýchto utajovaných skutočností.

4. Každý členský štát a GSR určia v rámci svojej štruktúry pozície, ktoré si vyžadujú prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším a ktoré si teda vyžadujú PSC pre príslušný stupeň.

III. POŽIADAVKY NA PREVIERKU PERSONÁLNEJ BEZPEČNOSTI

5. NSA alebo iné príslušné vnútroštátne orgány sú na základe doručenej a riadne autorizovanej žiadosti zodpovedné za zabezpečenie vykonávania bezpečnostných previerok svojich štátnych príslušníkov, ktorí potrebujú prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším. Normy vykonania týchto previerok sú stanovené vnútroštátnymi zákonmi a inými právnymi predpismi.

6. Ak má príslušná osoba bydlisko na území iného členského štátu alebo tretieho štátu, príslušné vnútroštátne orgány spolupracujú v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi s príslušným orgánom štátu bydliska. Členské štáty si v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi pri vykonávaní bezpečnostných previerok navzájom pomáhajú.

7. Ak to vnútroštátne zákony a iné právne predpisy umožňujú, NSA alebo iné príslušné vnútroštátne orgány môžu vykonávať previerky cudzích štátnych príslušníkov, ktorí potrebujú prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším. Normy vykonania týchto previerok sú stanovené vnútroštátnymi zákonmi a inými právnymi predpismi.

Kritériá bezpečnostného vyšetrovania

8. Skutočnosť, či je osoba lojálna, dôveryhodná a spoľahlivá na účely udelenia PSC na prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, sa stanovuje prostredníctvom bezpečnostného vyšetrovania. Príslušný vnútroštátny orgán uskutoční na základe zistení z tohto bezpečnostného vyšetrovania celkové vyhodnotenie. Jednotlivé negatívne zistenia nemusia nevyhnutne predstavovať dôvod na zamietnutie PSC. Prostredníctvom hlavných kritérií, ktoré sa na tento účel uplatňujú, by sa v rozsahu, v ktorom to umožňujú vnútroštátne zákony a iné právne predpisy, malo okrem iného preverovať, či osoba:

   a) spáchala alebo sa pokúsila spáchať čin špionáže, terorizmu, sabotáže, vlastizrady alebo podnecovania k vzbure, alebo zosnovala takýto čin, pomáhala niekomu pri takomto čine, alebo navádzala na spáchanie takéhoto činu;

   b) stýka sa alebo sa stýkala s osobami vykonávajúcimi špionážne, teroristické, sabotážne činnosti alebo osobami, ktoré boli odôvodnene podozrivé z takýchto činností, alebo so zástupcami organizácií alebo cudzích štátov vrátane zahraničných spravodajských služieb, ktoré môžu ohrozovať bezpečnosť EÚ a/alebo členských štátov, pokiaľ tento styk nebol povolený v rámci výkonu služobných povinností;

c) je alebo bola členom akejkoľvek organizácie, ktorá sa násilným, podvratným alebo iným nezákonným spôsobom pokúša okrem iného zvrhnúť vládu členského štátu, zmeniť ústavný poriadok členského štátu alebo zmeniť formu alebo politiky svojej vlády;

d) podporuje alebo podporovala organizáciu opísanú v písmene c), alebo udržiava alebo udržiavala úzky styk s členmi takýchto organizácií;

e) úmyselne zadržala významné informácie alebo skreslila alebo falšovala takéto informácie, a to najmä bezpečnostného charakteru, alebo úmyselne klamala pri vypĺňaní osobného bezpečnostného dotazníka alebo počas bezpečnostného pohovoru;

f) bola usvedčená z trestného činu alebo činov;

g) má záznam o závislosti na alkohole, užívaní drog a/alebo zneužívaní liekov;

h) vykonáva alebo vykonala skutky, ktoré môžu viesť k riziku vystavenia vydieraniu alebo nátlaku;

i) skutkom alebo slovami preukázala nečestnosť, nelojálnosť, nespoľahlivosť alebo nedôveryhodnosť;

j) vážne alebo opakovane porušila bezpečnostné predpisy alebo sa úspešne alebo neúspešne pokúsila o nepovolenú činnosť v súvislosti s komunikačnými a informačnými systémami;

k) môže byť vystavená nátlaku (napr. na základe toho, že má jednu alebo viacero štátnych príslušností iných štátov ako členských štátov EÚ, alebo prostredníctvom príbuzných alebo blízkych osôb, ktoré môžu byť zraniteľné zo strany zahraničných spravodajských služieb, teroristických skupín alebo iných podvratných organizácií, alebo osôb, ktorých zámery môžu ohrozovať bezpečnostné záujmy EÚ a/alebo členských štátov).

9. Keď je to vhodné, pri bezpečnostnom vyšetrovaní sa môže v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi prihliadať aj na finančnú situáciu a zdravotný stav osoby.

10. Keď je to vhodné, pri bezpečnostnom vyšetrovaní sa môže v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi prihliadať aj na charakter, konanie a okolnosti manžela/manželky, druha/družky alebo blízkeho rodinného príslušníka.

Požiadavky na previerku na účely prístupu k utajovaným skutočnostiam EÚ

Prvé udelenie PSC

11. Prvá PSC na účely prístupu k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET sa zakladá na bezpečnostnom vyšetrovaní, ktoré pokrýva najmenej posledných päť rokov alebo obdobie od dosiahnutia veku 18 rokov do súčasnosti podľa toho, ktoré z týchto období je kratšie, a zahŕňa:

a) vyplnenie vnútroštátneho osobného bezpečnostného dotazníka pre stupeň utajenia utajovaných skutočností, ku ktorým daná osoba potrebuje prístup; dotazník sa po vyplnení zasiela príslušnému bezpečnostnému orgánu;

b) overenie totožnosti/občianstva/štátnej príslušnosti – overí sa dátum a miesto narodenia osoby a jej totožnosť. Určí sa predchádzajúce a súčasné občianstvo a/alebo štátna príslušnosť osoby, čo zahŕňa vyhodnotenie rizika akéhokoľvek nátlaku zo strany zahraničných zdrojov napríklad z dôvodu predchádzajúceho miesta bydliska alebo predchádzajúcich stykov, a

c) preskúmanie národných a miestnych záznamov – preskúmajú sa vnútroštátne bezpečnostné a centrálne trestné záznamy, ak existujú, a/alebo iné porovnateľné štátne alebo policajné záznamy. Preveria sa záznamy orgánov presadzovania práva príslušných podľa miesta bydliska alebo zamestnania osoby.

12. Prvá PSC na účely prístupu k utajovaným skutočnostiam so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET sa zakladá na bezpečnostnom vyšetrovaní, ktoré pokrýva najmenej posledných desať rokov alebo obdobie od dosiahnutia veku 18 rokov do súčasnosti podľa toho, ktoré z týchto období je kratšie. Ak sa uskutočňujú pohovory v zmysle písmena e), vyšetrovanie pokrýva minimálne posledných sedem rokov alebo obdobie od dosiahnutia veku 18 rokov do súčasnosti podľa toho, ktoré z týchto období je kratšie. Okrem kritérií uvedených v bode 8 sa pred udelením PSC pre stupeň utajenia TRÉS SECRET UE/EU TOP SECRET tieto prvky preveria v rozsahu, ktorý umožňujú vnútroštátne zákony a iné právne predpisy; možno ich preveriť aj pred udelením PSC pre stupeň utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET, ak sa to vyžaduje vo vnútroštátnych zákonoch a iných právnych predpisoch:

a) finančná situácia – získajú sa informácie o finančnej situácii osoby s cieľom vyhodnotiť riziká súvisiace so zahraničným alebo domácim nátlakom z dôvodu finančných ťažkostí alebo s cieľom odhaliť nevysvetliteľné bohatstvo;

b) vzdelanie – získajú sa informácie na účely overenia vzdelania osoby na školách, univerzitách a iných vzdelávacích zariadeniach, ktoré navštevovala po veku 18 rokov alebo počas iného obdobia, ktoré preverujúci orgán považuje za vhodné;

c) zamestnanie – získajú sa informácie o súčasnom a predchádzajúcom zamestnaní s odkazom na zdroje, ako je záznam o zamestnaní a hodnotiace správy zamestnanca, a na zamestnávateľov alebo vedúcich pracovníkov;

d) vojenská služba – preverí sa služba osoby v ozbrojených silách (ak sa na osobu vzťahuje) a typ prepustenia a

e) pohovor – s osobou sa uskutoční pohovor (pohovory), pokiaľ sa ustanovujú vo vnútroštátnom práve a pokiaľ ich toto právo pripúšťa. Pohovory sa uskutočňujú aj s inými osobami, ktoré môžu poskytnúť nezaujaté hodnotenie o minulosti, aktivitách, lojalite, dôveryhodnosti a spoľahlivosti danej osoby. Pokiaľ je zaužívanou vnútroštátnou praxou požiadať skúmanú osobu o uvedenie osôb, ktoré môžu poskytnúť referencie, uskutoční sa pohovor aj s týmito osobami, pokiaľ neexistujú náležité dôvody to neurobiť.

13. V súlade s vnútroštátnymi zákonmi a inými právnymi predpismi sa môže v prípade potreby uskutočniť dodatočné vyšetrovanie zamerané na získanie všetkých dôležitých dostupných informácií o osobe a na preukázanie alebo vyvrátenie negatívnych informácií.

Predĺženie platnosti PSC

14. Po prvom udelení PSC a za predpokladu, že osoba neprerušila svoju službu vo verejnej správe alebo v GSR a naďalej potrebuje prístup k utajovaným skutočnostiam EÚ, sa táto PSC preskúma na účely predĺženia v lehotách, ktoré neprekračujú päť rokov v prípade previerky pre stupeň utajenia TRÉS SECRET UE/EU TOP SECRET a 10 rokov v prípade previerky pre stupeň utajenia SECRET UE/EU SECRET a CONFIDENTIEL UE/EU CONFIDENTIAL, ktoré začínajú plynúť od oznámenia výsledku posledného bezpečnostného vyšetrovania, o ktoré sa tieto previerky opierajú. Vo všetkých bezpečnostných vyšetrovaniach na účely predĺženia platnosti PSC sa vyhodnocuje obdobie, ktoré uplynulo od predchádzajúceho vyšetrovania.

15. Na účely predĺženia platnosti PSC sa preverujú prvky uvedené v bodoch 11 a 12.

16. Žiadosti o predĺženie platnosti sa podávajú včas tak, aby sa zohľadnil čas potrebný na vykonanie bezpečnostných vyšetrovaní. V prípade, že bola príslušnému NSA alebo inému príslušnému vnútroštátnemu orgánu doručená príslušná žiadosť o predĺženie a zodpovedajúci osobný bezpečnostný dotazník predtým, ako uplynie platnosť PSC, ale potrebné bezpečnostné vyšetrovanie sa ešte neukončilo, príslušný vnútroštátny orgán môže predĺžiť obdobie platnosti PSC o obdobie do 12 mesiacov, ak to umožňujú vnútroštátne zákony a iné právne predpisy. Ak sa ku koncu tohto 12 mesačného obdobia ešte stále bezpečnostné vyšetrovanie neukončilo, osobe sa pridelia úlohy, ktoré si nevyžadujú PSC.

Postupy PSC v GSR

17. V prípade úradníkov a iných zamestnancov GSR zasiela vyplnený osobný bezpečnostný dotazník národnému bezpečnostnému orgánu členského štátu, ktorého je osoba štátnym príslušníkom, bezpečnostný orgán GSR, ktorý požiada o vykonanie bezpečnostnej previerky pre stupeň utajenia utajovaných skutočností EÚ, ku ktorým bude táto osoba potrebovať prístup.

18. Ak GSR zistí o osobe, ktorá požiadala o vydanie PSC EÚ, relevantné informácie z hľadiska bezpečnostnej previerky, oznámi túto skutočnosť v súlade s príslušnými pravidlami a predpismi príslušnému NSA.

19. Po ukončení bezpečnostného vyšetrovania príslušný NSA oznámi bezpečnostnému orgánu GSR výsledok tohto vyšetrovania, a to v príslušnom formáte pre korešpondenciu stanovenom Bezpečnostným výborom.

a) Keď je výsledkom bezpečnostného vyšetrovania ubezpečenie, že nie je známe nič, čo by spochybňovalo lojalitu, dôveryhodnosť a spoľahlivosť osoby, menovací orgán GSR môže udeliť tejto dotknutej osobe PSC EÚ a do stanoveného dátumu jej povoliť prístup k utajovaným skutočnostiam EÚ do príslušného stupňa utajenia.

b) Keď výsledkom bezpečnostného vyšetrovania nie je takéto ubezpečenie, menovací orgán GSR informuje dotknutú osobu, ktorá môže požiadať menovací orgán o pohovor. Menovací orgán GSR môže požiadať príslušný NSA o ďalšie prípadné podrobnosti, ktoré môže na základe vnútroštátnych zákonov a iných právnych predpisov poskytnúť. Ak sa tento výsledok potvrdí, PSC EÚ sa neudelí.

20. Na bezpečnostné vyšetrovanie a získané výsledky sa vzťahujú príslušné zákony a iné právne predpisy, ktoré sú platné v dotknutom členskom štáte, vrátane tých, ktoré sa týkajú odvolania. Proti rozhodnutiam menovacieho orgánu GSR možno podať odvolanie v súlade so Služobným poriadkom úradníkov Európskej Únie a podmienkami zamestnávania ostatných zamestnancov Európskej Únie stanovenými v nariadení (EHS, Euratom, ESUO) č. 259/68 [1] (ďalej len „služobný poriadok a podmienky zamestnávania").

21. Ubezpečenie, z ktorého PSC EÚ vychádza, je platné pre každú funkciu, ktorú dotknutá osoba vykonáva v GSR alebo v Komisii, za predpokladu, že zostáva platné.

22. Ak sa obdobie služby osoby nezačne do 12 mesiacov od oznámenia výsledku bezpečnostného vyšetrovania menovaciemu orgánu GSR alebo ak sa služba osoby preruší na obdobie 12 mesiacov, počas ktorých táto osoba nie je zamestnaná v GSR ani na pozícii vo verejnej správe členského štátu, platnosť a náležitosť tohto výsledku sa overí u príslušného NSA.

23. Ak sa GSR oboznámi s informáciami týkajúcimi sa bezpečnostných rizík, ktoré predstavuje osoba, ktorá je držiteľom platnej PSC EÚ, GSR konajúci v súlade s príslušnými pravidlami a predpismi to oznámi príslušnému NSA. Ak NSA informuje GSR o odňatí ubezpečenia udeleného v súlade s bodom 19 písm. a) osobe, ktorá je držiteľom platnej PSC EÚ, menovací orgán GSR môže požiadať o akékoľvek podrobnosti, ktoré NSA môže na základe vnútroštátnych zákonov a iných právnych predpisov poskytnúť. Ak sa negatívne informácie potvrdia, PSC EÚ sa odníme a osobe sa zruší možnosť prístupu k utajovaným skutočnostiam EÚ a preradí sa z pozícií, kde takáto možnosť prístupu existuje alebo kde by táto osoba mohla predstavovať bezpečnostné riziko.

24. Každé rozhodnutie o odňatí PSC EÚ úradníka alebo iného zamestnanca GSR a ak je to vhodné, jeho dôvody sa oznámia dotknutej osobe, ktorá môže požiadať o pohovor s menovacím orgánom. Na informácie, ktoré poskytuje NSA, sa vzťahujú príslušné zákony a iné právne predpisy, ktoré sú platné v dotknutom členskom štáte, vrátane tých, ktoré sa týkajú odvolania. Proti rozhodnutiam menovacieho orgánu GSR možno podať odvolanie v súlade so služobným poriadkom a podmienkami zamestnávania.

25. Od národných expertov vyslaných pracovať v GSR na pozícii, ktorá si vyžaduje PSC EÚ, sa požaduje, aby pred začatím vykonávania funkcie predložili bezpečnostnému orgánu GSR platné národné PSC na účely prístupu k utajovaným skutočnostiam EÚ.

Záznamy o PSC

26. Záznamy o národných PSC, resp. PSC EÚ udelených na účely prístupu k utajovaným skutočnostiam EÚ uchovávajú členské štáty, resp. GSR. Tieto záznamy obsahujú aspoň stupeň utajenia utajovaných skutočností EÚ, ku ktorému sa osobe môže udeliť prístup (CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšší), dátum udelenia PSC a obdobie platnosti.

27. Príslušný bezpečnostný orgán môže vydať certifikát o previerke personálnej bezpečnosti (ďalej len PSCC – Personnel Security Clearance Certificate), v ktorom sa uvádza stupeň utajenia utajovaných skutočností EÚ, ku ktorým môže osobe udeliť prístup (CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšší), dátum platnosti príslušnej národnej PSC na účely prístupu k utajovaným skutočnostiam EÚ, resp. PSC EÚ a dátum ukončenia platnosti samotného certifikátu.

Výnimky z požiadavky na PSC

28. Prístup k utajovaným skutočnostiam EÚ v členských štátoch zo strany osôb, ktoré majú náležité povolenie na základe povahy svojej funkcie, sa stanovuje na základe vnútroštátnych zákonov a iných právnych predpisov; takéto osoby sú poučené o bezpečnostných povinnostiach v súvislosti s ochranou utajovaných skutočností EÚ.

IV. BEZPEČNOSTNÉ VZDELÁVANIE A INFORMOVANOSŤ

29. Každá osoba, ktorej sa udelila PSC, písomne potvrdí, že porozumela svojim povinnostiam týkajúcim sa ochrany utajovaných skutočností EÚ a následkom v prípade ich vyzradenia. Záznam o takomto písomnom potvrdení uchováva členský štát, resp. GSR.

30. Každá osoba, ktorá má povolený prístup k utajovaným skutočnostiam EÚ alebo od ktorej sa vyžaduje, aby s nimi manipulovala, je na začiatku informovaná a ďalej pravidelne poučovaná o ohrozeniach je povinná bezodkladne oznámiť príslušným bezpečnostným orgánom každý kontakt alebo aktivitu, ktoré považujú za podozrivý a neobvyklý.

31. Každá osoba, ktorá ukončila zamestnanie vyžadujúce si prístup k utajovaným skutočnostiam EÚ, je poučená o svojich povinnostiach naďalej chrániť utajované skutočnosti EÚ, čo potvrdí písomne, ak je to potrebné.

[1] Ú. v. ES L 56, 4.3.1968, s. 1.

V. OSOBITNÉ OKOLNOSTI

32. Ak to umožňujú vnútroštátne zákony a iné právne predpisy, previerka personálnej bezpečnosti, ktorú príslušný vnútroštátny orgán členského štátu udelil na účely prístupu k vnútroštátnym utajovaným skutočnostiam, môže na čas, kým sa neudelí národná PSC na prístup k utajovaným skutočnostiam EÚ, úradníkom členského štátu umožniť prístup k utajovaným skutočnostiam EÚ do rovnocenného stupňa utajenia stanoveného podľa ekvivalenčnej tabuľky uvedenej v dodatku B, ak je tento dočasný prístup potrebný z hľadiska záujmov EÚ. V prípade, že vnútroštátne zákony a iné právne predpisy takýto dočasný prístup k utajovaným skutočnostiam EÚ neumožňujú, NSA o tom informujú Bezpečnostný výbor.

33. V naliehavých prípadoch, ktoré sú náležite odôvodnené záujmami útvaru, môže menovací orgán GSR po porade s NSA členského štátu, ktorého je osoba štátnym príslušníkom, do ukončenia úplnej bezpečnostnej previerky a na základe predbežných preverení slúžiacich na overenie, či nie sú známe negatívne skutočnosti, udeliť dočasné povolenie úradníkom a iným zamestnancom GSR na prístup k utajovaným skutočnostiam EÚ pre konkrétnu úlohu. Takéto dočasné povolenie je platné počas obdobia, ktoré nepresahuje šesť mesiacov, a nemôže sa ním povoliť prístup k utajovaným skutočnostiam so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET. Každá osoba, ktorej sa udelilo dočasné oprávnenie, písomne potvrdí, že porozumela svojim povinnostiam týkajúcim sa ochrany utajovaných skutočností EÚ a následkom v prípade ich vyzradenia. Záznam o takomto písomnom potvrdení uchováva GSR.

34. Ak má byť osoba pridelená na pozíciu, ktorá si vyžaduje PSC pre stupeň utajenia, ktorý je o jeden stupeň vyšší ako stupeň utajenia, ktorého je osoba v súčasnosti držiteľom, táto osoba sa dočasne na túto pozíciu môže prideliť, ak:

a) naliehavú potrebu prístupu k utajovaným skutočnostiam EÚ s vyšším stupňom utajenia písomne odôvodní nadriadená osoba tejto osoby;

b) prístup sa obmedzí na konkrétne položky utajovaných skutočností EÚ, ktoré sú užitočné z hľadiska pridelenia;

c) osoba je držiteľom platnej národnej PSC alebo PSC EÚ;

d) začal sa postup na získanie povolenia pre stupeň utajenia, ktorý si daná pozícia vyžaduje;

e) príslušný orgán vykonal kontroly dostatočne preukazujúce, že táto osoba vážne alebo opakovane neporušila bezpečnostné predpisy;

f) príslušný orgán schválil pridelenie osoby a

g) záznam o výnimke vrátane uvedenia utajovaných skutočností, ku ktorým bol schválený prístup, sa uchováva v príslušnom utajovanom registri alebo podriadenom registri.

35. Uvedený postup sa používa v prípade jednorazového prístupu k utajovaným skutočnostiam EÚ so stupňom utajenia o jeden stupeň vyšším ako stupeň, pre ktorý bola osoba bezpečnostne preverená. Tento postup sa nevyužíva opakovane.

36. Za veľmi výnimočných okolností, t. j. pri misiách v nepriateľskom prostredí alebo počas obdobia rastúceho medzinárodného napätia, keď si to vyžadujú núdzové opatrenia, predovšetkým na účely záchrany životov, môžu členské štáty a generálny tajomník alebo jeho zástupca udeliť, ak je to možné písomne, prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET osobám, ktoré nie sú držiteľmi potrebnej PSC pod podmienkou, že takéto povolenie je absolútne nevyhnutné a neexistujú nijaké odôvodnené pochybnosti o lojalite, dôveryhodnosti a spoľahlivosti dotknutej osoby. O takomto povolení sa uchováva záznam s uvedením utajovaných skutočností, ku ktorým bol schválený prístup.

37. V prípade utajovaných skutočností so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET sa povolenie takéhoto núdzového prístupu obmedzuje na štátnych príslušníkov EÚ, ktorým bol udelený prístup k utajovaným skutočnostiam, ktorých stupeň utajenia na vnútroštátnej úrovni je rovnocenný stupňu utajenia TRÉS SECRET UE/EU TOP SECRET alebo SECRET UE/EU SECRET.

38. V prípade uplatnenia postupu stanoveného v bodoch 36 a 37 sa o tejto skutočnosti informuje Bezpečnostný výbor.

39. Ak vnútroštátne zákony a iné právne predpisy členských štátov ustanovujú v súvislosti s dočasným povolením, dočasným pridelením, jednorazovým prístupom alebo núdzovým prístupom osôb k utajovaným skutočnostiam prísnejšie pravidlá, postupy ustanovené v tomto oddiele sa vykonávajú v rámci akýchkoľvek obmedzení stanovených v príslušných vnútroštátnych zákonoch a iných právnych predpisoch.

40. Bezpečnostnému výboru sa zasiela výročná správa o využívaní postupov uvedených v tomto oddiele.

VI. ÚČASŤ NA ZASADNUTIACH V RADE

41. S výhradou bodu 28 osoby poverené, aby sa zúčastňovali na zasadnutiach Rady alebo jej prípravných orgánov, na ktorých sa rokuje o utajovaných skutočnostiach so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, sa môžu na týchto zasadnutiach zúčastňovať, len ak sa potvrdil stav ich PSC. Za delegátov zasielajú PSCC alebo iné doklady o PSC Bezpečnostnému úradu GSR príslušné orgány, alebo vo výnimočných prípadoch ich predkladá dotknutý delegát. V prípade potreby sa môže použiť súhrnný zoznam mien, ktorý poskytuje príslušný doklad o PSC.

42. Ak sa PSC na prístup k utajovaným skutočnostiam EÚ z bezpečnostných dôvodov odňala osobe, ktorej povinnosti si vyžadujú jej účasť na zasadnutiach Rady alebo jej prípravných orgánov, príslušný orgán o tom informuje GSR.

VII. PRÍPADNÝ PRÍSTUP K UTAJOVANÝM SKUTOČNOSTIAM EÚ

43. Ak by osoby, ktoré sa prijmú do zamestnania, mohli pri jeho výkone mať potenciálne prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšším, tieto osoby sa náležite bezpečnostne preveria alebo majú nepretržitý sprievod.

44. Kuriéri, príslušníci bezpečnostnej služby a sprievodu sú bezpečnostne preverení pre príslušný stupeň utajenia alebo preverení iným vhodným spôsobom v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi, poučení o bezpečnostných postupoch na ochranu utajovaných skutočností EÚ a informovaní o svojich povinnostiach v súvislosti s ochranou takýchto utajovaných skutočností, ktoré sú im zverené.

PRÍLOHA II

FYZICKÁ BEZPEČNOSŤ

I. ÚVOD

1. V tejto prílohe sa uvádzajú vykonávacie ustanovenia k článku 8. Stanovujú sa v nej minimálne požiadavky fyzickej ochrany objektov, budov, kancelárií, miestností a iných priestorov, v ktorých sa manipuluje s utajovanými skutočnosťami EÚ a v ktorých sa uchovávajú, ako aj priestorov, v ktorých sa nachádzajú CIS.

2. Na zabránenie neoprávnenému prístupu k utajovaným skutočnostiam EÚ sa vytvoria opatrenia fyzickej bezpečnosti, ktorými sa:

   a) zabezpečí, že s utajovanými skutočnosťami EÚ sa manipuluje vhodným spôsobom a že sú vhodným spôsobom uchovávané;

   b) umožní rozdelenie pracovníkov, pokiaľ ide o prístup k utajovaným skutočnostiam EÚ, na základe ich potreby poznať, a ak je to vhodné, na základe ich bezpečnostnej previerky;

   c) odradí od neoprávnených činností, zabráni sa im a zistia sa a

   d) zabráni utajenému alebo násilnému vstupu narušiteľa alebo sa takýto vstup oddiali.

II. POŽIADAVKY A OPATRENIA FYZICKEJ BEZPEČNOSTI

3. Opatrenia fyzickej bezpečnosti sa zvolia na základe posúdenia ohrozenia, ktoré vykonajú príslušné orgány. Na zabezpečenie úrovne fyzickej ochrany zodpovedajúcej vyhodnotenému riziku uplatňujú GSR a členské štáty vo svojich objektoch proces riadenia rizík na ochranu utajovaných skutočností EÚ. V procese riadenia rizík sa zohľadnia všetky relevantné faktory, a najmä na:

   a) stupeň utajenia utajovaných skutočností EÚ;

   b) formu uchovávaných utajovaných skutočností EÚ a ich množstvo s prihliadnutím na skutočnosť, že veľké množstvo alebo spojenie utajovaných skutočností EÚ si môžu vyžadovať uplatňovanie prísnejších ochranných opatrení;

   c) okolité prostredie a konštrukciu budov alebo priestorov, v ktorých sa utajované skutočnosti EÚ nachádzajú, a

   d) vyhodnotené ohrozenie zo strany spravodajských služieb, ktoré sa zameriavajú na EÚ alebo členské štáty, a zo strany sabotážnych, teroristických, podvratných alebo iných trestných činností.

4. Príslušný bezpečnostný orgán určuje na základe koncepcie hĺbkovej ochrany vhodnú kombináciu opatrení fyzickej bezpečnosti, ktoré sa uplatnia. Môže medzi ne patriť jedno alebo viaceré z týchto kritérií:

   a) obvodová bariéra: fyzická bariéra chrániaca hranicu priestoru, ktorý si vyžaduje ochranu;

   b) detekčné systémy proti narušeniu (ďalej len „IDS“ – Intrusion Detection System): IDS sa môžu použiť s cieľom zvýšiť úroveň bezpečnosti, ktorú zabezpečuje obvodová bariéra, alebo sa môže použiť v miestnostiach a budovách namiesto bezpečnostného personálu alebo na jeho doplnenie;

   c) kontrola vstupu: môže sa vykonávať kontrola vstupu do celého objektu, budovy alebo budov v rámci objektu alebo do priestorov alebo miestností v rámci budovy. Kontrola vstupu sa môže vykonávať elektronickými alebo elektromechanickými prostriedkami, môže ju vykonávať bezpečnostný personál a/alebo pracovník na recepcii alebo sa môže vykonávať akýmikoľvek inými fyzickými prostriedkami;

   d) bezpečnostný personál: vyškolený, kontrolovaný a v prípade potreby náležite bezpečnostne preverený bezpečnostný personál sa môže zamestnávať aj na odradenie osôb plánujúcich utajené narušenie;

   e) uzatvorený televízny okruh (ďalej len „CCTV“ – Closed Circuit Television): na preverenie incidentov a poplachov z IDS vo veľkých objektoch alebo na perimetroch môže bezpečnostný personál využívať CCTV;

   f) bezpečnostné osvetlenie: na odradenie potenciálneho narušiteľa a na zabezpečenie osvetlenia potrebného na účinný priamy dohľad zo strany bezpečnostného personálu alebo nepriamy dohľad prostredníctvom systému CCTV sa môže používať bezpečnostné osvetlenie a

   g) akýkoľvek iný vhodný fyzický prostriedok určený na odradenie alebo zistenie nepovoleného vstupu alebo na zabránenie strate alebo poškodeniu utajovaných skutočností EÚ.

5. Príslušný orgán môže byť oprávnený vykonávať pri vstupe a výstupe prehliadky, ktorých cieľom je odradiť od nepovoleného prinesenia vecí alebo nepovoleného odnesenia utajovaných skutočností EÚ z objektu alebo budovy.

6. Ak existuje riziko nahliadnutia do utajovaných skutočností EÚ, aj keď len náhodného, musia sa prijať primerané opatrenia na zabránenie tomuto riziku.

7. V prípade nových zariadení sa požiadavky fyzickej bezpečnosti definujú vo fáze plánovania a projektovania zariadení. V prípade existujúcich zariadení sa požiadavky fyzickej bezpečnosti uplatňujú v čo najväčšom rozsahu.

III. ZARIADENIA NA FYZICKÚ OCHRANU UTAJOVANÝCH SKUTOČNOSTÍ EÚ

8. Pri obstarávaní technických zariadení na fyzickú ochranu utajovaných skutočností EÚ (napríklad bezpečnostných úschovných objektov, skartovacích strojov, zámok do dverí, elektronických systémov na kontrolu vstupu, IDS, poplachových systémov atď.) príslušný bezpečnostný orgán zabezpečuje, že toto zariadenie spĺňa schválené technické normy a minimálne požiadavky.

9. Technické špecifikácie zariadení na fyzickú ochranu utajovaných skutočností EÚ sa ustanovia v bezpečnostných usmerneniach, ktoré schváli Bezpečnostný výbor.

10. Bezpečnostné systémy podliehajú pravidelnej inšpekcii a na zariadeniach sa vykonáva pravidelná údržba. Pri údržbových prácach sa prihliada na výsledok inšpekcií, aby sa zabezpečilo, že zariadenie naďalej funguje optimálnym spôsobom.

11. Pri každej inšpekcii sa opätovne posudzuje účinnosť jednotlivých bezpečnostných opatrení a celého bezpečnostného systému.

IV. FYZICKY CHRÁNENÉ PRIESTORY

12. Na účely fyzickej ochrany utajovaných skutočností EÚ sa zriadia dva typy fyzicky chránených priestorov alebo im rovnocenných priestorov na vnútroštátnej úrovni:

a) administratívne zóny a

b) zabezpečené priestory (vrátane technicky zabezpečených priestorov).

Všetky odkazy na administratívne zóny a zabezpečené priestory vrátane technicky zabezpečených priestorov v tomto rozhodnutí sa vzťahujú aj na rovnocenné priestory na vnútroštátnej úrovni.

13. Príslušný bezpečnostný orgán ustanoví, že priestor spĺňa požiadavky na označenie ako administratívna zóna, zabezpečený priestor alebo technicky zabezpečený priestor.

14. Pokiaľ ide o administratívne zóny:

a) stanoví sa viditeľne vymedzený perimeter, ktorý umožňuje kontrolu osôb a v prípade možnosti aj vozidiel;

b) prístup bez sprievodu sa udeľuje len tým osobám, ktorým príslušný orgán udelil náležite povolenie, a

c) všetky ostatné osoby majú nepretržitý sprievod alebo podliehajú rovnocenným kontrolám.

15. Pokiaľ ide o zabezpečené priestory:

a) stanoví sa viditeľne vymedzený a chránený perimeter, pričom každý vstup doň a východ z neho sa kontroluje pomocou preukazu alebo personálneho identifikačného systému;

b) prístup bez sprievodu sa udeľuje len bezpečnostne prevereným osobám, ktorým sa udelilo špecifické povolenie vstupu do priestoru vzhľadom na ich potrebu poznať;

c) všetky ostatné osoby majú nepretržitý sprievod alebo podliehajú rovnocenným kontrolám.

16. Ak vstup do zabezpečeného priestoru predstavuje zo všetkých praktických hľadísk priamy prístup k utajovaným skutočnostiam, ktoré obsahuje, uplatňujú sa tieto dodatočné požiadavky:

a) jasne sa označuje najvyšší stupeň utajenia utajovaných skutočností, ktoré sa bežne v tomto priestore nachádzajú;

b) od všetkých návštevníkov sa na vstup do tohto priestoru vyžaduje osobitné povolenie, musia mať nepretržitý sprievod a byť náležite bezpečnostne preverení, pokiaľ sa nezabezpečí, že nie je možný prístup k utajovaným skutočnostiam EÚ.

17. Zabezpečené priestory chránené proti aktívnemu odpočúvaniu sú ustanovené za technicky zabezpečené priestory. Tieto dodatočné požiadavky sa vzťahujú na:

a) takéto priestory sú vybavené systémom IDS, uzamknuté, keď sa v nich nikto nenachádza, a strážené, keď je v nich niekto prítomný. Všetky kľúče sa kontrolujú v súlade s časťou VI;

b) všetky osoby a veci vstupujúce do týchto priestorov sa kontrolujú;

c) v takýchto priestoroch sa pravidelne vykonáva fyzická a/alebo technická kontrola podľa požiadaviek príslušného bezpečnostného orgánu. Takéto kontroly sa musia vykonávať aj po každom neoprávnenom vstupe alebo podozrení na takýto vstup a

d) nesmú sa v nich nachádzať nijaké nepovolené komunikačné linky, nepovolené telefóny či iné nepovolené komunikačné zariadenia a elektrické alebo elektronické vybavenie.

18. Bez ohľadu na bod 17 písm. d) v prípade, že sa ohrozenie utajovaných skutočností EÚ vyhodnotí ako vysoké, skontroluje príslušný bezpečnostný orgán všetky komunikačné zariadenia a elektrické alebo elektronické vybavenie predtým, ako sa použijú v priestoroch, kde sa konajú zasadnutia alebo kde sa pracuje s utajovanými skutočnosťami so stupňom utajenia SECRET UE/EU SECRET a vyšším, aby sa zaistilo, že sa týmito zariadeniami neúmyselne alebo neoprávnene neprenesú za perimeter príslušného zabezpečeného priestoru žiadne zrozumiteľné informácie.

19. V zabezpečených priestoroch, v ktorých nevykonáva službukonajúci personál službu 24 hodín denne, sa podľa potreby vykonávajú kontroly na konci bežného pracovného času a v náhodných intervaloch mimo bežných pracovných hodín, pokiaľ nie je nainštalovaný systém IDS.

20. V prípade stretnutia s cieľom prerokovať utajované skutočnosti alebo na iné podobné účely sa zabezpečené priestory a technicky zabezpečené priestory môžu dočasne zriadiť v rámci administratívnej zóny.

21. Pre každý zabezpečený priestor sa vypracujú operačné bezpečnostné postupy, v ktorých sa stanoví:

a) stupeň utajenia utajovaných skutočností EÚ, s ktorými sa môže manipulovať alebo ktoré sa môžu uchovávať v tomto priestore;

b) opatrenia dohľadu a ochrany, ktoré sa musia uplatňovať;

c) osoby oprávnené na vstup do tohto priestoru bez sprievodu vzhľadom na ich potrebu poznať a bezpečnostnú previerku;

d) v prípade potreby postupy týkajúce sa sprievodu alebo ochrany utajovaných skutočností EÚ pri povoľovaní vstupu akýchkoľvek iných osôb do tohto priestoru;

e) akékoľvek ďalšie príslušné opatrenia a postupy.

22. V zabezpečených priestoroch sa vybudujú komorové trezory. Steny, podlahy, stropy, okná a uzamykateľné dvere musia byť schválené príslušným bezpečnostným orgánom a musia poskytovať ochranu, ktorá je rovnocenná ochrane poskytovanej bezpečnostnými úschovnými objektmi schválenými na uchovávanie utajovaných skutočností EÚ s rovnakým stupňom utajenia.

V. FYZICKÉ OCHRANNÉ OPATRENIA PRE MANIPULÁCIU S UTAJOVANÝMI SKUTOČNOSŤAMI EÚ A ICH UCHOVÁVANIE

23. S utajovanými skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED sa môže manipulovať:

a) v zabezpečenom priestore;

b) v administratívnej zóne za predpokladu, že utajované skutočnosti EÚ sú chránené pred prístupom zo strany neoprávnených osôb, alebo

c) mimo zabezpečeného priestoru alebo administratívnej zóny za predpokladu, že držiteľ prenáša tieto utajované skutočnosti EÚ v súlade s bodmi 28 až 40 prílohy III a zaviazal sa dodržiavať kompenzačné opatrenia ustanovené v bezpečnostných pokynoch, ktoré vydal príslušný bezpečnostný orgán, aby sa zabezpečilo, že utajované skutočnosti EÚ sú chránené pred prístupom neoprávnených osôb.

24. Utajované skutočnosti EÚ so stupňom utajenia RESTREINT UE/EU RESTRICTED sa uchovávajú vo vhodnom uzamknutom kancelárskom nábytku v administratívnej zóne alebo zabezpečenom priestore. Dočasne je možné ich uchovávať mimo zabezpečeného priestoru alebo administratívnej zóny za predpokladu, že držiteľ týchto utajovaných skutočností sa zaviazal dodržiavať kompenzačné opatrenia ustanovené v bezpečnostných pokynoch, ktoré vydal príslušný bezpečnostný orgán.

25. S utajovanými skutočnosťami EÚ so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET sa môže manipulovať:

    a) v zabezpečenom priestore;

    b) v administratívnej zóne za predpokladu, že utajované skutočnosti EÚ sú chránené pred prístupom zo strany neoprávnených osôb, alebo

    c) mimo zabezpečeného priestoru alebo administratívnej zóny za predpokladu, že držiteľ týchto utajovaných skutočností:

        i) prenáša tieto utajované skutočnosti EÚ v súlade s bodmi 28 až 40 prílohy III;

        ii) sa zaviazal dodržiavať kompenzačné opatrenia ustanovené v bezpečnostných pokynoch, ktoré vydal príslušný bezpečnostný orgán, aby sa zabezpečilo, že utajované skutočnosti EÚ sú chránené pred prístupom neoprávnených osôb;

        iii) má utajované skutočnosti EÚ vždy pod osobnou kontrolou a

        iv) v prípade dokumentov v papierovej podobe túto skutočnosť oznámil príslušnému registru.

26. Utajované skutočnosti EÚ so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET sa v zabezpečenom priestore uchovávajú v bezpečnostnom úschovnom objekte alebo komorovom trezore.

27. S utajovanými skutočnosťami EÚ so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET sa manipuluje v zabezpečenom priestore.

28. Utajované skutočnosti EÚ so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET sa uchovávajú v zabezpečenom priestore, pričom musí byť splnená jedna z týchto podmienok:

    a) informácie sa uchovávajú v bezpečnostnom úschovnom objekte, ktoré je v súlade s bodom 8 a uplatňujú sa jeden alebo viaceré z týchto dodatočných kontrolných mechanizmov:

        i) nepretržitá ochrana alebo kontroly vykonávané preverenými bezpečnostnými pracovníkmi alebo službukonajúcim personálom;

        ii) schválený IDS v kombinácii so zásahovým bezpečnostným personálom,

    alebo

    b) informácie sa uchovávajú v komorovom trezore vybavenom systémom IDS v kombinácii so zásahovým bezpečnostným personálom.

29. Pravidlá, ktorými sa spravuje prenos utajovaných skutočností EÚ medzi fyzicky chránenými priestormi, sú stanovené v prílohe III.

VI. KONTROLA KĽÚČOV A KOMBINÁCIÍ POUŽÍVANÝCH NA OCHRANU UTAJOVANÝCH SKUTOČNOSTÍ EÚ

30. Príslušný bezpečnostný orgán definuje postupy pre správu kľúčov a nastavení kombinácií na prístup do kancelárií, miestností, komorových trezorov a bezpečnostných úschovných objektov. Tieto postupy sú určené na ochranu proti neoprávnenému prístupu k utajovaným skutočnostiam EÚ.

31. Nastavenia kombinácií do pamäte ukladá čo najmenší možný počet osôb, ktoré ich potrebujú na výkon služobných povinností. Nastavenia kombinácií do bezpečnostných úschovných objektov a komorových trezorov, v ktorých sa uchovávajú utajované skutočnosti EÚ, sa menia:

    a) vždy, keď nastane zmena personálu, ktorý kombináciu pozná;

    b) vždy, keď došlo k vyzradeniu alebo existuje podozrenie vyzradenia;

    c) vždy po vykonaní údržby alebo opravy zámku a

    d) minimálne každých 12 mesiacov.

PRÍLOHA III

SPRÁVA UTAJOVANÝCH SKUTOČNOSTÍ

I. ÚVOD

1. V tejto prílohe sa uvádzajú vykonávacie ustanovenia k článku 9. Stanovujú sa v nej administratívne opatrenia pre správu utajovaných skutočností EÚ počas ich životného cyklu, ktorých cieľom je pomôcť pri odradení od úmyselného alebo náhodného vyzradenia alebo straty takýchto utajovaných skutočností, zistení tohto vyzradenia alebo straty a pri obnove bezpečnosti.

II. SPRÁVA UTAJOVANIA

Stupne utajenia a ich označenie

2. Informácie sa utajujú, ak je to potrebné na ochranu ich dôvernosti.

3. Zodpovednosť za určenie stupňa utajenia v súlade s príslušnými usmerneniami pre utajovanie a za prvú distribúciu utajovanej skutočnosti EÚ nesie jej pôvodca.

4. Stupeň utajenia utajovanej skutočnosti EÚ sa stanovuje podľa článku 2 ods. 2 na základe bezpečnostnej politiky, ktorá sa schváli v súlade s článkom 3 ods. 3.

5. Stupeň utajenia sa uvádza jasne a správne bez ohľadu na to, či má utajovaná skutočnosť EÚ písomnú, ústnu, elektronickú či inú podobu.

6. Jednotlivé časti daného dokumentu (napr. stránky, odseky, oddiely, doplnky, dodatky, pripojenia a prílohy) si môžu vyžadovať rôzny stupeň utajenia a podľa toho sa aj označujú, a to aj keď sa uchovávajú v elektronickej podobe.

7. Celkový stupeň utajenia dokumentu alebo spisu zodpovedá minimálne najvyššiemu stupňu utajenia jeho jednotlivej časti. Keď sa spájajú utajované skutočnosti z rôznych zdrojov, konečný produkt sa preskúma s cieľom určiť celkový stupeň utajenia, pretože si môže vyžadovať vyšší stupeň utajenia ako jeho jednotlivé časti.

8. Dokumenty, ktoré obsahujú časti podliehajúce rozdielnym stupňom utajenia, sa v maximálnej možnej miere usporadúvajú tak, aby sa časti s iným stupňom utajenia dali ľahko identifikovať a v prípade potreby oddeliť.

9. Stupeň utajenia listu alebo sprievodného listu obsahujúceho prílohy zodpovedá najvyššiemu stupňu utajenia príloh. Pôvodca príslušným označením jednoznačne uvedie stupeň jeho utajenia bez príloh, napríklad:

CONFIDENTIEL UE/EU CONFIDENTIAL

Bez prílohy (príloh) RESTREINT UE/EU RESTRICTED

Označenia

10. Okrem niektorého z označení stupňa utajenia podľa článku 2 ods. 2, môžu mať utajované skutočnosti EÚ aj doplňujúce označenie, napríklad:

a) identifikačný znak, ktorým sa označuje pôvodca;

b) upozornenia, kódové slová alebo akronymy, ktorými sa označuje oblasť činnosti, ktorej sa dokument týka, osobitná distribúcia na základe potreby poznať alebo obmedzenie použitia;

c) označenia prístupnosti;

d) prípadne dátum alebo konkrétnu udalosť, keď sa môže znížiť stupeň utajenia alebo utajenie zrušiť.

Skrátené označenia stupňov utajenia

11. Na označenie stupňa utajenia jednotlivých odsekov textu sa môžu používať štandardné skrátené označenia stupňov utajenia. Skratky nenahrádzajú plné označenia stupňov utajenia.

12. Na označenie stupňa utajenia oddielov alebo častí textu, ktoré sú kratšie ako jedna strana, možno v utajených dokumentoch EÚ používať tieto štandardné skratky:

TRÉS SECRET UE/EU TOP SECRET	TS-UE/EU-TS
SECRET UE/EU SECRET	S-UE/EU-S
CONFIDENTIEL UE/EU CONFIDENTIAL	C-UE/EU-C
RESTREINT UE/EU RESTRICTED	R-UE/EU-R

Vytvorenie utajovaných skutočností EÚ

13. Pri vytvorení utajovaného dokumentu EÚ:

a) každá strana sa zreteľne označí stupňom utajenia;

b) každá strana sa očísluje;

c) dokument má priradené referenčné číslo a predmet, ktoré samy osebe nie sú utajovanou skutočnosťou, pokiaľ nie sú ako utajované skutočnosti označené;

d) dokument má dátum;

e) na každej strane dokumentov so stupňom utajenia SECRET UE/EU SECRET a vyššiemu sa uvádza číslo vyhotovenia, pokiaľ sa dokumenty distribuujú vo viacerých vyhotoveniach.

14. Ak na utajovanú skutočnosť EÚ nie je možné uplatniť bod 13, prijmú sa iné primerané opatrenia v súlade s bezpečnostnými usmerneniami podľa článku 6 ods. 2.

Zníženie stupňa utajenia a zrušenie utajenia utajovanej skutočnosti EÚ

15. Ak je to možné, a predovšetkým v prípade utajovaných skutočností so stupňom utajenia RESTREINT UE/EU RESTRICTED pôvodca v čase vytvorenia utajovanej skutočnosti EÚ uvedie, či je možné znížiť jej stupeň utajenia alebo utajenie zrušiť k určitému dátumu alebo po istej udalosti. Pôvodcovia utajovanej skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED uvádzajú dátum alebo konkrétnu udalosť, keď sa utajenie zrušuje, s výnimkou prípadov, keď je neuvedenie riadne odôvodnené.

16. GSR vykonáva pravidelné posúdenie utajovaných skutočností EÚ, ktorých je držiteľom, aby stanovil, či je naďalej potrebný daný stupeň utajenia. GSR zriadi systém, ktorým minimálne každých päť rokov posudzuje stupeň utajenia evidovaných utajovaných skutočností EÚ, ktorých je pôvodcom. Takéto posúdenie nie je potrebné, keď pôvodca hneď na začiatku uviedol, že sa stupeň utajenia danej utajovanej skutočnosti automaticky zníži alebo sa utajenie zruší, a utajovaná skutočnosť bola príslušne označená.

III. EVIDENCIA UTAJOVANÝCH SKUTOČNOSTÍ EÚ NA BEZPEČNOSTNÉ ÚČELY

17. Pre každú organizačnú jednotku GSR a verejnej správy členského štátu, ktorá manipuluje s utajovanými skutočnosťami EÚ, sa určí príslušný register, aby sa zabezpečila manipulácia s utajovanými skutočnosťami EÚ v súlade s týmto rozhodnutím. Registre sa zriadia ako zabezpečené priestory podľa prílohy II.

18. Na účely tohto rozhodnutia znamená evidencia na bezpečnostné účely (ďalej len „evidencia“) uplatňovanie postupov, ktorými sa zaznamenáva životný cyklus veci vrátane jej distribúcie a zničenia.

19. Všetky veci so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a vyšším sa evidujú v určených registroch, keď sa doručia alebo keď opúšťajú organizačnú jednotku.

20. Centrálny register v rámci GSR vedie evidenciu o všetkých utajovaných skutočnostiach, ktoré Rada a GSR poskytujú tretím štátom a medzinárodným organizáciám, ako aj o všetkých utajovaných skutočnostiach, ktoré od tretích štátov alebo medzinárodných organizácií prijímajú.

21. V prípade CIS sa evidenčné postupy môžu vykonávať v rámci samotného CIS.

22. Rada schvaľuje bezpečnostnú politiku pre oblasť evidencie utajovaných skutočností EÚ na bezpečnostné účely.

Registre TRÉS SECRET UE/EU TOP SECRET

23. V členských štátoch a GSR sa určí centrálny register ako centrálny orgán na prijímanie a odosielanie utajovaných skutočností so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET. V prípade potreby sa môžu zriadiť podriadené registre, aby s týmito utajovanými skutočnosťami manipulovali na účely evidencie.

24. Tieto podriadené registre nesmú priamo odosielať dokumenty so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET iným podriadeným registrom toho istého centrálneho registra TRÉS SECRET UE/EU TOP SECRET alebo navonok, pokiaľ to uvedený centrálny register výslovne písomne nepovolí.

IV. ROZMNOŽOVANIE A PREKLAD UTAJOVANÝCH DOKUMENTOV EÚ

25. Dokumenty so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET sa nesmú rozmnožovať alebo prekladať bez predchádzajúceho písomného súhlasu pôvodcu.

26. Keď pôvodca dokumentov so stupňom utajenia SECRET UE/EU SECRET alebo nižším neuviedol nijakú výhradu týkajúcu sa rozmnožovania alebo prekladu, takéto dokumenty sa môžu na základe pokynu držiteľa rozmnožovať alebo prekladať.

27. Bezpečnostné opatrenia uplatniteľné na pôvodný dokument sa uplatňujú aj na kópie a preklady.

V. PRENOS UTAJOVANÝCH SKUTOČNOSTÍ EÚ FYZICKÝMI PROSTRIEDKAMI

28. Na prenos utajovaných skutočností EÚ fyzickými prostriedkami sa vzťahujú ochranné opatrenia uvedené v bodoch 30 až 40. Bez ohľadu na článok 9 ods. 4 pri prenose utajovaných skutočností EÚ na elektronických médiách možno ochranné opatrenia uvedené ďalej doplniť podľa pokynov príslušného bezpečnostného orgánu o príslušné technické protiopatrenia s cieľom minimalizovať riziko straty alebo vyzradenia.

29. Príslušné bezpečnostné orgány v GSR a členských štátoch vydáva pokyny, ktoré sa týkajú prenosu utajovaných skutočností EÚ, v súlade s týmto rozhodnutím.

Prenos v rámci budovy alebo samostatnej skupiny budov

30. Utajovaná skutočnosť EÚ prenášaná v rámci budovy alebo samostatnej skupiny budov sa prenáša zakrytá tak, aby nebolo možné zahliadnuť jej obsah.

31. Utajované skutočnosti so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET sa v rámci budovy alebo samostatnej skupiny budov prenášajú v zabezpečenej obálke, na ktorej je uvedené len meno adresáta.

V rámci EÚ

32. Utajovaná skutočnosť EÚ prenášaná fyzickými prostriedkami medzi budovami alebo objektmi v rámci EÚ sa musí zabaliť tak, aby sa ochránila pred neoprávnenou manipuláciou.

33. Prenos utajovaných skutočností so stupňom utajenia SECRET UE/EU SECRET alebo nižším fyzickými prostriedkami v rámci EÚ sa uskutočňuje takto:

a) podľa potreby vojenským, vládnym alebo diplomatickým kuriérom;

b) ručne pod podmienkou, že:

i) utajovanú skutočnosť EÚ má v prípade, že sa neuloží v súlade s požiadavkami stanovenými v prílohe II, doručovateľ neustále pri sebe;

ii) utajovaná skutočnosť EÚ sa počas cesty neotvorí ani sa s ňou nebude nikto oboznamovať na verejných miestach;

iii) osoby sú poučené o svojej bezpečnostnej zodpovednosti;

iv) osobám sa v prípade potreby poskytne kuriérske osvedčenie;

c) poštovou službou alebo komerčnou kuriérskou službou pod podmienkou, že:

i) je v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi držiteľkou príslušnej FSC;

ii) uplatňujú sa primerané opatrenia v súlade s minimálnymi požiadavkami, ktoré sa stanovia v bezpečnostných usmerneniach podľa článku 6 ods. 2.

V prípade prenosu fyzickými prostriedkami z jedného členského štátu do iného sa písmeno c) vzťahuje len na utajované skutočnosti po stupeň utajenia CONFIDENTIEL UE/EU CONFIDENTIAL.

34. Veci so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET (napr. zariadenia alebo stroje), ktoré nemožno prenášať spôsobom uvedeným v bode 33, sa prepravujú ako náklad obchodnými dopravnými spoločnosťami v súlade s prílohou V.

35. Prenos utajovaných skutočností so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET fyzickými prostriedkami medzi budovami alebo objektmi v rámci jedného členského štátu sa uskutočňuje vojenským, vládnym alebo prípadne diplomatickým kuriérom.

Prenos z EÚ na územie tretieho štátu

36. Utajovaná skutočnosť EÚ prenášaná z EÚ na územie tretieho štátu sa zabalí tak, aby sa ochránila pred neoprávnenou manipuláciou.

37. Fyzický prenos utajovaných skutočností so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET z EÚ na územie tretieho štátu sa uskutočňuje takto:

a) vojenským alebo diplomatickým kuriérom;

b) ručne pod podmienkou, že:

i) sa na obale nachádza úradná pečať alebo je utajovaná skutočnosť zabalená tak, že je zrejmé, že ide o úradnú zásielku, ktorá nepodlieha colnej ani bezpečnostnej kontrole;

ii) osoby majú kuriérske osvedčenie, v ktorom je zásielka uvedená a ktorým sa oprávňujú na jej prenos;

iii) utajovaná skutočnosť EÚ neopustí držbu prenášajúceho, pokiaľ sa neuchováva v súlade s požiadavkami vymedzenými v prílohe II;

iv) utajovaná skutočnosť EÚ sa počas cesty neotvorí ani sa s ňou nikto oboznamuje na verejných miestach a

v) osoby sú poučené o svojej bezpečnostnej zodpovednosti.

38. Prenos informácií so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET, ktoré EÚ sprístupní tretiemu štátu alebo medzinárodnej organizácii, sa uskutočňuje v súlade s príslušnými ustanoveniami dohody o bezpečnosti utajovaných skutočností alebo administratívneho dojednania podľa článku 12 ods. 2 písm. a) alebo b).

39. Utajované skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED sa môžu prenášať aj poštovou alebo komerčnou kuriérskou službou.

40. Prenos utajovaných skutočností so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET z EÚ fyzickými prostriedkami na územie tretieho štátu sa uskutočňuje vojenským alebo diplomatickým kuriérom.

VI. NIČENIE UTAJOVANÝCH DOKUMENTOV EÚ

41. Utajované dokumenty EÚ, ktoré už nie sú potrebné, sa môžu zničiť bez toho, aby boli dotknuté príslušné pravidlá a predpisy týkajúce sa archivácie.

42. Príslušný register ničí dokumenty, ktoré sa musia evidovať v súlade s článkom 9 ods. 2, na základe pokynu držiteľa alebo príslušného orgánu. Denníky a ostatné evidenčné záznamy sa príslušným spôsobom aktualizujú.

43. Pokiaľ ide o utajované dokumenty so stupňom utajenia SECRET UE/EU SECRET alebo TRÉS SECRET UE/EU TOP SECRET, ničenie sa vykonáva za prítomnosti svedka, ktorý je preverený minimálne pre stupeň utajenia dokumentu, ktorý sa ničí.

44. Pracovník registra a v prípade potreby aj svedok, ak sa vyžaduje jeho prítomnosť, podpíšu protokol o zničení, ktorý sa archivuje v registri. Register uchováva protokoly o zničení dokumentov so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET po dobu najmenej desiatich rokov a dokumentov so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET po dobu najmenej piatich rokov.

45. Utajované dokumenty vrátane dokumentov so stupňom utajenia RESTREINT UE/EU RESTRICTED sa ničia metódami, ktoré spĺňajú príslušné normy EÚ alebo rovnocenné normy alebo ktoré boli schválené členskými štátmi podľa národných technických noriem, aby sa zabránilo celkovej alebo čiastočnej rekonštrukcii dokumentu.

46. Médiá na elektronické uchovávanie používané na uchovávanie utajovaných skutočností EÚ sa ničia v súlade s bodom 36 prílohy IV.

VII. INŠPEKCIE A HODNOTIACE NÁVŠTEVY

47. Pojmom „inšpekcia“ sa ďalej označuje každá:

a) inšpekcia v zmysle článku 9 ods. 3 a článku 15 ods. 2 písm. e), f) a g) alebo

b) hodnotiaca návšteva v zmysle článku 12 ods. 5,

ktorých cieľom je posúdiť účinnosť opatrení prijatých na ochranu utajovaných skutočností EÚ.

48. Inšpekcie sa okrem iného vykonávajú na to, aby sa:

a) zabezpečilo dodržiavanie minimálnych noriem ochrany utajovaných skutočností EÚ ustanovených v tomto rozhodnutí;

b) zdôraznil význam bezpečnosti a účinného riadenia rizík u preverovaných subjektov;

c) odporučili protiopatrenia na zníženie konkrétnych následkov v prípade, že dôjde k strate dôvernosti, integrity alebo dostupnosti utajovaných skutočností, a

d) posilnili priebežné bezpečnostné vzdelávacie a informačné programy bezpečnostných orgánov.

49. Rada pred koncom každého kalendárneho roka prijme inšpekčný program uvedený v článku 15 ods. 1 písm. c) na nasledujúci rok. Konkrétne dátumy každej inšpekcie sa stanovia po dohode s dotknutou agentúrou alebo orgánom EÚ, členským štátom, tretím štátom alebo medzinárodnou organizáciou.

Vykonávanie inšpekcií

50. Inšpekcie sa vykonávajú s cieľom skontrolovať všetky príslušné pravidlá, predpisy a postupy preverovaného subjektu a overiť, či sú postupy subjektu v súlade so základnými zásadami a minimálnymi štandardmi ustanovenými v tomto rozhodnutí a v ustanoveniach, ktorými sa spravuje výmena utajovaných skutočností s týmto subjektom.

51. Inšpekcie sa vykonávajú v dvoch etapách. Pred samotnou inšpekciou sa usporiada prípravné zasadnutie, v prípade potreby aj za účasti dotknutého subjektu. Po tomto prípravnom zasadnutí vytvorí inšpekčný tím po dohode s príslušným subjektom podrobný inšpekčný program, ktorý zahŕňa všetky bezpečnostné oblasti. Inšpekčné tímy majú prístup na všetky miesta, kde sa manipuluje s utajovanými skutočnosťami EÚ, najmä do registrov a k prístupovým bodom do CIS.

52. Zodpovednosť za inšpekcie verejnej správy členských štátov nesie spoločný inšpekčný tím GSR a Komisie a tieto inšpekcie sa vykonávajú v plnej spolupráci s úradníkmi preverovaného subjektu.

53. Zodpovednosť za inšpekcie tretích štátov a medzinárodných organizácií nesie spoločný inšpekčný tím GSR a Komisie a tieto inšpekcie sa vykonávajú v plnej spolupráci s úradníkmi preverovaného tretieho štátu alebo medzinárodnej organizácie.

54. Inšpekcie agentúr a orgánov EÚ zriadených na základe hlavy V kapitoly 2 Zmluvy o EÚ, ako aj Europolu a Eurojustu vykonáva Bezpečnostný úrad GSR s pomocou expertov z NSA, na území ktorého sa agentúra alebo orgán nachádza. Na inšpekcii sa môže podieľať riaditeľstvo Európskej komisie pre bezpečnosť (ďalej len „ECSD“ – European Commission Security Directorate), ak si s danou agentúrou alebo orgánom pravidelne vymieňa utajované skutočnosti EÚ.

55. V prípade inšpekcií agentúr a orgánov EÚ zriadených na základe hlavy V kapitoly 2 Zmluvy o EÚ, ako aj Europolu a Eurojustu a tretích štátov a medzinárodných organizácií sa v súlade s podrobnými pravidlami, ktoré schváli Bezpečnostný výbor, vyžiada pomoc a príspevky odborníkov NSA.

Inšpekčné správy

56. Na konci inšpekcie sa preverovanému subjektu predkladajú hlavné závery a odporúčania. Neskôr sa pripraví inšpekčná správa, za ktorú zodpovedá bezpečnostný orgán GSR (Bezpečnostný úrad). Ak sa navrhli nápravné opatrenia alebo odporúčania, do správy by sa mali na odôvodnenie záverov zahrnúť dostatočne podrobné informácie. Správa sa zasiela príslušnému orgánu preverovaného subjektu.

57. V prípade inšpekcií verejnej správy členských štátov:

a) návrh inšpekčnej správy sa zašle dotknutému NSA, ktorý skontroluje, či je obsahovo správna a neobsahuje nijaké skutočnosti so stupňom utajenia vyšším ako RESTREINT UE/EU RESTRICTED;

b) pokiaľ dotknutý NSA členského štátu nepožiada o pozastavenie všeobecnej distribúcie, inšpekčné správy sa zasielajú členom Bezpečnostného výboru a ECSD; správa sa utajuje na stupni utajenia RESTREINT UE/EU RESTRICTED.

Bezpečnostný orgán GSR (Bezpečnostný úrad) zodpovedá za vypracovanie pravidelnej správy, v ktorej sa vyzdvihnú skúsenosti získané počas inšpekcií v členských štátoch v konkrétnom období a ktorú preskúma Bezpečnostný výbor.

58. V prípade hodnotiacich návštev v tretích štátoch a medzinárodných organizáciách sa správa zasiela Bezpečnostnému výboru a ECSD. Táto správa sa utajuje minimálne na stupni utajenia RESTREINT UE/EU RESTRICTED. Každé nápravné opatrenie sa preverí počas nasledujúcej návštevy a podá sa o ňom správa Bezpečnostnému výboru.

59. V prípade inšpekcií agentúr a orgánov EÚ zriadených na základe hlavy V kapitoly 2 Zmluvy o EÚ, ako aj Europolu a Eurojustu sa inšpekčná správa zasiela členom Bezpečnostného výboru a ECSD. Návrh inšpekčnej správy sa zasiela dotknutej agentúre alebo orgánu, ktoré skontrolujú, či je obsahovo správna a neobsahuje skutočnosti so stupňom utajenia vyšším ako RESTREINT UE/EU RESTRICTED. Každé nápravné opatrenie sa preverí počas nasledujúcej návštevy a podá sa o ňom správa Bezpečnostnému výboru.

60. Bezpečnostný orgán GSR vykonáva na účely ustanovené v bode 48 pravidelné inšpekcie organizačných jednotiek GSR.

Inšpekčný kontrolný zoznam

61. Bezpečnostný orgán GSR (Bezpečnostný úrad) vypracuje a aktualizuje inšpekčný kontrolný zoznam obsahujúci body, ktoré je potrebné skontrolovať počas inšpekcie. Tento kontrolný zoznam sa zasiela Bezpečnostnému výboru.

62. Informácie potrebné na vyplnenie kontrolného zoznamu sa získavajú predovšetkým počas inšpekcie od vedúcich bezpečnostných pracovníkov subjektu, v ktorom sa vykonáva inšpekcia. Po vyplnení podrobnými odpoveďami sa kontrolný zoznam po dohode so subjektom, v ktorom sa vykonáva inšpekcia, utajuje. Netvorí súčasť inšpekčnej správy.

PRÍLOHA IV

OCHRANA UTAJOVANÝCH SKUTOČNOSTÍ EÚ, S KTORÝMI SA MANIPULUJE V CIS

I. ÚVOD

1. V tejto prílohe sa uvádzajú vykonávacie ustanovenia článku 10.

2. Na účely bezpečnosti a správneho fungovania operácií v CIS sú dôležité tieto vlastnosti a pojmy IA:

hodnovernosť:	záruka, že informácie sú pravé a pochádzajú zo zdrojov *bona fide*,
dostupnosť:	vlastnosť charakterizovaná prístupnosťou informácií a ich použiteľnosťou na požiadanie oprávneného subjektu,
dôvernosť:	vlastnosť, ktorá znamená, že informácie sa nesprístupnia neoprávneným osobám, subjektom či procesom,
integrita:	vlastnosť charakterizovaná zabezpečením presnosti a úplnosti informácií a majetku,
nespochybniteľnosť:	schopnosť preukázať, že sa činnosť alebo udalosť uskutočnila, takže túto činnosť alebo udalosť nie je možné následne poprieť.

II. ZÁSADY INFORMAČNEJ BEZPEČNOSTI

3. Ustanovenia uvedené nižšie predstavujú základ bezpečnosti každého CIS, v ktorom sa manipuluje s utajovanými skutočnosťami EÚ. Podrobné požiadavky, ktorými sa vykonávajú tieto ustanovenia, sa vymedzia v bezpečnostných politikách a bezpečnostných usmerneniach pre IA.

Riadenie bezpečnostných rizík

4. Riadenie bezpečnostných rizík tvorí neoddeliteľnú súčasť činností pri definovaní, rozvíjaní, prevádzke a údržbe CIS. Riadenie rizík (hodnotenie, zabezpečenie, akceptácia, oznamovanie) spoločne vykonávajú ako nepretržitý proces zástupcovia vlastníkov systému, projektových orgánov, operačných orgánov a orgánov schvaľujúcich bezpečnosť, ktoré uplatňujú overený, transparentný a plne pochopiteľný proces vyhodnotenia rizík. Na začiatku procesu riadenia rizík sa jednoznačne vymedzí rozsah CIS a jeho majetku.

5. Príslušné orgány preskúmajú potenciálne hrozby pre CIS a zabezpečujú aktualizované a presné posúdenie hrozieb, ktoré zohľadňuje aktuálne operačné prostredie. Nepretržite aktualizujú svoje poznatky o slabinách a pravidelne preverujú posúdenie slabín s cieľom reagovať na meniace sa prostredie v oblasti informačných technológií (IT).

6. Cieľom zabezpečenia sa proti bezpečnostným rizikám je uplatňovať súbor bezpečnostných opatrení, čím sa zabezpečí rovnováha medzi požiadavkami používateľov, nákladmi a zvyškovým bezpečnostným rizikom.

7. Špecifické požiadavky, rozsah a miera podrobnosti stanovená príslušným SAA na certifikáciu CIS zodpovedajú vyhodnotenému riziku, pričom sa zohľadňujú všetky relevantné faktory vrátane stupňa utajenia utajovaných skutočností, s ktorými sa v CIS manipuluje. Certifikácia zahŕňa formálne vyhlásenie o zvyškovom riziku a akceptáciu zvyškového rizika zo strany zodpovedného orgánu.

Bezpečnosť počas celého životného cyklu CIS

8. Zaistenie bezpečnosti predstavuje požiadavku, ktorá musí byť splnená počas celého životného cyklu CIS od jeho spustenia do prevádzky po vyradenie.

9. Pre každú fázu životného cyklu sa stanoví úloha a interakcia každého účastníka podieľajúceho sa na činnosti CIS, pokiaľ ide o jeho bezpečnosť.

10. Každý CIS vrátane technických a iných bezpečnostných opatrení podlieha počas certifikácie bezpečnostnému testovaniu, ktorého cieľom je zaručiť, že sa dosiahla náležitá úroveň bezpečnosti, a overiť, že je správne implementovaný, integrovaný a konfigurovaný.

11. Počas prevádzky a údržby CIS, ako aj v prípade vzniku výnimočných okolností sa pravidelne vykonávajú bezpečnostné hodnotenia, inšpekcie a previerky.

12. Vývoj bezpečnostnej dokumentácie pre CIS počas jeho životného cyklu je neoddeliteľnou súčasťou procesu riadenia zmien a konfigurácií.

Najlepšie postupy

13. GSR a členské štáty spolupracujú na vypracovaní najlepších postupov na ochranu utajovaných skutočností EÚ, s ktorými sa manipuluje v CIS. Najlepšie postupy vymedzujú technické, fyzické, organizačné a procesné bezpečnostné opatrenia pre CIS s overenou účinnosťou proti daným ohrozeniam a slabinám.

14. Pri ochrane utajovaných skutočností EÚ, s ktorými sa manipuluje v CIS, sa využívajú skúsenosti, ktoré získali subjekty zabezpečujúce IA v EÚ i mimo nej.

15. Šírenie a následné zavedenie najlepších postupov pomáhajú dosiahnuť rovnocennú úroveň bezpečnosti rôznych CIS, ktoré prevádzkujú GSR a členské štáty, ktoré manipulujú s utajovanými skutočnosťami EÚ.

Hĺbková ochrana

16. Na zníženie rizika pre CIS sa zavádza škála technických a iných bezpečnostných opatrení, ktoré sa organizujú do viacerých vrstiev. Tieto opatrenia zahŕňajú:

a) *odradenie:* bezpečnostné opatrenia zamerané na odradenie protivníka od plánovania útoku na CIS;

b) *predchádzanie:* bezpečnostné opatrenia zamerané na zabránenie alebo zastavenie útoku na CIS;

c) *detekciu:* bezpečnostné opatrenia zamerané na zistenie výskytu útoku na CIS;

d) *odolnosť:* bezpečnostné opatrenia zamerané na obmedzenie následkov útoku na minimálny súbor informácií/majetku CIS a zabránenie ďalším škodám a

e) *obnovu:* bezpečnostné opatrenia zamerané na znovunastolenie bezpečnej situácie CIS.

Stupeň prísnosti takýchto bezpečnostných opatrení sa stanovuje na základe vyhodnotenia rizika.

17. Príslušné orgány zabezpečujú spôsobilosť reagovať na incidenty, ktoré môžu prekročiť organizačné a štátne hranice, koordinovať svoju reakciu a vymieňať si informácie o týchto incidentoch a súvisiacich rizikách (spôsobilosť núdzovej reakcie v súvislosti s počítačmi).

Zásada minimality a najnižších práv

18. S cieľom vyhnúť sa zbytočnému riziku sa implementujú len základné funkcie, zariadenia a služby potrebné na splnenie operačných požiadaviek.

19. Aby sa obmedzili akékoľvek škody vyplývajúce z porúch, omylov alebo neoprávneného využívania zdrojov CIS, majú používatelia CIS a automatizovaných procesov len taký prístup, práva alebo oprávnenia, ktoré potrebujú na plnenie svojich úloh.

20. Postupy na účely evidencie, ktoré vykonáva CIS, sa v prípade potreby preveria v rámci certifikačného postupu.

Informovanosť o informačnej bezpečnosti

21. Prvou obrannou líniou bezpečnosti CIS je informovanosť o rizikách a dostupných bezpečnostných opatreniach. Najmä všetci členovia personálu, ktorí prichádzajú do kontaktu s CIS počas jeho životného cyklu, majú byť poučení:

a) že bezpečnostné zlyhanie môže závažne poškodiť CIS;

b) o potenciálnych škodách pre tretie strany, ktoré môžu vyplynúť zo vzájomného prepojenia a vzájomnej závislosti, a

c) o svojej osobnej zodpovednosti za bezpečnosť CIS, ktorá sa odvíja od ich úloh v rámci systémov a procesov.

22. Na zabezpečenie pochopenia bezpečnostných povinností sa povinne vykonáva informačno-bezpečnostné vzdelávanie a odborná príprava pre dotknutý personál, ako aj vyšších riadiacich pracovníkov a používateľov CIS.

Hodnotenie a schvaľovanie bezpečnostných produktov IT

23. Požadovaná úroveň spoľahlivosti bezpečnostných opatrení, vymedzená ako úroveň ubezpečenia, sa stanovuje na základe procesu riadenia rizík a v súlade s príslušnými bezpečnostnými politikami a bezpečnostnými usmerneniami.

24. Tento stupeň spoľahlivosti sa preverí pomocou medzinárodne uznávaných alebo vnútroštátne schválených postupov a metodík. Tie predovšetkým zahŕňajú hodnotenie, kontroly a audit.

25. Kryptografické produkty na ochranu utajovaných skutočností EÚ vyhodnotí a schváli vnútroštátny CAA členského štátu.

26. Predtým, ako sa v súlade s článkom 10 ods. 6 odporučia na schválenie Rade alebo generálnemu tajomníkovi, tieto kryptografické produkty najprv prejdú úspešným hodnotením druhou stranou vykonaným náležite kvalifikovaným orgánom (ďalej len „AQUA“ – Appropriately Qualified Authority) členského štátu, ktorý nebol zapojený do projektu ani výroby tohto zariadenia. Podrobnosť hodnotenia druhou stranou závisí od predpokladaného najvyššieho stupňa utajenia utajovaných skutočností EÚ, ktoré sa majú týmito produktmi chrániť. Rada schváli bezpečnostnú politiku pre oblasť hodnotenia a schvaľovania kryptografických produktov.

27. Ak si to vyžadujú osobitné operačné okolnosti, môže Rada, prípadne generálny tajomník na základe odporúčania Bezpečnostného výboru upustiť od požiadaviek uvedených v bodoch 25 alebo 26 a udeliť v súlade s postupom podľa článku 10 ods. 6 dočasné schválenie na určité obdobie.

28. AQUA je CAA členského štátu certifikovaný na základe kritérií stanovených Radou na vykonanie druhého hodnotenia kryptografických produktov na ochranu utajovaných skutočností EÚ.

29. Rada schvaľuje bezpečnostnú politiku pre oblasť kvalifikovania a schvaľovania nekryptografických bezpečnostných produktov IT.

Prenos v zabezpečených priestoroch

30. Bez ohľadu na ustanovenia tohto rozhodnutia sa pri prenose utajovaných skutočností EÚ, ktorý sa uskutočňuje len v rámci zabezpečených priestorov, môže používať nešifrovaná distribúcia alebo šifrovanie na nižšej úrovni, ak to umožňuje výsledok procesu riadenia rizík a ak to schválil SAA.

Bezpečné prepojenie CIS

31. Na účely tohto rozhodnutia znamená prepojenie priame spojenie dvoch alebo viacerých systémov IT na účely spoločného využívania údajov a iných informačných zdrojov (napr. komunikačných), ktoré môže byť jednosmerné alebo viacsmerné.

32. CIS v prvej fáze pristupuje ku každému pripojenému systému IT ako nedôveryhodnému a na výmenu utajovaných skutočností uplatňuje ochranné opatrenia.

33. Všetky prepojenia CIS s iným systémom IT spĺňajú tieto základné požiadavky:

    a) funkčné alebo prevádzkové požiadavky takýchto prepojení stanovujú a schvaľujú príslušné orgány;

    b) prepojenie podlieha procesu riadenia rizík a certifikácii a musí ho schváliť príslušný SAA a

    c) na perimetri všetkých CIS sa zavedie obvodová ochrana (ďalej len „BPS“ – Boundary Protection Services).

34. Certifikovaný CIS nesmie mať nijaké prepojenie s nechránenou alebo verejnou sieťou okrem prípadu, ak má CIS schválenú ochranu BPS nainštalovanú na tento účel na rozhraní medzi týmto CIS a nechránenou alebo verejnou sieťou. Bezpečnostné opatrenia týkajúce sa takéhoto prepojenia prehodnocuje príslušný IAA a schvaľuje príslušný SAA.

    Keď sa nechránená alebo verejná sieť používa výhradne ako nosič dát, ktoré sú šifrované kryptografickým produktom schváleným v súlade s článkom 10, toto spojenie sa nepovažuje za prepojenie.

35. Priame alebo kaskádové prepojenie CIS certifikovaného na manipuláciu s utajovanými skutočnosťami so stupňom utajenia TRÉS SECRET UE/EU TOP SECRET s nechránenou alebo verejnou sieťou je zakázané.

Elektronické médiá na uchovávanie

36. Elektronické médiá na uchovávanie sa zničia v súlade s postupom schváleným príslušným bezpečnostným orgánom.

37. Elektronické médiá na uchovávanie možno opätovne používať a ich stupeň utajenia znížiť alebo zrušiť v súlade s postupom ustanoveným v súlade s článkom 6 ods. 1.

Núdzové situácie

38. Bez ohľadu na ustanovenia tohto rozhodnutia sa môžu v núdzových situáciách, ako napríklad pri bezprostredne hroziacej kríze alebo počas krízy, vojnového stavu alebo pri výnimočných operačných okolnostiach, uplatňovať osobitné postupy uvedené nižšie.

39. Utajované skutočnosti EÚ sa môžu so súhlasom príslušného orgánu prenášať šifrované kryptografickými produktmi, ktoré boli schválené pre nižší stupeň utajenia, alebo nešifrované, pokiaľ by akékoľvek zdržanie spôsobilo škody, ktoré jednoznačne prevyšujú škodu spôsobenú neoprávnenou manipuláciou s utajovanou vecou, a ak

a) odosielateľ a príjemca nemajú požadované šifrovacie zariadenie alebo nemajú nijaké šifrovacie zariadenie a

b) utajovanú vec nie je možné včas doručiť inými prostriedkami.

40. Utajované skutočnosti prenášané za okolností uvedených v bode 38 nesmú mať žiadne označenia alebo odkazy, ktorými by sa odlišovali od neutajovanej skutočnosti alebo skutočnosti , ktorá sa môže chrániť dostupným šifrovacím produktom. Príjemcovia sa o stupni utajenia skutočnosti bezodkladne informujú iným spôsobom.

41. V prípade uplatnenia ustanovení bodu 38 sa následne zasiela správa príslušnému orgánu a Bezpečnostnému výboru.

III. FUNKCIE A ORGÁNY INFORMAČNEJ BEZPEČNOSTI

42. V členských štátoch a GSR sa zriadia nižšie uvedené funkcie v oblasti IA. Tieto funkcie nemusia byť združené v jedinej organizačnej jednotke. Majú samostatné mandáty. Tieto funkcie a s nimi spojené povinnosti sa však môžu spojiť alebo zlúčiť do jednej organizačnej jednotky alebo rozdeliť do rôznych organizačných jednotiek pod podmienkou, že nedochádza ku vnútornému konfliktu záujmov alebo úloh.

Orgán pre informačnú bezpečnosť

43. IAA zodpovedá za:

a) vypracúvanie bezpečnostnej politiky a bezpečnostných usmernení v oblasti IA a monitorovanie ich účinnosti a vhodnosti;

b) ochranu a správu technických informácií týkajúcich sa kryptografických produktov;

c) zabezpečenie, že zvolené opatrenia IA na ochranu utajovaných skutočností EÚ spĺňajú príslušné politiky, ktorými sa spravuje ich vhodnosť a výber;

d) zabezpečenie, že kryptografické produkty sa vyberajú v súlade s politikami, ktorými sa spravuje ich vhodnosť a výber;

e) koordináciu odbornej prípravy a informovania o IA;

f) konzultáciu s poskytovateľom systému, bezpečnostnými subjektmi a zástupcami používateľov o bezpečnostných politikách a bezpečnostných usmerneniach pre IA a

g) zabezpečenie, že v odbornej podskupine Bezpečnostného výboru pre otázky IA sú kvalifikovaní odborníci.

Orgán pre TEMPEST

44. Orgán pre TEMPEST (ďalej len „TA“) zodpovedá za zabezpečenie súladu CIS s politikami a usmerneniami TEMPEST-u. Schvaľuje protiopatrenia TEMPEST-u pre zariadenia a produkty na ochranu utajovaných skutočností EÚ pre určený stupeň utajenia v danom operačnom prostredí.

Kryptografický schvaľovací orgán

45. Kryptografický schvaľovací orgán (ďalej len „CAA“ – Crypto Approval Authority) zabezpečuje, že kryptografické produkty sú v súlade s národnou kryptografickou politikou, resp. kryptografickou politikou Rady. Schvaľuje kryptografické produkty na ochranu utajovaných skutočností EÚ pre určený stupeň utajenia v danom operačnom prostredí. Pokiaľ ide o členské štáty, CAA je okrem toho zodpovedný za posudzovanie kryptografických produktov.

Kryptografický distribučný orgán

46. Kryptografický distribučný orgán (CDA) zodpovedá za:

a) správu a evidenciu kryptografických materiálov EÚ;

b) zabezpečenie, že sa uplatňujú vhodné postupy a kanály vytvorené na vedenie evidencie, bezpečnú manipuláciu, uchovávanie a distribúciu všetkých kryptografických materiálov EÚ, a

c) zabezpečenie postúpenia kryptografického materiálu EÚ osobe alebo od osoby a službe alebo od služby, ktorá ho používa.

Orgán bezpečnostnej certifikácie

47. SAA každého systému zodpovedá za:

a) zabezpečenie, že CIS spĺňa príslušné bezpečnostné politiky a bezpečnostné usmernenia, vydávanie potvrdenia o schválení CIS na účely manipulácie s utajovanými skutočnosťami EÚ do stanovenej úrovne utajenia v danom operačnom prostredí, stanovenie podmienok certifikácie a kritérií, za ktorých sa vyžaduje opätovné schválenie;

b) ustanovenie postupu bezpečnostnej certifikácie v súlade s príslušnými politikami a jednoznačné stanovenie podmienok pre schválenie CIS v jeho právomoci;

c) vymedzenie stratégie bezpečnostnej certifikácie, v ktorej sa stanoví úroveň podrobnosti týkajúca sa certifikácie zodpovedajúca požadovanej úrovni bezpečnosti;

d) preverovanie a schvaľovanie dokumentácie týkajúcej sa bezpečnosti, ktorá zahŕňa vyhlásenia o riadení rizík a o zvyškovom riziku, vyhlásenia o bezpečnostných požiadavkách špecifických pre systém (ďalej len „SSRS“ – System-Specific Security Requirement Statement), dokumentáciu overenia realizácie bezpečnosti a operačné bezpečnostné postupy (ďalej len „SecOPs“ – Security Operating Procedures), a zabezpečenie, že táto dokumentácia je v súlade s bezpečnostnými predpismi a politikami Rady;

e) kontrolu zavedenia bezpečnostných opatrení vzťahujúcich sa na CIS, pričom vykonáva bezpečnostné hodnotenia, inšpekcie alebo previerky alebo pomáha pri nich;

f) stanovovanie bezpečnostných požiadaviek (napríklad pre stupne previerky personálnej bezpečnosti) pre citlivé pozície vzhľadom na CIS;

g) potvrdenie výberu schválených kryptografických produktov a produktov TEMPEST, ktoré sa majú použiť na dosiahnutie bezpečnosti CIS;

h) schvaľovanie, prípadne účasť na spoločnom schválení pripojenia CIS k inému CIS a

i) konzultáciu o riadení bezpečnostných rizík, najmä zvyškového rizika, a podmienkach vydania potvrdenia o schválení s poskytovateľom systému, bezpečnostnými subjektmi a zástupcami používateľov.

48. SAA Generálneho sekretariátu Rady je zodpovedný za certifikáciu všetkých CIS v rámci pôsobnosti GSR.

49. Príslušný SAA členského štátu je zodpovedný za certifikáciu CIS a jeho komponentov, ktoré sa používajú v rámci pôsobnosti členského štátu.

50. Spoločná komisia pre bezpečnostnú certifikáciu (ďalej len „SAB“ – Security Accreditation Board) je zodpovedná za certifikáciu CIS, ktoré patria zároveň do pôsobnosti SAA Generálneho sekretariátu Rady aj SAA členských štátov. Skladá sa zo zástupcu SAA každého členského štátu a na jej zasadnutiach je prítomný zástupca SAA Komisie. Iné subjekty s uzlami v CIS sa prizývajú na zasadnutie, keď sa rokuje o danom systéme.

Predsedom SAB je zástupca SAA Generálneho sekretariátu Rady. SAB sa uznáša konsenzom zástupcov SAA inštitúcií, členských štátov a iných subjektov s uzlami v danom CIS. Podáva pravidelné správy o svojej činnosti Bezpečnostnému výboru a rovnako mu oznamuje všetky vydané potvrdenia o certifikácii.

Operačný orgán pre informačnú bezpečnosť

51. Operačný orgán pre IA každého systému zodpovedá za:

a) vytváranie v rámci procesu certifikácie CIS bezpečnostnej dokumentácie v súlade s bezpečnostnými politikami a bezpečnostnými usmerneniami, najmä SSRS vrátane vyhlásenia o zvyškovom riziku, postupoch SecOPs a šifrovacej stratégii;

b) účasť na výbere a testovaní technických bezpečnostných opatrení, zariadení a softvéru špecifických pre daný systém a dohľad nad ich zavádzaním a zabezpečenie ich bezpečnej inštalácie, konfigurácie a údržby v súlade s príslušnou bezpečnostnou dokumentáciou;

c) účasť na výbere bezpečnostných opatrení a zariadení TEMPEST, pokiaľ sa požadujú v SSRS, a v spolupráci s TA zabezpečenie ich bezpečnej inštalácie a údržby;

d) monitorovanie vykonávania a uplatňovania postupov SecOPs a v prípade potreby smie preniesť na majiteľa systému povinnosti týkajúce sa operačnej bezpečnosti;

e) správu kryptografických produktov a manipuláciu s nimi, zabezpečenie úschovy kryptografických a kontrolovaných položiek, a ak sa to požaduje, zabezpečenie generovania kryptografických premenných parametrov;

f) vykonávanie bezpečnostných analytických previerok a testov najmä s cieľom pripraviť príslušné správy o rizikách v zmysle požiadaviek SAA;

g) poskytovanie odbornej prípravy o IA pre daný CIS;

h) zavádzanie a fungovanie bezpečnostných opatrení špecifických pre CIS.

PRÍLOHA V

PRIEMYSELNÁ BEZPEČNOSŤ

I. ÚVOD

1. V tejto prílohe sa uvádzajú vykonávacie ustanovenia k článku 11. Obsahuje všeobecné bezpečnostné ustanovenia uplatniteľné na priemyselné alebo iné subjekty počas rokovaní pred uzavretím zmluvy a počas celého životného cyklu utajovanej zmluvy s GSR.

2. Rada schvaľuje politiku pre oblasť priemyselnej bezpečnosti, v ktorej uvádza predovšetkým podrobné požiadavky týkajúce sa FSC, bezpečnostných doložiek („SAL" – Security Aspects Letter), návštev a prenosu utajovaných skutočností EÚ.

II. BEZPEČNOSTNÉ PRVKY V UTAJOVANEJ ZMLUVE

Usmernenia pre určovanie stupňa utajenia (SCG – Security Classification Guide)

3. Pred začatím výberového konania alebo uzavretím utajovanej zmluvy určí GSR ako verejný obstarávateľ stupeň utajenia všetkých utajovaných skutočností, ktoré sa majú poskytnúť predkladateľom ponuky a dodávateľom, ako aj stupeň utajenia všetkých utajovaných skutočností, ktoré dodávateľ vytvorí. GSR na tento účel pripraví SCG, ktoré sa budú uplatňovať pri plnení zmluvy.

4. Pri určovaní stupňa utajenia rôznych prvkov utajenej zmluvy sa uplatňujú tieto zásady:

   a) GSR pri príprave SCG zohľadňuje všetky príslušné bezpečnostné hľadiská vrátane stupňa utajenia, ktorý utajovanej skutočnosti, poskytnutej a schválenej na použitie v súvislosti so zmluvou, určil jej pôvodca;

   b) celkový stupeň utajenia zmluvy nesmie byť nižší ako najvyšší stupeň utajenia ktoréhokoľvek z jej prvkov a

   c) ak je to relevantné, v prípade akejkoľvek zmeny, pokiaľ ide o stupeň utajenia utajovaných skutočností, ktoré dodávatelia vytvorili alebo ktoré sa im poskytli počas plnenia zmluvy, alebo v prípade následných zmien v SCG, GSR sa spojí s NSA/DSA členských štátov alebo s akýmkoľvek iným dotknutým príslušným bezpečnostným orgánom.

Bezpečnostná doložka (SAL)

5. Bezpečnostné požiadavky špecifické pre zmluvu sa opíšu v SAL. Ak je to vhodné, SAL obsahuje SCG a tvorí neoddeliteľnú súčasť utajovanej zmluvy alebo subdodávateľskej zmluvy.

6. SAL obsahuje ustanovenia, podľa ktorých musí dodávateľ a/alebo subdodávateľ dodržiavať minimálne normy ustanovené v tomto rozhodnutí. Nedodržanie týchto minimálnych noriem sa môže považovať za dostatočný dôvod na vypovedanie zmluvy.

Bezpečnostné pokyny pre program/projekt (PSI)

7. V závislosti od rozsahu programov alebo projektov, ktorých súčasťou je prístup k utajovaným skutočnostiam EÚ alebo manipulácia s nimi alebo ich uchovávanie, verejný obstarávateľ určený na riadenie programu alebo projektu môže pripraviť špecifické bezpečnostné pokyny pre program/projekt (ďalej len „PSI" – Programme/Project Security Instructions). PSI musí schváliť NSA/DSA alebo akýkoľvek iný príslušný bezpečnostný orgán členských štátov zapojený do programu/projektu a môžu obsahovať dodatočné bezpečnostné požiadavky.

III. PREVIERKA BEZPEČNOSTI ZARIADENIA (FSC)

8. NSA alebo DSA alebo akýkoľvek iný príslušný bezpečnostný orgán členského štátu udelí FSC, aby v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi preukázal, že priemyselný alebo iný subjekt je schopný vo svojich zariadeniach chrániť utajované skutočnosti EÚ na príslušnom stupni utajenia (CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET). Skôr, ako sa dodávateľovi alebo subdodávateľovi, alebo potenciálnemu dodávateľovi alebo subdodávateľovi poskytne alebo udelí prístup k utajovaným skutočnostiam EÚ, FSC sa predloží GSR ako verejnému obstarávateľovi.

9. Príslušný NSA alebo DSA pri vydávaní FSC aspoň:

   a) zhodnotí integritu priemyselného alebo iného subjektu;

   b) zhodnotí vlastníctvo, kontrolu alebo možný nenáležitý vplyv, ktorý možno považovať za bezpečnostné riziko;

c) overí, že priemyselný alebo akýkoľvek iný subjekt v zariadení zaviedol bezpečnostný systém, ktorý sa zahŕňa všetky príslušné bezpečnostné opatrenia potrebné na ochranu informácií a vecí so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET v súlade s požiadavkami ustanovenými v tomto rozhodnutí;

d) overí, či sa status personálnej bezpečnosti vedenia, majiteľov a zamestnancov, ktorí potrebujú prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET, stanovil v súlade s požiadavkami ustanovenými v tomto rozhodnutí;

e) overí, či priemyselný alebo akýkoľvek iný subjekt vymenoval úradníka pre bezpečnosť zariadenia, ktorý zodpovedá vedeniu za dodržiavanie bezpečnostných požiadaviek v rámci tohto subjektu.

10. V prípade potreby GSR ako verejný obstarávateľ oznámi príslušnému NSA/DSA alebo akémukoľvek inému príslušnému bezpečnostnému orgánu, že FSC je potrebné počas fázy pred uzavretím zmluvy alebo na účely plnenia zmluvy. FSC alebo PSC sa vyžaduje počas fázy pred uzavretím zmluvy, ak sa počas predkladania ponúk musia poskytnúť utajované skutočnosti so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET.

11. Verejný obstarávateľ neuzavrie utajovanú zmluvu s predkladateľom ponuky, ktorého uprednostňuje, kým mu NSA/DSA alebo akýkoľvek iný príslušný bezpečnostný orgán členského štátu, v ktorom má dotknutý dodávateľ alebo subdodávateľ sídlo, nepotvrdí, že príslušné FSC bolo v potrebných prípadoch vydané.

12. Príslušný NSA/DSA alebo akýkoľvek iný príslušný bezpečnostný orgán, ktorý vydal FSC, oznamuje GSR ako verejnému obstarávateľovi všetky zmeny, ktoré majú vplyv na FSC. V prípade subdodávateľskej zmluvy sa NSA/DSA alebo akýkoľvek iný príslušný bezpečnostný orgán informuje zodpovedajúcim spôsobom.

13. Odňatie FSC príslušným NSA/DSA alebo akýmkoľvek iným príslušným bezpečnostným orgánom predstavuje pre GSR ako verejného obstarávateľa dostatočný dôvod na vypovedanie utajovanej zmluvy alebo na vylúčenie účastníka zo súťaže.

IV. UTAJOVANÉ ZMLUVY A SUBDODÁVATEĽSKÉ ZMLUVY

14. V prípade, že sa utajované skutočnosti EÚ predkladateľovi ponuky poskytujú počas fázy pred uzavretím zmluvy, výzva obsahuje ustanovenie, že predkladateľ ponuky, ktorý nepredloží ponuku alebo nie je vybratý, je povinný v stanovenej lehote vrátiť všetky utajované dokumenty.

15. Po uzavretí utajovanej zmluvy alebo subdodávateľskej zmluvy GSR ako verejný obstarávateľ oznámi NSA/DSA alebo akémukoľvek inému príslušnému bezpečnostnému orgánu daného dodávateľa alebo subdodávateľa bezpečnostné ustanovenia utajovanej zmluvy.

16. Keď sa takéto zmluvy vypovedajú, GSR ako verejný obstarávateľ (a/alebo NSA/DSA alebo prípadne akýkoľvek iný príslušný bezpečnostný orgán v prípade subdodávateľskej zmluvy) to bezodkladne oznámi NSA/DSA alebo akémukoľvek inému príslušnému bezpečnostnému orgánu členského štátu, v ktorom má dodávateľ alebo subdodávateľ sídlo.

17. Od dodávateľov alebo subdodávateľov sa spravidla požaduje, aby po ukončení utajovanej zmluvy alebo subdodávateľskej zmluvy vrátili verejnému obstarávateľovi všetky utajované skutočnosti EÚ, ktorých sú držiteľmi.

18. V SAL sa ustanovia špecifické ustanovenia týkajúce sa manipulácie s utajovanými skutočnosťami EÚ počas plnenia zmluvy alebo po jej ukončení.

19. Ak sa dodávateľovi alebo subdodávateľovi povolí, aby si ponechal utajované skutočnosti EÚ po ukončení zmluvy, dodávateľ alebo subdodávateľ musí naďalej spĺňať minimálne normy uvedené v tomto rozhodnutí a chrániť dôvernosť utajovaných skutočností EÚ.

20. Podmienky, za ktorých môže dodávateľ uzatvárať subdodávateľské zmluvy, sa musia vymedziť vo výzve na predkladanie ponúk a v zmluve.

21. Dodávateľ musí získať povolenie od GSR ako verejného obstarávateľa skôr, ako zadá niektorú z častí utajovanej zmluvy subdodávateľom. S priemyselnými alebo inými subjektmi so sídlom v štáte, ktorý nie je členským štátom EÚ a neuzavrel s EÚ dohodu o bezpečnosti utajovaných skutočností, sa nesmie uzavrieť žiadna subdodávateľská zmluva.

22. Dodávateľ je zodpovedný za zabezpečenie toho, aby boli všetky subdodávateľské činnosti realizované v súlade s minimálnymi normami stanovenými v tomto rozhodnutí, a nesmie poskytnúť utajované skutočnosti EÚ subdodávateľovi bez predchádzajúceho písomného súhlasu verejného obstarávateľa.

23. Pokiaľ ide o utajované skutočnosti EÚ, ktoré vytvoril alebo s ktorými manipuluje dodávateľ alebo subdodávateľ, práva pôvodcu vykonáva verejný obstarávateľ.

V. NÁVŠTEVY VYKONÁVANÉ V SÚVISLOSTI S UTAJOVANÝMI ZMLUVAMI

24. Ak GSR, dodávatelia a subdodávatelia potrebujú na účely plnenia utajovanej zmluvy prístup k utajovaným skutočnostiam so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL a SECRET UE/EU SECRET v objektoch druhej strany, spoločne organizujú návštevy svojich objektov v spolupráci s NSA/DSA alebo akýmkoľvek iným dotknutým príslušným bezpečnostným orgánom. V súvislosti so špecifickými projektmi však NSA/DSA môžu súhlasiť aj s postupom, pri ktorom sa takéto návštevy môžu organizovať priamo.

25. Všetci návštevníci sú držiteľmi príslušných PSC a majú potrebu poznať na účely prístupu k utajovaným skutočnostiam EÚ, ktoré sa týkajú zmluvy s GSR.

26. Návštevníkom sa udelí prístup len k utajovaným skutočnostiam EÚ, ktoré sa týkajú účelu návštevy.

VI. PRENOS UTAJOVANÝCH SKUTOČNOSTÍ EÚ

27. Pokiaľ ide o prenos utajovaných skutočností EÚ elektronickými prostriedkami, uplatňujú sa príslušné ustanovenia článku 10 a prílohy IV.

28. Pokiaľ ide o prenos utajovaných skutočností EÚ fyzickými prostriedkami, uplatňujú sa príslušné ustanovenia prílohy III v súlade s vnútroštátnymi zákonmi a inými právnymi predpismi.

29. Pri určovaní bezpečnostných opatrení pre prepravu utajovaných vecí ako nákladu sa uplatňujú tieto zásady:

a) bezpečnosť sa zaisťuje počas všetkých etáp prepravy z miesta pôvodu do miesta konečného určenia;

b) úroveň ochrany zásielky sa určuje podľa stupňa utajenia veci s najvyšším stupňom utajenia, ktorá sa v nej nachádza;

c) pre spoločnosti poskytujúce prepravu sa musí získať FSC príslušného stupňa. V takýchto prípadoch je personál, ktorý so zásielkou manipuluje, bezpečnostne preverený v súlade s prílohou I;

d) pred každou cezhraničnou prepravou veci so stupňom utajenia CONFIDENTIEL UE/EU CONFIDENTIAL alebo SECRET UE/EU SECRET odosielateľ vypracuje plán prepravy, ktorý schvália NSA/DSA alebo akýkoľvek iný dotknutý príslušný bezpečnostný orgán;

e) cesty sa vykonávajú priamo z miesta pôvodu do miesta určenia a uskutočňujú sa v čo najkratšom čase, aký umožňujú okolnosti;

f) ak je to možné, trasy ciest by mali prechádzať len cez územia členských štátov. Cesty cez tretie štáty by sa mali realizovať len v prípade, ak ich povolia NSA/DSA alebo akýkoľvek iný príslušný bezpečnostný orgán štátov odosielateľa aj príjemcu.

VII. POSTÚPENIE UTAJOVANÝCH SKUTOČNOSTÍ EÚ DODÁVATEĽOM, KTORÍ SA NACHÁDZAJÚ V TRETÍCH ŠTÁTOCH

30. Postúpenie utajovaných skutočností EÚ dodávateľom a subdodávateľom, ktorí sa nachádzajú v tretích štátoch, sa uskutočňuje v súlade s bezpečnostnými opatreniami dohodnutými medzi GSR ako verejným obstarávateľom a NSA/DSA dotknutého tretieho štátu, v ktorom má dodávateľ sídlo.

VIII. MANIPULÁCIA S UTAJOVANÝMI SKUTOČNOSŤAMI SO STUPŇOM UTAJENIA RESTREINT UE/EU RESTRICTED A ICH UCHOVÁVANIE

31. GSR ako verejný obstarávateľ môže podľa potreby v spolupráci s NSA/DSA členského štátu a na základe zmluvných ustanovení vykonávať návštevy zariadení dodávateľa/subdodávateľa s cieľom preveriť, či sa uplatňujú príslušné bezpečnostné opatrenia potrebné na ochranu utajovaných skutočností EÚ so stupňom utajenia RESTREINT UE/EU RESTRICTED, ako sa to požaduje v zmluve.

32. GSC ako verejný obstarávateľ informuje NSA/DSA alebo akékoľvek iné príslušné bezpečnostné orgány o zmluvách alebo subdodávateľských zmluvách, ktoré obsahujú utajované skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED, v takom rozsahu, ako to ukladajú vnútroštátne zákony a iné právne predpisy.

33. FSC ani PSC pre dodávateľov alebo subdodávateľov a ich personál sa nevyžaduje pre zmluvy GSR, ktoré obsahujú utajované skutočnosti so stupňom utajenia RESTREINT UE/EU RESTRICTED.

34. Bez ohľadu na akékoľvek požiadavky ustanovené vo vnútroštátnych zákonoch a iných právnych predpisoch, ktoré sa týkajú FSC alebo PSC, GSR ako verejný obstarávateľ preskúma odpovede na výzvy na predloženie ponuky, ktoré sa týkajú zmlúv, v rámci ktorých je potrebný prístup k utajovaným skutočnostiam so stupňom utajenia RESTREINT UE/EU RESTRICTED.

35. Podmienky, za ktorých môže dodávateľ uzatvárať subdodávateľské zmluvy, sú v súlade s bodom 21.

36. Ak sa v rámci zmluvy manipuluje s utajovanými skutočnosťami so stupňom utajenia RESTREINT UE/EU RESTRICTED v CIS, ktorý prevádzkuje dodávateľ, GSR ako verejný obstarávateľ zabezpečí, aby sa v zmluve alebo subdodávateľskej zmluve uviedli potrebné technické a administratívne požiadavky týkajúce sa certifikácie CIS zodpovedajúce vyhodnotenému riziku, pričom sa zohľadnia všetky relevantné faktory. Rozsah certifikácie takého CIS dohodnú verejný obstarávateľ a príslušný NSA/DSA.

PRÍLOHA VI

VÝMENA UTAJOVANÝCH SKUTOČNOSTÍ S TRETÍMI ŠTÁTMI A MEDZINÁRODNÝMI ORGANIZÁCIAMI

I. ÚVOD

1. V tejto prílohe sa uvádzajú vykonávacie ustanovenia k článku 12.

II. RÁMCE VÝMENY UTAJOVANÝCH SKUTOČNOSTÍ

2. Ak Rada rozhodne o dlhodobej potrebe výmeny utajovaných skutočností:

— uzavrie sa dohoda o bezpečnosti utajovaných skutočností alebo

— uzavrie sa správne dojednanie

v súlade s článkom 12 ods. 2 a oddielov III a IV na základe odporúčania Bezpečnostného výboru.

3. Ak sa majú utajované skutočnosti EÚ vytvorené na účely operácie SBOP poskytnúť tretiemu štátu alebo medzinárodnej organizácii, ktorá alebo ktorý sa zúčastňujú na tejto operácii, a keď neexistuje ani jeden z rámcov uvedených v bode 2, výmena utajovaných skutočností EÚ s prispievajúcim tretím štátom alebo medzinárodnou organizáciou sa v súlade s oddielom V spravuje:

— rámcovou dohodou o účasti alebo

— dohodou o účasti *ad hoc*, alebo

— v prípade, že ani jedna z týchto dohôd neexistuje, správnym dojednaním *ad hoc*.

4. Ak neexistuje ani jeden z rámcov uvedených v bodoch 2 a 3 a ak sa prijalo rozhodnutie o výnimočnom poskytnutí utajovaných skutočností EÚ tretiemu štátu alebo medzinárodnej organizácii *ad hoc* v súlade s oddielom VI, vyžiada sa písomné ubezpečenie, v ktorom sa dotknutý tretí štát alebo medzinárodná organizácia zaviažu, že budú chrániť všetky utajované skutočnosti EÚ, ktoré sa im poskytnú, v súlade s základnými zásadami a minimálnymi štandardmi stanovenými v tomto rozhodnutí.

III. DOHODY O BEZPEČNOSTI UTAJOVANÝCH SKUTOČNOSTÍ

5. V dohodách o bezpečnosti utajovaných skutočností sa ustanovujú základné zásady a minimálne štandardy, ktorými sa riadi výmena utajovaných skutočností medzi EÚ a tretím štátom alebo medzinárodnou organizáciou.

6. V dohodách o bezpečnosti utajovaných skutočností sa ustanovujú technické vykonávacie dojednania, ktoré sa dohodnú medzi Bezpečnostným úradom GSR, ECSD a príslušným bezpečnostným orgánom dotknutého tretieho štátu alebo medzinárodnej organizácie. V týchto dojednaniach sa prihliada na úroveň ochrany zabezpečenú uplatňovanými bezpečnostnými predpismi a zavedenými bezpečnostnými štruktúrami a postupmi v dotknutom treťom štáte alebo medzinárodnej organizácii. Schvaľuje ich Bezpečnostný výbor.

7. Utajované skutočnosti EÚ sa nesmú vymieňať elektronickými prostriedkami, pokiaľ sa to výslovne neustanoví v dohode o bezpečnosti utajovaných skutočností alebo technických vykonávacích dojednaniach.

8. V dohodách o bezpečnosti utajovaných skutočností sa ustanovuje, že predtým, ako sa uskutoční výmena utajovaných skutočností na základe danej dohody, Bezpečnostný úrad GSR a ECSD odsúhlasia, že prijímajúca strana je schopná poskytnuté utajované skutočnosti primerane chrániť a zabezpečovať.

9. Keď Rada uzavrie dohodu o bezpečnosti utajovaných skutočností, pre každú stranu sa určí register, ktorý je hlavným vstupným a výstupným bodom na výmenu utajovaných skutočností.

10. Na účely posúdenia účinnosti bezpečnostných predpisov, štruktúr a postupov v dotknutom treťom štáte alebo medzinárodnej organizácii uskutočňuje Bezpečnostný úrad GSR spolu s ECSD a po vzájomnej dohode s dotknutým tretím štátom alebo medzinárodnou organizáciou hodnotiace návštevy. Tieto hodnotiace návštevy sa vykonávajú podľa príslušných ustanovení prílohy III a posudzuje sa počas nich:

a) regulačný rámec uplatniteľný na ochranu utajovaných skutočností;

b) všetky osobitné charakteristiky bezpečnostnej politiky a spôsobu organizácie bezpečnosti v treťom štáte alebo medzinárodnej organizácii, ktoré môžu mať vplyv na stupeň utajovaných skutočností, ktoré sa môžu vymieňať;

c) uplatňované bezpečnostné opatrenia a postupy a

d) postupy bezpečnostnej previerky pre stupeň utajenia utajovaných skutočností EÚ, ktoré sa majú poskytovať.

11. Tím, ktorý v mene EÚ uskutočňuje hodnotiacu návštevu, posúdi, či bezpečnostné predpisy a postupy v danom treťom štáte alebo medzinárodnej organizácii sú vhodné na účely ochrany utajovaných skutočností EÚ s daným stupňom utajenia.

12. Zistenia z takýchto návštev sa uvádzajú v správe, na základe ktorej Bezpečnostný výbor stanoví najvyšší stupeň utajenia utajovaných skutočností EÚ, ktoré sa môžu s dotknutou treťou stranou vymieňať vo papierovej podobe, a ak je to vhodné, elektronickými prostriedkami, ako aj akékoľvek osobitné podmienky pre výmenu utajovaných skutočností s touto stranou.

13. Predtým, ako Bezpečnostný výbor schváli vykonávacie dojednania, vynaloží sa maximálne úsilie na to, aby sa s cieľom určiť charakter a účinnosť uplatňovaného bezpečnostného systému vykonala plnohodnotná bezpečnostná hodnotiaca návšteva daného tretieho štátu alebo medzinárodnej organizácie. V prípade, že to nie je možné, však Bezpečnostný úrad GSR poskytne Bezpečnostnému výboru čo najúplnejšiu správu, opierajúcu sa o informácie, ktoré má k dispozícii, v ktorej ho informuje o uplatniteľných bezpečnostných predpisoch a spôsobe organizácie bezpečnosti v dotknutom treťom štáte alebo medzinárodnej organizácii.

14. Bezpečnostný výbor môže rozhodnúť, že predtým, ako preskúma výsledok hodnotiacej návštevy, danému tretiemu štátu alebo medzinárodnej organizácii sa nesmú poskytnúť nijaké utajované skutočnosti EÚ alebo sa takéto utajované skutočnosti môžu poskytnúť len do určeného stupňa utajenia, alebo môže pre poskytovanie utajovaných skutočností EÚ tomuto štátu alebo organizácii ustanoviť iné osobitné podmienky. Daný tretí štát alebo medzinárodnú organizáciu o tom informuje Bezpečnostný úrad GSR.

15. Po vzájomnej dohode s dotknutým tretím štátom alebo medzinárodnou organizáciou vykonáva Bezpečnostný úrad GSR pravidelné následné hodnotiace návštevy s cieľom overiť, že uplatňované dojednania aj naďalej spĺňajú dohodnuté minimálne normy.

16. Po nadobudnutí platnosti dohody o bezpečnosti utajovaných skutočností a začatí výmeny utajovaných skutočností s dotknutým tretím štátom alebo medzinárodnou organizáciou môže Bezpečnostný výbor rozhodnúť o zmene najvyššieho stupňa utajenia utajovaných skutočností EÚ, ktoré sa môžu v papierovej podobe alebo elektronickými prostriedkami vymieňať, a to najmä na základe ktorejkoľvek následnej hodnotiacej návštevy.

IV. SPRÁVNE DOJEDNANIA

17. V prípade dlhodobej potreby výmeny utajovaných skutočností s tretím štátom alebo medzinárodnou organizáciou so stupňom utajenia spravidla nie vyšším ako RESTREINT UE/EU RESTRICTED a v prípade, že Bezpečnostný výbor stanovil, že daná strana nemá dostatočne rozvinutý bezpečnostný systém na to, aby sa s ňou mohla uzavrieť dohoda o bezpečnosti utajovaných skutočností, môže generálny tajomník na základe súhlasu Rady uzavrieť s príslušnými orgánmi daného tretieho štátu alebo medzinárodnej organizácie správne dojednanie.

18. Ak je z naliehavých operačných dôvodov potrebné urýchlene ustanoviť rámec pre výmenu utajovaných skutočností, Rada môže vo výnimočných prípadoch rozhodnúť, že sa správne dojednanie uzatvorí na účely výmeny utajovaných skutočností s vyšším stupňom utajenia.

19. Správne dojednania majú spravidla formu výmeny listov.

20. Skôr, ako sa skutočne poskytnú utajované skutočnosti EÚ danému tretiemu štátu alebo medzinárodnej organizácii, vykoná sa hodnotiaca návšteva uvedená v bode 10 a Bezpečnostnému výboru sa predloží správa, ktorú tento musí považovať za uspokojivú. Ak však existujú výnimočné dôvody na naliehavú výmenu utajovaných skutočností, ktoré sa dajú na vedomie Rade, utajované skutočnosti EÚ sa môžu poskytnúť, pokiaľ sa vynaloží plné úsilie, aby sa takáto hodnotiaca návšteva uskutočnila čo najskôr.

21. Elektronickými prostriedkami sa neuskutočňuje nijaká výmena utajovaných skutočností EÚ, pokiaľ sa to v správnom dojednaní výslovne neustanoví.

V. VÝMENA UTAJOVANÝCH SKUTOČNOSTÍ V KONTEXTE OPERÁCIÍ SBOP

22. Účasť tretích štátov a medzinárodných organizácií na operáciách SBOP sa spravuje rámcovými dohodami o účasti. Tieto dohody obsahujú ustanovenia o poskytovaní utajovaných skutočností EÚ vytvorených na účely operácií SBOP prispievajúcim tretím štátom alebo medzinárodným organizáciám. Najvyšší stupeň utajenia utajovaných skutočností EÚ, ktoré sa môžu vymieňať, je RESTREINT UE/EU RESTRICTED pre civilné operácie SBOP a CONFIDENTIEL UE/EU CONFIDENTIAL pre vojenské operácie SBOP, pokiaľ sa v rozhodnutí, ktorým sa daná operácia SBOP zriaďuje, neustanoví inak.

23. Dohody o účasti *ad hoc* uzatvorené na účely konkrétnej operácie SBOP obsahujú ustanovenia o poskytovaní utajovaných skutočností EÚ vytvorených na účely tejto operácie prispievajúcemu tretiemu štátu alebo medzinárodnej organizácii. Najvyšší stupeň utajenia utajovaných skutočností EÚ, ktoré sa môžu vymieňať, je RESTREINT UE/EU RESTRICTED pre civilné operácie SBOP a CONFIDENTIEL UE/EU CONFIDENTIAL pre vojenské operácie SBOP, pokiaľ sa v rozhodnutí, ktorým sa daná operácia SBOP zriaďuje, neustanoví inak.

24. Správne dojednania *ad hoc* o účasti tretieho štátu alebo medzinárodnej organizácie na konkrétnej operácii SBOP sa môžu okrem iného týkať poskytnutia utajovaných skutočností EÚ vytvorených na účely tejto operácie danému tretiemu štátu alebo medzinárodnej organizácii. Takéto správne dojednania *ad hoc* sa uzatvárajú v súlade s postupmi ustanovenými v bodoch 17 a 18 oddielu IV. Najvyšší stupeň utajenia utajovaných skutočností EÚ, ktoré sa môžu vymieňať, je RESTREINT UE/EU RESTRICTED pre civilné operácie SBOP a CONFIDENTIEL UE/EU CONFIDENTIAL pre vojenské operácie SBOP, pokiaľ sa v rozhodnutí, ktorým sa daná operácia SBOP zriaďuje, neustanoví inak.

25. Pred začatím vykonávania ustanovení o poskytovaní utajovaných skutočností EÚ na základe bodov 22, 23 a 24 sa nevyžadujú nijaké vykonávacie dojednania ani hodnotiace návštevy.

26. V prípade, keď hostiteľský štát, na ktorého území sa operácia SBOP vykonáva, neuzavrel dohodu o bezpečnosti utajovaných skutočností ani nemá správne dojednanie s EÚ na výmenu utajovaných skutočností a nastane konkrétna a okamžitá operačná potreba, môže sa ustanoviť správne dojednanie *ad hoc*. Táto možnosť sa musí ustanoviť v rozhodnutí, ktorým sa táto operácia SBOP zriaďuje. Poskytovanie utajovaných skutočností EÚ za takýchto okolností sa obmedzuje na utajované skutočnosti, ktoré sa vytvorili na účely operácie SBOP a ktorých stupeň utajenia nie je vyšší ako RESTREINT UE/EU RESTRICTED. Na základe takéhoto správneho dojednania *ad hoc* sa hostiteľský štát zaviaže chrániť utajované skutočnosti EÚ v súlade s minimálnymi normami, ktoré nie sú menej prísne ako minimálne normy stanovené v tomto rozhodnutí.

27. V ustanoveniach o utajovaných skutočnostiach, ktoré sa vkladajú do rámcových dohôd o účasti, dohôd o účasti *ad hoc* a správnych dojednaní *ad hoc* uvedených v bodoch 22 až 24, sa ustanovuje, že dotknutý tretí štát alebo medzinárodná organizácia zabezpečia, že ich personál vyslaný do akejkoľvek operácie bude chrániť utajované skutočnosti EÚ v súlade s bezpečnostnými predpismi Rady a ďalšími pokynmi, ktoré vydajú príslušné orgány vrátane velenia operácie.

28. Ak sa neskôr medzi EÚ a prispievajúcim tretím štátom alebo medzinárodnou organizáciou uzavrie dohoda o bezpečnosti utajovaných skutočností, má prednosť pred každou rámcovou dohodou o účasti, dohodou o účasti *ad hoc* alebo správnym dojednaním *ad hoc*, pokiaľ ide o výmenu utajovaných skutočností EÚ a manipuláciu s nimi.

29. Na základe rámcovej dohody o účasti, dohody o účasti ad hoc alebo správneho dojednania ad hoc s tretím štátom alebo medzinárodnou organizáciou nie je povolená nijaká výmena utajovaných skutočností EÚ elektronickými prostriedkami, pokiaľ sa to v dotknutej dohode alebo dojednaní výslovne neustanoví.

30. Utajované skutočnosti EÚ vytvorené na účely operácie SBOP sa môžu sprístupniť personálu vyslanému v rámci danej operácie tretími štátmi alebo medzinárodnými organizáciami v súlade s bodmi 22 až 29. Pri povoľovaní prístupu takéhoto personálu k utajovaným skutočnostiam EÚ v objektoch alebo CIS operácie SBOP sa musia uplatňovať opatrenia (vrátane zaznamenávania sprístupnených utajovaných skutočností EÚ) s cieľom znížiť riziko straty alebo vyzradenia. Takéto opatrenia sa stanovia v príslušných plánovacích dokumentoch alebo dokumentoch misie.

VI. VÝNIMOČNÉ POSKYTNUTIE UTAJOVANÝCH SKUTOČNOSTÍ EÚ *AD HOC*

31. V prípade, keď neexistuje nijaký rámec v zmysle oddielov III až V a keď Rada alebo jeden z jej prípravných orgánov rozhodnú o výnimočnej potrebe poskytnutia utajovaných skutočností EÚ tretiemu štátu alebo medzinárodnej organizácii, GSR:

a) v možnej miere overí u bezpečnostných orgánov dotknutého tretieho štátu alebo medzinárodnej organizácie, že jeho alebo jej bezpečnostné predpisy, štruktúry a postupy zaručujú ochranu poskytnutých utajovaných skutočností EÚ, ktorá zodpovedá normám, ktoré nie sú menej prísne ako normy stanovené v tomto rozhodnutí;

b) vyzve Bezpečnostný výbor, aby na základe informácii, ktoré sú k dispozícii, vydal odporúčanie, pokiaľ ide o dôveryhodnosť, ktorú možno prikladať týmto bezpečnostným predpisom, štruktúram a postupom v treťom štáte alebo medzinárodnej organizácii, ktorému alebo ktorej sa majú utajované skutočnosti EÚ poskytnúť.

32. Ak Bezpečnostný výbor vydá v súvislosti s poskytnutím utajovaných skutočností EÚ kladné odporúčanie, záležitosť sa postúpi Výboru stálych predstaviteľov (COREPER), ktorý prijme rozhodnutie o ich poskytnutí.

33. Ak Bezpečnostný výbor vydá v súvislosti s poskytnutím utajovaných skutočností EÚ záporné odporúčanie:

a) pri záležitostiach týkajúcich sa SZBP/SBOP prerokuje vec Politický a bezpečnostný výbor, ktorý poskytne odporúčanie na rozhodnutie COREPER-u;

b) pri ostatných záležitostiach vec prerokuje COREPER, ktorý prijme rozhodnutie.

34. V prípade potreby a pod podmienkou predchádzajúceho písomného súhlasu pôvodcu môže COREPER rozhodnúť o tom, že sa môže poskytnúť len časť utajovaných skutočností, alebo že sa tieto utajované skutočnosti môžu poskytnúť len v prípade, že sa najprv zníži alebo zruší stupeň ich utajenia, alebo že sa utajované skutočnosti, ktoré sa majú poskytnúť, pripravia bez toho, aby sa odkázalo na zdroj alebo pôvodný stupeň utajenia EÚ.

35. Po rozhodnutí o poskytnutí utajovanej skutočnosti EÚ postúpi GSR dotknutý dokument, na ktorom sa uvedie označenie prístupnosti tretieho štátu alebo medzinárodnej organizácie, ktorej sa poskytuje. Pred vlastným poskytnutím alebo pri ňom sa dotknutá tretia strana písomne zaviaže, že bude utajované skutočnosti EÚ, s ktorými sa oboznámi, chrániť v súlade so základnými zásadami a minimálnymi štandardmi stanovenými v tomto rozhodnutí.

VII. PRÁVOMOC POSKYTOVAŤ UTAJOVANÉ SKUTOČNOSTI EÚ TRETÍM ŠTÁTOM ALEBO MEDZINÁRODNÝM ORGANIZÁCIÁM

36. V prípade, keď na výmenu utajovaných skutočností s tretím štátom alebo medzinárodnou organizáciou existuje rámec podľa bodu 2, Rada prijme rozhodnutie, ktorým udelí generálny tajomník právomoc poskytovať utajované skutočnosti EÚ v súlade so zásadou súhlasu pôvodcu danému tretiemu štátu alebo medzinárodnej organizácii.

37. V prípade, keď na výmenu utajovaných skutočností s tretím štátom alebo medzinárodnou organizáciou existuje rámec podľa bodu 3, právomoc poskytovať utajované skutočnosti EÚ v súlade s rozhodnutím, ktorým sa operácia SBOP zriaďuje, a v súlade so zásadou súhlasu pôvodcu má generálny tajomník.

38. Generálny tajomník môže tieto právomoci delegovať na vyšších úradníkov GSR alebo iné osoby, ktoré patria do jeho právomoci.

Dodatky

Dodatok A

Vymedzenie pojmov

Dodatok B

Ekvivalenčná tabuľka stupňov utajenia

Dodatok C

Zoznam národných bezpečnostných orgánov (NSA)

Dodatok D

Zoznam skratiek

Dodatok A

VYMEDZENIE POJMOV

Na účely tohto rozhodnutia sa uplatňujú tieto vymedzenia pojmov:

„bezpečnostná doložka“ (SAL) je súbor osobitných zmluvných podmienok vydaných verejným obstarávateľom, v ktorom sa stanovujú bezpečnostné požiadavky alebo prvky zmluvy vyžadujúce si bezpečnostnú ochranu a ktorý tvorí neoddeliteľnú súčasť každej utajovanej zmluvy, ktorá si vyžaduje prístup k utajovaným skutočnostiam EÚ alebo v rámci ktorej sa takéto utajované skutočnosti tvoria;

„bezpečnostné vyšetrovanie“ sú vyšetrovacie postupy vykonávané v súlade so zákonmi a inými právnymi predpismi dotknutého členského štátu príslušným vnútroštátnym orgánom členského štátu s cieľom získať ubezpečenie, že nie je známe nič, čo by bránilo udeliť tejto osobe národnú PSC alebo PSC EÚ, ktorou sa danej osobe udeľuje prístup k utajovaným skutočnostiam EÚ do stanoveného stupňa utajenia (CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyššieho);

„bezpečnostný pokyn pre program/projekt“ (PSI) je zoznam bezpečnostných postupov, ktoré sa uplatňujú v rámci konkrétneho programu/projektu s cieľom štandardizovať bezpečnostné postupy. V priebehu programu/projektu sa môže revidovať;

„bezpečnostný režim prevádzky“ je vymedzenie podmienok, za ktorých CIS vykonáva činnosť, na základe stupňa utajenia utajovaných skutočností, s ktorými sa v ňom manipuluje, a stupňov previerok, formálnych schválení prístupu a potreby poznať týkajúcej sa jeho používateľov. Pri manipulácii s utajovanými skutočnosťami a ich prenose existujú štyri bezpečnostné režimy: vyhradený režim, režim vysokej bezpečnosti, režim kompartmentácie a viacúrovňový bezpečnostný režim prevádzky;

— „vyhradený režim“ je režim prevádzky, v ktorom sú VŠETKY osoby s prístupom do CIS preverené pre najvyšší stupeň utajenia utajovaných skutočností, s ktorými sa v CIS manipuluje, a so všeobecnou potrebou poznať VŠETKY utajované skutočnosti, s ktorými sa v CIS manipuluje;

— „režim vysokej bezpečnosti“ je režim prevádzky, v ktorom sú VŠETKY osoby s prístupom do CIS preverené pre najvyšší stupeň utajenia skutočností, s ktorými sa v CIS manipuluje, ale NIE VŠETKY osoby s prístupom do CIS majú všeobecnú potrebu poznať utajované skutočnosti, s ktorými sa v CIS manipuluje; prístup k informáciám môže udeliť jednotlivec;

— „režim kompartmentácie“ je režim prevádzky, v ktorom sú VŠETKY osoby s prístupom do CIS preverené pre najvyšší stupeň utajenia skutočností, s ktorými sa v CIS manipuluje, ale nie všetky osoby s prístupom do CIS majú formálne povolenie na prístup ku VŠETKÝM utajovaným skutočnostiam, s ktorými sa v CIS manipuluje; formálne povolenie znamená, že na rozdiel od udeľovania prístupu na základe úvahy jednotlivca existuje formálna ústredná správa kontroly prístupu;

— „viacúrovňový bezpečnostný režim prevádzky“ je režim prevádzky, v ktorom sú NIE VŠETKY osoby s prístupom do CIS preverené pre najvyšší stupeň utajenia utajovaných skutočností, s ktorými sa v CIS manipuluje, a NIE VŠETKY osoby s prístupom do CIS majú všeobecnú potrebu poznať utajované skutočnosti, s ktorými sa v rámci tohto CIS manipuluje.

„certifikácia“ je proces, ktorý vedie k formálnemu vyhláseniu orgánu bezpečnostnej certifikácie (SAA), že za predpokladu, že sa zaviedol schválený súbor technických, fyzických, organizačných a procesných bezpečnostných opatrení, je systém v konkrétnom bezpečnostnom režime vo svojom operačnom prostredí schválený na činnosť s definovaným stupňom utajenia na prijateľnej úrovni rizika;

„certifikát o previerke personálnej bezpečnosti“ (Personnel Security Clearance Certificate – PSCC) je certifikát vydaný príslušným orgánom, ktorým sa potvrdzuje, že osoba je bezpečnostne preverená a je držiteľom platnej národnej PSC alebo PSC EÚ, a v ktorom sa uvádza stupeň utajenia utajovaných skutočností EÚ, ku ktorým sa môže tejto osobe udeliť prístup (CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyšší), dátum platnosti príslušnej PSC a dátum skončenia platnosti samotného certifikátu;

„dodávateľ“ je fyzická alebo právnická osoba právne spôsobilá uzatvárať zmluvy;

„dokument“ je každá zaznamenaná informácia bez ohľadu na jej podobu alebo vlastnosti;

„držiteľ“ je riadne oprávnená osoba, u ktorej sa zistila potreba poznať a ktorá má v držbe položku utajovaných skutočností EÚ, a preto zodpovedá za jej ochranu;

„evidencia“ – pozri prílohu III bod 18;

„fyzická bezpečnosť“ – pozri článok 8 ods. 1;

„hĺbková ochrana“ je uplatňovanie škály bezpečnostných opatrení, ktoré sa organizujú do viacerých vrstiev;

„informačná bezpečnosť“ – pozri článok 10 ods. 1;

„komunikačný a informačný systém“ („CIS“) – pozri článok 10 ods. 2;

„kryptografický materiál“ sú kryptografické algoritmy, kryptografický hardvér a softvérové moduly a produkty vrátane údajov o ich implementácii a príslušnej dokumentácie a kryptografické kľúče;

„majetok“ je všetko, čo má pre organizáciu, jej činnosť a existenciu hodnotu, vrátane informačných zdrojov, ktoré slúžia na podporu plnenia jej úloh;

„manipulácia“ s utajovanými skutočnosťami EÚ je akýkoľvek úkon v súvislosti s utajovanými skutočnosťami EÚ, ktorý sa môže vykonať počas ich životného cyklu. Patrí sem vytváranie, spracúvanie, prenos, zníženie stupňa utajenia, zrušenie utajenia a zničenie. V súvislosti s CIS sem patrí aj zhromažďovanie, zobrazovanie, prenášanie a uchovávanie;

„ohrozenie“ je potenciálna príčina neželaného incidentu, ktorého výsledkom môže byť poškodenie organizácie alebo akéhokoľvek systému, ktorý používa; takéto ohrozenia môžu byť náhodné alebo úmyselné (so zlým úmyslom) a sú charakterizované svojimi prvkami hrozby, potenciálnymi cieľmi a metódami útoku;

„operácia SBOP“ je vojenská alebo civilná operácia krízového riadenia na základe hlavy V Zmluvy;

„personálna bezpečnosť“ – pozri článok 7 ods. 1;

„pôvodca“ je inštitúcia, agentúra alebo orgán EÚ, členský štát, tretí štát alebo medzinárodná organizácia, v ktorej právomoci sa utajované skutočnosti vytvorili a/alebo zaviedli do štruktúr EÚ;

„prepojenie“ pozri prílohu IV bod 31;

„previerka bezpečnosti zariadenia“ (FSC) je správne rozhodnutie NSA alebo DSA, že z hľadiska bezpečnosti poskytuje zariadenie primeranú ochranu utajovaných skutočností EÚ pre určený stupeň utajenia a jeho zamestnanci, ktorí potrebujú prístup k utajovaným skutočnostiam EÚ, boli primerane bezpečnostne preverení a poučení o príslušných bezpečnostných požiadavkách pre prístup k utajovaným skutočnostiam EÚ a ich ochranu;

„previerka personálnej bezpečnosti“ (PSC) je jeden z týchto pojmov alebo obidva:

— „previerka personálnej bezpečnosti EÚ“ (PSC EÚ) na prístup k utajovaným skutočnostiam EÚ je povolenie menovacieho orgánu GSR, ktoré sa prijíma v súlade s týmto rozhodnutím na základe ukončenej bezpečnostnej previerky vykonanej príslušnými orgánmi členského štátu a ktorým sa potvrdzuje, že sa osobe môže za predpokladu, že sa zistila jej potreba poznať , do určeného dňa udeliť prístup k utajovaným skutočnostiam EÚ do určeného stupňa utajenia (CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyššieho); takáto osoba sa označuje ako „bezpečnostne preverená“;

— „národná previerka personálnej bezpečnosti“ (národná PSC) na prístup k utajovaným skutočnostiam EÚ je vyhlásenie príslušného orgánu členského štátu, ktoré sa vydáva na základe ukončenej bezpečnostnej previerky vykonanej príslušnými orgánmi členského štátu a ktorým sa potvrdzuje, že sa osobe môže za predpokladu, že sa zistila jej potreba poznať, do určeného dňa môže udeliť prístup k utajovaným skutočnostiam EÚ do určeného stupňa utajenia (CONFIDENTIEL UE/EU CONFIDENTIAL alebo vyššieho); takáto osoba sa označuje ako „bezpečnostne preverená“;

„priemyselná bezpečnosť“ – pozri článok 11 ods. 1;

„priemyselný a iný subjekt“ je subjekt, ktorý dodáva tovar, vykonáva práce alebo poskytuje služby; môže zahŕňať subjekty pôsobiace v oblasti priemyslu, obchodu, služieb, vedy, výskumu, vzdelávania alebo rozvoja alebo samostatne zárobkovo činnú osobu;

„proces riadenia bezpečnostných rizík“ je celkový proces zameraný na určenie, kontrolu a minimalizáciu neistých udalostí, ktoré môžu mať vplyv na bezpečnosť organizácie alebo akéhokoľvek systému, ktorý používa. Zahŕňa všetky činnosti vzťahujúce sa na riziká vrátane ich vyhodnocovania, zabezpečenia sa proti nim, akceptácie a oznamovania;

„riziko“ je možnosť, že dané ohrozenie využije vnútorné a vonkajšie slabiny organizácie alebo niektorého zo systémov, ktorý táto organizácia používa, a tým spôsobí organizácii a jej hmotnému alebo nehmotnému majetku škodu. Meria sa kombináciou pravdepodobnosti, že sa ohrozenia naplnia, a ich následkov.

— „akceptácia rizika“ je rozhodnutie po zabezpečení sa proti rizikám znášať ďalšiu existenciu zvyškového rizika;

— „vyhodnotenie rizika“ pozostáva z určenia ohrození a slabín a vykonania príslušnej analýzy rizík, t. j. analýzy ich pravdepodobnosti a následkov;

— „oznamovanie rizika“ pozostáva z budovania informovanosti o rizikách medzi používateľskými komunitami CIS, informovania schvaľovacích orgánov o týchto rizikách a podávania správ o nich operačným orgánom;

— „zabezpečenie sa proti riziku“ pozostáva zo zmiernenia, odstránenia alebo zmenšenia rizika (prostredníctvom vhodnej kombinácie technických, fyzických, organizačných a procesných opatrení), prenosu rizika alebo jeho monitorovania;

„slabina“ je slabá stránka akejkoľvek povahy, ktorú môže zneužiť jedno alebo viacero ohrození. Slabinu môže predstavovať opomenutie alebo sa môže týkať nedostatočnosti kontroly z hľadiska jej intenzity, úplnosti alebo súdržnosti a môže byť technického, procesného, fyzického, organizačného alebo operačného charakteru;

„správa utajovaných skutočností“ – pozri článok 9 ods. 1;

„TEMPEST“ je vyšetrovanie, skúmanie a kontrola elektromagnetického žiarenia predstavujúceho ohrozenie a opatrenia na jeho potlačenie;

„určený bezpečnostný orgán“ (DSA) je orgán podliehajúci národnému bezpečnostnému orgánu (NSA) členského štátu, ktorý je zodpovedný za informovanie priemyselných alebo iných subjektov o vnútroštátnej politike vo všetkých záležitostiach priemyselnej bezpečnosti a za usmerňovanie a podporu pri jej vykonávaní. Úlohu DSA môže vykonávať NSA alebo iný príslušný orgán;

„usmernenia pre určovanie stupňa utajenia“ (SCG) je dokument, v ktorom sa opisujú prvky programu alebo zmluvy, ktoré sa utajujú, s uvedením uplatniteľných bezpečnostných stupňov utajenia. SCG sa môžu v priebehu existencie programu alebo zmluvy rozšíriť a stupeň utajenia prvkov utajovaných skutočností sa môže zmeniť alebo znížiť; ak SCG existujú, tvoria súčasť doložky SAL;

„utajovaná skutočnosť EÚ“ – pozri článok 2 ods. 1;

„utajovaná subdodávateľská zmluva“ je zmluva medzi dodávateľom GSR a iným dodávateľom (t. j. subdodávateľom) o dodaní tovaru, vykonaní prác alebo poskytnutí služieb, ktorej plnenie si vyžaduje alebo zahŕňa prístup k utajovaným skutočnostiam EÚ alebo ich vytvorenie;

„utajovaná zmluva“ je zmluva medzi GSR a dodávateľom o dodaní tovaru, vykonaní prác alebo poskytnutí služieb, ktorej plnenie si vyžaduje alebo zahŕňa prístup k utajovaným skutočnostiam EÚ alebo ich vytvorenie;

„vec“ je každý dokument alebo prístroj či zariadenie vyrobené alebo v procese výroby;

„zníženie stupňa utajenia“ je zníženie úrovne utajenia;

„zrušenie utajenia“ je odstránenie akéhokoľvek stupňa utajenia;

„zvyškové riziko“ je riziko, ktoré zostáva po uplatnení bezpečnostných opatrení, vzhľadom na to, že nie je zabezpečená ochrana proti všetkým ohrozeniam a nie je možné odstrániť všetky slabiny;

„životný cyklus CIS“ je celkové trvanie existencie CIS, ktoré zahŕňa prvotný zámer, koncept, plánovanie, analýzu požiadaviek, projektovanie, vývoj, testovanie, uvedenie do prevádzky, prevádzku, údržbu a vyradenie.

Dodatok B

EKVIVALENČNÁ TABUĽKA STUPŇOV UTAJENIA

EÚ	TRÉS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgicko	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	(1)
Bulharsko	Строго секретно	Секретно	Поверително	За служебно ползване
Česká republika	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Dánsko	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Nemecko	STRENG GEHEIM	GEHEIM	VS (2) – VERTRAULICH	VS – NUR FÜR DEN DIENSTGEBRAUCH
Estónsko	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Írsko	Top Secret	Secret	Confidential	Restricted
Grécko	Άκρως Απόρρητο skratka: ΑΑΠ	Απόρρητο skratka: (ΑΠ)	Εμπιστευτικό skratka: (ΕΜ)	Περιορισμένης Χρήσης skratka: (ΠΧ)
Španielsko	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Francúzsko	Très Secret Défense	Secret Défense	Confidentiel Défense	(3)
Taliansko	Segretissimo	Segreto	Riservatissimo	Riservato
Cyprus	Άκρως Απόρρητο skratka: (ΑΑΠ)	Απόρρητο skratka: (ΑΠ)	Εμπιστευτικό skratka: (ΕΜ)	Περιορισμένης Χρήσης skratka: (ΠΧ)
Lotyšsko	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Litva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Luxembursko	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Maďarsko	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Oghla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Holandsko	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep VERTROUWELIJK
Rakúsko	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Poľsko	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalsko	Muito Secreto	Secreto	Confidencial	Reservado
Rumunsko	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu

EÚ	TRÉS SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Slovinsko	Strogo tajno	Tajno	Zaupno	Interno
Slovensko	Prísne tajné	Tajné	Dôverné	Vyhradené
Fínsko	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švédsko (4)	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Spojené kráľovstvo	Top Secret	Secret	Confidential	Restricted

(1) Označenie Diffusion Restreinte/Beperkte Verspreiding nie je v Belgicku stupňom utajenia. Belgicko manipuluje s utajovanými skutočnosťami so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ a chráni ich spôsobom, ktorý nie je menej prísny, ako si vyžadujú normy a postupy uvedené v bezpečnostných predpisoch Rady Európskej únie.
(2) Nemecko: VS = Verschlusssache.
(3) Francúzsko vo svojom vnútroštátnom systéme nepoužíva stupeň utajenia „RESTREINT“. Francúzsko spracúva a chráni utajované skutočnosti so stupňom utajenia „RESTREINT UE/EU RESTRICTED“ spôsobom, ktorý nie je menej prísny, ako si vyžadujú normy a postupy uvedené v bezpečnostných predpisoch Rady Európskej únie.
(4) Švédsko: označenie bezpečnostnej klasifikácie v hornom riadku používajú orgány obrany a označenia v dolnom riadku ostatné orgány.

Dodatok C

ZOZNAM NÁRODNÝCH BEZPEČNOSTNÝCH ORGÁNOV (NSA)

BELGICKO
Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles

Tel. sekretariát: +32 25014542
Fax: +32 25014596
E-mail: nvo-ans@diplobel.fed.be

DÁNSKO
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
2860 Søborg

Tel.: +45 33148888
Fax: +45 33430190

Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
2100 Copenhagen Ø

Tel.: +45 33325566
Fax: +45 33931320

BULHARSKO
State Commission on Information Security
90 Cherkovna Str.
1505 Sofia

Tel.: +359 29215911
Fax: +359 29873750
E-mail: dksi@government.bg
Website: www.dksi.bg

NEMECKO
Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
11014 Berlin

Tel.: +49 3018681 0
Fax: +49 30186811441
E-mail: oesIII3@bmi.bund.de

ČESKÁ REPUBLIKA
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
150 06 Praha 56

Tel.: +420 257283335
Fax: +420 257283110
E-mail: czech.nsa@nbu.cz
Website: www.nbu.cz

ESTÓNSKO
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
15094 Tallinn

Tel.: +372 7170113, +372 7170117
Fax: +372 7170213
E-mail: nsa@kmin.ee

ÍRSKO
National Security Authority
Department of Foreign Affairs
76 - 78 Harcourt Street
Dublin 2 Ireland

Tel.: +353 14780822
Fax: +353 14082959

ŠPANIELSKO
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
28023 Madrid

Tel.: +34 913725000
Fax: +34 913725808
E-mail: nsa-sp@areatec.com

GRÉCKO
Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΓ 1020 -Χολαργός (Αθήνα)
Ελλάδα

Τηλέφωνα: +30 2106572045 (ώρες γραφείου)
+ 30/210/657 20 09 (ώρες γραφείου)
Φαξ: +30 2106536279
+30 2106577612

Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
STG 1020 Holargos – Athens

Tel.: +30 2106572045
+30 2106572009
Fax: +30 2106536279
+30 2106577612

FRANCÚZSKO
Secrétariat général de la défense et de la sécurité nationale
Sous-direction Protection du secret (SGDSN/PSD)
51 Boulevard de la Tour-Maubourg
75700 Paris 07 SP

Tel.: +33 1/71758177
Fax: +33 171758200

TALIANSKO
Presidenza del Consiglio dei Ministri
Autorità Nazionale per la Sicurezza
D.I.S. - U.C.Se.
Via di Santa Susanna, 15
00187 Roma

Tel.: +39 0661174266
Fax: +39 064885273

CYPRUS
ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ
ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ
Εθνική Αρχή Ασφάλειας (ΕΑΑ)
Υπουργείο Άμυνας
Λεωφόρος Εμμανουήλ Ροΐδη 4
1432 Λευκωσία, Κύπρος

Τηλέφωνα: +357 22807569, +357 22807643,
+357 22807764
Τηλεομοιότυπο: +357 22302351

Ministry of Defence
Minister's Military Staff
National Security Authority (NSA)
4 Emanuel Roidi street
1432 Nicosia

Tel.: +357 22807569, +357 22807643,
+357 22807764
Fax: +357 22302351
E-mail: cynsa@mod.gov.cy

LUXEMBURSKO
Autorité nationale de Sécurité
Boîte postale 2379
1023 Luxembourg

Tel.: +352 24782210 central
+352 24782253 direct
Fax: +352 24782243

MAĎARSKO
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
1357 Budapest

Tel.: +361 3469652
Fax: +361 3469658
E-mail: nbf@nbf.hu
Website: www.nbf.hu

MALTA
Ministry of Justice and Home Affairs
P.O. Box 146
Valletta

Tel.: +356 21249844
Fax: +356 25695321

LOTYŠSKO
National Security Authority
Constitution Protection Bureau of the Republic of Latvia
P.O.Box 286
1001 Riga

Tel.: +371 67025418
Fax: +371 67025454
Email: ndi@sab.gov.lv

LITVA
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(The Commission for Secrets Protection Coordination of the Republic of Lithuania
National Security Authority)
Gedimino 40/1
01110 Vilnius

Tel.: +370 52663201,
+370 52663202
Fax: +370 52663200
E-mail: nsa@vsd.lt

HOLANDSKO
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
2500 EA Den Haag

Tel.: +31 703204400
Fax: +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
2500 ES Den Haag

Tel.: +31 703187060
Fax: +31 703187522

RAKÚSKO
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
1014 Wien

Tel.: +43 1531152594
Fax: +43 1531152615
E-mail: ISK@bka.gv.at

POĽSKO
Agencja Bezpieczeństwa Wewnętrznego – ABW
(Internal Security Agency)
2A Rakowiecka St.
00-993 Warszawa

Tel.: +48 225857360
Fax: +48 225858509
E-mail: nsa@abw.gov.pl
Website: www.abw.gov.pl

Służba Kontrwywiadu Wojskowego
(Military Counter-Intelligence Service)
Classified Information Protection Bureamu
Oczki 1
02-007 Warszawa

Tel.: +48 226841247
Fax: +48 226841076
E-mail: skw@skw.gov.pl

RUMUNSKO
Oficiul Registrului Național al Informațiilor Secrete de Stat
(Romanian NSA – ORNISS
National Registry Office for Classified Information)
4 Mures Street
012275 Bucharest

Tel.: +40 212245830
Fax: +40 212240714
E-mail: nsa.romania@nsa.ro
Website: www.orniss.ro

PORTUGALSKO
Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69
1300-342 Lisboa

Tel.: +351 213031710
Fax: +351 213031711

SLOVINSKO
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana

Tel.: +386 14781390
Fax: +386 14781399

SLOVENSKO
Národný bezpečnostný úrad
(National Security Authority)
Budatínska 30
P.O. Box 16
850 07 Bratislava

Tel.: +421 268692314
Fax: +421 263824005
Website: www.nbusr.sk

ŠVÉDSKO
Utrikesdepartementet
(Ministry for Foreign Affairs)
SSSB
103 39 Stockholm

Tel.: +46 84051000
Fax: +46 87231176
E-mail: ud-nsa@foreign.ministry.se

FÍNSKO
National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
00023 Government

Tel. 1: +358 916056487
Tel. 2: +358 916056484
Fax: +358 916055140
E-mail: NSA@formin.fi

SPOJENÉ KRÁĽOVSTVO
UK National Security Authority
Room 335, 3rd Floor
70 Whitehall
London
SW1A 2AS

Tel. 1: +44 2072765649
Tel. 2: +44 2072765697
Fax: +44 2072765651
Email: UK-NSA@cabinet-office.x.gsi.gov.uk

Dodatok D

ZOZNAM SKRATIEK

Akronym	Význam
AQUA	Náležite kvalifikovaný orgán (Appropriately Qualified Authority)
BPS	Obvodová ochrana (Boundary Protection Services)
CAA	Kryptografický schvaľovací orgán (Crypto Approval Authority)
CCTV	Uzatvorený televízny okruh (Closed Circuit Television)
CDA	Kryptografický distribučný orgán (Crypto Distribution Authority)
CIS	Komunikačný a informačný systém (Communication and Information System)
COREPER	Výbor stálych zástupcov (Comité des représentants permanents)
DSA	Určený bezpečnostný orgán (Designated Security Authority)
ECSD	Riaditeľstvo Európskej komisie pre bezpečnosť (European Commission Security Directorate)
FSC	Previerka bezpečnosti zariadenia (Facility Security Clearance)
GSR	Generálny sekretariát Rady
IA	Informačná bezpečnosť (Information Assurance)
IAA	Orgán pre informačnú bezpečnosť (Information Assurance Authority)
IDS	Detekčné systémy proti narušeniu (Intrusion Detection System)
IT	Informačné technológie
NSA	Národný bezpečnostný orgán (National Security Authority)
OZEÚ	Osobitný zástupca EÚ
PSC	Previerka personálnej bezpečnosti (Personnel Security Clearance)
PSCC	Certifikát o previerke personálnej bezpečnosti (Personnel Security Clearance Certificate)
PSI	Bezpečnostné pokyny pre program/projekt (Programme/Project Security Instructions)
SAA	Orgán bezpečnostnej certifikácie (Security Accreditation Authority)
SAB	Spoločná komisia pre bezpečnostnú certifikáciu (Security Accreditation Board)
SAL	Bezpečnostná doložka (Security Aspects Letter)
SBOP	Spoločná bezpečnostná a obranná politika
SCG	Usmernenia pre určovanie stupňa utajenia (Security Classification Guide)
SecOPs	Operačné bezpečnostné postupy (Security Operating Procedures)
SSRS	Bezpečnostné požiadavky špecifické pre systém (System-Specific Security Requirement Statement)
SZBP	Spoločná zahraničná a bezpečnostná politika
TA	Orgán pre TEMPEST (TEMPEST Authority)