Šis dokumentas yra skirtas tik informacijai, ir institucijos nėra teisiškai atsakingos už jo turinį

►B

KOMISIJOS SPRENDIMAS

2001 m. lapkričio 29 d.

iš dalies keičiantis jos darbo tvarkos taisykles

(pranešta dokumentu Nr. C(2001) 3031)

(2001/844/EB, EAPB, Euratomas)

(OL L 317, 2001 12 3, p. 1)

iš dalies keičiamas:

		Oficialusis leidinys		
		Nr.	puslapis	data
►M1	2005 m. vasario 3 d. Komisijos sprendimas 2005/94/EB, Euratomas	L 31	66	2005 2 4
►M2	2006 m. sausio 31 d. Komisijos sprendimas 2006/70/EB, Euratomas	L 34	32	2006 2 7
►M3	2006 m. rugpjūčio 2 d. Komisijos sprendimas 2006/548/EB, Euratomas	L 215	38	2006 8 5
►M4	2013 m. vasario 21 d. Komisijos reglamentas (ES) Nr. 519/2013	L 158	74	2013 6 10

▼B

KOMISIJOS SPRENDIMAS

2001 m. lapkričio 29 d.

iš dalies keičiantis jos darbo tvarkos taisykles

(pranešta dokumentu Nr. C(2001) 3031)

(2001/844/EB, EAPB, Euratomas)

EUROPOS BENDRIJŲ KOMISIJA,

atsižvelgdama į Europos Bendrijos steigimo sutartį, ypač į jos 218 straipsnio 2 dalį,

atsižvelgdama į Europos anglių ir plieno bendrijos steigimo sutartį, ypač į jos 16 straipsnį,

atsižvelgdama į Europos atominės energijos bendrijos steigimo sutartį, ypač į jos 131 straipsnį,

atsižvelgdama į Europos Sąjungos sutartį, ypač į jos 28 straipsnio 1 dalį ir 41 straipsnio 1 dalį,

NUSPRENDĖ:

1 straipsnis

Komisijos nuostatos dėl saugumo, kurių tekstas pridedamas prie šio sprendimo, pridedamos prie Komisijos darbo tvarkos taisyklių kaip jų priedas.

2 straipsnis

Šis sprendimas įsigalioja jo paskelbimo *Europos Bendrijų oficialiajame leidinyje* dieną.

Jis taikomas nuo 2001 m. gruodžio 1 d.

▼B

PRIEDAS

KOMISIJOS NUOSTATOS DĖL SAUGUMO

Kadangi:

(1) Siekiant plėtoti Komisijos veiklą tose srityse, kuriose yra reikalingas tam tikras konfidencialumo laipsnis, tikslinga sukurti visaapimančią saugumo sistemą, tinkamą Komisijai, kitoms EB steigimo sutartimi ar Europos Sąjungos sutartimi arba remiantis šiomis sutartimis įsteigtoms institucijoms, įstaigoms, biurams ir agentūroms, valstybėms narėms ir visiems Europos Sąjungos įslaptintos informacijos (toliau – ES įslaptinta informacija) gavėjams.

(2) Siekdama garantuoti sukurtos saugumo sistemos veiksmingumą, Komisija padarys ES įslaptintą informaciją prieinamą tik toms išorės institucijoms, kurios užtikrins, jog imasi visų priemonių, reikalingų šias nuostatas tiksliai atitinkančioms taisyklėms taikyti.

(3) Šios nuostatos nepažeidžia 1958 m. liepos 31 d. Reglamento Nr. 3, įgyvendinančio Europos atominės energijos bendrijos steigimo sutarties 24 straipsnį ([1]), 1990 m. birželio 11 d. Tarybos reglamento (EB) Nr. 1588/90 dėl konfidencialių statistinių duomenų perdavimo Europos Bendrijų statistikos tarnybai ([2]) ir 1995 m. lapkričio 23 d. Komisijos sprendimo C (95) 1510 (galutinis) dėl informacinių sistemų apsaugos.

(4) Siekiant užtikrinti sklandžią Sąjungos sprendimų priėmimo proceso eigą, Komisijos saugumo sistema yra pagrįsta principais, išdėstytais 2001 m. kovo 19 d. Tarybos sprendime 2001/264/EB, patvirtinančiame Tarybos saugumo nuostatas ([3]).

(5) Komisija pabrėžia, kaip svarbu, kad kitos institucijos prireikus laikytųsi Sąjungos ir jos valstybių narių interesams apsaugoti reikalingų konfidencialumo taisyklių ir normų.

(6) Komisija pripažįsta, kad būtina sukurti savo saugumo koncepciją, atsižvelgiant į visus saugumo elementus ir ypatingą Komisijos, kaip institucijos, pobūdį.

(7) Šios nuostatos nepažeidžia Sutarties 255 straipsnio ir 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 1049/2001 dėl viešo naudojimosi Europos Parlamento, Tarybos ir Komisijos dokumentai ([4]).

▼M2

(8) Šios nuostatos nepažeidžia Sutarties 286 straipsnio ir 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamento (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo.

▼B

1 straipsnis

Šiame priede yra išdėstytos Komisijos saugumo taisyklės.

([1]) OL L 17/58, 1958 10 6, p. 406/58.
([2]) OL L 151, 1990 6 15, p. 1.
([3]) OL L 101, 2001 4 11, p. 1.
([4]) OL L 145, 2001 5 31, p. 43.

▼B

2 straipsnis

1. Už saugumą atsakingas Komisijos narys imasi tinkamų priemonių, kad užtikrintų, jog, tvarkydami ES įslaptintą informaciją, Komisijos pareigūnai, kiti tarnautojai ir Komisijai padedantis personalas tiek pačioje Komisijoje, tiek visose Komisijos patalpose, tarp jų – Sąjungoje veikiančiose Komisijos atstovybėse, biuruose ir jos delegacijose trečiosiose šalyse, laikytųsi 1 straipsnyje minimų taisyklių, taip pat kad tų taisyklių laikytųsi kiti išoriniai Komisijos sutarčių partneriai.

▼M3

Kai sutartyje arba susitarime dėl dotacijos tarp Komisijos ir išorės rangovo arba gavėjo numatytas ES įslaptintos informacijos tvarkymas rangovo arba gavėjo patalpose, tinkamos priemonės, kurių turi imtis minėtas išorės rangovas arba gavėjas siekdamas užtikrinti, kad bus laikomasi 1 straipsnyje minėtų taisyklių tvarkant ES įslaptintą informaciją, turi būti sutarties arba susitarimo dėl dotacijos neatskiriama dalis.

▼B

2. Valstybėms narėms, kitoms Sutartimis arba remiantis Sutartimis įsteigtoms institucijoms, įstaigoms, biurams ir agentūroms suteikiama teisė gauti ES įslaptintą informaciją, jeigu jos užtikrins, kad, tvarkydamos ES įslaptintą informaciją, savo tarnybose ir patalpose laikysis taisyklių, tiksliai atitinkančių 1 straipsnyje minimas taisykles, ypač tai taikoma:

a) valstybių narių nuolatinių atstovybių Europos Sąjungoje nariams ir nacionalinių delegacijų nariams, dalyvaujantiems Komisijos arba jos organų posėdžiuose arba kitoje Komisijos veikloje;

b) kitiems ES įslaptintą informaciją tvarkantiems valstybių narių nacionalinių administracinių įstaigų nariams, dirbantiems tiek valstybėse narėse, tiek užsienyje;

c) su ES įslaptinta informacija dirbantiems išoriniams sutarčių partneriams ir pagalbiniam personalui.

3 straipsnis

Trečiosios šalys, tarptautinės organizacijos ir kitos įstaigos gali gauti ES įslaptintą informaciją, jeigu užtikrina, kad, tvarkydamos tą informaciją, laikysis 1 straipsnyje minėtas taisykles tiksliai atitinkančių taisyklių.

4 straipsnis

Laikydamasis pagrindinių principų ir minimalių saugumo standartų, išdėstytų priedo I dalyje, už saugumą atsakingas Komisijos narys gali imtis priedo II dalyje numatytų priemonių.

5 straipsnis

Nuo tos dienos, kai bus imtos taikyti, šios nuostatos pakeis:

a) 1994 m. lapkričio 30 d. Komisijos sprendimą C (94) 3282 dėl saugumo priemonių, taikomų rengiant arba perduodant įslaptintą informaciją Europos Sąjungos veikloje;

b) 1999 m. vasario 25 d. Komisijos sprendimą C (99) 423 dėl galimybės naudotis Komisijos turima įslaptinta informacija suteikimo Europos Komisijos pareigūnams ir kitiems darbuotojams tvarkos.

▼B

6 straipsnis

Nuo tos dienos, kai bus imta taikyti šias nuostatas, visai iki tol Komisijos turėtai įslaptintai informacijai, išskyrus Euratomo įslaptintą informaciją:

a) jei ji buvo Komisijos sukurta, jos slaptumo žyma bus laikoma pakeista žyma „►**M1** RESTREINT UE ◄“, jei jos autorius iki 2002 m. sausio 31 d. nenusprendžia suteikti informacijai kitą slaptumo žymą. Tokiu atveju autorius informuoja visus atitinkamo dokumento gavėjus;

b) jei ji buvo sukurta ne Komisijos autorių, išlaiko savo pradinę slaptumo žymą ir todėl bus laikoma lygiaverčio slaptumo žymos laipsnio ES įslaptinta informacija, jei jos autorius nesutinka, kad informacija būtų išslaptinta arba kad jos slaptumo žymos laipsnis būtų sumažintas.

▼B

PRIEDAS

SAUGUMO TAISYKLĖS

Turinys

I DALIS. PAGRINDINIAI SAUGUMO PRINCIPAI IR MINIMALŪS STANDARTAI

1. ĮVADAS

2. BENDRIEJI PRINCIPAI

3. SAUGUMO PAGRINDAI

4. INFORMACIJOS APSAUGOS PRINCIPAI

4.1. **Tikslai**

4.2. **Sąvokų apibrėžimai**

4.3. **Įslaptinimas**

4.4. **Saugumo priemonių paskirtis**

5. APSAUGOS ORGANIZAVIMAS

5.1. **Bendri minimalūs standartai**

5.2. **Organizavimas**

6. PERSONALO SAUGUMAS

6.1. **Personalo tikrinimas**

6.2. **Asmens patikimumo pažymėjimų registravimas**

6.3. **Personalo saugumo instruktažas**

6.4. **Vadovų atsakomybė**

6.5. **Personalo saugumas**

7. FIZINIS SAUGUMAS

7.1. **Apsaugos poreikis**

7.2. **Tikrinimas**

7.3. **Pastatų saugumas**

7.4. **Nenumatytoms aplinkybėms skirti planai**

8. INFORMACIJOS SAUGUMAS

9. KITŲ TYČINĖS ŽALOS DARYMO FORMŲ KONTROLĖ IR PASIPRIEŠINIMAS SABOTAŽUI

10. ĮSLAPTINTOS INFORMACIJOS PERDAVIMAS TREČIOSIOMS ŠALIMS ARBA TARPTAUTINĖMS ORGANIZACIJOMS

II DALIS. SAUGUMO ORGANIZAVIMAS KOMISIJOJE

11. UŽ SAUGUMĄ ATSAKINGAS KOMISIJOS NARYS

12. KOMISIJOS SAUGUMO POLITIKOS PATARĖJŲ GRUPĖ

13. KOMISIJOS SAUGUMO VALDYBA

14. ►M2 KOMISIJOS SAUGUMO DIREKTORATAS ◄

15. SAUGUMO TIKRINIMAI

16. SLAPTUMO ŽYMOS, JŲ GALIOJIMO ŽYMOS IR KVALIFIKACINĖS ŽYMOS

16.1. **Slaptumo žymų laipsniai**

▼B

16.2. **Slaptumo žymos ogaliojimo žymos**

16.3. **Kvalifikacinės žymos**

16.4. **Slaptumo žymos dėjimas**

16.5. **Slaptumo žymos galiojimo žymų dėjimas**

17. ĮSLAPTINIMO TVARKYMAS

17.1. **Bendrosios nuostatos**

17.2. **Slaptumo žymų naudojimas**

17.3. **Slaptumo žymos laipsnio sumažinimas ir išslaptinimas**

18. FIZINIS SAUGUMAS

18.1. **Bendrosios nuostatos**

18.2. **Saugumo reikalavimai**

18.3. **Fizinės apsaugos priemonės**

18.3.1. *Saugumo zonos*

18.3.2. *Administracinė zona*

18.3.3. *Įėjimo ir išėjimo kontrolė*

18.3.4. *Apsaugos patruliai*

18.3.5. *Apsaugos konteineriai ir ugniai bei įsilaužimui atsparūs kambariai*

18.3.6. *Užraktai*

18.3.7. *Raktų ir kombinacijų kontrolė*

18.3.8. *Į įsibrovimą reaguojanti įranga*

18.3.9. *Aprobuoti įrengimai*

18.3.10. *Fizinė kopijavimo aparatų ir telefaksų apsauga*

18.4. **Apsauga nuo pamatymo ir slapto pasiklausymo**

18.4.1. *Pamatymas*

18.4.2. *Slaptas pasiklausymas*

18.4.3. *Elektroninių ir įrašymo įrengimų įsinešimas*

18.5. **Techniškai apsaugotos zonos**

19. BENDROS PRINCIPO „BŪTINA ŽINOTI“ TAIKYMO IR ES PERSONALO PATIKIMUMO TIKRINIMO TAISYKLĖS

19.1. **Bendrosios nuostatos**

19.2. **Specialios naudojimosi informacija, pažymėta slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, taisyklės**

19.3. **Specialios naudojimosi informacija, pažymėta slaptumo žymomis ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄, taisyklės**

19.4. **Specialios naudojimosi informacija, pažymėta slaptumo žyma ►M1 RESTREINT UE ◄, taisyklės**

19.5. **Perkėlimai**

19.6. **Specialios instrukcijos**

▼B

20. ASMENS PATIKIMUMO PAŽYMĖJIMŲ IŠDAVIMO KOMISIJOS PAREIGŪNAMS IR KITIEMS DARBUOTOJAMS TVARKA

21. ES ĮSLAPTINTŲ DOKUMENTŲ RENGIMAS, PLATINIMAS, PERDAVIMAS, KURJERIO ASMENS PATIKIMUMAS, PAPILDOMOS KOPIJOS, VERTIMAI IR IŠTRAUKOS

21.1. **Rengimas**

21.2. **Platinimas**

21.3. **ES įslaptintų dokumentų perdavimas**

21.3.1. *Pakavimas, kvitai*

21.3.2. *Perdavimas pastate arba pastatų komplekse*

21.3.3. *Perdavimas toje pat valstybėje*

21.3.4. *Perdavimas iš vienos valstybės į kitą*

21.3.5. *ES riboto naudojimo dokumentų perdavimas*

21.4. **Kurjerio asmens patikimumas**

21.5. **Elektroninės ir kitokios techninės perdavimo priemonės**

21.6. **ESįslaptintų dokumentų papildomos kopijos, ištraukos bei vertimai**

22. ESĮI REGISTRATŪROS, APŽIŪROS, TIKRINIMAI, ARCHYVAVIMAS IR NAIKINIMAS

22.1. **ESĮI vietinės registratūros**

22.2. **Dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūra**

22.2.1. *Bendrosios nuostatos*

22.2.2. *Centrinė dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūra*

22.2.3. *Dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ subregistrtūros*

22.3. **ES įslaptintų dokumentų inventorizacija, apžiūros ir tikrinimai**

22.4. **ES įslaptintų dokumentų archyvavimas**

22.5. **ES įslaptintų dokumentų naikinimas**

22.6. **Naikinimas nenumatytais atvejais**

23. SAUGUMO PRIEMONĖS, TAIKOMOS SPECIALIEMS NE KOMISIJOS PATALPOSE VYKSTANTIEMS POSĖDŽIAMS, KURIUOSE NAUDOJAMA ES ĮSLAPTINTA INFORMACIJA

23.1. **Bendrosios nuostatos**

23.2. **Atsakomybė**

23.2.1. ►M2 *Komisijos Saugumo direktoratas* ◄

23.2.2. *Posėdžių apsaugos pareigūnas (PAP)*

23.3. **Saugumo priemonės**

23.3.1. *Saugumo zonos*

23.3.2. *Leidimai*

23.3.3. *Fotografinės ir garso įrangos kontrolė*

▼B

23.3.4. *Portfelių, nešiojamųjų kompiuterių ir paketų tikrinimas*

23.3.5. *Techninė apsauga*

23.3.6. *Delegacijų dokumentai*

23.3.7. *Saugus dokumentų laikymas*

23.3.8. *Kabinetų tikrinimas*

23.3.9. *ES įslaptintos informacijos atliekų atidavimas*

24. SAUGUMO PAŽEIDIMAI IR ES ĮSLAPTINTŲ DOKUMENTŲ NETEISĖTAS ATSKLEIDIMAS

24.1. **Sąvokų oapibrėžimai**

24.2. **Pranešimas apie saugumo pažeidimus**

24.3. **Teisiniai veiksmai**

25. INFORMACINIŲ TECHNOLOGIJŲ IR RYŠIŲ SISTEMOMIS TVARKOMOS ES ĮSLAPTINTOS INFORMACIJOS APSAUGA

25.1. **Įvadas**

25.1.1. *Bendrosios nuostatos*

25.1.2. *Grėsmė sistemoms ir jų pažeidžiamumas*

25.1.3. *Svarbiausia saugumo priemonių paskirtis*

25.1.4. *Sistemai pritaikyta saugumo reikalavimų suvestinė (SSRS)*

25.1.5. *Sistemos darbo saugumo režimai*

25.2. **Sąvokų oapibrėžimai**

25.3. **Atsakomybė saugumo srityje**

25.3.1. *Bendrosios nuostatos*

25.3.2. *Saugumo akreditavimo institucija (SAI)*

25.3.3. *INFOSAUGOS (INFOSEC) institucija (II)*

25.3.4. *Techninių sistemų valdytojas (TSV)*

25.3.5. *Informacijos savininkas (IS)*

25.3.6. *Vartotojai*

25.3.7. *INFOSAUGOS mokymas*

25.4. **Netechninės saugumo priemonės**

25.4.1. *Personalo saugumas*

25.4.2. *Fizinis saugumas*

25.4.3. *Naudojimosi sistema kontrolė*

25.5. **Techninės saugumo priemonės**

25.5.1. *Informacijos saugumas*

25.5.2. *Informacijos kontrolė ir atskaitomyb*

25.5.3. *Išimamų kompiuterinių duomenų saugojimo laikmenų tvarkymas ir kontrolė*

▼B

25.5.4. *Kompiuterinių duomenų saugojimo laikmenų išslaptinimas ir naikinimas*

25.5.5. *Ryšių priemonių saugumas*

25.5.6. *Įrengimo ir spinduliavimo saugumas*

25.6. **Saugumas tvarkant įslaptintą informaciją**

25.6.1. *Saugumo valdymo tvarka (SOT)*

25.6.2. *Programinės įrangos apsauga/konfigūravimo tvarkymas*

25.6.3. *Pažeistos programinės įrangos/kompiuterio virusų buvimo tikrinimas*

25.6.4. *Aptarnavimas*

25.7. **Tiekimas**

25.7.1. *Bendrosios nuostatos*

25.7.2. *Akreditavimas*

25.7.3. *Vertinimas ir atestavimas*

25.7.4. *Įprastas saugumo savybių tikrinimas tęstiniam akreditavimui*

25.8. **Laikinas arba atsitiktinis naudojimas**

25.8.1. *Mikrokompiuterių/asmeninių kompiuterių saugumas*

25.8.2. *Nuosavų IT įrengimų naudojimas atliekant Komisijos tarnybines pareigas*

25.8.3. *Sutarties partnerio ar šalies – narės tiekiamų IT įrengimų naudojimas atliekant Komisijos tarnybines pareigas*

26. ES ĮSLAPTINTOS INFORMACIJOS PERDAVIMAS TREČIOSIOMS ŠALIMS ARBA TARPTAUTINĖMS ORGANIZACIJOMS

26.1.1. *ES įslaptintos informacijos perdavimą reglamentuojantys principai*

26.1.2. *Bendradarbiavimo lygiai*

26.1.3. *Susitarimai dėl saugumo*

1 PRIEDĖLIS. **Nacionalinių įslaptintos informacijos žymų palyginimas**

2 PRIEDĖLIS. **Praktinis slaptumo žymų vadovas**

3 PRIEDĖLIS. **ES įslaptintos informacijos perdavimo trečiosioms šalims arba tarptautinėms organizacijoms vadovas: 1 lygio bendradarbiavimas**

4 PRIEDĖLIS. **ES įslaptintos informacijos perdavimo trečiosioms šalims arba tarptautinėms organizacijoms vadovas: 2 lygio bendradarbiavimas**

5 PRIEDĖLIS. **ES įslaptintos informacijos perdavimo trečiosioms šalims arba tarptautinėms organizacijoms vadovas: 3 lygio bendradarbiavimas**

6 PRIEDĖLIS: **Santrumpos**

▼B

I DALIS. PAGRINDINIAI SAUGUMO PRINCIPAI IR MINIMALŪS STANDARTAI

1. ĮVADAS

Šiose nuostatose pateikiami pagrindiniai saugumo principai ir minimalūs standartai, kurių deramai laikytis turi visi Komisijos darbuotojai ir visi ES įslaptintos informacijos gavėjai, kad būtų garantuotas saugumas ir kad kiekvienas būtų užtikrintas, jog pasiektas bendras saugumo lygis.

2. BENDRIEJI PRINCIPAI

Komisijos saugumo politika yra neatskiriama bendros vidaus valdymo politikos dalis, grindžiama jos bendrą politiką reguliuojančiais principais.

Prie šių principų priskiriami teisėtumas, skaidrumas, atskaitingumas ir subsidiarumas (proporcingumas).

Teisėtumas – tai būtinybė vykdant saugumo funkcijas griežtai išlikti teisinio reguliavimo ribose bei atitikti teisinius reikalavimus. Tai taip pat reiškia, kad atsakomybė saugumo srityje turi būti pagrįsta tinkamomis teisinėmis nuostatomis. Visa apimtimi taikomi Personalo nuostatai, ypač jų 17 straipsnis dėl personalo įpareigojimo neatskleisti Komisijos informacijos ir jų VI dalis dėl drausminių priemonių. Galiausiai teisėtumo principas reiškia, kad saugumo pažeidimus Komisijos atsakomybės ribose reikia nagrinėti vadovaujantis Komisijos politika drausminių priemonių atžvilgiu ir jos bendradarbiavimo su valstybėmis narėmis baudžiamosios teisenos srityje politika.

Skaidrumas – tai visų saugumo taisyklių ir nuostatų aiškumo, siekiant įvairių tarnybų ir sričių pusiausvyros (fizinis saugumas bei informacijos apsauga ir pan.), taip pat nuoseklios bei konstruktyvios sąmoningumo saugumo srityje politikos reikmė. Dėl skaidrumo taip pat reikalingas aiškus rašytinis saugumo priemonių įgyvendinimo vadovas.

Atskaitingumas reiškia, kad pareigos saugumo srityje bus aiškiai apibrėžtos. Be to, atskaitingumas žymi poreikį reguliariai tikrinti, ar pareigos tinkamai vykdomos.

Subsidiarumas, arba proporcingumas, reiškia, kad saugumu pasirūpinama pačiu žemiausiu lygmeniu ir kiek įmanoma arčiau Komisijos generalinių direktoratų bei tarnybų. Tai taip pat reiškia, kad saugumo veikla apsiriboja tomis sritims, kurioms saugumas tikrai reikalingas. Galiausiai subsidiarumas reiškia, kad saugumo priemonės turi leisti taikyti mažiausiai žalos darančią apsaugą ir būti proporcingos ginamiems interesams bei tikrai arba galimai grėsmei tiems interesams.

3. SAUGUMO PAGRINDAS

Patikimo saugumo pagrindu yra:

a) kiekvienoje valstybėje narėje – nacionalinė saugumo organizacija, atsakinga už:

   1) informacijos apie šnipinėjimą, sabotažą, terorizmą ir kitokią ardomąją veiklą rinkimą ir registravimą;

   2) informacijos ir patarimų apie grėsmės saugumui pobūdį ir apsaugos nuo jos priemones teikimą savo Vyriausybėms, o per jas – Komisijai;

▼B

b) kiekvienoje valstybėje narėje ir Komisijoje – techninė informacijos saugumo institucija (INFOSEC), kuri dirbdama su atitinkama saugumo institucija atsako už informacijos apie bei patarimų dėl techninių grėsmių saugumui ir apsaugos nuo jų priemones teikimą;

c) nuolatinis Vyriausybinių institucijų ir Europos institucijų atitinkamų tarnybų bendradarbiavimas, kad prireikus būtų nustatyta ir rekomenduota:

1) kuriuos asmenis, informaciją ir šaltinius reikia apsaugoti;

2) bendri apsaugos standartai;

d) glaudus bendradarbiavimas tarp ►M2 Komisijos Saugumo direktorato ◄ ir kitų Europos institucijų saugumo tarnybų, taip pat su NATO Saugumo biuru (NSB).

4. INFORMACIJOS APSAUGOS PRINCIPAI

4.1. **Tikslai**

Svarbiausi informacijos apsaugos tikslai yra:

a) apsaugoti ES įslaptintą informaciją (ESĮI) nuo šnipinėjimo, neteisėto atskleidimo arba platinimo be leidimo;

b) apsaugoti ryšių ir informacijos sistemose bei tinkluose tvarkomą ES įslaptintą informaciją nuo grėsmės jos slaptumui, vientisumui ir prieinamumui;

c) apsaugoti Komisijos pastatus, kuriuose laikoma ES informacija, nuo sabotažo ir tyčinio žalojimo;

d) pažeidimo atveju įvertinti padarytą žalą, apriboti jos padarinius ir imtis būtinų jos pašalinimo priemonių.

4.2. **Sąvokų apibrėžimai**

Šiose taisyklėse:

a) „ES įslaptinta informacija“ (ESĮI) – bet kokia informacija ir medžiaga, kurią atskleidus be leidimo, gali būti padaryta įvairaus laipsnio žalos ES interesams arba vienai ar daugiau jos valstybių narių, nepriklausomai nuo to, ar ta informacija atsirado Europos Sąjungoje, ar yra gauta iš valstybių narių, trečiųjų šalių ar tarptautinių organizacijų;

b) „dokumentas“ – bet koks laiškas, užrašas, protokolas, ataskaita, memorandumas, signalas/pranešimas, eskizas, nuotrauka, skaidrė, filmas, žemėlapis, schema, planas, užrašų knygutė, trafaretas, nuorašams naudotas kalkinis popierius, rašomosios mašinėlės arba spausdintuvo juostelė, kasetė, kompiuterio diskelis, kompaktinis diskas (CD-ROM) arba kitokia fizinė laikmena, kurioje yra užrašyta informacija;

c) „medžiaga“ – b punkte apibūdintas dokumentas, taip pat visa pagaminta arba gaminama įranga;

d) „būtina žinoti“ – darbuotojo poreikis turėti galimybę naudotis ES įslaptinta informacija, kad galėtų vykdyti tam tikrą funkciją arba atlikti užduotį;

e) „leidimas“ – ►M2 Komisijos Saugumo direktorato direktoriaus ◄ sprendimas suteikti asmeniui teisę naudotis tam tikro slaptumo žymos laipsnio ESĮI, priimtas remiantis teigiama nacionalinės saugumo institucijos pagal nacionalinę teisę oficialiai atlikto asmens patikrinimo saugumo požiūriu išvada;

▼B

f) „įslaptinimas“ – tinkamo saugumo lygio suteikimas informacijai, kurią atskleidus be leidimo gali būti padaryta tam tikra žala Komisijos arba valstybių narių interesams;

g) „laipsnio sumažinimas“ *(déclassement)* – slaptumo žymos laipsnio sumažinimas;

h) „išslaptinimas“ *(déclassification)* – visų slaptumo žymų panaikinimas;

i) „autorius“ – tinkamai įgaliotas įslaptinto dokumento autorius. Komisijos departamentų vadovai gali įgalioti savo personalą inicijuoti ESĮI;

j) „Komisijos departamentai“ – Komisijos departamentai ir tarnybos, įskaitant kabinetus, visose veiklos vietose, tarp jų Jungtinis tyrimų centras, Sąjungoje veikiančios atstovybės ir biurai bei delegacijos trečiosiose šalyse.

4.3. **Įslaptinimas**

a) Atrenkant dėl slaptumo saugotiną informaciją bei medžiagą ir įvertinant, koks turi būti jos apsaugos laipsnis, reikalingas atidumas ir patirtis. Labai svarbu, kad saugotinos informacijos ir medžiagos apsaugos laipsnis atitiktų jų svarbą saugumo požiūriu. Siekiant užtikrinti sklandų informacijos tekėjimą, imamasi veiksmų, kad įslaptinimas nebūtų nei per didelis, nei per mažas.

b) Įslaptinimo sistema – šių principų įgyvendinimo priemonė; numatant ir organizuojant kovos su šnipinėjimu, sabotažu, terorizmu ir kitokiomis grėsmėmis veiksmus reikia laikytis panašios įslaptinimo sistemos, kad labiausiai apsaugoti būtų svarbiausi pastatai, kuriuose laikoma įslaptinta informacija, ir lengviausiai pažeidžiamos vietos juose.

c) Atsakomybė už informacijos įslaptinimą tenka tiktai informacijos autoriui.

d) Slaptumo žymos laipsnis priklauso tik nuo įslaptinamos informacijos turinio.

e) Tais atvejais, kai sugrupuojami keli informacijos vienetai, tai grupei skiriamas slaptumo žymos laipsnis turi būti ne mažesnis už aukščiausią slaptumo žymos laipsnį turinčio informacijos vieneto laipsnį. Tačiau informacijos rinkiniui galima suteikti aukštesnį už sudedamosioms dalims suteiktą slaptumo žymos laipsnį.

f) Slaptumo žyma suteikiama tik tuomet, kai ji reikalinga, ir tik reikalingam laikui.

4.4. **Saugumo priemonių paskirtis**

Saugumo priemonės:

a) taikomos visiems galintiems naudotis įslaptinta informacija asmenims, įslaptintos informacijos laikmenoms, visiems pastatams, kuriuose yra tokios informacijos ir svarbių įrengimų;

b) sukuriamos, kad būtų galima nustatyti asmenis, kurių būklė gali kelti grėsmę įslaptintos informacijos ir svarbių įrengimų, kuriuose laikoma įslaptinta informacija, saugumui, ir neprileisti tokių asmenų prie minėtos informacijos arba juos atleisti;

▼B

c) neleidžia jokiam leidimo neturinčiam asmeniui naudotis įslaptinta informacija arba įrengimais, kuriuose tokia informacija laikoma;

d) užtikrina įslaptintos informacijos skleidimą tik pagal visiems saugumo aspektams svarbiausią „būtina žinoti“ principą;

e) užtikrina visos, tiek įslaptintos, tiek neįslaptintos, ir ypač ypač elektromagnetinėse laikmenose laikomos, apdorotos arba perduotos informacijos vientisumą (t. y., užkerta kelią klastojimui arba taisymui ar ištrynimui be leidimo) ir galimybę ja naudotis (t. y., naudotis informacija nėra uždraudžiama tiems, kuriems ji reikalinga, ir turintiesiems leidimą ja naudotis).

5. APSAUGOS ORGANIZAVIMAS

5.1. **Bendri minimalūs standartai**

Komisija užtikrina, kad visi ESĮI gavėjai pačioje institucijoje ir jos kompetencijai priklausančiose institucijose, tame tarpe visi departamentai ir sutarčių partneriai, laikysis bendrų minimalių saugumo standartų, kad ES įslaptinta informacija būtų perduodama įsitikinus, jog ji bus taip pat atsakingai tvarkoma. Prie tokių minimalių standartų priskiriami patikimumo pažymėjimų personalui išdavimo kriterijai ir ES įslaptintos informacijos apsaugos procedūros.

Komisija suteikia teisę išorės įstaigoms naudotis ESĮI tik jei šios užtikrina, kad tvarkydamos ESĮI griežtai laikysis bent šiuos minimalius standartus tiksliai atitinkančių nuostatų.

▼M3

Tokie minimalūs standartai taip pat taikomi, kai Komisija sudarydama sutartį arba susitarimą dėl dotacijos paveda užduotis, susijusias su ES įslaptinta informacija, kurias vykdant susiduriama su tokia informacija ir (arba) tokia informacija yra užduoties dalis, pramonės arba kitiems subjektams: šie bendri minimalūs standartai nurodyti II dalies 27 skyriuje.

▼B

5.2. **Organizavimas**

Komisijoje apsauga organizuojama dviem lygiais:

a) visos Komisijos lygmeniu veikia ►M2 Komisijos Saugumo direktoratas ◄ su Saugumo akreditavimo institucija, kuri veikia ir kaip šifravimo institucija (ŠI), ir kaip TEMPEST institucija, ir kaip informacijos saugumo institucija (INFOSEC), su viena arba keliomis centrinėmis ESĮI registratūromis, kurių kiekviena turi po vieną ar daugiau registro kontrolės pareigūnų (RKP);

b) Komisijos departamentų lygmeniu už saugumą atsako vienas ar daugiau vietos saugumo pareigūnų (VSP), vienas ar daugiau centrinių informatikos saugumo pareigūnų (CISP), vietos informatikos saugumo pareigūnai (VISP) ir vietinės ES įslaptintos informacijos registratūros, turinčios vieną arba daugiau registro kontrolės pareigūnų;

c) centrinės saugumo įstaigos teikia operatyvinę pagalbą vietos saugumo įstaigoms.

6. PERSONALO SAUGUMAS

6.1. **Personalo tikrinimas**

Visi asmenys, kurie prašo leisti naudotis informacija, pažymėta ►M1 CONFIDENTIEL UE ◄ arba aukštesnio laipsnio slaptumo žyma, prieš suteikiant jiems tokią galimybę, yra tinkamai patikrinami. Panašiai patikrinti reikalaujama ir asmenis, į kurių pareigas įeina ryšių ir informacijos sistemų, kuriose laikoma įslaptinta informacija, techninės operacijos arba priežiūra. Toks tikrinimas turi leisti nustatyti, ar tie asmenys:

a) yra neabejotinai lojalūs;

▼B

b) turi tokių charakterio savybių ir kompetenciją, kurie neleidžia abejoti jų garbingumu naudojantis įslaptinta informacija;

c) gali pasiduoti užsienio arba kitų šaltinių spaudimui.

Ypač atidžiai turi būti tikrinami asmenys:

d) kuriems bus suteikta galimybė naudotis slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėta informacija;

e) einantys tokias pareigas, kad nuolat turi naudotis dideliu kiekiu slaptumo žyma ►M1 SECRET UE ◄ pažymėtos informacijos;

f) kurių pareigos suteikia jiems specialią galimybę naudotis uždaromis ryšių ir informacijos sistemomis, kartu ir galimybę be leidimo naudotis dideliu kiekiu ES įslaptintos informacijos arba techninio sabotažo veiksmais smarkiai pakenkti užduočių vykdymui.

Punktuose d, e, ir f apibūdintais atvejais reikėtų kiek tik įmanoma panaudoti operatyvinius tyrimo metodus.

Kai asmenis, kurių atžvilgiu negalima remtis „būtina žinoti“ principu, reikia įdarbinti tokiame darbe, kuriame jie galėtų naudotis ES įslaptinta informacija (pvz., pasiuntiniai, apsaugos darbuotojai, priežiūros personalas, valytojai ir kt.), pirmiausia jie tinkamai patikrinami pagal saugumo kriterijus.

6.2. **Asmens patikimumo pažymėjimų registravimas**

Visi Komisijos departamentai, tvarkantys ES įslaptintą informaciją arba turintys uždarų ryšių arba informacijos sistemų, registruoja tam paskirtam personalui išduotus asmens patikimumo pažymėjimus. Kiekvienas pažymėjimas prireikus tikrinamas, kad būtų užtikrinta, jog jis atitinka dabartines to asmens funkcijas; jie pakartotinai tikrinami prioritetine tvarka, jei gaunama naujos informacijos, kad tolesnis paskyrimas darbui su įslaptinta informacija nebeatitinka saugumo interesų. Patikimumo pažymėjimų registrą jo kompetencijai priskirtoje srityje veda Komisijos departamento vietos saugumo pareigūnas.

6.3. **Personalo saugumo instruktažas**

Visi galimybes naudotis įslaptinta informacija sudarančias pareigas einantys darbuotojai, pradėdami eiti pareigas ir reguliariai vėliau, saugumo sumetimais nuodugniai instruktuojami apie saugumo reikalavimų poreikį ir jų vykdymo tvarką. Tokie darbuotojai privalo raštu patvirtinti, kad susipažino su esamais saugumo reikalavimais ir kad juos visiškai supranta.

6.4. **Vadovų atsakomybė**

Vadovai privalo žinoti, kurie jų darbuotojai dirba su įslaptinta informacija arba gali naudotis uždaromis ryšių ar informacijos sistemomis, bei registruoti ir pranešti apie visus galinčius turėti įtakos saugumui incidentus arba pažeidimus.

6.5. **Personalo saugumas**

Nustatoma tvarka, užtikrinanti, kad, gavus tam tikram asmeniui nepalankios informacijos, išsiaiškinama, ar jis dirba su įslaptinta informacija arba ar gali naudotis uždaromis ryšių arba informacijos sistemomis, ir informuojamas ►M2 Komisijos Saugumo direktoratas ◄. Nustačius, kad toks asmuo kelia grėsmę saugumui, jam neleidžiama atlikti pareigų arba jis nušalinamas nuo pareigų, kurias eidamas gali kelti grėsmę saugumui.

▼B

7. FIZINIS SAUGUMAS

7.1. **Apsaugos poreikis**

Fizinio saugumo priemonių, taikytinų užtikrinant ES įslaptintos informacijos apsaugą, veiksmingumo laipsnis turi būti proporcingas laikomos informacijos ir medžiagos slaptumui, kiekiui ir galimai grėsmei. Visi ES įslaptintos informacijos laikytojai laikosi vienodos tos informacijos įslaptinimo praktikos ir paiso bendrų apsaugos standartų, susijusių su saugomos informacijos ir medžiagos laikymu, perdavimu ir naikinimu.

7.2. **Tikrinimas**

Prieš išeidami iš zonų, kuriose be priežiūros paliekama ES įslaptinta informacija, už jos laikymą atsakingi asmenys užtikrina, kad ji būtų paliekama saugiai ir kad yra aktyvuotos visos apsaugos priemonės (užraktai, signalizacija ir kt.). Tolesni nepriklausomi tikrinimai atliekami po darbo valandų.

7.3. **Pastatų saugumas**

Pastatai, kuriuose kaupiama ES įslaptinta informacija arba laikomos uždaros ryšių ir informacijos sistemos, saugomi, kad į juos nepatektų leidimo neturintys asmenys. ES įslaptintos informacijos apsaugos pobūdis, pvz., langų grotos, durų užraktai, apsauga prie įėjimų, automatizuotos priėjimo kontrolės sistemos, apsaugos tikrinimai ir patruliai, signalizacijos sistemos, į įsibrovimą reaguojančios sistemos ir sarginiai šunys, priklauso nuo:

a) saugotinos informacijos ir medžiagos slaptumo lygio, kiekio ir jų laikymo vietos pastate;

b) šios informacijos ir medžiagos apsaugos konteinerių kokybės;

c) pastato savybių ir vietos.

Ryšių ir informacijos sistemų apsaugos pobūdis analogiškai priklauso nuo laikomo turto vertės ir galimos žalos, jei kiltų grėsmė saugumui, įvertinimo, nuo pastato, kuriame sistema laikoma, savybių bei vietos ir nuo sistemos vietos pastate.

7.4. **Nenumatytoms aplinkybėms skirti planai**

Iš anksto parengiami išsamūs planai, kaip apsaugoti įslaptintą informaciją ištikus vietinio arba nacionalinio masto nelaimei.

8. INFORMACIJOS SAUGUMAS

Informacijos saugumas (INFOSEC) yra susijęs su ES įslaptintos informacijos apdorojimui, laikymui arba perdavimui ryšių, informacijos arba kitokiomis elektroninėmis sistemomis apsaugoti nuo tyčinio arba atsitiktinio pakenkimo jos slaptumui, vientisumui arba galimybei ja naudotis skirtų saugumo priemonių nustatymu ir taikymu. Imamasi atitinkamų kontrapriemonių, sutrukdant pasinaudoti ES įslaptinta informacija leidimo neturintiems vartotojams ar neleisti naudotis ES įslaptinta informacija leidimą turintiems vartotojams bei užkertant kelią ES įslaptintos informacijos klastojimui arba jos taisymui ar sunaikinimui neturint tam leidimo.

▼B

9. KITŲ TYČINĖS ŽALOS DARYMO FORMŲ KONTROLĖ IR PASIPRIEŠINIMAS SABOTAŽUI

Nuo sabotažo ir tyčinio žalos padarymo geriausiai apsaugo fizinės atsargumo priemonės svarbiems įrenginiams, kuriuose kaupiama įslaptinta informacija, apsaugoti; vien personalo tikrinimas nėra pakankamas šių priemonių pakaitalas. Kompetentinga nacionalinė institucija yra prašoma teikti informaciją apie šnipinėjimą, sabotažą, terorizmą ir kitokią ardomąją veiklą.

10. ĮSLAPTINTOS INFORMACIJOS PERDAVIMAS TREČIOSIOMS ŠALIMS ARBA TARPTAUTINĖMS ORGANIZACIJOMS

Komisija kolegialiai priima sprendimą dėl jos sukurtos ES įslaptintos informacijos perdavimo trečiajai šaliai arba tarptautinei organizacijai. Jei Komisija nėra norimos perduoti informacijos autorius, ji pirmiausia turi gauti tikrojo autoriaus sutikimą perduoti tą informaciją. Jei autoriaus negalima nustatyti, sprendimą priima Komisija.

Jei Komisija gauna įslaptintos informacijos iš trečiųjų valstybių, tarptautinių organizacijų arba iš kitų trečiųjų šalių, tai informacijai suteikiama apsauga, atitinkanti jos slaptumo lygį ir prilygstanti šiose nuostatose ES įslaptintai informacijai nustatytiems standartams arba informaciją perduodančios trečiosios šalies reikalaujamiems aukštesnio lygio standartams. Gali būti atliekami abipusiai tikrinimai.

Pirmiau išvardyti principai įgyvendinami pagal II dalies 26 skirsnio ir 3, 4 ir 5 priedėlių išsamias nuostatas.

II DALIS. SAUGUMO ORGANIZAVIMAS KOMISIJOJE

11. UŽ SAUGUMĄ ATSAKINGAS KOMISIJOS NARYS

Už saugumą atsakingas Komisijos narys:

a) įgyvendina Komisijos saugumo politiką;

b) svarsto Komisijos arba jos kompetentingų įstaigų nurodytas saugumo problemas;

c) glaudžiai bendradarbiaudamas su valstybių narių nacionalinėmis saugumo (arba kitomis tinkamomis) institucijomis (toliau – NSI), nagrinėja Komisijos saugumo politikos keitimo klausimus.

Už saugumą atsakingas Komisijos narys visų pirma atsako už:

a) su Komisijos veikla susijusių visų saugumo reikalų koordinavimą;

b) prašymų, kad NSI pagal 20 skirsnį Komisijoje dirbantiems darbuotojams išduotų asmens patikimumo pažymėjimus, perdavimą valstybių narių paskirtoms institucijoms;

c) ES įslaptintos informacijos nutekėjimo tyrimą arba nurodymą atlikti tokį tyrimą, jei, pagal *prima facie* (pirminius) įrodymus, jis įvyko Komisijoje;

d) prašymą atitinkamoms saugumo institucijoms pradėti tyrimą, kai panašu, kad ES įslaptintos informacijos nutekėjimas įvyko už Komisijos ribų, ir tyrimo koordinavimą, kai jame dalyvauja daugiau nei viena saugumo institucija;

e) reguliarius ES įslaptintos informacijos apsaugai skirtų saugumo priemonių patikrinimus;

▼B

f) glaudaus bendradarbiavimo su visomis suinteresuotomis saugumo institucijomis palaikymą siekiant bendro saugumo koordinavimo;

g) nuolatinį Komisijos saugumo politikos ir procedūrų patikslinimą ir, jei reikia, atitinkamų rekomendacijų rengimą. Atsižvelgiant į tai, už saugumą atsakingas Komisijos narys Komisijai pateikia ►M2 Komisijos Saugumo direktorato ◄ parengtą metinį tikrinimo planą.

12. KOMISIJOS SAUGUMO POLITIKOS PATARĖJŲ GRUPĖ

Sudaroma Komisijos Saugumo politikos patarėjų grupė. Ją sudaro grupei pirmininkaujantis už saugumą atsakingas Komisijos narys arba jo deleguotas asmuo, taip pat kiekvienos valstybės narės NSI atstovas. Gali būti kviečiami ir kitų Europos institucijų atstovai. Kai nagrinėjami su EK ir ES atitinkamomis decentralizuotomis agentūromis susiję klausimai, taip pat gali būti kviečiami tų agentūrų atstovai.

Komisijos Saugumo politikos patarėjų grupė renkasi pirmininko arba kurio nors grupės nario kvietimu. Grupės užduotis – nagrinėti ir vertinti visus svarbius saugumo klausimus ir prireikus teikti rekomendacijas Komisijai.

▼M2

13. KOMISIJOS SAUGUMO TARYBA

Įkuriama Komisijos Saugumo taryba. Ją sudaro Administracijos ir personalo generalinis direktorius (jis pirmininkauja tarybai), už saugumą atsakingo Komisijos nario kabineto narys, Pirmininko kabineto narys, Komisijos krizių valdymo grupei pirmininkaujantis generalinio sekretoriaus pavaduotojas, Teisės tarnybos, Išorės santykių, Teisingumo, laisvės ir saugumo, Jungtinio tyrimų centro, Informatikos ir Vidaus audito tarnybos generaliniai direktoriai bei Komisijos Saugumo direktorato direktorius arba minėtų asmenų atstovai. Gali būti kviečiami kiti Komisijos pareigūnai. Ji vertina Komisijos saugumo priemones ir teikia rekomendacijas šioje srityje už saugumą atsakingam Komisijos nariui.

▼B

14. ►M2 KOMISIJOS SAUGUMO DIREKTORATAS ◄

Kad atliktų 11 skirsnyje minėtas pareigas, už saugumą atsakingas Komisijos narys saugumo priemonėms koordinuoti, prižiūrėti ir įgyvendinti savo žinioje turi ►M2 Komisijos Saugumo direktoratą ◄.

►M2 Komisijos Saugumo direktorato direktorius ◄ yra pagrindinis už saugumą atsakingo Komisijos nario patarėjas saugumo klausimais ir kartu veikia kaip Saugumo politikos patarėjų grupės sekretorius. Todėl jis vadovauja saugumo taisyklių atnaujinimo darbui ir koordinuoja saugumo priemones su valstybių narių kompetentingomis institucijomis, o prireikus – ir su tarptautinėmis organizacijomis, saugumo sutartimis susijusiomis su Komisija. Jis yra už tokius kontaktus atsakingas pareigūnas.

►M2 Komisijos Saugumo direktorato direktorius ◄ atsako už Komisijos IT sistemų ir tinklų akreditavimą. ►M2 Komisijos Saugumo direktorato direktorius ◄, suderinęs su atitinkamomis NSI, priima sprendimus dėl IT sistemų ir tinklų, apimančių Komisiją ir bet kurį kitą ES įslaptintos informacijos gavėją, akreditavimo.

▼B

15. SAUGUMO TIKRINIMAI

►M2 Komisijos Saugumo direktoratas ◄ reguliariai tikrina ES įslaptintos informacijos apsaugai skirtas saugumo priemones.

►M2 Komisijos Saugumo direktoratui ◄ atlikti šią užduotį gali padėti kitų ESĮI laikančių ES institucijų saugumo tarnybos arba valstybių narių nacionalinės saugumo institucijos ([1]).

Valstybės narės pageidavimu, abiem šalims susitarus, ESĮI tikrinimą Komisijoje gali atlikti šios valstybės NSI kartu su ►M2 Komisijos Saugumo direktoratas ◄.

16. SLAPTUMO ŽYMOS, JŲ GALIOJIMO ŽYMOS IR SPAUDAI

16.1. **Slaptumo žymų laipsniai** ([2])

Informacija įslaptinama tokiais slaptumo žymų laipsniais (taip pat žr. 2 priedėlį):

►M1 TRES SECRET UE/EU TOP SECRET ◄: ši žyma suteikiama tik tai informacijai ir medžiagai, kurią atskleidus be leidimo, gali būti padaryta ypač didelė žala svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams.

►M1 SECRET UE ◄: ši žyma suteikiama tik tai informacijai ir medžiagai, kurią atskleidus be leidimo, gali būti labai pakenkta svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams.

►M1 CONFIDENTIEL UE ◄: ši žyma suteikiama tai informacijai ir medžiagai, kurią atskleidus be leidimo, gali būti pakenkta svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams.

►M1 RESTREINT UE ◄: ši žyma suteikiama tai informacijai ir medžiagai, kurios atskleidimas be leidimo gali būti nenaudingas svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams.

Jokios kitos slaptumo žymos yra neleistinos.

16.2. **Slaptumo žymos galiojimo žymos**

Slaptumo žymos galiojimo terminams nustatyti (įslaptintai informacijai, kuriai taikomas automatinis slaptumo laipsnio sumažinimas arba išslaptinimas) gali būti naudojamos sutartos slaptumo žymos galiojimo žymos. Tokios žymos gali būti „IKI… (laikas/data)“ arba „IKI… (įvykis)“.

Kai reikia riboti įslaptintos informacijos platinimą ir ją tvarkyti specialiu būdu, šalia slaptumo žymų naudojamos papildomos įslaptinimą nurodančios žymos, tokios kaip CRYPTO arba bet kurios kitos ES pripažįstamos žymos.

Slaptumo žymos galiojimo žymos naudojamos tik kartu su slaptumo žymomis.

16.3. **Kvalifikacinės žymos**

Kvalifikacines žymas galima naudoti, kai reikia tiksliai apibrėžti dokumento taikymo sritį arba pažymėti specialų jo platinimą vadovaujantis „būtina žinoti“ principu ar nurodyti, kada baigiasi draudimas platinti (neįslaptintos informacijos atveju).

Kvalifikacinė žyma nėra slaptumo žyma, todėl negali būti naudojama vietoje jos.

([1]) Nepažeidžiant 1961 m. Vienos konvencijos dėl diplomatinių santykių ir 1965 m. balandžio 8 d. Protokolo dėl Europos Bendrijų privilegijų ir imunitetų.

([2]) Žr.1 priedėlyje ES, NATO, VES ir valstybių narių slaptumo žymų palyginamąją lentelę.

▼B

Dokumentams, susijusiems su Sąjungos arba vienos ar daugiau jos valstybių narių saugumu ir gynyba arba su kariniu ar nekariniu krizių valdymu, ir tų dokumentų kopijoms suteikiama ESGP kvalifikacinė žyma.

16.4. **Slaptumo žymos dėjimas**

Slaptumo žyma dedama taip:

a) ant dokumentų, žymimų slaptumo žyma ►M1 RESTREINT UE ◄, – mechaninėmis arba elektroninėmis priemonėmis;

b) ant dokumentų, žymimų slaptumo žyma ►M1 CONFIDENTIEL UE ◄, – mechaninėmis priemonėmis ar ranka arba spausdinant ant iš anksto antspauduoto ir registruoto popieriaus;

c) ant dokumentų, žymimų slaptumo žyma ►M1 SECRET UE ◄ ir ►M1 TRES SECRET UE/EU TOP SECRET ◄, – mechaninėmis priemonėmis arba ranka.

16.5. **Slaptumo žymos galiojimo žymų dėjimas**

Slaptumo žymos galiojimo žymos dedamos tiesiai po slaptumo žyma, tomis pačiomis priemonėmis, kaip ir slaptumo žymos.

17. ĮSLAPTINIMO TVARKYMAS

17.1. **Bendrosios nuostatos**

Informacija įslaptinama tik tuomet, kai tai reikalinga. Slaptumo žyma turi būti aiškiai ir teisingai nurodyta ir taikoma tik tol, kol informaciją reikia saugoti.

Atsakomybė už informacijos įslaptinimą ir už bet kokį paskesnį slaptumo žymos laipsnio sumažinimą arba informacijos išslaptinimą tenka tik informacijos autoriui.

Komisijos pareigūnai ir kiti darbuotojai informaciją įslaptina, jos slaptumo žymos laipsnį sumažina arba informaciją išslaptina tik gavę savo departamento vadovo nurodymą arba sutikimą.

Detali įslaptintų dokumentų naudojimo tvarka parengta taip, kad būtų užtikrinta derama juose esančios informacijos apsauga.

Asmenų, galinčių siūlyti dokumentus, žymimus slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, turi būti kuo mažiau, o jų pavardės turi būti įtrauktos į ►M2 Komisijos Saugumo direktorato ◄ sudarytą sąrašą.

17.2. **Slaptumo žymų naudojimas**

Dokumento slaptumas nustatomas pagal 16 skirsnyje apibrėžtą jo turinio slaptumą. Svarbu, kad įslaptinimas būtų taikomas teisingai ir nuosaikiai. Tai ypač taikytina slaptumo žymai ►M1 TRES SECRET UE/EU TOP SECRET ◄.

Įslaptinamo dokumento autorius turi prisiminti minėtas taisykles ir išvengti pernelyg aukšto ar pernelyg žemo slaptumo žymos laipsnio suteikimo.

2 priedėlyje pateikiamas praktinis įslaptinimo vadovas.

Prireikus atitinkamo dokumento atskiriems lapams, dalims, skyriams, priedams ir priedėliams suteikti skirtingas slaptumo žymas, jie ir yra atitinkamai įslaptinami. Visas dokumentas įslaptinamas pagal aukščiausią slaptumo žymos laipsnį turinčią jo dalį.

▼B

Pridedamų dokumentų lydraščių arba atžymų slaptumo žymos laipsnis atitinka priedų aukščiausio laipsnio slaptumo žymas. Jei tokie dokumentai pateikiami atskirai nuo priedų, autorius turi aiškiai nurodyti, koks slaptumo žymos laipsnis jiems suteikiamas.

Viešą naudojimą reglamentuoja Reglamentas (EB) Nr. 1049/2001.

17.3. **Slaptumo žymos laipsnio sumažinimas ir išslaptinimas**

ES įslaptintų dokumentų slaptumo žymos laipsnis gali būti sumažintas arba jie gali būti visai išslaptinti tik leidus jų autoriui, ir prireikus pasitarus su kitomis suinteresuotomis šalimis. Dokumentų slaptumo žymos laipsnio sumažinimas arba jų išslaptinimas patvirtinamas raštu. Dokumento autorius atsako už to dokumento gavėjų informavimą apie slaptumo žymos pakeitimą, o šie atitinkamai atsako už kitų adresatų, kuriems jie yra nusiuntę dokumentą arba jo kopiją, informavimą apie slaptumo žymos pakeitimą.

Jei įmanoma, ant įslaptinto dokumento jo autorius nurodo datą, laikotarpį arba įvykį, nuo kurio turinio slaptumo žymos laipsnis gali būti sumažintas arba dokumentas išslaptintas. Priešingu atveju dokumentų autoriai peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad garantuotų, jog reikalingas pradinis įslaptinimas.

18. FIZINIS SAUGUMAS

18.1. **Bendrosios nuostatos**

Svarbiausi fizinio saugumo priemonių tikslai yra neleisti leidimo neturinčiam asmeniui naudotis ES įslaptinta informacija ir (arba) medžiaga, užkirsti kelią įrangos ir kitokio turto vagystėms bei niokojimui ir priekabiavimui ar kitokios formos agresijai personalo, kitų darbuotojų bei lankytojų atžvilgiu.

18.2. **Saugumo reikalavimai**

Visos patalpos, zonos, pastatai, kambariai, ryšių ir informacijos sistemos ir kt., kuriuose saugoma ES įslaptinta informacija ir (arba) su ja dirbama, yra saugomos tinkamomis fizinės apsaugos priemonėmis.

Sprendžiant, koks fizinio saugumo lygis reikalingas, atsižvelgtina į visus svarbius veiksnius, pavyzdžiui:

a) informacijos ir (arba) medžiagos slaptumo žymą;

b) laikomos informacijos kiekį ir formą (pvz., spausdintinė kopija, kompiuterinių duomenų saugojimo laikmenos);

c) vietoje įvertinta prieš ES, valstybes nares ir (arba) kitas ES įslaptintą informaciją laikančias institucijas arba trečiąsias šalis nukreiptų žvalgybos tarnybų keliama grėsmė, ypač dėl sabotažo, terorizmo ir kitų rūšių ardomosios ir (arba) nusikalstamos veiklos.

Fizinio saugumo priemonės sukuriamos tam, kad būtų:

a) sutrukdyta įsibrauti slaptai arba įsiveržti jėga;

b) sutrukdyti ir atskleisti nelojalaus personalo veiksmai arba atgrasinta nuo tokių veiksmų;

c) neleista ES įslaptinta informacija pasinaudoti tiems, kuriems nėra būtina ją žinoti.

▼B

18.3. **Fizinės apsaugos priemonės**

18.3.1. *Saugumo zonos*

Zonos, kuriose dirbama su ►M1 CONFIDENTIEL UE ◄ arba aukštesnio laipsnio slaptumo žyma pažymėta informacija arba kuriose tokia informacija saugoma, yra organizuojamos ir įrengiamos taip, kad atitiktų vieną iš šių reikalavimų:

a) I klasės saugumo zona: zona, kurioje dokumentai su ►M1 CONFIDENTIEL UE ◄ arba aukštesnio laipsnio slaptumo žyma yra tvarkomi ir saugomi tokiu būdu, kad įėjus į zoną galima visais praktiniais tikslais naudotis įslaptinta informacija. Tokiai zonai yra reikalinga:

   i) aiškiai atribota ir apsaugota erdvė, kiekvienas įėjimas ar išėjimas iš kurios yra kontroliuojamas;

   ii) įėjimo kontrolės sistema, kuri leidžia į zoną įeiti tik deramai patikrintiems ir specialų leidimą turintiems asmenims;

   iii) paprastai zonoje laikomos informacijos, t. y. informacijos, kuria galima naudotis įėjus, slaptumo žymų laipsnio specifikacija.

b) II klasės saugumo zona: zona, kurioje su ►M1 CONFIDENTIEL UE ◄ arba aukštesnio laipsnio slaptumo žyma pažymėtais dokumentais dirbama arba jie saugomi tokiu būdu, kad dėl viduje sukurtų kontrolės priemonių jie yra apsaugomi taip, kad jais negalėtų pasinaudoti leidimo neturintys asmenys, pavyzdžiui, patalpos, kuriose yra reguliariai su ►M1 CONFIDENTIEL UE ◄ arba aukštesnio laipsnio slaptumo žyma pažymėtais dokumentais dirbančios ir juos saugančios tarnybos. Tokiai zonai yra reikalinga:

   i) aiškiai atribota ir apsaugota erdvė, kiekvienas įėjimas ar išėjimas iš kurios yra kontroliuojamas;

   ii) įėjimo kontrolės sistema, kuri be palydos leidžia į zoną įeiti tik deramai patikrintiems ir specialų leidimą turintiems asmenims. Visiems kitiems asmenims turi būti užtikrinta palyda arba lygiavertė kontrolė, kad neturintieji leidimo negalėtų naudotis ES įslaptinta informacija ir nekontroliuojamai įeiti į zonas, kuriose taikomas techninis saugumo patikrinimas.

   Zonos, kuriose nėra visą parą budinčio personalo, tikrinamos iškart po įprastų darbo valandų, kad būtų užtikrinta, jog ES įslaptinta informacija yra tinkamai saugoma.

18.3.2. *Administracinė zona*

Aplink I ir II klasės saugumo zonas arba pakeliui į jas gali būti sukurta mažesnio saugumo administracinė zona. Tokiai zonai reikalinga aiškiai atribota erdvė, sudaranti galimybes tikrinti personalą ir transporto priemones. Tokiose zonose dirbama tik su slaptumo žyma ►M1 RESTREINT UE ◄ pažymėta ir neįslaptinta informacija, tik tokia informacija gali būti jose saugoma.

18.3.3. *Įėjimo ir išėjimo kontrolė*

Įėjimas į I ir II klasės saugumo zonas ir išėjimas iš jų kontroliuojamas leidimų arba asmens atpažinimo sistemomis, taikomomis visam šiose zonose paprastai dirbančiam personalui. Taip pat sukuriama lankytojų tikrinimo sistema, kuri neleidžia ES įslaptinta informacija naudotis neturint atitinkamo leidimo. Papildomai prie leidimų sistemos gali būti naudojami automatizuoti identifikavimo įrenginiai, tačiau jie laikytini papildoma, bet apsaugos personalo visiškai nepakeičiančia priemone. Pasikeitus grėsmės įvertinimui, pvz., per žymių asmenų vizitus, gali prireikti imtis griežtesnių įėjimo ir išėjimo kontrolės priemonių.

▼B

18.3.4. *Apsaugos patruliai*

I ir II klasės saugumo zonų patruliai dirba pasibaigus įprastoms darbo valandoms, kad ES turtas nebūtų neteisėtai atskleistas, sunaikintas arba prarastas. Patruliavimo dažnumas nustatomas atsižvelgiant į vietos aplinkybes, tačiau rekomenduotina patruliuoti kas dvi valandas.

18.3.5. *Apsaugos konteineriai ir ugniai bei įsilaužimui atsparūs kambariai*

ES įslaptintai informacijai saugoti naudojami trijų klasių konteineriai:

— A klasė: nacionaliniu lygiu sertifikuoti informacijai, pažymėtai slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, I arba II klasės saugumo zonose saugoti skirti konteineriai;

— B klasė: nacionaliniu lygiu sertifikuoti informacijai, pažymėtai slaptumo žyma ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄, I arba II klasės saugumo zonose saugoti skirti konteineriai;

— C klasė: tarnybiniai baldai, tinkami tiktai slaptumo žyma ►M1 RESTREINT UE ◄ pažymėtai informacijai saugoti.

I ir II klasės saugumo zonose įrengtuose ugniai ir įsilaužimui atspariuose kambariuose ir visose I klasės saugumo zonose, kur atvirose lentynose arba brėžiniuose, žemėlapiuose ir pan. yra laikoma informacija su ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma, sienos, grindys, lubos ir durys su užraktais turi būti SAI sertifikuotos kaip suteikiančios apsaugą, kuri atitinka apsaugos konteinerio klasę, patvirtintą to paties laipsnio slaptumo žymos informacijai saugoti.

18.3.6. *Užraktai*

Apsaugos konteinerių ir ugniai ir įsilaužimui atsparių kambarių, kuriuose laikoma ES įslaptinta informacija, užraktai turi atitikti tokias normas:

— A grupė: nacionaliniu lygiu sertifikuoti A klasės konteineriams,

— B grupė: nacionaliniu lygiu sertifikuoti B klasės konteineriams,

— C grupė: tinkami tik C klasės tarnybiniams baldams.

18.3.7. *Raktų ir kombinacijų kontrolė*

Apsaugos konteinerių raktai iš Komisijos pastatų neišnešami. Apsaugos konteinerių kombinacijas įsimena tie asmenys, kuriems privalu jas žinoti. Už atsarginių raktų ir užrašytos kiekvienos kombinacijos, skirtų naudoti nenumatytais atvejais, laikymą atsako atitinkamo Komisijos departamento vietos saugumo pareigūnas; užrašytos kombinacijos laikomos atskiruose antspauduotuose nepermatomuose vokuose. Darbiniai raktai, atsarginiai apsaugos raktai ir užrašytos kombinacijos laikomi atskiruose apsaugos konteineriuose. Tokie raktai ir užrašytos kombinacijos saugomi ne mažiau griežtai, nei medžiaga, kuria naudotis jie suteikia galimybę.

Apsaugos konteinerių kombinacijas turi žinoti kiek įmanoma mažiau žmonių. Kombinacijos keičiamos:

a) gavus naują konteinerį;

b) pasikeitus personalui;

c) neteisėtai atskleidus informaciją arba įtarus, kad tai padaryta;

d) pageidautina kas šešis mėnesius ir būtinai ne rečiau kaip kartą per metus.

▼B

18.3.8. *Į įsibrovimą reaguojanti įranga*

Kai ES įslaptintai informacijai apsaugoti yra naudojamos signalizacijos sistemos, uždaros grandinės videostebėjimo sistemos ir kiti elektroniniai prietaisai, būtinas atsarginis elektros energijos tiekimo šaltinis, užtikrinantis sistemos tolesnį veikimą nutrūkus pagrindiniam energijos tiekimui. Kitas esminis reikalavimas yra tas, kad signalizacija įsijungtų ar apsaugos personalas būtų kitaip patikimai įspėtas sutrikus šioms sistemoms ar mėginant jas sugadinti.

18.3.9. *Aprobuoti įrengimai*

►M2 Komisijos Saugumo direktoratas ◄ veda atnaujintus įslaptintai informacijai įvairiomis išsamiai apibrėžtomis aplinkybėmis ir sąlygomis saugoti jo aprobuotų apsaugos įrengimų sąrašus pagal tipą ir modelį. ►M2 Komisijos Saugumo direktoratas ◄ tuos sąrašus sudaro *inter alia* remdamasis iš NSI gauta informacija.

18.3.10. *Fizinė kopijavimo aparatų ir telefaksų apsauga*

Kopijavimo aparatai ir telefaksai fiziškai apsaugomi taip, kad būtų užtikrinta, jog jais naudosis tik leidimą apdoroti įslaptintą informaciją turintys asmenys ir kad visi įslaptinti objektai bus tinkamai kontroliuojami.

18.4. **Apsauga nuo pamatymo ir slapto pasiklausymo**

18.4.1. *Pamatymas*

Tiek dieną, tiek naktį imamasi visų tinkamų priemonių, užtikrinančių, kad ES įslaptintos informacijos netgi atsitiktinai nepamatų joks leidimo tam neturintis asmuo.

18.4.2. *Slaptas pasiklausymas*

Tarnybos ir zonos, kuriose nuolat yra svarstoma informacija su ►M1 SECRET UE ◄ ir aukštesnio laipsnio slaptumo žyma, esant atitinkamai rizikai turi būti apsaugomos nuo galimo pasyvaus arba aktyvaus slapto pasiklausymo. Už tokio pasiklausymo rizikos vertinimą atsako ►M2 Komisijos Saugumo direktoratas ◄, prireikus pasikonsultavęs su NSI.

18.4.3. *Elektroninių ir įrašymo įrengimų įsinešimas*

Be išankstinio ►M2 Komisijos Saugumo direktorato direktoriaus ◄ leidimo į saugumo zonas arba techniškai saugomas zonas neleidžiama įsinešti mobiliųjų telefonų, asmeninių kompiuterių, įrašymo prietaisų, kamerų ar kitų elektroninių arba įrašymo įrengimų.

Kad nustatytų, kokių apsaugos priemonių reikia imtis patalpų, kuriose egzistuoja pasyvaus (pvz., sienų, durų, grindų ir lubų izoliacija, garso stiprumo matavimai) ir aktyvaus (pvz., mikrofonų paieška) slapto pasiklausymo pavojus, atžvilgiu, ►M2 Komisijos Saugumo direktoratas ◄ gali kreiptis pagalbos į NSI ekspertus.

Taip pat ►M2 Komisijos Saugumo direktorato direktoriaus ◄ prašymu už techninį saugumą atsakingi NSI ekspertai prireikus gali patikrinti telekomunikacijų įrangą ir bet kokią elektrinę ar elektroninę biuro įrangą, naudojamą per ►M1 SECRET UE ◄ ar aukštesnio slaptumo žymos laipsnio posėdžius.

▼B

18.5. **Techniškai apsaugotos zonos**

Tam tikras zonas galima išskirti kaip techniškai saugias. Atliekamas specialus tikrinimas į jas įeinant. Tokios zonos, kai jose nedirbama, patvirtintu būdu laikomos užrakintos, o visi raktai laikomi apsaugos raktais. Tokios zonos reguliariai fiziškai tikrinamos, taip pat ir tuo atveju, kai nustatoma ar įtariama, kad į jas įeita be leidimo.

Kad būtų stebima įrangos ir baldų vietų kaita, padaromas detalus inventoriaus planas. Į tokią zoną neįnešami jokie baldai ar įranga, kol jų rūpestingai nepatikrina apsaugos personalas, specialiai parengtas ieškoti pasiklausymo priemonių. Paprastai techniškai apsaugotose zonose tiesti ryšių linijų neleidžiama be išankstinio atitinkamos institucijos leidimo.

19. BENDROS PRINCIPO „BŪTINA ŽINOTI“ TAIKYMO IR ES PERSONALO PATIKIMUMO TIKRINIMO TAISYKLĖS

19.1. **Bendrosios nuostatos**

Naudotis ES įslaptinta informacija leidžiama tik asmenims, kuriems ją būtina žinoti, kad galėtų atlikti savo pareigas arba vykdyti užduotis. Naudotis žymomis ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄ pažymėta informacija leidžiama tik asmenims, turintiems atitinkamą asmens patikimumo pažymėjimą.

Nustatyti, kam taikytinas „būtina žinoti“ principas, privalo departamentas, kuriame atitinkamas asmuo turi būti įdarbintas.

Kiekvienas departamentas turi reikalauti patikrinti asmens patikimumą.

Asmenį patikrinus, jam yra išduodamas „ES asmens patikimumo pažymėjimas“, kuriame nurodomas informacijos, kuria asmuo gali naudotis, slaptumo žymos laipsnis ir pažymėjimo galiojimo laikas.

ES asmens patikimumo pažymėjimas, išduotas tam tikram slaptumo žymos laipsniui, gali suteikti jo turėtojui teisę naudotis žemesnio slaptumo žymos laipsnio informacija.

Pareigūnais ar kitokiais darbuotojais nesantys asmenys, tokie kaip išoriniai sutarčių partneriai, ekspertai arba konsultantai, su kuriais gali prireikti aptarti arba kuriems gali prireikti parodyti ES įslaptintą informaciją, privalo turėti ES asmens patikimumo pažymėjimus dėl teisės naudotis ES įslaptinta informacija, bei yra trumpai supažindinami su jų atsakomybe už saugumą.

Viešą naudojimąsi reglamentuoja Reglamentas (EB) Nr. 1049/2001.

19.2. **Specialios naudojimosi informacija, pažymėta slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, taisyklės**

Visi asmenys, kuriems reikia naudotis informacija, pažymėta slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, pirmiausia patikrinami, ar turi teisę tokia informacija naudotis.

Visus asmenis, kurie turi naudotis informacija, pažymėta slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, nurodo už saugumą atsakingas Komisijos narys, o jų pavardės įrašomos atitinkamame įslaptintos informacijos, pažymėtos slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, registre. Šį registrą sukuria ir tvarko ►M2 Komisijos Saugumo direktoratas ◄.

▼B

Prieš gaudami leidimą naudotis informacija, pažymėta slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, visi asmenys pasirašo dokumentą, patvirtinantį, kad jie buvo supažindinti su Komisijos saugumo procedūromis, kad visiškai supranta savo ypatingą pareigą saugoti slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtą informaciją, ir supranta padarinius, kuriuos numato ES taisyklės bei nacionaliniai teisės ir administraciniai aktai, jei įslaptinta informacija tyčia arba dėl neatsargumo patektų į leidimo neturinčio asmens rankas.

Jei žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėta informacija asmenys turi naudotis posėdžiuose ir pan., kompetentingi tarnybos arba įstaigos, kurioje tie asmenys dirba, kontrolės pareigūnai posėdį organizuojančią įstaigą informuoja, kad tie asmenys turi atitinkamus leidimus.

Visų asmenų, kurie toliau nebeeina su būtinybe naudotis slaptumo žyma žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėta informacija susijusių pareigų, pavardės išbraukiamos iš turinčių teisę naudotis informacija su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ asmenų sąrašo. Be to, visų tokių asmenų dėmesys dar kartą atkreipiamas į jų ypatingą pareigą saugoti informaciją, pažymėtą slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄. Jie taip pat pasirašo pasižadėjimus, kad nenaudos ir neperduos turimų žinių apie slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtą informaciją.

19.3. **Specialios naudojimosi informacija, pažymėta slaptumo žymomis ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄, taisyklės**

Visi asmenys, kuriems reikia naudotis slaptumo žymomis ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄ pažymėta informacija, pirmiausia yra patikrinami atitinkamai slaptumo žymos laipsniui.

Visi asmenys, kuriems reikia naudotis slaptumo žymomis ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄ pažymėta informacija, supažindinami su atitinkamomis saugumo taisyklėmis ir neatsargumo padariniais.

Jei slaptumo žymomis ►M1 SECRET UE ◄ arba ►M1 CONFIDENTIEL UE ◄ pažymėta informacija asmenys turi naudotis posėdžiuose ir pan., juos įdarbinusios įstaigos saugumo pareigūnas posėdį organizuojančią įstaigą informuoja, kad tie asmenys turi atitinkamus leidimus.

19.4. **Specialios naudojimosi informacija, pažymėta slaptumo žyma ►M1 RESTREINT UE ◄, taisyklės**

Asmenys, galintys naudotis slaptumo žyma ►M1 RESTREINT UE ◄ pažymėta informacija, supažindinami su saugumo taisyklėmis ir neatsargumo padariniais.

19.5. **Perkėlimai**

Kai personalo narys yra perkeliamas iš pareigų, kurias eidamas turėjo dirbti su ES įslaptinta medžiaga, registratūra prižiūri, kad pareigas paliekantis pareigūnas tą medžiagą tinkamai perduotų jo pareigas eisiančiam pareigūnui.

Kai personalo narys yra perkeliamas į kitas pareigas, kurias eidamas turės dirbti su ES įslaptinta medžiaga, vietos saugumo pareigūnas jį atitinkamai instruktuoja.

19.6. **Specialios instrukcijos**

Asmenys, kurie turi dirbti su ES įslaptinta informacija, pradėdami eiti pareigas ir vėliau periodiškai yra supažindinami su:

a) dėl neatsargių pokalbių saugumui kylančiais pavojais;

b) atsargumo priemonėmis, kurių jie turi imtis bendraudami su spauda ir tam tikrų interesų grupių atstovais;

▼B

c) prieš ES ir valstybes nares nukreiptos žvalgybos tarnybų veiklos, kiek ji siejasi su ES įslaptinta informacija ir veikla, keliama grėsme;

d) įpareigojimu nedelsiant informuoti atitinkamas saugumo institucijas apie kiekvieną įtarimų dėl šnipinėjimo sukeliantį mėginimą arba veikimo būdą, arba apie bet kokias neįprastas su saugumu susijusias aplinkybes.

Visi asmenys, kurie paprastai dažnai kontaktuoja su atstovais tų valstybių, kurių žvalgybos tarnybų veikla, kiek tai siejasi su ES įslaptinta informacija ir veikla, yra nukreipta prieš ES ir valstybes nares, yra trumpai instruktuojami apie įprastinius įvairių žvalgybos tarnybų darbo metodus.

Komisija nėra nustačiusi saugumo taisyklių, skirtų asmenų, patikrintų dėl teisės naudotis ES įslaptinta informacija, privačioms kelionėms į bet kurią valstybę. Vis dėlto ►M2 Komisijos Saugumo direktoratas ◄ jam pavaldžius pareigūnus ir kitus tarnautojus supažindina su kelionių taisyklėmis, kurios gali būti jiems taikomos.

20. ASMENS PATIKIMUMO PAŽYMĖJIMŲ IŠDAVIMO KOMISIJOS PAREIGŪNAMS IR KITIEMS DARBUOTOJAMS TVARKA

a) Tik Komisijos pareigūnai ir kiti jos darbuotojai arba Komisijoje dirbantys asmenys, kurie dėl savo pareigų ir tarnybos reikalavimų turi būti susipažinę su Komisijos laikoma įslaptinta informacija arba turi ją naudoti, gali naudotis tokia informacija.

b) Kad a punkte minimi asmenys galėtų naudotis slaptumo žymomis ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄ pažymėta informacija, jie privalo šio skirsnio c ir d punktuose nustatyta tvarka gauti leidimą.

c) Leidimas išduodamas tik asmenims, kurių patikimumą i–n punktuose nurodyta tvarka yra patikrinusios valstybių narių kompetentingos nacionalinės institucijos (NSI).

d) ►M2 Komisijos Saugumo direktorato direktorius ◄ atsako už a, b ir c punktuose minimų leidimų išdavimą.

e) Leidimą jis išduoda, gavęs valstybės narės kompetentingos nacionalinės institucijos nuomonę, pagrįstą i–n punktuose nurodyta tvarka atlikto patikimumo patikrinimo rezultatais.

f) ►M2 Komisijos Saugumo direktoratas ◄ veda nuolat aktualizuojamą visų pažeidžiamų pareigų, kurias nurodo atitinkami Komisijos departamentai, ir visų asmenų, kuriems išduotas (laikinasis) leidimas, sąrašą.

g) Penkerius metus galiojantis leidimas negali galioti ilgiau, nei reikia užduotims, kurioms jis buvo išduotas, atlikti. Leidimą galima atnaujinti e punkte nurodyta tvarka.

h) Leidimą panaikina ►M2 Komisijos Saugumo direktorato direktorius ◄, jei mano, kad tam yra pagrindo. Apie kiekvieną sprendimą panaikinti leidimą pranešama atitinkamam asmeniui, kuris gali prašyti, kad ►M2 Komisijos Saugumo direktorato direktorius ◄ ir kompetentinga nacionalinė institucija jį išklausytų.

▼B

i) Patikimumo tikrinimas atliekamas padedant atitinkamam asmeniui ►M2 Komisijos Saugumo direktorato direktoriaus ◄ prašymu. Patikrinimą turi atlikti tos valstybės narės, kurios pilietis yra leidimo prašantis asmuo, kompetentinga nacionalinė institucija. Jei tas asmuo nėra ES valstybės narės pilietis, ►M2 Komisijos Saugumo direktorato direktorius ◄ atlikti patikimumo patikrinimą paprašo tą ES valstybę narę, kurioje jis turi nuolatinę gyvenamąją vietą arba dažniausiai gyvena.

j) Pagal tikrinimo tvarką reikalaujama, kad atitinkamas asmuo užpildytų asmens informacijos anketą.

k) ►M2 Komisijos Saugumo direktorato direktorius ◄ savo prašyme nurodo įslaptintos informacijos, kuria asmuo galėtų naudotis, pobūdį ir slaptumo žymos laipsnį, kad kompetentinga nacionalinė institucija galėtų atlikti tikrinimą ir pateikti savo nuomonę dėl to, kokio slaptumo žymos laipsnio informacija derėtų leisti naudotis šiam asmeniui.

l) Visą patikimumo tikrinimo tvarką bei gautus rezultatus reglamentuoja atitinkamoje valstybėje narėje galiojančios normos ir taisyklės, įskaitant su apeliacijomis susijusias normas ir taisykles.

m) Valstybės narės kompetentingai nacionalinei institucijai pateikus teigiamą nuomonę, ►M2 Komisijos Saugumo direktorato direktorius ◄ gali atitinkamam asmeniui išduoti leidimą;

n) Apie neigiamą kompetentingos nacionalinės institucijos nuomonę pranešama atitinkamam asmeniui, kuris gali paprašyti ►M2 Komisijos Saugumo direktorato direktorių ◄ jį išklausyti. Jei ►M2 Komisijos Saugumo direktorato direktorius ◄ mano, kad tai reikalinga, jis gali prašyti kompetentingą nacionalinę instituciją tolesnių paaiškinimų. Jei neigiama nuomonė patvirtinama, leidimas neišduodamas.

o) Visi asmenys, kuriems leidimai išduoti pagal d ir e punktus, išduodant leidimą bei reguliariai vėliau reikiamai instruktuojami apie įslaptintos informacijos apsaugą ir tokios apsaugos užtikrinimo priemones. Tokie asmenys pasirašo deklaracijas, kuriose patvirtina išklausę instrukcijas ir įsipareigoja jų laikytis.

p) ►M2 Komisijos Saugumo direktorato direktorius ◄ imasi visų reikalingų priemonių šiam skirsniui, ypač teisę naudotis leidimą turinčių asmenų sąrašu reguliuojančioms taisyklėms, įgyvendinti.

q) Išimtiniais atvejais, esant tarnybinei būtinybei, ►M2 Komisijos Saugumo direktorato direktorius ◄, pateikęs pranešimą kompetentingoms nacionalinėms institucijoms ir per mėnesį nesulaukęs jų atsakymo, gali, laukdamas i punkte minėto tikrinimo rezultatų, išduoti laikinąjį leidimą ne daugiau kaip šešiems mėnesiams.

r) Taip išduoti preliminarūs ir laikinieji leidimai nesuteikia teisės naudotis slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėta informacija; teisė naudotis šia informacija suteikiama tik pareigūnams, kurių pagal i punktą atlikto patikimumo tikrinimo rezultatai buvo teigiami. Laukiant tikrinimo rezultatų, pareigūnams, kuriuos prašoma patikrinti dėl galėjimo naudotis slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėta informacija, galima išduoti tiek preliminarius, tiek laikinuosius leidimus naudotis informacija, pažymėta ►M1 SECRET UE ◄ ar žemesnio laipsnio slaptumo žymomis.

▼B

21. ES ĮSLAPTINTŲ DOKUMENTŲ RENGIMAS, PLATINIMAS, PERDAVIMAS, KURJERIO ASMENS PATIKIMUMAS, PAPILDOMOS KOPIJOS, VERTIMAI IR IŠTRAUKOS

21.1. **Rengimas**

1. ES slaptumo žymos naudojamos 16 skirsnyje nustatyta tvarka, ►M1 SECRET UE ◄ ar aukštesnio laipsnio slaptumo žymos dedamos centre kiekvieno puslapio viršuje ir apačioje, puslapiai numeruojami. Kiekviename ES įslaptintame dokumente turi būti nurodomi jo numeris ir data. Dokumentuose, pažymėtuose slaptumo žymomis ►M1 TRES SECRET UE/EU TOP SECRET ◄ ir ►M1 SECRET UE ◄, dokumento numeris nurodomas kiekviename puslapyje. Jei dokumentas platinamas keliais egzemplioriais, kiekvieno iš jų pirmajame puslapyje kartu su bendru puslapių skaičiumi rašomas kopijos numeris. Visi priedai ir pridedami dokumentai išvardijami dokumento su ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma pirmajame puslapyje.

2. Dokumentus su ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma spausdina, verčia, archyvuoja, fotografuoja, kopijuoja į magnetines laikmenas arba mikrofilmuoja tik dėl teisės naudotis ne žemesnio už svarstomojo dokumento slaptumo žymos laipsnio dokumentais patikrinti asmenys.

3. Įslaptintų dokumentų gamybą kompiuteriu reglamentuojančios nuostatos išdėstytos 25 skirsnyje.

21.2. **Platinimas**

1. ES įslaptinta informacija platinama tik ją žinoti privalantiems asmenims, turintiems atitinkamus asmens patikimumo pažymėjimus. Pirmojo platinimo adresatus nustato dokumento autorius.

2. Dokumentai, pažymėti slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, platinami per ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūras (žr. 22.2 punktą). Kompetentinga registratūra gali įgalioti ryšių centro vadovą padaryti tiek pranešimų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ kopijų, kiek nurodyta gavėjų sąraše.

3. Dokumentus su ►M1 SECRET UE ◄ ir žemesnio laipsnio slaptumo žyma gavėjas gali vadovaudamasis „būtina žinoti“ principu platinti kitiems adresatams. Tačiau dokumentą sukūrusios institucijos turi aiškiai suformuluoti norimus dokumento platinimo apribojimus. Kai tokie apribojimai yra nurodyti, adresatai gali perskirstyti dokumentus tik gavę juos pateikusių institucijų leidimą.

4. Kiekvieną dokumentą su ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma jį pristatant į arba išsiunčiant iš generalinio direktorato ar tarnybos registruoja departamento vietinė ESĮI registratūra. Įrašyti duomenys (numeriai, data, tam tikrais atvejais – kopijos numeris) turi padėti identifikuoti dokumentą ir yra įrašomi į registracijos knygą arba specialią apsaugotą kompiuterinę laikmeną (žr. 22.1 punktą).

21.3. **ES įslaptintų dokumentų perdavimas**

21.3.1. *Pakavimas, kvitai*

1. Dokumentai su ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma perduodami atspariuose, nepermatomuose dvigubuose vokuose. Vidinis vokas pažymimas atitinkama ES slaptumo žyma, ir, jei įmanoma, ant jo taip pat yra užrašomos gavėjo pareigos ir jo adresas.

▼B

2. Atplėšti vidinį voką ir patvirtinti įdėtų dokumentų gavimą gali tik registro kontrolės pareigūnas (žr. 22.1 punktą) arba jo pavaduotojas, jei laiškas nėra adresuotas konkrečiam asmeniui. Tokiu atveju atitinkama registratūra (žr. 22.1 punktą) užregistruoja laiško gavimą, ir tik asmuo, kuriam jis adresuotas, gali atplėšti vidinį voką ir patvirtinti jame esančių dokumentų gavimą.

3. Gavimo kvitas įdedamas į vidinį voką. Kvite, kuris nėra įslaptinamas, nurodomas registracijos numeris, data ir dokumento kopijos numeris, tačiau niekada nenurodoma dokumento antraštė.

4. Vidinis vokas įdedamas į išorinį voką, ant kurio, kad būtų galima patvirtinti gavimą, nurodomas paketo numeris. Slaptumo žyma niekuomet nededama ant išorinio voko.

5. Dokumentams su ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma kurjeriams ir pasiuntiniams duodami pakvitavimai, kuriuose nurodomas gauto paketo numeris.

21.3.2. *Perdavimas pastate arba pastatų komplekse*

Atitinkamame pastate arba pastatų komplekse įslaptinti dokumentai gali būti gabenami antspauduotame voke, ant kurio užrašoma tik adresato pavardė, jei tą voką gabena asmuo, turintis tų dokumentų saugumo žymos laipsnį atitinkantį patikimumo pažymėjimą.

21.3.3. *Perdavimas valstybėje*

1. Valstybėje dokumentus, pažymėtus slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, perduoda tik oficiali kurjerių tarnyba arba asmenys, kuriems yra leista naudotis slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėta informacija.

2. Kai slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtam dokumentui perduoti už pastato arba pastatų komplekso ribų yra naudojama kurjerių tarnyba, ji laikosi šiame skyriuje nustatytų įpakavimo ir kvitų išrašymo nuostatų. Pristatymo tarnybos turi būti taip aprūpintos kadrais, kad būtų užtikrinta, jog paketus su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtais dokumentais visą laiką tiesiogiai prižiūrėtų atsakingas pareigūnas.

3. Išimtiniais atvejais slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtus dokumentus tik naudojimui posėdžiuose ir diskusijose už pastato arba pastatų komplekso ribų gali pasiimti pasiuntiniais nesantys pareigūnai, jeigu:

   a) atitinkamas pareigūnas turi leidimą naudotis dokumentais, pažymėtais ►M1 TRES SECRET UE/EU TOP SECRET ◄ slaptumo žyma;

   b) gabenimo būdas atitinka dokumentų, pažymėtų slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, gabenimą reglamentuojančias taisykles;

   c) pareigūnas jokiomis aplinkybėmis dokumentų, pažymėtų slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, nepalieka be priežiūros;

   d) yra pasirengta taip pasiimamų dokumentų sąrašą laikyti dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūroje, kurioje jie laikomi, juos pažymėti registre ir pagal šį sąrašą patikrinti sugrįžus.

4. Atitinkamoje valstybėje dokumentus, pažymėtus slaptumo žymomis ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄, galima siųsti arba paštu, jei tokį perdavimo būdą leidžia nacionalinės teisės aktai ir jis atitinka tokių teisės aktų nuostatas, arba per kurjerių tarnybą, arba per asmenis, kuriems yra suteiktas leidimas naudotis ES įslaptinta informacija.

▼B

5. Remdamasis šiomis taisyklėmis, ►M2 Komisijos Saugumo direktoratas ◄ parengia instrukcijas ES įslaptintus dokumentus gabenantiems darbuotojams. Gabenantys darbuotojai turi tas instrukcijas perskaityti ir pasirašyti. Instrukcijose ypač aiškiai pasakyta, kad dokumentai jokiomis aplinkybėmis:

   a) negali likti be juos gabenančio asmens priežiūros, nebent jie saugiai padedami pagal 18 skirsnio nuostatas;

   b) negali likti be priežiūros viešajame transporte arba asmeniniame automobilyje, arba tokiose vietose kaip restoranai ar viešbučiai. Jų negalima palikti viešbučių seifuose arba be priežiūros – viešbučių kambariuose;

   c) negali būti skaitomi viešosiose vietose, tokiose kaip orlaiviai arba traukiniai.

21.3.4. *Perdavimas iš vienos valstybės į kitą*

1. Medžiagą su ►M1 SECRET UE ◄ ir aukštesnio laipsnio slaptumo žyma gabena ES diplomatinių ar karinių kurjerių tarnybos.

2. Tačiau gali būti leista asmeniškai gabenti dokumentus, pažymėtus slaptumo žymomis ►M1 SECRET UE ◄ arba ►M1 TRES SECRET UE/EU TOP SECRET ◄, jeigu gabenimo sąlygos užtikrina, kad dokumentai nepaklius į leidimo neturinčių asmenų rankas.

3. Už saugumą atsakingas Komisijos narys gali leisti asmeniškai gabenti dokumentus tuomet, kai nėra galimybės pasinaudoti diplomatiniais arba kariniais kurjeriais arba kai pasinaudojus tokiais kurjeriais būtų vėluojama pristatyti dokumentus ir būtų padaryta žalos ES operacijoms, nes medžiaga atitinkamam gavėjui skubiai reikalinga. ►M2 Komisijos Saugumo direktoratas ◄ parengia ►M1 SECRET UE ◄ ir žemesnio laipsnio slaptumo žyma pažymėtų dokumentų gabenimo iš vienos valstybės į kitą, kai tai daro diplomatiniais arba kariniais kurjeriais nesantys asmenys, instrukcijas. Instrukcijose reikalaujama, kad:

   a) dokumentus gabenantis asmuo turėtų atitinkamą asmens patikimumo pažymėjimą;

   b) atitinkamame departamente arba registratūroje būtų laikomi įrašai apie visus tokiu būdu gabentus dokumentus;

   c) ant paketų arba maišų su ES medžiaga būtų specialus spaudas, kuris užkirstų kelią muitinės tikrinimui, ir identifikavimo etiketės bei nurodymai radėjui;

   d) dokumentus gabenantis asmuo su savimi turėtų visų ES valstybių narių pripažįstamą kurjerio pažymėjimą ir (arba) misijos orderį, įgalinantį jį gabenti atitinkamą paketą;

   e) keliaujant sausuma nebūtų kertama ES nepriklausančių valstybių teritorija ar jų sienos, nebent siunčiančioji valstybė turėtų specialią tos valstybės garantiją;

   f) dokumentus gabenančio asmens kelionės planai (įskaitant kelionės tikslus, maršrutus ir naudojamas transporto priemones) atitiktų ES taisykles arba atitinkamas nacionalines taisykles, jei šios yra griežtesnės;

   g) medžiaga neliktų be ją gabenančio asmens priežiūros, nebent ji būtų saugiai padedama pagal 18 skirsnio nuostatas;

   h) medžiaga neliktų be priežiūros viešajame transporte arba privačiuose automobiliuose, arba tokiose vietose kaip restoranai arba viešbučiai. Jos negalima palikti viešbučių seifuose arba be priežiūros viešbučių kambariuose;

   i) jei tarp gabenamos medžiagos yra dokumentų, jų negalima skaityti viešose vietose (pvz., orlaiviuose, traukiniuose ir pan.).

▼B

4. Asmuo, paskirtas gabenti įslaptintą medžiagą, turi perskaityti ir pasirašyti trumpą saugumo instrukciją, kurioje suformuluojami bent jau pirmiau išvardyti nurodymai ir procedūros, kurių reikia laikytis kritiniu atveju arba tuomet, kai paketą su įslaptinta medžiaga nori patikrinti muitinės arba oro uosto apsaugos pareigūnai.

21.3.5. *ES riboto naudojimo dokumentų perdavimas*

Nėra nustatyta jokių specialių nuostatų dėl dokumentų, pažymėtų ►M1 RESTREINT UE ◄ slaptumo žyma, perdavimo, išskyrus tai, kad juos gabenant turi būti užtikrinta, jog jie nepakliūtų į leidimo neturinčių asmenų rankas.

21.4. **Kurjerio asmens patikimumas**

Visi kurjeriai ir pasiuntiniai, kurių funkcija yra gabenti dokumentus, pažymėtus slaptumo žymomis ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄, privalo turėti atitinkamus asmens patikimumo pažymėjimus.

21.5. **Elektroninės ir kitokios techninės perdavimo priemonės**

1. Tam, kad ES įslaptinta informacija būtų saugiai perduodama, sukurtos ryšių apsaugos priemonės. Tokiam ES įslaptintos informacijos perdavimui taikomos taisyklės išsamiai išdėstytos 25 skirsnyje.

2. ►M1 CONFIDENTIEL UE ◄ ir ►M1 SECRET UE ◄ slaptumo žymomis pažymėtą informaciją gali perduoti tik akredituoti ryšių centrai, tinklai ir (arba) terminalai bei sistemos.

21.6. **ES įslaptintų dokumentų papildomos kopijos, ištraukos bei vertimai**

1. Tik dokumentų autoriai gali leisti kopijuoti arba versti slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtus dokumentus.

2. Jei asmenys, neturintys asmens patikimumo pažymėjimų, suteikiančių teisę naudotis dokumentais su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, prašo informacijos, kuri, nors ir yra dokumentuose su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, bet jai ši žyma netaikoma, ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūros vadovui (žr. 22.2 punktą) gali būti leista parengti reikalingą kiekį to dokumento ištraukų. Jis kartu imasi reikalingų veiksmų, užtikrindamas, kad toms ištraukoms būtų suteikta tinkamo laipsnio slaptumo žyma.

3. Dokumentus su ►M1 SECRET UE ◄ ir žemesnio laipsnio slaptumo žyma adresatas gali kopijuoti ir versti laikydamasis šių saugumo taisyklių ir tik tuomet, kai tai griežtai atitinka „būtina žinoti“ principą. Dokumentų kopijoms ir vertimams taikomos tos pačios saugumo priemonės, kaip ir dokumento originalui.

22. ESĮI REGISTRATŪROS, APŽIŪROS, TIKRINIMAI, ARCHYVAVIMAS IR NAIKINIMAS

22.1. **ESĮI vietinės registratūros**

1. Kiekviename Komisijos departamente esant reikalui už dokumentų, pažymėtų slaptumo žymomis ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄, registravimą, kopijavimą, siuntimą, laikymą archyve ir naikinimą atsako viena arba daugiau vietinių ESĮI registratūrų.

2. Jei departamente nėra vietinės ESĮI registratūros, jos funkcijas vykdo Generalinio sekretoriato vietinė ESĮI registratūra.

3. Vietinės ESĮI registratūros atsiskaito departamento, iš kurio gauna instrukcijas, vadovui. Šioms registratūroms vadovauja Registrų kontrolės pareigūnas (RKP).

▼B

4. Su nuostatų dėl darbo su ESĮI dokumentais taikymu bei atitikimu tinkamoms saugumo priemonėms susijusiais klausimais jas prižiūri vietos saugumo pareigūnas.

5. Į vietines ESĮI registratūras skiriami pareigūnai turi turėti pagal 20 skirsnio nuostatas išduotus leidimus naudotis ESĮI.

6. Atitinkamo departamento vadovui pavaldžios vietinės ESĮI registratūros:

   a) registruoja, kopijuoja, verčia, perduoda, siunčia ir naikina tokią informaciją;

   b) veda įslaptintos informacijos registrą;

   c) reguliariai kelia klausimą dėl būtinybės laikyti tam tikrą informaciją įslaptintą.

7. Vietinės ESĮI registratūros veda registrą, kuriame nurodoma:

   a) įslaptintos informacijos parengimo data;

   b) slaptumo žymos laipsnis;

   c) įslaptinimo termino pabaiga;

   d) informacijos rengėjo pavardė ir padalinys;

   e) gavėjas arba gavėjai (numeruojami);

   f) dalykas;

   g) numeris;

   h) tiražuotų kopijų skaičius;

   i) departamentui pateiktos įslaptintos informacijos inventorizacijos rengimas;

   j) įslaptintos informacijos išslaptinimo ir slaptumo žymos laipsnio sumažinimo registras.

8. 21 skirsnyje nustatytos bendrosios taisyklės taikomos Komisijos vietinėms ESĮI registratūroms, kiek jų nepakeičia šiame skirsnyje nustatytos specialios taisyklės.

22.2. **Dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūra**

22.2.1. *Bendrosios nuostatos*

1. Centrinė dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūra užtikrina, kad dokumentai su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ būtų registruojami, tvarkomi ir platinami pagal šias saugumo taisykles. Dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūrai vadovauja dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registro kontrolės pareigūnas.

2. Centrinė dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūra veikia kaip pagrindinė Komisijos priėmimo ir siuntimo įstaiga darbui su kitomis ES institucijomis, valstybėmis narėmis, tarptautinėmis organizacijomis ir trečiosiomis šalimis, su kuriomis Komisija yra sudariusi susitarimus dėl saugumo procedūrų keičiantis įslaptinta informacija.

3. Prireikus steigiamos už vidinį slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtų dokumentų valdymą atsakingos subregistratūros; jos veda nuolat aktualizuojamą jų saugomų dokumentų judėjimo registrą.

▼B

4. Centrinei dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūrai pavaldžios dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ subregistratūros steigiamos 22.2.3 punkte nustatyta tvarka esant ilgalaikiam poreikiui. Jei slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtais dokumentais reikia naudotis tik kartais arba laikinai, tokie dokumentai gali būti išduodami ir nesteigiant dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ subregistratūros, jei nustatomos taisyklės, užtikrinančios, kad tie dokumentai išliktų atitinkamos dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūros kontroliuojami ir kad būtų laikomasi visų fizinių ir personalo saugumo priemonių.

5. Be specialaus centrinės dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūros leidimo subregistratūros negali tiesiogiai perduoti dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ kitoms tos pačios centrinės registratūros subregistratūroms.

6. Visos subregistratūros, nepriklausančios tai pačiai centrinei registratūrai, dokumentais su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ keičiasi per centrines dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūras.

22.2.2. *Centrinė dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūra*

Kaip kontrolės pareigūnas, centrinės dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūros vadovas atsako už:

a) dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ perdavimą pagal 21.3 punkto nuostatas;

b) visų jai priklausančių dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ subregistratūrų, paskirtų kontrolės pareigūnų ir jų įgaliotų pavaduotojų pavardžių ir parašų sąrašo vedimą;

c) visų centrinės registratūros platinamų dokumentų, pažymėtų slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, registratūrų išduotų kvitų laikymą;

d) laikomų ir platinamų dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registro tvarkymą;

e) visų centrinių dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūrų, su kuriomis jis paprastai susirašinėja, jų paskirtų kontrolės pareigūnų bei įgaliotų jų pavaduotojų pavardžių ir parašų aktualizuoto sąrašo vedimą;

f) visų registratūroje laikomų slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtų dokumentų fizinį saugumą pagal 18 skirsnyje išdėstytas taisykles.

22.2.3. *Dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ subregistratūros*

Kaip kontrolės pareigūnas, dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ subregistratūros vadovas atsako už:

a) dokumentų, pažymėtų slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, perdavimą pagal 21.3 punkto nuostatas;

b) naujausio visų turinčių teisę naudotis jo prižiūrima informacija su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ asmenų sąrašo vedimą;

c) slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtų dokumentų platinimą pagal dokumento autoriaus instrukcijas arba pagal „būtina žinoti“ principą, pirmiausia patikrinus, ar adresatas turi būtiną asmens patikimumo pažymėjimą;

d) visų slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtų dokumentų, laikomų ar cirkuliuojančių jam kontroliuojant, bei kitoms dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūroms perduotų dokumentų aktualaus registro tvarkymą ir visų atitinkamų kvitų saugojimą;

▼B

e) dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūrų, su kuriomis keistis slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtais dokumentais jis yra įgaliotas, paskirtų kontrolės pareigūnų ir jų pavaduotojų pavardžių ir parašų aktualaus sąrašo vedimą;

f) visų subregistratūroje laikomų slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtų dokumentų fizinį saugumą pagal 18 skirsnyje išdėstytas taisykles.

22.3. **ES įslaptintų dokumentų inventorizacija, apžiūros ir tikrinimai**

1. Kasmet kiekviena dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūra pagal šį skirsnį atlieka detalią dokumentų su žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ inventorizaciją. Dokumentas laikomas inventorizuotu, jei jis fiziškai yra registratūroje, yra dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registratūros, į kurią jis išsiųstas, kvitas, dokumento sunaikinimo pažyma arba nurodymas sumažinti šio dokumento slaptumo žymos laipsnį arba dokumentą išslaptinti. Metinių inventorizacijų duomenys kasmet ne vėliau kaip iki balandžio 1 d. perduodami už saugumą atsakingam Komisijos nariui.

2. Dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ subregistratūros savo metinių inventorizacijų duomenis perduoda centrinei registratūrai, kuriai jos yra atskaitingos, jos nustatytą dieną.

3. Žemesnio nei ►M1 TRES SECRET UE/EU TOP SECRET ◄ slaptumo žymos laipsnio ES įslaptinti dokumentai pagal už saugumą atsakingo Komisijos nario instrukcijas tikrinami viduje.

4. Šių patikrinimų metu turi būti nustatyta, ar, dokumentų saugotojo nuomone:

a) galima sumažinti kai kurių dokumentų slaptumo žymos laipsnį arba juos išslaptinti;

b) dokumentai turėtų būti sunaikinti.

22.4. **ES įslaptintų dokumentų archyvavimas**

1. ESĮI archyvuojama visus 18 skirsnyje išvardytus reikalavimus atitinkančiomis sąlygomis.

2. Kad būtų sumažinta archyvavimo problemų, visų registratūrų kontrolės pareigūnams leidžiama dokumentus, pažymėtus slaptumo žymomis ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄, mikrofilmuoti arba kitaip perrašyti į magnetines arba optines laikmenas, jei:

a) mikrofilmuoja/perrašo asmenys, turintys galiojantį darbui su atitinkamo slaptumo laipsnio dokumentais tinkamą asmens patikimumo pažymėjimą;

b) mikrofilmui/laikmenai užtikrinamas tas pats saugumo lygmuo kaip ir dokumentų originalams;

c) apie bet kurio dokumento su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ mikrofilmavimą/perrašymą yra informuojamas jo autorius;

d) filmų ritėse arba kitose laikmenose laikomi tik dokumentai, pažymėti ta pačia slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, ►M1 SECRET UE ◄ arba ►M1 CONFIDENTIEL UE ◄;

▼B

e) bet kurio dokumento, pažymėto žymomis ►M1 TRES SECRET UE/EU TOP SECRET ◄ arba ►M1 SECRET UE ◄, mikrofilmavimas/perrašymas aiškiai fiksuojamas metinės inventorizacijos apraše;

f) mikrofilmuotų arba kitaip perrašytų dokumentų originalai sunaikinami pagal 22.5 punkte išdėstytas taisykles.

3. Šios taisyklės taip pat taikomos bet kuriai kitai leistinai saugojimo formai, pvz., elektromagnetinėms laikmenoms arba optiniams diskams.

22.5. **ES įslaptintų dokumentų naikinimas**

1. Kad ES įslaptinti dokumentai nebūtų be reikalo kaupiami, dokumentai, kuriuos įstaigos vadovas laiko pasenusiais arba kurių yra daugiau nei reikia, kaip įmanoma skubiau sunaikinami tokiu būdu:

a) slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtus dokumentus sunaikina tik už juos atsakinga centrinė registratūra. Kiekvienas sunaikintas dokumentas įrašomas į sunaikinimo pažymą, kurią pasirašo dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ kontrolės pareigūnas ir naikinimą stebėjęs pareigūnas, turintis dirbti su dokumentais, pažymėtais slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, tinkamą patikimumo pažymėjimą. Tai pažymima atitinkamoje registro knygoje;

b) sunaikinimo pažymas kartu su paskirstymo lapais registratūra saugo 10 metų. Kopijos dokumento autoriui arba atitinkamai centrinei registratūrai siunčiamos tik tuomet, kai jų paprašoma;

c) dokumentai su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, taip pat ir visos juos rengiant susidariusios įslaptintos informacijos atliekos, pavyzdžiui, sugadintos kopijos, darbiniai projektai, išspausdinti užrašai, lankstūs diskeliai, stebint dokumentų su slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ registro kontrolės pareigūnui yra sunaikinami juos sudeginant, paverčiant minkšta mase, supjaustant arba kitaip susmulkinant, kad jie taptų neatgaminamais ir neatkuriamos formos.

2. Slaptumo žyma ►M1 SECRET UE ◄ pažymėtus dokumentus sunaikina už juos atsakinga registratūra; naikinimą stebi asmens patikimumo pažymėjimą turintis asmuo ir yra naudojamas vienas iš 1 dalies c punkte nurodytų būdų. Naikinamieji dokumentai su slaptumo žyma ►M1 SECRET UE ◄ įrašomi į pasirašomas sunaikinimo pažymas, kurias kartu su platinimo formomis registratūra saugo ne mažiau kaip trejus metus.

3. Slaptumo žyma ►M1 CONFIDENTIEL UE ◄ pažymėtus dokumentus sunaikina už juos atsakinga registratūra; naikinimą stebi asmens patikimumo pažymėjimą turintis asmuo ir yra naudojamas vienas iš 1 dalies c punkte nurodytų būdų. Jų sunaikinimas užregistruojamas pagal už saugumą atsakingo Komisijos nario instrukcijas.

4. Slaptumo žyma ►M1 RESTREINT UE ◄ pažymėtus dokumentus pagal už saugumą atsakingo Komisijos nario instrukcijas sunaikina už juos atsakinga registratūra arba naudotojas.

22.6. **Naikinimas nenumatytais atvejais**

1. Komisijos departamentai, atsižvelgdami į vietos sąlygas, parengia ES įslaptintos medžiagos apsaugojimo kritiniais atvejais planus, kurie prireikus gali apimti ir sunaikinimo ar evakuacijos nenumatytais atvejais planus. Juose pateikiami nurodymai, kurių reikia laikytis norint apsaugoti ES įslaptintą informaciją nuo patekimo į leidimo ja naudotis neturinčių asmenų rankas.

▼B

2. Pasirengimas apsaugoti ir (arba) kritiniais atvejais sunaikinti medžiagą, pažymėtą slaptumo žymomis ►M1 SECRET UE ◄ ir ►M1 CONFIDENTIEL UE ◄, jokiu būdu neturi pakenkti medžiagos, pažymėtos slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄, apsaugai arba sutrukdyti ją, taip pat ir šifravimo įrangą, sunaikinti – tai padaryti yra aukščiausio prioriteto užduotis.

3. Priemones, kurių imamasi šifravimo įrangos apsaugai ir naikinimui nenumatytais atvejais, nustato specialios instrukcijos.

4. Instrukcijomis, laikomomis antspauduotame voke, turi būti galima pasinaudoti nedelsiant. Naikinimo priemonės/įrankiai turi būti prieinamos.

23. SAUGUMO PRIEMONĖS, TAIKOMOS SPECIALIEMS NE KOMISIJOS PATALPOSE VYKSTANTIEMS POSĖDŽIAMS, KURIUOSE NAUDOJAMA ES ĮSLAPTINTA INFORMACIJA

23.1. **Bendrosios nuostatos**

Kai Komisijos ar kiti svarbūs posėdžiai vyksta ne Komisijos patalpose ir kai dėl ypač didelio nagrinėjamų klausimų arba naudojamos informacijos slaptumo reikalingi ypatingi saugumo reikalavimai, imamasi toliau aprašytų saugumo priemonių. Šios priemonės skirtos tik ES įslaptintos informacijos apsaugai; gali būti numatytos ir kitos saugumo priemonės.

23.2. **Atsakomybė**

23.2.1. ►M2 *Komisijos Saugumo direktoratas* ◄

►M2 Komisijos Saugumo direktoratas ◄ bendradarbiauja su kompetentinga valstybės narės, kurios teritorijoje vyksta posėdis (priimančiosios valstybės narės), institucija, kad būtų užtikrintas Komisijos ir kitų svarbių posėdžių saugumas ir delegatų bei jų personalo apsauga. Saugumo užtikrinimo požiūriu jis turi garantuoti, kad:

a) būtų parengti planai, kokių priemonių bus imtasi esant saugumo rizikai ar kilus su saugumu susijusių incidentų, ypač numatant ES įslaptintų dokumentų saugaus laikymo biuruose priemones;

b) būtų imtasi priemonių, leidžiančių naudotis Komisijos ryšių sistemomis ES slaptiems pranešimams priimti ir perduoti. Prireikus priimančiosios valstybės narės gali būti paprašyta leisti naudotis saugiomis telefono sistemomis.

Rengiantis posėdžiui ►M2 Komisijos Saugumo direktoratas ◄ veikia kaip patarėjas saugumo klausimais; prireikus jo atstovai turi padėti ir patarti posėdžių apsaugos pareigūnui (PAP) ir delegacijoms.

Kiekvienos dalyvaujančios posėdyje delegacijos prašoma paskirti apsaugos pareigūną, kuris būtų atsakingas už savo delegacijos saugumo reikalus ir už ryšio su posėdžių apsaugos pareigūnu, o prireikus – su ►M2 Komisijos Saugumo direktorato ◄ atstovu palaikymą.

23.2.2. *Posėdžių apsaugos pareigūnas (PAP)*

Paskiriamas posėdžių apsaugos pareigūnas, kuris atsako už vidaus saugumo priemonių bendrą parengimą bei kontrolę ir už koordinavimą su kitomis susijusiomis saugumo institucijomis. Priemonės, kurių imasi PAP, apskritai siejasi su:

a) apsaugos priemonėmis posėdžio vietoje, siekiant užtikrinti, kad posėdis vyktų be jokių pavojų bet kokios jame naudojamos ES įslaptintos informacijos saugumui galinčių sukelti incidentų;

▼B

b) personalo, kuriam leidžiama būti posėdžio vietoje, delegacijų zonose ir konferencijų kambariuose, ir bet kokių įrengimų tikrinimu;

c) nuolatiniu koordinavimu su priimančiosios valstybės narės kompetentingomis institucijomis ir ►M2 Komisijos Saugumo direktoratu ◄;

d) saugumo instrukcijų įtraukimu į posėdžių dosjė, tinkamai atsižvelgiant į šiose saugumo taisyklėse ir kitose svarbiose saugumo instrukcijose išdėstytus reikalavimus.

23.3. **Saugumo priemonės**

23.3.1. *Saugumo zonos*

Sukuriamos tokios saugumo zonos:

a) II klasės saugumo zona, į kurią pagal poreikį gali įeiti projektų rengimo kambarys, Komisijos biurai bei dauginimo įranga ir delegacijų biurai;

b) I klasės saugumo zona, į kurią įeina konferencijų patalpa, vertėjų ir garso inžinieriaus kabinos;

c) administracinės zonos, kurioje yra spaudos zona ir tos posėdžio vietos patalpos, kurios naudojamos administracijai, maitinimui bei apgyvendinimui, ir zonos šalia spaudos centro ir posėdžio vietos.

23.3.2. *Leidimai*

Pagal delegacijų praneštus jų poreikius PAP išduoda atitinkamus leidimus. Jei reikia, juose gali būti skiriamieji ženklai, nurodantys, į kurias apsaugos zonas patekti atitinkamas leidimas suteikia teisę.

Posėdžių saugumo instrukcijos reikalauja, kad posėdžių vietoje visi susiję asmenys matomoje vietoje visą laiką segėtų leidimus, kad prireikus apsaugos personalas galėtų juos patikrinti.

Be atitinkamus leidimus turinčių posėdžio dalyvių, į posėdžio vietą įleidžiama kuo mažiau žmonių. Tik nacionalinių delegacijų pageidavimu PAP leidžia joms posėdžio metu priimti lankytojus. Lankytojams išduodami lankytojo pažymėjimai. Užpildoma lankytojo leidimo forma – įrašoma jo pavardė ir lankomo asmens pavardė. Lankytojus visą laiką lydi apsaugos darbuotojas arba lankomas asmuo. Lankytojo leidimo formą su savimi turi lydintysis asmuo, kuris, kai lankytojas išeina iš posėdžio, apsaugos darbuotojams ją grąžina kartu su lankytojo pažymėjimu.

23.3.3. *Fotografinės ir garso įrangos kontrolė*

Į I klasės saugumo zoną negalima įnešti jokių kamerų ar įrašymo įrengimų, išskyrus įrengimus, kuriuos nešasi atitinkamus PAP leidimus gavę fotografai ir garso inžinieriai.

23.3.4. *Portfelių, nešiojamųjų kompiuterių ir paketų tikrinimas*

Turintieji leidimus įeiti į saugumo zoną paprastai gali portfelius ir nešiojamuosius kompiuterius (su savo maitinimo šaltiniu) įsinešti netikrintus. Jei delegacijoms pristatomi paketai, jos gali juos priimti, paketas tokiu atveju patikrinamas delegacijos apsaugos pareigūno, peršviečiamas specialia įranga arba jį atidaro ir patikrina apsaugos personalas. Jei PAP mano, kad tai reikalinga, gali būti numatytos griežtesnės portfelių ir paketų tikrinimo priemonės.

▼B

23.3.5. *Techninė apsauga*

Techninės apsaugos komanda gali padaryti posėdžių kambarį techniškai saugų bei posėdžio metu užtikrinti elektroninę priežiūrą.

23.3.6. *Delegacijos dokumentai*

Delegacijos atsako už ES įslaptintų dokumentų pristatymą į susirinkimus ir iš jų. Jos taip pat atsako už tų dokumentų tikrinimą ir saugumą, kai juos naudoja joms skirtose patalpose. Priimančiąją valstybę galima paprašyti padėti gabenti įslaptintus dokumentus į posėdžio vietą arba iš jos.

23.3.7. *Saugus dokumentų laikymas*

Jei Komisija arba delegacijos negali savo įslaptintų dokumentų saugoti pagal patvirtintas normas, jos gali tuos dokumentus, įdėtus į antspauduotą voką, pasirašytinai atiduoti saugoti Posėdžių apsaugos pareigūnui, kad šis dokumentus saugotų pagal patvirtintas normas.

23.3.8. *Kabinetų tikrinimas*

Posėdžių apsaugos pareigūnas pasirūpina Komisijos ir delegacijų kabinetų patikrinimu po kiekvienos darbo dienos, kad būtų užtikrinta, jog visi ES įslaptinti dokumentai yra laikomi saugioje vietoje. Jei taip nėra, jis imasi tinkamų priemonių.

23.3.9. *ES įslaptintos informacijos atliekų atidavimas*

Visos atliekos laikomos ES įslaptintos informacijos atliekomis, o Komisija ir delegacijos aprūpinamos joms pašalinti skirtomis šiukšlių dėžėmis arba maišais. Prieš palikdamos joms skirtas patalpas Komisija ir delegacijos nuneša atliekas posėdžių apsaugos pareigūnui, kuris jas sunaikina pagal taisykles.

Posėdžiui pasibaigus, visi naudoti, bet nei Komisijai, nei delegacijoms nebereikalingi dokumentai laikomi atliekomis. Prieš atšaukiant posėdžiui taikytas saugumo priemones, atliekama nuodugni Komisijos ir delegacijų patalpų apžiūra. Dokumentai, kuriems buvo pasirašytas kvitas, atitinkamais atvejais sunaikinami, kaip nurodyta 22.5 punkte.

24. SAUGUMO PAŽEIDIMAI IR ES ĮSLAPTINTŲ DOKUMENTŲ NETEISĖTAS ATSKLEIDIMAS

24.1. **Sąvokų apibrėžimai**

Saugumo pažeidimu laikomas Komisijos saugumo taisyklėms priešingas veiksmas arba neveikimas, galintys kelti pavojų ES įslaptintai informacijai arba ją neteisėtai atskleisti.

ES įslaptintos informacijos neteisėtu atskleidimu laikomas jos visos arba jos dalies patekimas į leidimo tam neturinčių asmenų rankas, t. y. į rankas tų asmenų, kurie neturi asmens patikimumo pažymėjimo arba neatitinka „būtina žinoti“ principo, arba jei yra tikimybė, kad tai atsitiko.

ES įslaptinta informacija gali būti neteisėtai atskleista dėl nerūpestingumo, neapdairumo ar neatsargumo, taip pat dėl prieš ES ar jos valstybes nares nukreiptos apie ES įslaptintą informaciją ar veiklą sužinoti siekiančių tarnybų arba ardomąja veikla užsiimančių organizacijų veiklos.

24.2. **Pranešimas apie saugumo pažeidimus**

Visi su ES įslaptinta informacija dirbantys asmenys yra trumpai informuojami apie jų pareigas šioje srityje. Jie iškart praneša apie kiekvieną pastebėtą saugumo pažeidimą.

▼B

Kai vietos saugumo pareigūnas ar posėdžių apsaugos pareigūnas nustato arba jam yra pranešama apie ES įslaptintos informacijos saugumo pažeidimą, ES įslaptintos informacijos pametimą arba dingimą, jis laiku imasi veiksmų, kad:

a) išsaugotų įrodymus;

b) nustatytų faktus;

c) įvertintų ir sumažintų padarytą žalą;

d) neleistų tam dar kartą atsitikti;

e) informuotų reikiamas institucijas apie saugumo pažeidimo pasekmes.

Šiam tikslui pateikiama tokia informacija:

i) atitinkamos informacijos apibūdinimas, įskaitant jos slaptumo žymą, registracijos ir kopijos numerius, datą, autorių, temą ir apimtį;

ii) trumpas saugumo pažeidimo aplinkybių apibūdinimas, įskaitant datą bei laiką, per kurį informacija buvo neteisėtai atskleista;

iii) pažymima, ar informuotas tos informacijos autorius.

Kiekviena apsaugos institucija, vos pastebėjusi galimą saugumo pažeidimą, privalo nedelsiant pranešti apie tai ►M2 Komisijos Saugumo direktoratui ◄.

Apie informacijos su slaptumo žyma ►M1 RESTREINT UE ◄ saugumo pažeidimus pranešti reikia tik tuomet, kai tie pažeidimai yra neįprasto pobūdžio.

Už saugumą atsakingas Komisijos narys, gavęs informaciją apie saugumo pažeidimą:

a) praneša apie tai atitinkamą įslaptintą informaciją sukūrusiai institucijai;

b) paprašo atitinkamų saugumo institucijų pradėti tyrimą;

c) koordinuoja tyrimą, kai pažeidimas siejasi su daugiau nei viena saugumo institucija;

d) gauna ataskaitą, kurioje yra nurodytos pažeidimo aplinkybės, data arba laikotarpis, per kurį pažeidimas galėjo būti padarytas ir buvo nustatytas, bei išsamiai aprašytas atitinkamos medžiagos turinys bei nurodytas jos slaptumo žymos laipsnis. Ataskaitoje pranešama ir apie žalą, padarytą ES arba vienos ar daugiau jos valstybių narių interesams, taip pat apie veiksmus, kurių imtasi, kad toks pažeidimas negalėtų pasikartoti.

Informaciją parengusi institucija informuoja dokumento adresatus ir duoda jiems atitinkamas instrukcijas.

24.3. **Teisiniai veiksmai**

Asmuo, dėl kurio kaltės buvo neteisėtai atskleista ES įslaptinta informacija, yra baudžiamas drausmine nuobauda pagal atitinkamas teisės normas ir nuostatas, visų pirma Personalo taisyklių VI dalį. Ši nuobauda neužkerta kelio bet kokiems tolesniems teisiniams veiksmams.

Jei reikalinga, remdamasis 24.2 punkte minima ataskaita už saugumą atsakingas Komisijos narys imasi visų reikalingų veiksmų, kad kompetentingos nacionalinės institucijos galėtų pradėti baudžiamąjį procesą.

▼B

25. INFORMACINIŲ TECHNOLOGIJŲ IR RYŠIŲ SISTEMOMIS TVARKOMOS ES ĮSLAPTINTOS INFORMACIJOS APSAUGA

25.1. **Įvadas**

25.1.1. *Bendrosios nuostatos*

Saugumo politika ir reikalavimai taikomi visoms ryšių ir informacinėms sistemoms bei tinklams (toliau – sistemos), kuriose apdorojama ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma pažymėta informacija. Jie taikomi kaip papildantys 1995 m. lapkričio 23 d Komisijos sprendimą C (95) 1510 (galutinis) dėl informacinių sistemų apsaugos.

Sistemoms, kuriose apdorojama slaptumo žyma ►M1 RESTREINT UE ◄ pažymėta informacija, taip pat reikalingos tos informacijos slaptumą apsaugančios saugumo priemonės. Visoms sistemoms reikalingos saugumo priemonės, apsaugančios jų bei jose esančios informacijos vientisumą ir prieinamumą.

Komisijos taikoma IT saugumo politika apima šiuos elementus:

— ji yra neatskiriama bendrojo saugumo dalis ir papildo visus informacijos saugumo, asmenų saugumo ir fizinio saugumo elementus,

— pasiskirstymą pareigomis tarp techninių sistemų savininkų, techninėse sistemose saugomos ir apdorojamos ESĮI savininkų, IT saugumo specialistų ir vartotojų,

— kiekvienos IT sistemos saugumo principų ir reikalavimų aprašymą,

— tų principų ir reikalavimų patvirtinimą įgaliotoje institucijoje,

— atsižvelgimą į konkrečias grėsmes ir pažeidžiamumą IT srityje.

25.1.2. *Grėsmė sistemoms ir jų pažeidžiamumas*

Grėsmę galima apibrėžti kaip atsitiktinio arba sąmoningo pakenkimo saugumui galimybę. Sistemų atžvilgiu toks pakenkimas apimtų vienos arba kelių iš šių savybių praradimą: konfidencialumo, vientisumo ar prieinamumo. Pažeidžiamumas apibrėžiamas kaip menka arba nepakankama kontrolė, kuri palengvintų ar sudarytų galimybę atsirasti grėsmei tam tikram objektui arba tikslui.

ES įslaptinta ir neįslaptinta informacija, tvarkoma sistemose greitam atkūrimui, perdavimui ir naudojimui pritaikyta archyvuota forma, yra atvira daugeliui grėsmių, įskaitant galimybę leidimo neturintiems vartotojams pasinaudoti informacija arba, atvirkščiai, neleidimą ja pasinaudoti leidimą turintiems vartotojams. Taip pat egzistuoja informacijos atskleidimo, klastojimo, keitimo arba ištrynimo neturint tam leidimo grėsmė. Be to, sudėtingi ir kartais jautrūs įrengimai yra brangūs, neretai būna sunku juos greitai pataisyti arba pakeisti.

25.1.3. *Svarbiausia saugumo priemonių paskirtis*

Šiame skirsnyje aprašomų saugumo priemonių svarbiausia paskirtis – apsaugoti ES įslaptintą informaciją nuo jos atskleidimo neturint tam leidimo (konfidencialumo praradimas) ir nuo jos vientisumo bei prieinamumo netekimo. Kad būtų užtikrintas tinkamas ES įslaptintą informaciją tvarkančių sistemų saugumas, ►M2 Komisijos Saugumo direktoratas ◄ nustato atitinkamus bendrojo saugumo standartus bei kiekvienai sistemai specialiai sukurtas atitinkamas saugumo procedūras ir metodus.

▼B

25.1.4. *Sistemai pritaikyta saugumo reikalavimų suvestinė (SSRS)*

Reikia, kad techninių sistemų valdytojas (TSV, žr. 25.3.4 punktą) ir informacijos savininkas (IS, žr. 25.3.5 punktą), prireikus bendradarbiaudami su projekto personalu bei ►M2 Komisijos Saugumo direktorato ◄ (kaip INFOSAUGOS institucija – II, žr. 25.3.3 punktą) ir jų padedami, visoms ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma pažymėtą informaciją tvarkančioms sistemoms sukurtų sistemai pritaikytą saugumo reikalavimų suvestinę, kurią patvirtintų saugumo akreditavimo institucija (SAI, žr. 25.3.2 skirsnį).

Sistemai pritaikytos saugumo reikalavimų suvestinės (SSRS) taip pat reikalaujama, jei saugumo akreditavimo institucija (SAI) su naudojimosi ►M1 RESTREINT UE ◄ slaptumo žyma pažymėta arba neįslaptinta informacija galimybe bei jos vientisumu susijusią padėtį laiko kritiška.

SSRS suformuluojama pradinėje projekto fazėje ir jo eigoje plėtojama ir tobulinama, bei įvairiuose projekto ir sistemų gyvavimo ciklo etapuose atlieka skirtingus uždavinius.

25.1.5. *Sistemos darbo saugumo režimai*

Visos sistemos, apdorojančios ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma pažymėtą informaciją, akredituojamos dirbti vienu, o jei reikalaujama – įvairiais laiko tarpais ir daugiau nei vienu iš toliau nurodytų saugumo režimų arba nacionaliniu tokio modelio atitikmeniu:

a) priskirtas/dedikuotas;

b) aukšto lygio sistema;

c) daugialaipsnis.

25.2. **Sąvokų apibrėžimai**

„Akreditacija“ – sistemai suteiktas leidimas jos operacinėje aplinkoje apdoroti ES įslaptintą informaciją ir to patvirtinimas.

Pastaba:

Tokia akreditacija suteikiama įdiegus visas tinkamas saugumo procedūras ir pasiekus pakankamą sisteminių resursų apsaugos lygį. Akreditacija paprastai suteikiama remiantis SSRS ir apima:

a) sistemos akreditavimo tikslo konstatavimą, ypač tai, kokio slaptumo žymos laipsnio informacija bus apdorojama ir koks siūlomas sistemos arba tinklo saugumo režimas (-ai);

b) rizikos valdymo peržiūrą, siekiant nustatyti pažeidžiamumą, grėsmes ir kovos su jomis priemones;

c) saugumo operacijų tvarką (SOT) su išsamiu numatytų procesų aprašymu (pvz., numatomi režimai, funkcijos), taip pat ir sistemos saugumo ypatybių aprašymu, sudarančiu pagrindą akreditavimui;

d) saugumo savybių diegimo ir palaikymo planą;

e) sistemos saugumo arba tinklo saugumo pradinio bei tolesnio testavimo, vertinimo ir atestavimo planą;

f) atestavimą, jei reikia, kartu su kitais akreditavimo elementais.

▼B

„Centrinio informacijos saugumo pareigūnas“ (CISP) – tai centrinės IT tarnybos pareigūnas, koordinuojantis ir prižiūrintis centralizuotas saugumo priemonių sistemas.

„Atestavimas“ – oficialaus liudijimo, prie kurio pridedama nepriklausoma vertinimo ir rezultatų, sistemos saugumo reikalavimų atitikties arba kompiuterių saugumo produktų atitikties iš anksto nubrėžtiems saugumo reikalavimams laipsnio apžvalga, išdavimas.

„Ryšių saugumas“ (RS) – saugumo priemonių taikymas telekomunikacijoms, neleidžiant leidimo neturintiems asmenims pasinaudoti vertinga informacija, kurią jie gautų valdydami arba analizuodami ryšių srautus, arba garantuojant tokių ryšių srautų autentiškumą.

Pastaba:

Tokios priemonės yra šifravimas, perdavimo ir priėmimo saugumas, be to, procedūrų, fizinis, personalo, dokumentų ir kompiuterių saugumas.

„Kompiuterių saugumas“ (KS) - kompiuterinės įrangos, gamintojo programinės įrangos ir programinės įrangos saugumo savybių pritaikymas kompiuterinei sistemai, siekiant apsaugoti informaciją, užkirsti kelią neįgaliotiems asmenims ja manipuliuoti ir ją pakeisti/ištrinti arba apsisaugoti nuo sistemos išėjimo iš rikiuotės (Denial of Service).

„Kompiuterių saugos produktas“ – bendras kompiuterinis saugumo modulis, integruojamas į IT sistemą, siekiant užtikrinti tvarkomos informacijos konfidencialumą, vientisumą ar prieinamumą arba tas savybes paryškinti.

„Priskirtas/dedikuotas saugumo operacijų režimas“ – toks režimas, kai VISI asmenys laikomi tinkamais naudotis aukščiausio sistemoje tvarkomos informacijos slaptumo žymos laipsnio informacija ir turinčiais pagal „būtina žinoti“ principą susipažinti su VISA sistemoje tvarkoma informacija.

Pastabos:

1) Kadangi visi naudotojai atitinka „būtina žinoti“ principą, sistemoje nebūtina kompiuterinio saugumo priemonėmis atriboti skirtingos informacijos.

2) Kitos saugumo priemonės (pvz., fizinės, personalo ir procedūrų) turi atitikti reikalavimus, keliamus aukščiausiam sistemoje tvarkomos informacijos slaptumo žymos laipsniui ir visoms informacijos kategorijoms.

„Vertinimas“ – atitinkamos institucijos atliekamas išsamus sistemos saugumo aspektų arba šifravimo ar kompiuterių saugos produktų detalus techninis tyrimas.

Pastabos:

1) Vertinant tikrinama, ar iš tiesų yra reikalaujamos saugumo funkcijos bei ar nėra pavojingo pašalinio tokių funkcijų poveikio, bei įvertinamas tokių funkcijų nepažeidžiamumas.

2) Atliekant vertinimą yra apibrėžiamas atitikimo sistemos saugumo reikalavimams arba kompiuterių saugos produktų reikalavimams laipsnis, bei nustatomas sistemos, šifravimo ar kompiuterinės saugos produkto patikimo funkcionavimo garantijų lygis.

„Informacijos savininkas“ (IS) – institucija (departamento vadovas), atsakinga už informacijos sukūrimą, apdorojimą ir naudojimą, taip pat ir už sprendimą, kam suteikti teisę naudotis informacija.

▼B

„Informacijos saugumas“ (INFOSAUGA) – saugumo priemonių taikymas siekiant ryšių, informacijos ir kitose elektroninėse sistemose apdorojamą, saugomą arba perduodamą informaciją apsaugoti nuo netyčinio arba tyčinio konfidencialumo, vientisumo arba prieinamumo praradimo ir neleisti prarasti pačių sistemų vientisumo ir prieinamumo.

„INFOSAUGOS priemonės“ – kompiuterių, perdavimo, skleidimo ir kriptogramų saugumas, grėsmių informacijai bei sistemoms atskleidimas, dokumentavimas ir atrėmimas.

„IT aplinka“ – zona, kurioje yra vienas arba daugiau kompiuterių, jų vietiniai periferiniai ir saugojimo elementai, valdymo elementai ir priskirti tinklo ir ryšių įrengimai.

Pastaba:

Šiai zonai nepriklauso atskirtos zonos, kuriose yra įrengti nuotoliniai periferiniai prietaisai arba terminalai/nutolusios darbo vietos, nors tie prietaisai ir būtų sujungti su IT zonoje esančiais įrengimais.

„IT tinklas“ – visuma geografiniu atžvilgiu išsklaidytų, tarpusavyje keitimuisi duomenimis sujungtų IT sistemų, apimanti tarpusavyje sujungtas IT sistemas ir jų sąsajas su pagalbiniais duomenų arba ryšių tinklais.

Pastabos:

1) IT tinklas gali naudotis vienu arba keliais, tarpusavyje keitimuisi duomenimis sujungtais ryšių tinklais; keletas IT tinklų gali naudotis bendru ryšių tinklu.

2) IT tinklas vadinamas „vietiniu“, jei jis jungia kelis vienoje vietoje esančius kompiuterius.

„IT tinklo saugumo savybės“ – tinklą sudarančių individualių IT sistemų saugumo savybės kartu su papildomais komponentais ir savybėmis, susijusiais su pačiu tinklu (pvz., ryšiai tinkle, saugumo identifikavimo ir ženklinimo mechanizmai bei procedūros, prisijungimo kontrolė, programos ir audito takeliai), reikalingi, kad įslaptinta informacija būtų tinkamai apsaugoma.

„IT sistema“ – įrengimų, metodų ir procedūrų, o prireikus ir personalo sistema, vykdanti informacijos apdorojimo funkcijas.

Pastabos:

1) Tai yra visuma informacijai sistemoje tvarkyti pritaikytų įrengimų.

2) Tokios sistemos gali būti naudojamos konsultacijoms, valdymui, kontrolei, ryšiams, moksliniam arba administraciniam taikymui, taip pat ir tekstams apdoroti.

3) Sistemos ribos paprastai apibrėžiamos kaip vieno TSV kontroliuojami elementai.

4) IT sistema gali turėti posistemes, kai kurios iš jų pačios yra IT sistemos.

▼B

„IT sistemos saugumo savybės“ – visos kompiuterinės įrangos/gamintojo programinės įrangos/programinės įrangos funkcijos, ypatybės ir savybės, valdymo procedūros, apskaitomumo procedūros, prisijungimo kontrolė, IT aplinka, nuotolinio terminalo/darbo vietos aplinka, tvarkymo apribojimai, fizinė struktūra ir prietaisai, personalo ir ryšių kontrolė, kurie reikalingi, kad IT sistemoje tvarkomai įslaptintai informacijai būtų užtikrintas deramas apsaugos lygis.

„Vietos informatikos saugumo pareigūnas“ (VISP) – Komisijos departamento pareigūnas, atsakingas už saugumo priemonių koordinavimą ir priežiūrą savo teritorijoje.

„Daugialaipsnis saugumo operacijų režimas“ – toks režimas, kai NE VISI galintys naudotis sistema asmenys turi leidimą naudotis aukščiausio sistemoje tvarkomos informacijos slaptumo žymos laipsnio informacija ir kai NE VISI galintys naudotis sistema asmenys laikomi turinčiais pagal „būtina žinoti“ principą susipažinti su bendra sistemoje tvarkoma informacija.

Pastabos:

1) Šiuo metu šis operacijų režimas leidžia tvarkyti įvairių slaptumo žymos laipsnių ir mišrių informacijos kategorijų pavadinimų informaciją.

2) Tai, kad ne visi naudotojai atitinka „būtina žinoti“ principą ir ne visi asmenys turi naudotis aukščiausio slaptumo žymos laipsnio informacija leidžiančius asmens patikimumo pažymėjimus, lemia, kad kompiuterinio saugumo priemonėmis turi būti užtikrinta galimybė pasirinktinai naudotis sistemoje esančia informacija bei ją atriboti.

„Nuotolinio terminalo/darbo vietos aplinka“ – už IT aplinkos ribų esanti zona, kurioje yra kompiuterių įrengimai, jų vietinė periferinė įranga arba terminalai/-darbo vietos ir bet kokie susiję ryšių įrengimai.

„Saugumo operacijų procedūros“ – tai techninių sistemų valdytojo nustatytos procedūros, kai yra apibrėžiami saugumo reikalams būtini principai, atliktinos operacijų procedūros ir personalo atsakomybė.

„AUKŠTO LYGIO SISTEMOS saugumo operacijų režimas“ – tai toks režimas, kai VISI galintys naudotis sistema asmenys turi leidimą naudotis aukščiausio sistemoje tvarkomos informacijos slaptumo žymos laipsnio informacija, tačiau NE VISI galintys naudotis sistema asmenys laikomi turinčiais pagal „būtina žinoti“ principą susipažinti su bendra sistemoje tvarkoma informacija.

Pastabos:

1) Tai, kad ne visi naudotojai atitinka „būtina žinoti“ principą, lemia, jog kompiuterinio saugumo priemonėmis turi būti užtikrinta galimybė pasirinktinai naudotis sistemoje esančia informacija bei ją atriboti.

2) Kitos saugumo priemonės (pvz., fizinės, personalo ir procedūrų) turi atitikti reikalavimus, keliamus aukščiausiam sistemoje tvarkomos informacijos slaptumo žymos laipsniui ir visoms informacijos kategorijoms.

3) Jei nėra nustatyta kitaip, visa sistemoje šiuo operacijų režimu tvarkoma arba per ją gaunama informacija kartu su informacijos išeiga yra saugoma kaip atitinkamos kategorijos bei aukščiausio apdorotos informacijos slaptumo žymos laipsnio informacija, nebent esama žymėjimo funkcija būtų pakankamai patikima.

▼B

„Sistemai pritaikyta saugumo reikalavimų suvestinė“ (SSRS) – tai išsamus ir tikslus saugumo principų, kurių reikia laikytis, ir detalių saugumo reikalavimų, kuriuos reikia atitikti, nustatymas. Jis pagrįstas Komisijos saugumo politika ir rizikos įvertinimu arba jį nulemia operacijų aplinkos kriterijai, žemiausias personalo saugumo patikrinimo lygis, aukščiausias tvarkomos informacijos slaptumo žymos laipsnis, saugumo operacijų režimas arba vartotojo reikalavimai. SSRS yra neatskiriama projekto dokumentų, pateiktų atitinkamoms institucijoms tvirtinti techniniu, biudžeto ir saugumo aspektais, dalis. Galutinės formos SSRS yra išsamus atitinkamos sistemos saugumo prielaidų aprašas.

„Techninių sistemų valdytojas“ (TSV) – institucija, atsakinga už sistemos sukūrimą, tvarkymą, jos darbą ir uždarymą.

„Tempest“ apsaugos priemonės – tai priemonės, skirtos įrangai ir ryšių infrastruktūrai apsaugoti nuo įslaptintos informacijos atskleidimo be leidimo dėl netyčinio elektromagnetinio spinduliavimo ir laidumo.

25.3. **Atsakomybė saugumo srityje**

25.3.1. *Bendrosios nuostatos*

12 skirsnyje apibrėžtos Komisijos Saugumo politikos patarėjų grupės pareigos apima ir INFOSAUGOS reikalavimus. Grupė savo veiklą organizuoja taip, galėtų šiais klausimais teikti ekspertų patarimus.

►M2 Komisijos Saugumo direktoratas ◄ atsako už išsamių šio skirsnio nuostatomis pagrįstų INFOSAUGOS nuostatų parengimą.

Iškilus saugumo problemoms (incidentai, nusižengimai taisyklėms ir pan.), ►M2 Komisijos Saugumo direktoratas ◄ nedelsiant imasi veiksmų.

►M2 Komisijos Saugumo direktoratas ◄ turi INFOSAUGOS padalinį.

25.3.2. *Saugumo akreditavimo institucija (SAI)*

►M2 Komisijos Saugumo direktorato direktorius ◄ veikia kaip Komisijos saugumo akreditavimo institucija. SAI atsako už bendrus saugumo reikalus bei už konkrečias INFOSAUGOS, ryšių saugumo, šifravimo saugumo ir, „Tempest“ saugumo sritis.

SAI užtikrina, kad sistemos atitiktų Komisijos saugumo politiką. Viena iš jos užduočių – aprobuoti savo informacinėje aplinkoje iki tam tikro slaptumo žymos laipsnio įslaptintą ES informaciją tvarkančią sistemą.

Komisijos SAI jurisdikcijai priklauso visos Komisijos patalpose veikiančios sistemos. Kai skirtingi sistemos komponentai patenka į Komisijos SAI ir kitų SAI jurisdikciją, visos suinteresuotos pusės gali paskirti bendrą Komisijos SAI koordinuojamą akreditavimo valdybą.

25.3.3. *INFOSAUGOS institucija (II)*

►M2 Komisijos Saugumo direktorato ◄ INFOSAUGOS padalinio vadovas veikia kaip Komisijos INFOSAUGOS institucija. INFOSAUGOS institucija atsako už:

— techninių patarimų ir pagalbos SAI teikimą,

— pagalbą kuriant SSRS,

▼B

— SSRS patikrinimą siekiant užtikrinti šių saugumo taisyklių, INFOSAUGOS politikos ir jos struktūros dokumentų atitiktį,

— dalyvavimą, kai reikia, akreditavimo forumuose/valdybose ir INFOSAUGOS rekomendacijų dėl akreditavimo teikimą SAI,

— pagalbą INFOSAUGOS mokymo ir švietimo veiklai,

— techninius patarimus dėl su INFOSAUGA susijusių incidentų tyrimo,

— techninės politikos vadovo sukūrimą siekiant užtikrinti tik akredituotos programinės įrangos naudojimą.

25.3.4. *Techninių sistemų valdytojas (TSV)*

Už sistemų kontrolės ir konkrečių saugumo savybių įdiegimą bei vykdymą atsako šios sistemos valdytojas, t. y., techninių sistemų valdytojas (TSV). Centralizuotai valdomoms sistemoms paskiriamas centrinis informacijos saugumo pareigūnas (CISP). Kiekvienas departamentas paprastai paskiria vietos informacijos saugumo pareigūną (VISP). TSV taip pat atsako už saugumo operacijų tvarkos (SOT) sukūrimą bei už visą sistemos gyvavimo ciklą, prasidedantį projekto koncepcijos kūrimo etapu ir pasibaigiantį sistemos galutiniu utilizavimu.

TSV smulkiai apibrėžia saugos standartus ir procedūras, kurių turi laikytis sistemos tiekėjai.

Prireikus TSV dalį savo pareigų gali perduoti vietos informatikos saugumo pareigūnui. Tas pats asmuo gali vykdyti įvairias INFOSAUGOS funkcijas.

25.3.5. *Informacijos savininkas (IS)*

Informacijos savininkas atsako už ESĮI (ir kitokią informaciją), kurią reikia įtraukti, apdoroti ir sudaryti techninėmis sistemomis. Jis apibrėžia reikalavimus, susijusius su galimybe naudotis šia sistemose esančia informacija. Jis gali perduoti šią pareigą savo srities informacijos valdytojui arba duomenų bazės valdytojui.

25.3.6. *Vartotojai*

Visi vartotojai privalo užtikrinti, kad jų veiksmai nepalankiai nepaveiks sistemos, kuria jie naudojasi, saugumo.

25.3.7. *INFOSAUGOS mokymas*

INFOSAUGOS švietimas ir mokymas yra prieinamas visiems personalo nariams, kuriems jo reikia.

25.4. **Netechninės saugumo priemonės**

25.4.1. *Personalo saugumas*

Sistemos vartotojai, atsižvelgiant į jų specifinėje sistemoje apdorojamos informacijos slaptumo žymos laipsnį ir turinį, privalo turėti atitinkamus patikimumo pažymėjimus bei atitikti „būtina žinoti“ principą. Galimybė dirbti su tam tikrais įrenginiais arba naudotis su sistemų saugumu susijusia informacija suteikiama tik pagal Komisijos nustatytas procedūras gavus specialų pažymėjimą.

SAI nurodo visus saugumo prasme svarbius postus ir apibrėžia patikimumo pažymėjimo lygmenį bei priežiūrą, reikalingą visiems tuose postuose dirbantiems personalo nariams.

Sistemos specifikuojamos ir kuriamos taip, kad būtų lengviau paskirstyti pareigas ir atsakomybę personalui neleidžiant vienam asmeniui įgyti visaapimančių žinių arba kontroliuoti esminių sistemos saugumo elementų.

▼B

IT ir nuotolinio terminalo/darbo vietos aplinkoje, kurioje gali būti keičiamas sistemos saugumas, negali dirbti tik vienas leidimą turintis pareigūnas arba kitas darbuotojas.

Sistemos saugumo nustatymai gali būti keičiami ne mažiau kaip dviejų leidimą turinčių darbuotojų kartu.

25.4.2. *Fizinis saugumas*

IT ir nuotolinio terminalo/darbo vietos aplinkoje (apibrėžtoje 25.2 punkte), kurioje IT priemonėmis apdorojama informacija su ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma arba kurioje yra reali galimybė pasinaudoti tokia informacija, priklausomai nuo poreikio sukuriamos ES I ir II klasės saugumo zonos.

25.4.3. *Naudojimosi sistema kontrolė*

Visa informacija ir medžiaga, leidžianti kontroliuoti galimybę naudotis sistema, saugoma pagal aukščiausiam informacijos, kuria naudotis ji sudaro galimybę, slaptumo žymos laipsniui ir atitinkamai informacijos kategorijai taikomus reikalavimus.

Informacija ir medžiaga, leidžianti kontroliuoti galimybę naudotis sistema, sunaikinama pagal 25.5.4 punkto nuostatas, jei ji toliau nebenaudojama šiam tikslui.

25.5. **Techninės saugumo priemonės**

25.5.1. *Informacijos saugumas*

Informacijos autoriui pavedama identifikuoti ir įslaptinti visus informacijos turinčius dokumentus, nepriklausomai nuo to, ar tai spausdintinės kopijos, ar kompiuterinių duomenų saugojimo laikmenos. Kiekvienas spausdintinės kopijos lapas pažymimas puslapio viršuje ir apačioje nurodoma slaptumo žyma. Tiek spausdintinei, tiek kompiuterinių duomenų saugojimo laikmenose laikomai informacijai suteikiama to laipsnio slaptumo žyma, kuria buvo pažymėta aukščiausio slaptumo žymos laipsnio dokumentą sudarant panaudota informacija. Sistemos veikimo būdas taip pat gali turėti įtakos ta sistema sudarytos informacijos slaptumo žymos laipsniui.

Komisijos departamentams ir jų informacijos laikytojams pavedama apsvarstyti informacijos atskirų elementų rinkinio problematiką bei išvadas, kurias leidžia daryti susiję elementai, ir nustatyti, ar visai šiai informacijai neturėtų būti suteiktas aukštesnis slaptumo žymos laipsnis.

Tai, kad informacija gali būti trumpas kodas, perdavimo kodas arba bet kokios formos binarinis atvaizdavimas, nesuteikia jokios saugumo garantijos, todėl neturėtų įtakoti informacijos įslaptinimo.

Perduodant informaciją iš vienos sistemos į kitą, perdavimo metu ir priimančiojoje sistemoje ji saugoma originalią informacijos slaptumo žymą ir kategoriją atitinkančiu būdu.

Visos kompiuterinių duomenų saugojimo laikmenos tvarkomos tokiu būdu, kuris atitinka saugomos informacijos aukščiausio laipsnio slaptumo žymą arba laikmenos etiketę, ir visą laiką tinkamai saugomos.

Pakartotinai užrašyti ES įslaptintą informaciją naudojamos kompiuterinių duomenų saugojimo laikmenos išlaiko aukščiausio laipsnio slaptumo žymą, kuria jos kada nors buvo naudojamos, kol tos informacijos slaptumo laipsnis nėra sumažinamas ar ta informacija nėra išslaptinama, arba kol laikmenų slaptumo lygmuo nėra atitinkamai sumažinamas arba jos nėra išslaptinamos ar sunaikinamos pagal SAI patvirtintas nuostatas (žr. 25.5.4 punktą).

▼B

25.5.2. *Informacijos kontrolė ir atskaitomybė*

Naudojimasis ►M1 SECRET UE ◄ ir aukštesnio laipsnio slaptumo žyma pažymėta informacija registruojamas ir protokoluojamas automatiškai (audito takeliai) arba ranka. Protokolai saugomi pagal šias saugumo taisykles.

IT aplinkoje laikoma ES įslaptinta informacija gali būti tvarkoma kaip vienas įslaptintas dokumentas ir neturi būti registruojama, jei medžiaga yra identifikuota, pažymėtas jos slaptumo žymos laipsnis bei ji yra tinkamai kontroliuojama.

Kai informacija surenkama iš ES įslaptintą informaciją tvarkančios sistemos ir iš IT aplinkos perduodama į nuotolinio terminalo/darbo vietos aplinką, SAI patvirtinus nustatomos informacijos kontrolės ir registravimo procedūros. Informacijai su ►M1 SECRET UE ◄ ir aukštesnio laipsnio slaptumo žyma prie tokių procedūrų priskiriami specialūs nurodymai dėl informacijos apskaitomybės.

25.5.3. *Išimamų kompiuterinių duomenų saugojimo laikmenų tvarkymas ir kontrolė*

Visos išimamos kompiuterinių duomenų saugojimo laikmenos su ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma tvarkomos kaip medžiaga ir joms taikomos bendros taisyklės. Atitinkamus identifikavimo ir įslaptinimo žymenis reikia priderinti prie konkrečios laikmenų fizinės išvaizdos, kad jie būtų aiškiai atpažįstami.

Vartotojai atsako už tai, kad ES įslaptinta informacija būtų laikoma atitinkama slaptumo žyma pažymėtose ir tinkamai saugomose laikmenose. Nustatoma tvarka, užtikrinanti, kad visų slaptumo žymos laipsnių ES įslaptinta informacija kompiuterinių duomenų saugojimo laikmenose būtų saugoma pagal šias saugumo taisykles.

25.5.4. *Kompiuterinių duomenų saugojimo laikmenų išslaptinimas ir naikinimas*

SAI patvirtinta tvarka kompiuterinių duomenų saugojimo laikmenų, naudojamų ES įslaptintai informacijai užrašyti, slaptumo lygmuo gali būti sumažintas arba jos gali būti išslaptintos.

Kompiuterinių duomenų saugojimo laikmenos, kuriose buvo saugota slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėta įslaptinta informacija arba ypatingos kategorijos informacija, neišslaptinamos ir pakartotinai nenaudojamos.

Jei kompiuterinių duomenų saugojimo laikmenų negalima išslaptinti arba pakartotinai panaudoti, jos sunaikinamos pirmiau minėta tvarka.

25.5.5. *Ryšių priemonių saugumas*

►M2 Komisijos Saugumo direktorato direktorius ◄ veikia kaip Šifravimo institucija.

Kai ES įslaptinta informacija yra perduodama elektromagnetinio ryšio priemonėmis, tokių perdavimų konfidencialumui, vientisumui ir prieinamumui užtikrinti taikomos specialios priemonės. SAI nustato perdavimų apsaugos nuo pasiklausymo ir perėmimo reikalavimus. Ryšių priemonėmis perduodama informacija saugoma laikantis konfidencialumo, vientisumo ir prieinamumo užtikrinimo reikalavimų.

Kai konfidencialumui, vientisumui ir prieinamumui užtikrinti yra reikalingi šifravimo metodai, tokius metodus ir su jais susijusias priemones specialiai tam tikslui akredituoja kaip Šifravimo institucija veikianti SAI.

▼B

Perduodant informaciją su ►M1 SECRET UE ◄ ir aukštesnio laipsnio slaptumo žyma konfidencialumas saugomas taikant šifravimo metodus arba priemones, patvirtintus už saugumą atsakingo Komisijos nario, kuris pasikonsultuoja su Komisijos Saugumo politikos patarėjų grupe. Perduodant informaciją, pažymėtą žymomis ►M1 CONFIDENTIEL UE ◄ ar ►M1 RESTREINT UE ◄, konfidencialumas saugomas taikant šifravimo metodus arba priemones, patvirtintus Komisijos Šifravimo institucijos, pasikonsultavus su Komisijos Saugumo politikos patarėjų grupe.

ES įslaptintos informacijos perdavimui taikomos taisyklės yra detaliai išdėstomos specialiose saugumo instrukcijose, kurias tvirtina ►M2 Komisijos Saugumo direktoratas ◄, pasikonsultavęs su Komisijos Saugumo politikos patarėjų grupe.

Esant išskirtinėms aplinkybėms, žymomis ►M1 RESTREINT UE ◄, ►M1 CONFIDENTIEL UE ◄ ir ►M1 SECRET UE ◄ pažymėta informacija gali būti perduodama atviru tekstu, jei informacijos savininkas kiekvieną atvejį aiškiai leidžia ir tinkamai užregistruoja. Išskirtinės aplinkybės yra:

a) gresianti arba esama krizė, konfliktas arba karinė padėtis;

b) kai ypač svarbus yra perdavimo greitis, o šifravimo priemonės nepasiekiamos, ir kai manoma, kad perduodama informacija negalės būti laiku panaudota siekiant pakenkti vykdomiems veiksmams.

Sistema turi būti pajėgi prireikus neleisti pasinaudoti įslaptinta informacija viename ar visuose nuotoliniuose terminaluose/darbo vietose arba ją fiziškai išjungiant, arba specialių SAI aprobuotų programinės įrangos funkcijų pagalba.

25.5.6. *Įrengimo ir spinduliavimo saugumas*

Pradinis sistemų instaliavimas ir kiekvienas svarbesnis jų pakeitimas organizuojamas taip, kad jį atliktų tik asmens patikimumo pažymėjimus turintys sistemų instaliavimo specialistai, nuolat prižiūrimi techniškai kvalifikuoto personalo, turinčio patikimumo patikrinimo pažymėjimus, leidžiančius naudotis ES įslaptinta informacija, kuri pagal slaptumo žymos laipsnį atitinka aukščiausią informacijos, kuri bus saugoma ir tvarkoma atitinkama sistema, slaptumo žymos laipsnį.

Sistemos, kuriose apdorojama ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma pažymėta informacija, saugomos taip, kad jų apsaugai negrėstų pavojus dėl elektromagnetinio spinduliavimo ir laidumo, kurių tyrimo ir kontrolės priemonės vadinamos „Tempest“.

„Tempest“ apsaugos priemones tikrina ir tvirtina „Tempest“ institucija (žr. 25.3.2 punktą).

25.6. **Saugumas tvarkant įslaptintą informaciją**

25.6.1. *Saugumo operacijų tvarka (SOT)*

Saugumo operacijų tvarka (SOT) nustato saugumo principus, operacijų procedūras ir personalo atsakomybę. Už SOT parengimą atsako techninių sistemų valdytojas (TSV).

25.6.2. *Programinės įrangos apsauga/konfigūravimo tvarkymas*

Taikomųjų programų saugumas įvertinamas remiantis pačios programos įslaptinimo įvertinimu, o ne pagal informacijos, kurią ji turi apdoroti, įslaptinimą. Naudojamos programinės įrangos versijos reguliariai tikrinamos siekiant užtikrinti jų vientisumą ir teisingą veikimą.

▼B

Naujos arba pakeistos programinės įrangos versijos ES įslaptintai informacijai apdoroti nenaudojamos tol, kol jų nepatikrina TSV.

25.6.3. *Pažeistos programinės įrangos/kompiuterinių virusų buvimo tikrinimas*

Pagal SAI reikalavimus reguliariai tikrinama, ar neatsirado pažeistos programinės įrangos/kompiuterinių virusų.

Visos į Komisiją patenkančios kompiuterinių duomenų saugojimo laikmenos prieš jų instaliavimą į kurią nors sistemą yra patikrinamos, ar programinė įranga nėra pažeista ir ar jos nėra užkrėstos kompiuteriniais virusais.

25.6.4. *Aptarnavimas*

Kontraktuose ir procedūriniuose nurodymuose dėl planinio ir neplaninio sistemų, kurioms yra parengtas SSRS, aptarnavimo tiksliai apibrėžiami reikalavimai, keliami aptarnavimo personalui, pasirengimui ir į IT aplinką įsinešamai reikiamai įrangai.

Reikalavimai yra aiškiai išdėstomi SSRS, o aptarnavimo tvarka – SOT. Rangovo aptarnavimo paslaugos, kai reikia pasinaudoti nuotolinėmis diagnostinėmis procedūromis, leistinos ypatingais atvejais, esant griežtai saugumo kontrolei ir tik turint SAI leidimą.

25.7. **Tiekimas**

25.7.1. *Bendrosios nuostatos*

Kiekvienas kuriamai sistemai naudojamas saugumo produktas turi būti arba jau įvertintas ir patvirtintas, arba šiuo metu pagal tarptautiniu lygiu pripažintus kriterijus (tokius kaip Bendrieji informacinių technologijų saugumo vertinimo kriterijai, ISO 15408) vertinamas ir atestuojamas vienos iš ES valstybių narių atitinkamos vertinimo ir atestavimo institucijos. Reikalingos specialios procedūros Patariamojo pirkimų kontraktų komiteto (PPKK) pritarimui.

Priimant sprendimą dėl to, ar lizinguoti, ar pirkti įrangą, ypač kompiuterinių duomenų saugojimo laikmenas, reikia turėti galvoje tai, kad įranga, kuri nors kartą buvo naudota ES įslaptintai informacijai tvarkyti, negali būti pernuomojama už tinkamai saugios aplinkos ribų, prieš tai SAI sutikimu jos neišslaptinus. Reikia atsižvelgti ir į tai, kad SAI ne visada duos tokį sutikimą.

25.7.2. *Akreditavimas*

Visas sistemas, kurioms turi būti parengtas SSRS, prieš pradedant jomis tvarkyti ES įslaptintą informaciją turi akredituoti SAI, remdamasi SSRS, SOT pateikta informacija ir bet kuriais kitais atitinkamais dokumentais. Posistemės ir nuotoliniai terminalai/darbo vietos akredituojamos kaip visų sistemų, prie kurių jie yra prijungti, dalis. Kai sistemą naudoja ir Komisija, ir kitos organizacijos, Komisija ir atitinkamos saugumo institucijos tarpusavyje susitaria dėl akreditavimo.

Akreditavimą galima atlikti pagal atitinkamai sistemai pritaikytą ir SAI apibrėžtą akreditavimo strategiją.

25.7.3. *Vertinimas ir atestavimas*

Tam tikrais atvejais prieš akreditaciją kompiuterinės įrangos, gamintojo programinės įrangos ir apskritai programinės įrangos sistemos saugumo savybės yra įvertinamos ir atestuojamos kaip tinkamos reikiamo slaptumo žymos laipsnio informacijai saugoti.

Vertinimo ir atestavimo reikalavimai įtraukiami planuojant sistemą ir aiškiai suformuluojami SSRS.

▼B

Vertinimą ir atestavimą pagal patvirtintą vadovą TSV vardu atlieka techniškai kvalifikuotas ir tinkamus patikimumo pažymėjimus turintis personalas.

Atitinkamą personalą gali skirti valstybės narės paskirta vertinimo ir akreditavimo institucija arba jos paskirti atstovai, pvz., kompetentingas ir patikrintas sutarties partneris.

Vertinimas ir atestavimas gali būti supaprastinamas (pvz., vertinami tik integravimo aspektai), jei sistemos yra pagrįstos nacionaliniu lygiu įvertintais ir atestuotais kompiuterių saugumo produktais.

25.7.4. *Įprastas saugumo savybių tikrinimas tęstiniam akreditavimui*

TSV nustato įprasto tikrinimo procedūras, užtikrinančias visų sistemos saugumo savybių tinkamumą naudoti.

Pakeitimai, dėl kurių sistemą reikėtų iš naujo akredituoti arba kuriuos pirmiau turėtų patvirtinti SAI, turi būti aiškiai nurodyti ir suformuluoti SSRS. Po kiekvieno pakeitimo, taisymo arba kiekvieno gedimo, galėjusių neigiamai paveikti sistemos saugumo savybes, TSV turi užtikrinti patikrinimą, kuris garantuotų tinkamą saugumo savybių veikimą. Sistemos akreditacijos pratęsimas paprastai priklauso nuo patikrinimų sėkmingumo.

Visas sistemas, kuriose yra įdiegtos saugumo savybės, reguliariai tikrina arba kontroliuoja SAI. Slaptumo žyma ►**M1** TRES SECRET UE/EU TOP SECRET ◄ pažymėtą informaciją apdorojančios sistemos tikrinamos ne rečiau kaip kartą per metus.

25.8. **Laikinas arba atsitiktinis naudojimas**

25.8.1. *Mikrokompiuterių/asmeninių kompiuterių saugumas*

Mikrokompiuteriai/asmeniniai kompiuteriai (AK) su fiksuotais diskais (arba kitomis pastoviomis laikmenomis), veikiantys atskirai arba sujungti į tinklą, ir nešiojamosios kompiuterinės priemonės (pvz., nešiojamieji AK ir elektroninės „užrašų knygutės“) su fiksuotais kietaisiais diskais yra laikomi informacinėmis laikmenomis ta pačia prasme, kaip ir lankstieji diskeliai arba kitos išimamos kompiuterinių duomenų saugojimo laikmenos.

Šiai įrangai suteikiamos apsaugos – prieinamumo, apdorojimo, saugojimo ir gabenimo požiūriu – lygmuo turi atitikti bet kada joje laikytos arba apdorotos informacijos aukščiausią slaptumo žymos laipsnį (tol, kol pagal patvirtintą tvarką tas laipsnis nebus sumažintas arba informacija nebus išslaptinta).

25.8.2. *Nuosavų IT įrenginių naudojimas atliekant Komisijos tarnybines pareigas*

ES įslaptintai informacijai tvarkyti draudžiama naudoti saugojimo galimybių turinčias nuosavas išimamas kompiuterinių duomenų saugojimo laikmenas, programinę įrangą ir kompiuterinę įrangą (pvz., asmeninius kompiuterius ir nešiojamąją kompiuterinę įrangą).

Neturint ►**M2** Komisijos Saugumo direktorato direktoriaus ◄ raštiško leidimo, į jokią I ir II klasės zoną, kurioje dirbama su ES įslaptinta informacija, neleidžiama įsinešti nuosavos kompiuterinės įrangos, programinės įrangos ir laikmenų. Toks leidimas gali būti išduodamas tik išimtiniais atvejais dėl techninių priežasčių.

▼B

25.8.3. *Sutarties partnerio ar šalies narės tiekiamų IT įrengimų naudojimas atliekant Komisijos tarnybines pareigas*

Leisti Komisijoje tarnybiniais tikslais naudoti sutarties partnerio IT įrengimus ir programinę įrangą gali ►M2 Komisijos Saugumo direktorato direktorius ◄. Šalies narės tiekiamus IT įrengimus ir programinę įrangą taip pat gali būti leista naudoti; tuo atveju IT įrengimai perduodami atitinkamai Komisijos inventoriaus kontrolei. Bet kuriuo atveju, jei ES įslaptintai informacijai apdoroti naudojami IT įrengimai, yra konsultuojamasi su SAI, kad tuos įrengimus naudojant taikomi INFOSAUGOS elementai būtų tinkamai apsvarstyti ir įgyvendinti.

26. ES ĮSLAPTINTOS INFORMACIJOS PERDAVIMAS TREČIOSIOMS ŠALIMS ARBA TARPTAUTINĖMS ORGANIZACIJOMS

26.1.1. *ES įslaptintos informacijos perdavimą reglamentuojantys principai*

Komisija kolegialiai priima sprendimą dėl ES įslaptintos informacijos perdavimo trečiosioms šalims arba tarptautinėms organizacijoms, atsižvelgdama į:

— tokios informacijos pobūdį ir turinį,

— gavėjui taikomą „būtina žinoti“ principą,

— naudos Europos Sąjungai įvertinimą.

Perduoti rengiamos ES įslaptintos informacijos autoriaus prašoma jo sutikimo.

Sprendimai kiekvienu atveju priimami atskirai, atsižvelgiant į:

— norimą bendradarbiavimo su atitinkamomis trečiosiomis šalimis arba tarptautinėmis organizacijomis laipsnį,

— jų patikimumą, kuris priklauso nuo toms valstybėms arba organizacijoms patikėtos ES įslaptintos informacijos slaptumo žymos laipsnio ir tose šalyse bei organizacijose ir Europos Sąjungoje taikomų saugumo taisyklių suderinamumo. Komisijos Saugumo politikos patarėjų grupė šiuo klausimu pateikia Komisijai savo techninę išvadą.

Priimdamos ES įslaptintą informaciją, trečiosios šalys arba tarptautinės organizacijos garantuoja, kad perduota informacija nebus naudojama jokiems kitiems tikslams, išskyrus tuos, dėl kurių informacija yra perduodama arba ja yra keičiamasi, ir kad jie garantuos Komisijos reikalaujamą saugumą.

26.1.2. *Bendradarbiavimo lygiai*

Nusprendusi, kad įslaptinta informacija gali būti perduodama atitinkamai valstybei ar tarptautinei organizacijai arba su ja gali būti keičiamasi ta informacija, Komisija taip pat priima sprendimą dėl galimo bendradarbiavimo lygio. Bendradarbiavimo lygis ypač priklauso nuo tos valstybės ar tarptautinės organizacijos taikomos saugumo politikos ir nuostatų.

Yra trys bendradarbiavimo lygiai:

1 lygis

Bendradarbiavimas su trečiosiomis šalimis ar tarptautinėmis organizacijomis, kurių saugumo politika ir nuostatos yra labai artimos ES saugumo politikai ir nuostatoms.

2 lygis

Bendradarbiavimas su trečiosiomis šalimis ar tarptautinėmis organizacijomis, kurių saugumo politika ir nuostatos žymiai skiriasi nuo ES saugumo politikos ir nuostatų.

▼B

3 lygis

Atsitiktinis bendradarbiavimas su trečiosiomis šalimis ar tarptautinėmis organizacijomis, kurių saugumo politikos ir nuostatų negalima įvertinti.

Kiekvienas bendradarbiavimo lygis nulemia procedūras ir saugumo priemones, išsamiau apibūdintas 3, 4 ir 5 priedėliuose.

26.1.3. *Susitarimai dėl saugumo*

Nusprendusi, kad yra nuolatinis arba ilgalaikis poreikis keistis įslaptinta informacija su trečiosiomis šalimis ar kitomis tarptautinėmis organizacijomis, Komisija su jomis sudaro „Susitarimus dėl saugumo keičiantis įslaptinta informacija tvarkos“, kuriuose apibrėžiami bendradarbiavimo tikslai ir abipusės informacijos, kuria keičiamasi, apsaugos taisyklės.

Esant 3 lygio atsitiktiniam bendradarbiavimui, kuris pagal apibrėžimą yra riboto laiko ir kuriuo siekiama ribotų tikslų, „Susitarimus dėl saugumo keičiantis įslaptinta informacija tvarkos“ gali pakeisti paprasti sutarimo memorandumai, apibrėžiantys įslaptintos informacijos, kuria bus keičiamasi, pobūdį ir abipusius įsipareigojimus dėl tos informacijos, jei jos slaptumo žymos laipsnis ne aukštesnis už ►M1 RESTREINT UE ◄.

Prieš pateikiant susitarimų dėl saugumo tvarkos ir sutarimo memorandumų projektus Komisijai sprendimui priimti, juos svarsto Komisijos Saugumo politikos patarėjų grupė.

Už saugumą atsakingas Komisijos narys bet kokios reikalingos pagalbos kreipiasi į valstybių narių NSI, kad užtikrintų, jog perduodama informacija bus naudojama ir saugoma pagal susitarimų dėl saugumo tvarkos ar sutarimo memorandumų nuostatas.

▼M3

27. BENDRI MINIMALŪS PRAMONĖS SAUGUMO STANDARTAI

27.1. **Įvadas**

Šiame skyriuje aptariami pramoninės veiklos saugumo aspektai, kurie yra svarbūs vedant derybas ir sudarant sutartis arba susitarimus dėl dotacijų, pagal kuriuos pramonės ir kitiems subjektams pavedamos užduotys, susijusios su ES įslaptinta informacija, kurias vykdant susiduriama su tokia informacija ir (arba) tokia informacija yra užduoties dalis, taip pat jiems vykdant šias sutartis, įskaitant ES įslaptintos informacijos perdavimą arba galimybę su ja susipažinti viešųjų pirkimų procedūros ir kvietimų teikti paraiškas metu (paraiškų pateikimo laikotarpiu ir vedant derybas iki sutarties sudarymo).

27.2. **Apibrėžtys**

Šiuose bendruose minimaliuose standartuose vartojamos tokios sąvokos:

a) įslaptinta sutartis – produktų tiekimo, darbų vykdymo, patalpų ar paslaugų teikimo sutartis arba susitarimas dėl dotacijos, kuriuos vykdant būtina susipažinti su ES įslaptinta informacija arba tokią informaciją kurti;

b) įslaptinta subrangos sutartis – rangovo arba dotacijos gavėjo su kitu rangovu (t. y. subrangovu) sudaroma prekių tiekimo, darbų vykdymo, patalpų arba paslaugų teikimo sutartis, kurią vykdant būtina susipažinti su ES įslaptinta informacija arba tokią informaciją kurti;

c) rangovas – ekonominių operacijų vykdytojas arba juridinis asmuo, turintis veiksnumą sudaryti sutartis arba gauti dotacijas;

▼M3

d) paskirtoji saugumo institucija (DSA) – ES valstybės narės Nacionalinei saugumo institucijai (NSA) atskaitinga institucija, kuri atsako už pramonės arba kitų subjektų informavimą apie nacionalinę politiką visais pramoninio saugumo klausimais ir duoda nurodymus bei padeda ją įgyvendinti. DSA funkciją gali vykdyti NSA;

e) patalpų saugumo patikrinimas (FSC) – NSA ir (arba) DSA atliekamas administracinis nustatymas, kad saugumo požiūriu patalpose nurodyto įslaptinimo laipsnio ES įslaptintai informacijai gali būti užtikrintas tinkamas saugumas ir kad buvo atliktas jose dirbančio personalo, kuriam reikia susipažinti su ES įslaptinta informacija, patikimumo patikrinimas ir jis buvo informuotas apie atitinkamus saugumo reikalavimus, būtinus norint susipažinti su ES įslaptinta informacija ir ją apsaugoti;

f) pramonės arba kitas subjektas – rangovas arba subrangovas, tiekiantis prekes, atliekantis darbus arba teikiantis paslaugas; tai gali būti pramonės, prekybiniai, paslaugų, moksliniai, mokslinių tyrimų, švietimo arba vystymo subjektai;

g) pramoninis saugumas – apsaugos priemonių ir procedūrų taikymas siekiant užkirsti kelią, atskleisti ir ištaisyti derybų iki sutarties sudarymo ir įslaptintų sutarčių vykdymo metu rangovo arba subrangovo tvarkomos ES įslaptintos informacijos praradimą arba neteisėtą atskleidimą;

h) nacionalinė saugumo institucija (NSA) – ES valstybės narės Vyriausybės institucija, kuriai tenka galutinė atsakomybė už ES įslaptintos informacijos apsaugą toje valstybėje narėje;

i) bendras sutarties slaptumo žymos laipsnis – visos sutarties arba susitarimo dėl dotacijos slaptumo žymos nustatymas remiantis informacijos ir (arba) medžiagos, kuri turi arba gali būti surinkta, perduota arba su kuria gali būti susipažinta pagal bet kurį visos sutarties arba susitarimo dėl dotacijos elementą, slaptumo žymomis. Bendras sutarties slaptumo žymos laipsnis negali būti žemesnis nei aukščiausia bet kurio jos elemento slaptumo žyma, tačiau gali būti aukštesnis dėl visumos poveikio;

j) saugumo aspektų paaiškinimas (SAL) – specialių sutartinių sąlygų rinkinys, kurį parengia susitariančioji institucija ir kuris yra įslaptintos sutarties, pagal kurią gali būti susipažįstama su ES įslaptinta informacija arba tokia informacija gali būti surinkta, sudėtinė dalis – jame nurodomi saugumo reikalavimai arba sutarties elementai, kurių saugumą būtina užtikrinti;

k) įslaptinimo vadovas (SCG) – dokumentas, kuriame aprašomi programos, sutarties arba susitarimo dėl dotacijos įslaptinti elementai, nurodant taikomus slaptumo žymų laipsnius. SCG gali būti papildomas programos arba sutarties vykdymo laikotarpiu ir informacijos elementams gali būti suteiktos naujos slaptumo žymos arba jų slaptumo žymos laipsnis gali būti sumažintas. SCG turi būti SAL dalis.

27.3. **Organizavimas**

a) Įslaptinta sutartimi Komisija gali valstybėje narėje įregistruotiems pramonės ar kitiems subjektams gali pavesti užduotis, susijusias su ES įslaptinta informacija, kurias vykdant susiduriama su tokia informacija ir (arba) tokia informacija yra užduoties dalis;

b) Komisija užtikrina, kad sudarant įslaptintas sutartis būtų laikomasi visų su šiais minimaliais standartais susijusių reikalavimų;

c) Komisija įtraukia į darbą susijusią arba susijusias NSA taikydama šiuos minimalius pramoninio saugumo standartus. NSA gali perteikti šias užduotis vienai arba kelioms DSA;

▼M3

d) galutinė atsakomybė už ES įslaptintos informacijos apsaugą pramonės arba kituose subjektuose tenka jų vadovybei;

e) sudarant įslaptintą sutartį arba subrangos sutartį, kuriai taikomi šie minimalūs standartai, Komisija ir (arba) atitinkamai NSA ir (arba) DSA nedelsdami praneš valstybės narės, kurioje yra įregistruotas rangovas arba subrangovas, NSA ir (arba) DSA.

27.4. **Įslaptintos sutartys ir įslaptinti sprendimai dėl dotacijų**

a) Suteikiant įslaptintoms sutartims arba susitarimams dėl dotacijos slaptumo žymą turi būti atsižvelgiama į šiuos principus:

— Komisija atitinkamai nustato sutarties aspektus, kurių apsaugą būtina užtikrinti, ir su tuo susijusią slaptumo žymą; tai darydama ji turi atsižvelgti į pirminę slaptumo žymą, kurią iki sutarties sudarymo surinktai informacijai suteikė jos autorius,

— bendras sutarties slaptumo žymos laipsnis negali būti žemesnis nei aukščiausia bet kurio jos elemento slaptumo žyma,

— ES įslaptinta informacija, surinkta vykdant veiklą pagal sutartį, įslaptinama laikantis įslaptinimo vadovo,

— atitinkamais atvejais Komisija yra atsakinga už bendro sutarties slaptumo žymos laipsnio arba bet kurio jos elemento slaptumo žymos keitimą pasikonsultavus su autoriumi ir už visų suinteresuotųjų šalių informavimą,

— rangovui arba subrangovui perduota arba vykdant veiklą pagal sutartį surinkta įslaptinta informacija negali būti naudojama kitais tikslais nei apibrėžtieji įslaptintoje sutartyje ir negali būti atskleidžiama trečiosioms šalims be išankstinio rašytinio autoriaus sutikimo.

b) Komisija ir susijusių valstybių narių NSA ir (arba) DSA turi užtikrinti, kad rangovai ir subrangovai, su kuriais sudarytos įslaptintos sutartys, susijusios su informacija, pažymėta slaptumo žyma CONFIDENTIEL UE arba didesnio slaptumo žyma, imtųsi visų tinkamų priemonių tokiai jiems perduotai arba vykdant įslaptintą sutartį jų surinktai ES įslaptintai informacijai apsaugoti laikantis nacionalinių įstatymų ir kitų teisės aktų. Dėl saugumo reikalavimų nesilaikymo įslaptinta sutartis gali būti nutraukta.

c) Turi būti atliktas visų pramonės arba kitų subjektų, dalyvaujančių vykdant įslaptintas sutartis, pagal kurias suteikiama galimybė susipažinti su informacija, pažymėta slaptumo žyma CONFIDENTIEL UE arba didesnio slaptumo žyma, nacionalinis FSC. FSC atlieka valstybės narės NSA ir (arba) DSA, kad patvirtintų, jog patalpose gali būti suteikta ir užtikrinta atitinkamo slaptumo žymos laipsnio ES įslaptintos informacijos tinkama apsauga.

d) Sudarant įslaptintą sutartį patalpų saugumo pareigūnas (FSO), paskirtas rangovo arba subrangovo vadovybės, privalo prašyti atlikti visų asmenų, įdarbintų toje valstybėje narėje registruotuose pramonės arba kituose subjektuose, kuriems dėl jų pareigų pagal įslaptintą sutartį reikia susipažinti su ES informacija, pažymėta slaptumo žymomis CONFIDENTIEL UE arba didesnio slaptumo žyma, personalo patikimumo patikrinimą, kurį turi atlikti ir išduoti liudijantį dokumentą tos valstybės narės NSA ir (arba) DSA laikydamosi nacionalinių teisės aktų.

▼**M3**

e) Į įslaptintas sutartis turi būti įtrauktas SAL, kaip apibrėžta 27 dalies b punkto j papunktyje. SCG turi būti įtrauktas į SAL.

f) Prieš pradėdamas derybas dėl įslaptintos sutarties, Komisija susisieks su valstybės narės, kurioje yra įregistruoti atitinkami pramoniniai ar kiti subjektai, NSA ir (arba) DSA, kad gautų patvirtinimą, jog yra atliktas ir galioja jų FSC, atitinkantis sutarties slaptumo žymos laipsnį.

g) Susitariančioji institucija negali sudaryti įslaptintos sutarties su pasirinktu ekonominių operacijų vykdytoju negavusi galiojančio FSC liudijimo.

h) Sutartims, susijusioms su informacija, pažymėta RESTREINT UE, FSC nereikia, išskyrus atvejus, kai tai privaloma pagal valstybių narių nacionalinius įstatymus ir kitus teisės aktus.

i) Skelbiant konkursą įslaptintoms sutartims sudaryti, turi būti nurodoma, kad paraiškos nepateikęs ekonominių operacijų vykdytojas arba ekonominių operacijų vykdytojas, kuris nebuvo pasirinktas, privalo per nurodytą laiką grąžinti visus dokumentus.

j) Rangovui gali tekti įvairiais lygiais vesti derybas su subrangovais dėl įslaptintų subrangos sutarčių. Rangovas atsako už tai, kad visa subrangos veikla būtų vykdoma laikantis šiame skyriuje pateikiamų bendrų minimalių standartų. Tačiau rangovas negali perduoti subrangovui ES įslaptintos informacijos arba medžiagos be išankstinio rašytinio autoriaus sutikimo.

k) Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, turi būti nurodytos skelbiant konkursą arba kvietimą teikti paraiškas ir įslaptintoje sutartyje. Su subjektais, įregistruotais valstybėje, kuri nėra ES valstybė narė, subrangos sutartys negali būti sudaromos be aiškaus rašytinio Komisijos leidimo.

l) Visą sutarties galiojimo laiką Komisija stebi saugumo nuostatų laikymąsi, koordinuodama veiklą su atitinkama DSA ir (arba) NSA. Sužinojus apie saugumo incidentus, apie juos pranešama laikantis šių Saugumo taisyklių II dalies 24 skyriaus nuostatų. Apie visus FSC pakeitimus arba panaikinimą nedelsiant pranešama Komisijai ir visoms kitoms NSA ir (arba) DSA, kurioms apie jį buvo pranešta.

m) Nutraukiant įslaptintą sutartį arba subrangos sutartį, Komisija ir (arba) atitinkamai NSA ir (arba) DSA nedelsdami praneš valstybės narės, kurioje yra įregistruotas rangovas arba subrangovas, NSA ir (arba) DSA.

n) Nutraukus arba įvykdžius įslaptintą sutartį arba įslaptintą subrangos sutartį, rangovai ir subrangovai privalo ir toliau laikytis šiame skyriuje nurodytų bendrų minimalių standartų ir užtikrinti įslaptintos informacijos konfidencialumą.

o) Konkrečios nuostatos dėl įslaptintos informacijos sunaikinimo pasibaigus sutarties laikui bus nustatytos SAL arba kitose susijusiose nuostatose, kuriose nustatomi saugumo reikalavimai.

p) Šiame skyriuje numatyti įsipareigojimai ir sąlygos taikomi *mutatis mutandis* procedūroms, kai sprendimu suteikiamos dotacijos ir ypač šių dotacijų gavėjams. Sprendimuose dėl dotacijos nustatomi įsipareigojimai gavėjams.

▼M3

27.5. **Apsilankymai**

Dėl Komisijos darbuotojų apsilankymų valstybių narių pramonės arba kituose subjektuose, vykdančiuose ES įslaptintas sutartis, turi būti susitariama su atitinkama NSA ir (arba) DSA. Dėl pramonės arba kitų subjektų darbuotojų apsilankymų, susijusių su ES įslaptintomis sutartimis, turi susitarti atitinkamos NSA ir (arba) DSA. Tačiau su ES įslaptinta sutartimi susijusios NSA ir (arba) DSA gali susitarti dėl tvarkos, pagal kurią dėl pramonės arba kitų subjektų darbuotojų apsilankymų gali būti susitariama tiesiogiai.

27.6. **ES įslaptintos informacijos perdavimas ir gabenimas**

a) Perduodant ES įslaptintą informaciją taikomos šių Saugumo taisyklių II dalies 21 skyriaus nuostatos. Šias nuostatas papildo tarp valstybių narių galiojančios procedūros.

b) ES įslaptintos medžiagos, susijusios su įslaptintomis sutartimis, tarptautinis gabenimas atliekamas laikantis valstybių narių nacionalinės tvarkos. Nagrinėjant tarptautinio gabenimo saugumo procedūras bus taikomi šie principai:

   — saugumas užtikrinamas visais gabenimo etapais ir visomis aplinkybėmis, nuo kilmės vietos iki galutinės paskirties vietos,

   — siuntai suteikiamas apsaugos laipsnis nustatomas pagal joje esančios medžiagos aukščiausią slaptumo žymos laipsnį,

   — prireikus atliekamas gabenimą užtikrinančių bendrovių FSC. Tokiais atvejais siuntą tvarkantis personalas patikrinamas laikantis šiame skyriuje pateikiamų bendrų minimalių standartų,

   — kelionės kiek įmanoma vykdomos nuo punkto iki punkto ir užbaigiamos taip greitai, kaip leidžia aplinkybės,

   — kai įmanoma, turėtų būti pasirenkami maršrutai tik per ES valstybių narių teritorijas. Maršrutais per valstybes, kurios nėra ES valstybės narės, turėtų būti gabenama tik gavus siuntėjo ir gavėjo valstybių NSA ir (arba) DSA leidimus,

   — prieš vežant ES įslaptintą medžiagą gabenimo planą parengia siuntėjas, o patvirtina – atitinkamos NSA ir (arba) DSA.

▼M1

1 priedėlis

NACIONALINIO SAUGUMO KLASIFIKACIJŲ PALYGINIMAS

ES klasifikacija	TRES SECRET UE/EU TOP SECRET	SECRET UE	CONFIDENTIEL UE	RESTREINT UE
VES klasifikacija	FOCAL TOP SECRET	WEU SECRET	WEU CONFIDENTIAL	WEU RESTRICTED
Euratomo klasifikacija	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA RESTRICTED
NATO klasifikacija	COSMIC TOP SECRET	NATO SECRET	NATO CONFIDENTIAL	NATO RESTRICTED
Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Belgija	Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	Diffusion restreinte Beperkte Verspreiding
Kipras	Άκρως Απόρρητο	Απόρρητο	Εμπιστευτικό	Περιορισμένης Χρήσης
Čekijos Respublika	Přísn tajné	Tajné	Důvěrné	Vyhrazené
Danija	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Estija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Vokietija	Streng geheim	Geheim	VS ([1]) — Vertraulich	VS — Nur für den Dienstgebrauch
Graikija	Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
Suomija	Erittäin salainen	Erittäin salainen	Salainen	Luottamuksellinen
Prancūzija	Très Secret Défense ([2])	Secret Défense	Confidentiel Défense	

▼M4

Kroatija	Vrlo tajno	Tajno	Povjerljivo	Ograničeno

▼M1

Airija	Top Secret	Secret	Confidential	Restricted
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Latvija	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lietuva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Liuksemburgas	Très Secret	Secret	Confidentiel	Diffusion restreinte

▼**M1**

Vengrija	Szigorúan titkos !	Titkos !	Bizalmas !	Korlátozott terjesztésű !
Malta	L-Ghola Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nyderlandai	Stg ([3]). Zeer Geheim	Stg. Geheim	Stg. Confidentieel	Departementaalvertrouwelijk
Lenkija	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalija	Muito Secreto	Secreto	Confidencial	Reservado
Slovėnija	Strogo tajno	Tajno	Zaupno	SVN Interno
Slovakija	Prísne tajné	Tajné	Dôverné	Vyhradené
Ispanija	Secreto	Reservado	Confidencial	Difusión Limitada
Švedija	Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
Jungtinė Karalystė	Top Secret	Secret	Confidential	Restricted

([1]) VS = Verschlusssache
([2]) Klasifikacija „Très Secret Défense“, apimanti vyriausybinius klausimus, gali būti pakeista tik gavus Ministro Pirmininko leidimą.
([3]) Stg = staatsgeheim

2 priedėlis

PRAKTINIS SLAPTUMO ŽYMŲ VADOVAS

Šis vadovas yra informacinis, jis negali būti aiškinamas kaip keičiantis esmines 16, 17, 20 ir 21 skirsnių nuostatas.

Slaptumo žyma	Kada	Kas	Žymos dėjimas	Slaptumo žymos laipsnio sumažinimas/išslaptinimas/sunaikinimas	
				Kas	Kada
►**M1** TRES SECRET UE/EU TOP SECRET ◄: Ši žyma suteikiama tik tai informacijai ir medžiagai, kurią atskleidus be leidimo, gali būti padaryta ypač didelė žala svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams [16.1].	Tikėtina, kad atskleidus slaptumo žyma ►**M1** TRES SECRET UE/EU TOP SECRET ◄ pažymėtus dalykus, — iškiltų tiesioginė grėsmė ES arba vienos iš valstybių narių ar draugiškos valstybės vidaus stabilumui; — būtų ypač smarkiai pakenkta santykiams su draugiškomis Vyriausybėmis; — būtų netekta labai daug gyvybių; — būtų ypač smarkiai pakenkta valstybių narių arba kitų bendrininkų pajėgų operacijų veiksmingumui ar saugumui arba besitęsiančiam ypač vertingų saugumo ir žvalgybos operacijų veiksmingumui; — būtų padaryta didelė ilgalaikė žala ES arba valstybių narių ekonomikai.	Tinkamai įgalioti asmenys (autoriai), generaliniai direktoriai, tarnybų vadovai [17.1]. Autoriai nurodo datą, laiką arba atvejį, kada turinio slaptumo laipsnis gali būti sumažintas arba dokumentas išslaptintas [16.2]. Kitais atvejais jie peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad garantuotų, jog reikalingas pradinis įslaptinimas [17.3].	Slaptumo žyma ►**M1** TRES SECRET UE/EU TOP SECRET ◄, o tam tikrais atvejais apsaugos galiojimo laikotarpį nurodantys ženklai ir (arba) gynybos kvalifikacinė žyma ESGP dedama ant šios kategorijos dokumentų mechaninėmis priemonėmis arba ranka [16.4, 16.5, 16.3]. ES slaptumo žymos ir apsaugos galiojimo laikotarpį nurodantys ženklai dedami centre kiekvieno puslapio viršuje ir apačioje, puslapiai numeruojami. Kiekvienas dokumentas turi registracijos numerį ir datą; šis registracijos numeris rašomas kiekviename puslapyje. Jei dokumentai turi būti platinami keliais egzemplioriais, ant kiekvieno iš jų pirmajame puslapyje kartu su bendru puslapių skaičiumi rašomas kopijos numeris. Visi priedai ir pridedami dokumentai išvardijami dokumento pirmajame puslapyje [21.1].	Išslaptinimas arba slaptumo žymos laipsnio sumažinimas yra autoriaus kompetencija. Jis apie pakeitimą informuoja suinteresuotus adresatus, kuriems yra nusiuntęs dokumentą arba padaręs jo kopiją [17.3]. Dokumentus, pažymėtus slaptumo žyma ►**M1** TRES SECRET UE/EU TOP SECRET ◄, sunaikina už juos atsakinga centrinė registratūra arba subregistratūra. Kiekvienas sunaikintas dokumentas įrašomas į sunaikinimo pažymą, kurią pasirašo dokumentų su slaptumo žyma ►**M1** TRES SECRET UE/EU TOP SECRET ◄ kontrolės pareigūnas ir naikinimą stebėjęs pareigūnas, turintis dirbti su slaptumo žyma ►**M1** TRES SECRET UE/EU TOP SECRET ◄ pažymėtais dokumentais tinkamą patikimumo pažymėjimą. Pranešimas apie tai įrašomas atitinkamoje registro knygoje. Sunaikinimo pažymas kartu su paskirstymo lapais registratūra saugo 10 metų [22.5].	Atliekamos kopijos ir nebereikalingi dokumentai yra sunaikinami [22.5]. Dokumentai su ►**M1** TRES SECRET UE/EU TOP SECRET ◄ slaptumo žyma, taip pat ir visos įslaptintos informacijos atliekos, susidariusios rengiant tuos dokumentus, tokios kaip sugadintos kopijos, darbiniai projektai, išspausdintos pastabos, nuorašams naudotas kalkinis popierius, stebint dokumentų su slaptumo žyma ►**M1** TRES SECRET UE/EU TOP SECRET ◄ kontrolės pareigūnui yra sunaikinami sudeginant, paverčiant minkšta mase, supjaustant arba kitaip susmulkinant, kad jų turinys ar forma negalėtų būti atkurti [22.5].

Slaptumo žyma	Kada	Kas	Žymos dėjimas	Slaptumo žymos laipsnio sumažinimas/išslaptinimas/sunaikinimas	
				Kas	Kada
►M1 SECRET UE ◄: Ši žyma suteikiama tik tai informacijai ir medžiagai, kurią atskleidus be leidimo, gali būti labai pakenkta svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams.	Tikėtina, kad atskleidus slaptumo žyma ►M1 SECRET UE ◄ pažymėtus dalykus: — būtų sukelta tarptautinė įtampa; — būtų padaryta didelė žala santykiams su draugiškomis Vyriausybėmis; — iškiltų grėsmė gyvybei arba būtų labai pakenkta viešajai tvarkai arba asmens saugumui ir laisvei; — būtų smarkiai pakenkta valstybių narių arba kitų bendrininkų pajėgų operacijų veiksmingumui ar saugumui arba besitęsiančiam labai vertingų saugumo ir žvalgybos operacijų veiksmingumui — būtų padaryta didelė materialinė žala ES arba vienos iš jos valstybių narių finansiniams, monetariniams, ekonominiams ir prekybiniams interesams.	Įgalioti asmenys autoriai), generaliniai direktoriai, tarnybų vadovai [17.1]. Autoriai nurodo datą, laiką, kada turinio slaptumo laipsnis gali būti sumažintas arba dokumentas išslaptintas [16.2]. Kitais atvejais jie peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad garantuotų, jog reikalingas pradinis įslaptinimas [17.3].	Slaptumo žyma ►M1 SECRET UE ◄, o tam tikrais atvejais apsaugos galiojimo laikotarpį nurodantys ženklai ir (arba) gynybos kvalifikacinė žyma ESGP dedama ant atitinkamos kategorijos dokumentų mechaninėmis priemonėmis arba ranka [16.4, 16.5, 16.3]. ES slaptumo žymos ir apsaugos galiojimo laikotarpį nurodantys ženklai dedami centre kiekvieno puslapio viršuje ir apačioje, puslapiai numeruojami. Kiekvienas dokumentas turi registracijos numerį ir datą; šis registracijos numeris rašomas kiekviename puslapyje. Jei dokumentas dauginamas keliais egzemplioriais, ant kiekvieno iš jų pirmajame puslapyje kartu su bendru puslapių skaičiumi rašomas kopijos numeris. Visi priedai ir pridedami dokumentai išvardijami dokumento pirmajame puslapyje [21.1].	Išslaptinimas ir slaptumo laipsnio sumažinimas yra autoriaus kompetencija. Jis apie pakeitimą informuoja suinteresuotus adresatus, kuriems yra nusiuntęs dokumentą arba padaręs jo kopiją [17.3]. Dokumentus, pažymėtus slaptumo žyma ►M1 SECRET UE ◄, sunaikina už tokius dokumentus atsakinga registratūra; naikinimą stebi patikimumo pažymėjimą turintis asmuo. Naikinamieji dokumentai su slaptumo žyma ►M1 SECRET UE ◄ įrašomi į pasirašytas sunaikinimo pažymas, kurias kartu su platinimo formomis registratūra saugo ne mažiau kaip trejus metus [22.5].	Atliekamos kopijos ir nebereikalingi dokumentai yra sunaikinami [22.5]. Dokumentai su slaptumo žyma ►M1 SECRET UE ◄, tarp jų ir visos įslaptintos informacijos atliekos, susidariusios rengiant tuos dokumentus, tokios kaip sugadintos kopijos, darbiniai projektai, išspausdintos pastabos ir nuorašams naudotas kalkinis popierius, yra sunaikinami sudeginant, paverčiant minkšta mase, supjaustant arba kitaip susmulkinant, kad jų turinys ar forma negalėtų būti atkurti [22.5].
►M1 CONFIDENTIEL UE ◄:	Tikėtina, kad atskleidus slaptumo žyma ►M1 CONFIDENTIEL UE ◄ pažymėtus dalykus, — būtų padaryta konkreti žala diplomatiniams santykiams, t. y. būtų sukeltas oficialus protestas arba kitokios sankcijos;	Įgalioti asmenys (autoriai), generaliniai direktoriai ir tarnybų vadovai [17.1].	Slaptumo žyma ►M1 CONFIDENTIEL UE ◄, o tam tikrais atvejais apsaugos galiojimo laikotarpį nurodantys ženklai ir (arba) gynybos kvalifikacinė žyma ESGP dedama ant atitinkamos kategorijos dokumentų mechaninėmis priemonėmis ar ranka arba spausdinama ant iš anksto antspauduoto ir registruoto popieriaus [16.4, 16.5, 16.3].	Išslaptinimas ir slaptumo laipsnio sumažinimas yra autoriaus kompetencija. Jis apie pakeitimą informuoja suinteresuotus adresatus, kuriems yra nusiuntęs dokumentą arba padaręs kopiją [17.3].	Atliekamos kopijos ir nebereikalingi dokumentai yra sunaikinami [22.5].

▼B

Slaptumo žyma	Kada	Kas	Žymos dėjimas	Slaptumo žymos laipsnio sumažinimas/išslaptinimas/sunaikinimas	
				Kas	Kada
Ši žyma suteikiama tai informacijai ir medžiagai, kurią atskleidus be leidimo, gali būti pakenkta svarbiausiems Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams [16.1].	— būtų pakenkta asmens saugumui arba laisvei; — būtų pakenkta valstybių narių arba kitų bendrininkų pajėgų operacijų veiksmingumui arba vertingų saugumo ir žvalgybos operacijų veiksmingumui; — būtų iš esmės sumažintas svarbių organizacijų finansinis gyvybingumas; — būtų sutrukdyta tyrimams arba palengvintas sunkių nusikaltimų darymas; — iš esmės būtų veikiama prieš ES arba valstybių narių finansinius, monetarinius, ekonominius ir prekybinius interesus; — būtų rimtai kliudoma esminių ES politikų parengimui arba vykdymui; — nutrauktų arba kitaip iš esmės sugriautų svarbias ES veiklas.	Autoriai nurodo datą arba laiką, kada turinio slaptumo laipsnis gali būti sumažintas arba dokumentas išslaptintas. Kitais atvejais jie peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad garantuotų, jog reikalingas pradinis įslaptinimas [17.3].	ES slaptumo žymos dedamos centre kiekvieno puslapio viršuje ir apačioje, puslapiai numeruojami. Kiekvienas dokumentas turi registracijos numerį ir datą. Visi priedai ir pridedami dokumentai išvardijami dokumento pirmajame puslapyje [21.1].	Dokumentus su slaptumo žyma ►M1 CONFIDENTIEL UE ◄ sunaikina už tokius dokumentus atsakinga registratūra; naikinimą stebi patikimumo pažymėjimą turintis asmuo. Jų sunaikinimas užregistruojamas pagal nacionalines nuostatas, o Komisijos arba ES decentralizuotose agentūrose - pagal ►M2 už saugumą atsakingo Komisijos nario ◄ instrukcijas [22.5].	Dokumentai su slaptumo žyma ►M1 CONFIDENTIEL UE ◄, taip pat ir visos įslaptintos informacijos atliekos, susidariusios rengiant tuos dokumentus, tokios kaip sugadintos kopijos, darbiniai projektai, išspausdintos pastabos ir nuorašams naudotas kalkinis popierius, yra sunaikinami sudeginant, paverčiant minkšta mase, supjaustant arba kitaip susmulkinant, kad jų turinys ar forma negalėtų būti atkurti [22.5].

Slaptumo žyma	Kada	Kas	Žymos dėjimas	Slaptumo žymos laipsnio sumažinimas/išslaptinimas/sunaikinimas	
				Kas	Kada
►M1 RESTREINT UE ◄: Ši žyma suteikiama tai informacijai ir medžiagai, kurios atskleidimas be leidimo gali būti nenaudingas Europos Sąjungos arba vienos ar daugiau jos valstybių narių interesams [16.1].	Tikėtina, kad atskleidus slaptumo žyma ►M1 RESTREINT UE ◄ pažymėtus dalykus, — būtų nepalankiai paveikti diplomatiniai santykiai; — būtų sukelta daug rūpesčių asmenims; — būtų sunkiau palaikyti valstybių narių arba kitų bendrininkų operacijų veiksmingumą arba saugumą; — būtų padaryta finansinių nuostolių asmenims ir verslo įmonėms arba jiems būtų lengviau gauti neteisėtą pelną arba naudą; — būtų sulaužyti rimti susitarimai, kuriais išsaugomas iš trečiųjų šalių gautos informacijos konfidencialumas; — būtų sulaužyti įstatyminiai informacijos atskleidimo apribojimai; — būtų pakenkta tyrimams arba palengvintas nusikaltimų darymas; — ES ir valstybės narės, vesdamos prekybos arba politines derybas su trečiosiomis šalimis, patektų į nepalankią padėtį; — būtų trukdoma kliudoma esminių ES politikų parengimui arba vykdymui; — būtų susilpnintas tinkamas ES ir jos veiklos valdymas.	Įgalioti asmenys (autoriai), generaliniai direktoriai, tarnybų vadovai [17.1]. Autoriai nurodo datą, laiką arba atvejį, kada turinio slaptumo laipsnis gali būti sumažintas arba dokumentas išslaptintas [16.2]. Kitais atvejais jie peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad garantuotų, jog reikalingas pradinis įslaptinimas [17.3].	Slaptumo žyma ►M1 RESTREINT UE ◄, o tam tikrais atvejais apsaugos galiojimo laikotarpį nurodantys ženklai ir (arba) gynybos kvalifikacinė žyma ESGP dedama ant atitinkamos kategorijos dokumentų mechaninėmis priemonėmis arba ranka. [16.4, 16.5, 16.3]. ES slaptumo žymos spausdinamos centre kiekvieno puslapio viršuje ir apačioje, puslapiai numeruojami. Kiekvienas dokumentas turi registracijos numerį ir datą [21.1].	Išslaptinimas yra autoriaus kompetencija. Jis apie išslaptinimą informuoja suinteresuotus adresatus, kuriems yra nusiuntęs dokumentą arba padaręs jo kopiją [17.3]. Dokumentus su slaptumo žyma ►M1 RESTREINT UE ◄ sunaikina už juos atsakinga registratūra arba vartotojas pagal ►M2 už saugumą atsakingo Komisijos nario ◄ instrukcijas [22.5].	Atliekamos kopijos ir nebereikalingi dokumentai yra sunaikinami [22.5].

▼B

3 priedėlis

ES įslaptintos informacijos perdavimo trečiosioms šalims arba tarptautinėms organizacijoms vadovas: 1 lygio bendradarbiavimas

TVARKA

1. Teisė perduoti ES įslaptintą informaciją valstybėms, kurios nėra Europos Sąjungos narės, arba kitoms tarptautinėms organizacijoms, kurių saugumo politika ir nuostatos yra palyginamos su ES politika ir nuostatomis, priklauso Komisijai, kaip kolegialiai institucijai.

2. Kol nėra sudarytas susitarimas dėl saugumo, už saugumą atsakingas Komisijos narys yra kompetentingas nagrinėti prašymus perduoti ES įslaptintą informaciją.

3. Tai darydamas jis:

   — stengiasi gauti perduotinos ESĮI autorių nuomonę,

   — užmezga reikalingus ryšius su tą informaciją gaunančių valstybių arba tarptautinių organizacijų saugumo įstaigomis, kad patikrintų, ar jų saugumo politika ir nuostatos gali užtikrinti, jog perduota įslaptinta informacija būtų saugoma taip, kaip reikalaujama šiose saugumo taisyklėse,

   — stengiasi gauti Komisijos Saugumo politikos patarėjų grupės nuomonę apie informaciją gaunančių valstybių arba tarptautinių organizacijų patikimumą.

4. Už saugumą atsakingas Komisijos narys prašymą ir Komisijos Saugumo politikos patarėjų grupės nuomonę pateikia Komisijai sprendimui priimti.

SAUGUMO PRIEMONĖS, KURIAS TURI TAIKYTI GAVĖJAI

5. Apie Komisijos sprendimą leisti perduoti ES įslaptintą informaciją už saugumą atsakingas Komisijos narys informuoja ją gaunančias valstybes arba tarptautines organizacijas.

6. Sprendimas perduoti įslaptintą informaciją įsigalioja tik po to, kai gavėjai raštu patvirtina, kad jie:

   — nenaudos informacijos jokiems kitiems tikslams, išskyrus tuos, dėl kurių susitarta;

   — saugos informaciją taip, kaip reikalaujama šiose saugumo taisyklėse ir ypač toliau išdėstytose specialiose nuostatose.

7. Personalas

   a) Galimybė naudotis ES įslaptinta informacija yra griežtai ribojama ir pagal „būtina žinoti“ principą suteikiama tik pareigūnams, kurie turi ja naudotis, kad atliktų tarnybines pareigas.

   b) Visi pareigūnai arba atitinkamos valstybės piliečiai, kuriems bus leista naudotis ►M1 CONFIDENTIEL UE ◄ arba aukštesnio slaptumo žymos laipsnio įslaptinta informacija, turi turėti slaptumo žymos laipsnį atitinkamą patikimumo pažymėjimą arba kitą atitinkamą leidimą, išduotus ar suteiktus jų valstybės Vyriausybės.

8. Dokumentų perdavimas

   a) Praktinė dokumentų perdavimo tvarka aptariama susitarime. Kol toks susitarimas bus sudarytas, taikomos 21 skirsnio nuostatos. Susitarime visų pirma nurodomos registratūros, kurioms turi būti siunčiama ES įslaptinta informacija.

▼B

b) Jei į įslaptintą informaciją, kurią Komisija leidžia perduoti, įeina slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėta informacija, ją gaunanti valstybė arba tarptautinė organizacija įsteigia centrinę ES registratūrą, o prireikus – ES subregistratūras. Šios registratūros taiko šių saugumo taisyklių 22 skirsnį tiksliai atitinkančias nuostatas.

9. Registracija

Kai tik registratūra gauna ►M1 CONFIDENTIEL UE ◄ arba aukštesnio slaptumo žymos laipsnio ES įslaptintą informaciją, ji įtraukia dokumentą į specialų šios organizacijos registrą, turintį skiltis, kuriose įrašoma dokumento gavimo data ir informacija apie dokumentą (data, registracijos numeris ir egzemplioriaus numeris), jo slaptumo žyma, pavadinimas, gavėjo pavardė ir pareigos, kvito grąžinimo data ir dokumento grąžinimo ES autoriui arba dokumento sunaikinimo data.

10. Sunaikinimas

a) ES įslaptinti dokumentai sunaikinami pagal šių saugumo taisyklių 22 skirsnyje išdėstytą instrukciją. Įslaptintų dokumentų, pažymėtų slaptumo žymomis ►M1 SECRET UE ◄ ir ►M1 TRES SECRET UE/EU TOP SECRET ◄, sunaikinimo pažymų kopijos nusiunčiamos tuos dokumentus atsiuntusiai ES registratūrai.

b) ES įslaptinti dokumentai įtraukiami į juos gaunančių įstaigų įslaptintų dokumentų naikinimo nenumatytais atvejais planus.

11. Dokumentų apsauga

Imamasi visų priemonių, kad leidimo neturintys asmenys negalėtų pasinaudoti ES įslaptinta informacija.

12. Kopijos, vertimai ir ištraukos

Slaptumo žyma ►M1 CONFIDENTIEL UE ◄ arba ►M1 SECRET UE ◄ pažymėto dokumento kopijos, vertimai ar ištraukos negali būti daromos be atitinkamos saugumo organizacijos vadovo leidimo; šios organizacijos vadovas kopijas, vertimus ar ištraukas patikrina, užregistruoja ir prireikus antspauduoja.

Leidimą kopijuoti arba versti slaptumo žyma ►M1 TRES SECRET UE/EU TOP SECRET ◄ pažymėtą dokumentą suteikia tik jį sukūrusi institucija, kuri nurodo, kiek kopijų leidžiama padaryti; jeigu dokumentą sukūrusios institucijos negalima nustatyti, prašymas perduodamas ►M2 Komisijos Saugumo direktoratui ◄.

13. Saugumo pažeidimai

Kai yra pažeistas ES įslaptinto dokumento saugumas arba įtariama, kad tai padaryta, su sąlyga, kad yra sudarytas susitarimas dėl saugumo, nedelsiant imamasi tokių veiksmų:

a) atliekamas tyrimas, kad būtų nustatytos saugumo pažeidimo aplinkybės;

b) pranešama ►M2 Komisijos Saugumo direktoratui ◄, atitinkamai nacionalinei saugumo institucijai ir dokumentą sukūrusiai institucijai arba aiškiai konstatuojama, kad ši institucija nėra informuota, jei tai nebuvo padaryta;

c) imamasi veiksmų, kad būtų sumažinti saugumo pažeidimo padariniai;

d) apsvarstomos ir įdiegiamos priemonės, kurios užkirstų kelią pakartotiniam pažeidimui;

e) įdiegiamos ►M2 Komisijos Saugumo direktorato ◄ rekomenduotos priemonės, turinčios užkirsti kelią pakartotiniam pažeidimui.

▼B

14. Tikrinimai

Pagal susitarimą su atitinkamomis valstybėmis arba tarptautinėmis organizacijomis ►M2 Komisijos Saugumo direktoratui ◄ leidžiama įvertinti priemonių, turinčių apsaugoti perduotą ES įslaptintą informaciją, veiksmingumą.

15. Atsiskaitymas

Jei yra sudarytas susitarimas dėl saugumo, valstybė arba tarptautinė organizacija tol, kol laiko ES įslaptintą informaciją, kasmet iki tos dienos, kurią buvo išduotas leidimas perduoti informaciją, turi pateikti ataskaitą, patvirtinančią, kad laikomasi šių saugumo taisyklių.

▼B

4 priedėlis

ES įslaptintos informacijos perdavimo trečiosioms šalims arba tarptautinėms organizacijoms vadovas: 2 lygio bendradarbiavimas

TVARKA

1. Teisė perduoti ES įslaptintą informaciją trečiosioms šalims arba tarptautinėms organizacijoms, kurių saugumo politika ir nuostatos gerokai skiriasi nuo ES politikos ir nuostatų, priklauso šios informacijos autoriui. Teisė perduoti Komisijos sukurtą ESĮI priklauso Komisijai kaip kolegialiai institucijai.

2. Iš esmės gali būti perduodama ne aukštesnio kaip ►M1 SECRET UE ◄ laipsnio slaptumo žyma pažymėta informacija. Neperduodama informacija, saugoma specialiomis slaptumo žymos galiojimo žymomis ir kvalifikacinėmis žymomis.

3. Kol nėra sudarytas susitarimas dėl saugumo, už saugumą atsakingas Komisijos narys yra kompetentingas nagrinėti prašymus perduoti ES įslaptintą informaciją.

4. Tai darydamas jis:

   — stengiasi gauti perduotinos ESĮI autorių nuomonę,

   — užmezga reikalingus ryšius su informaciją gaunančių valstybių arba tarptautinių organizacijų saugumo įstaigomis, kad gautų informaciją apie jų saugumo politiką ir nuostatas ir ypač kad sudarytų įslaptintos informacijos slaptumo žymų, taikomų ES ir atitinkamoje valstybėje arba tarptautinėje organizacijoje, palyginamąją lentelę,

   — surengia Komisijos Saugumo politikos patarėjų grupės posėdį arba prireikus supaprastinta rašytine (nutylėjimo) procedūra paprašo valstybių narių nacionalinių saugumo institucijų patikrinti Komisijos Saugumo politikos patarėjų grupės išvadas.

5. Komisijos Saugumo politikos patarėjų grupė pateikia savo nuomonę apie:

   — informaciją gaunančių valstybių arba tarptautinių organizacijų patikimumą, įvertinant saugumo riziką ES arba jos valstybėms narėms,

   — informacijos gavėjų gebėjimo apsaugoti ES perduotą įslaptintą informaciją įvertinimą,

   — pasiūlymus dėl praktinių procedūrų tvarkant ES įslaptintą informaciją (pvz., išbraukyto teksto versijų pateikimas) ir perduotus dokumentus (ES įslaptintos informacijos antraščių, specialių kvalifikacinių žymų palikimas arba panaikinimas ir t. t.),

   — informacijos slaptumo žymos laipsnio sumažinimą arba jos išslaptinimą iki jos perdavimo ją gaunančioms šalims arba tarptautinėms organizacijoms.

6. Už saugumą atsakingas Komisijos narys siunčia prašymą ir Komisijos Saugumo politikos patarėjų grupės nuomonę Komisijai sprendimui priimti.

SAUGUMO TAISYKLĖS, KURIŲ TURI LAIKYTIS GAVĖJAI

7. Už saugumą atsakingas Komisijos narys informuoja informaciją gaunančias valstybes arba tarptautines organizacijas apie Komisijos sprendimą leisti perduoti ES įslaptintą informaciją ir atitinkamus apribojimus.

▼B

8. Sprendimas perduoti įslaptintą informaciją įsigalioja tik po to, kai gavėjai raštu patvirtina, kad jie:

— nenaudos informacijos jokiems kitiems tikslams, išskyrus tuos, dėl kurių susitarta,

— saugos informaciją taip, kaip reikalaujama Komisijos nuostatose.

9. Jei Komisija, gavusi Komisijos Saugumo politikos patarėjų grupės formalią nuomonę, nepatvirtina specialių ES įslaptintų dokumentų tvarkymo procedūrų (slaptumo žymos, kvalifikacinių žymų ir t. t.), taikomos tokios apsaugos taisyklės.

10. Personalas

a) Galimybė naudotis ES įslaptinta informacija yra griežtai ribojama ir pagal „būtina žinoti“ principą suteikiama tik pareigūnams, kurie turi ja naudotis, kad atliktų tarnybines pareigas.

b) Visi pareigūnai arba atitinkamos valstybės piliečiai, kuriems bus leista naudotis Komisijos perduodama įslaptinta informacija, turi turėti nacionalinį patikimumo pažymėjimą arba kitą tinkamą leidimą naudotis atitinkamo ir pagal palyginamąją lentelę lygiaverčio ES žymai slaptumo laipsnio žyma pažymėta informacija.

c) Tie nacionaliniai asmens patikimumo pažymėjimai ir leidimai perduodami susipažinti ►M2 Komisijos Saugumo direktorato direktoriui ◄.

11. Dokumentų perdavimas

Praktinė dokumentų perdavimo tvarka aptariama susitarime. Kol toks susitarimas bus sudarytas, taikomos 21 skirsnio nuostatos. Susitarime visų pirma nurodomos registratūros, kurioms ES įslaptinta informacija turi būti siunčiama, bei nurodomi tikslūs adresai, kur tie dokumentai siunčiami, taip pat ES įslaptintai informacijai perduoti naudojamos kurjerio ir pašto tarnybos.

12. Gautų dokumentų registravimas gavimo vietoje

Adresato valstybės NSI arba ją atitinkanti institucija, savo Vyriausybės vardu priimanti Komisijos persiunčiamą įslaptintą informaciją, arba informaciją gaunančios tarptautinės organizacijos saugumo biuras užveda specialų registrą, kuriame registruoja gautą ES įslaptintą informaciją. Registre yra skiltys, kuriose įrašoma dokumento gavimo data, informacija apie dokumentą (data, registracijos numeris ir kopijos numeris), jo slaptumo žyma, pavadinimas, gavėjo pavardė arba pareigos, kvito grąžinimo data ir dokumento grąžinimo ES arba jo sunaikinimo data.

13. Dokumentų grąžinimas

Gavėjui grąžinant įslaptintą dokumentą Komisijai, laikomasi punkte „Dokumentų perdavimas“ nurodytos tvarkos.

14. Apsauga

a) Nenaudojami dokumentai yra saugomi nacionalinei įslaptintai medžiagai su tokia pat slaptumo žyma saugoti atestuotame apsaugos konteineryje. Ant konteinerio neturi būti nuorodų apie jo turinį, su kuriuo gali susipažinti tik leidimą tvarkyti ES įslaptintą informaciją turintys asmenys. Kai naudojami kombinacijų užraktai, kombinaciją žino tik tie valstybės arba tarptautinės organizacijos pareigūnai, kurie turi leidimus naudotis konteineryje saugoma ES įslaptinta informacija, o kombinacija keičiama kas šešis mėnesius arba dažniau, jei pareigūnas pakeičiamas, panaikinamas nors vieno kombinaciją žinančio pareigūno asmens patikimumo pažymėjimas arba gresia neteisėtas atskleidimas.

▼B

b) ES įslaptintus dokumentus iš apsaugos konteinerių išima tik leidžiantį naudotis ES įslaptinta informacija patikimumo pažymėjimą turinys ir „būtina žinoti“ principą atitinkantys pareigūnai. Kol dokumentai yra jų žinioje, jie atsako už saugią tų dokumentų priežiūrą, o ypač už tai, kad dokumentais nepasinaudotų joks leidimo neturintis asmuo. Jie taip pat užtikrina, kad dokumentai baigus jais naudotis bei po darbo valandų būtų saugomi apsaugos konteineriuose.

c) Be ►M2 Komisijos Saugumo direktorato ◄ leidimo nedaromos dokumento su ►M1 CONFIDENTIEL UE ◄ arba aukštesnio laipsnio slaptumo žyma fotokopijos ir ištraukos.

d) Kartu su ►M2 Komisijos Saugumo direktoratu ◄ nustatoma ir patvirtinama skubaus ir visiško dokumentų sunaikinimo nenumatytais atvejais tvarka.

15. Fizinis saugumas

a) Nenaudojami apsaugos konteineriai, skirti ES įslaptintiems dokumentams saugoti, visą laiką laikomi užrakinti.

b) Jei į kambarį, kuriame laikomi tokie apsaugos konteineriai, turi patekti arba jame turi dirbti remontininkai ar valytojai, juos visą laiką lydi valstybės arba organizacijos saugumo tarnybos narys ar asmuo, kuris atsako už to kambario saugumo priežiūrą.

c) Po įprastinių darbo valandų (naktimis, savaitgaliais ir švenčių dienomis) apsaugos konteinerius, kuriuose laikomi ES įslaptinti dokumentai, saugo arba apsauga, arba automatinė signalizacija.

16. Saugumo pažeidimai

Kai yra pažeistas ES įslaptinto dokumento saugumas arba įtariama, kad tai padaryta, nedelsiant yra imamasi tokių veiksmų:

a) nedelsiant nusiunčiama ataskaita ►M2 Komisijos Saugumo direktoratui ◄ arba valstybės narės, kuri ėmėsi iniciatyvos persiųsti dokumentus, NSI (su kopija ►M2 Komisijos Saugumo direktoratui ◄);

b) atliekamas tyrimas, kurį baigus saugumo įstaigai (žr. a punktą) nusiunčiama išsami ataskaita. Paskui imamasi būtinų priemonių padėčiai ištaisyti.

17. Tikrinimai

Pagal susitarimą su atitinkamomis valstybėmis arba tarptautinėmis organizacijomis ►M2 Komisijos Saugumo direktoratui ◄ leidžiama įvertinti priemonių, turinčių apsaugoti perduotą ES įslaptintą informaciją, veiksmingumą.

18. Atsiskaitymas

Jei yra sudarytas susitarimas dėl saugumo, valstybė arba tarptautinė organizacija tol, kol laiko ES įslaptintą informaciją, kasmet iki tos dienos, kurią buvo išduotas leidimas perduoti informaciją, turi pateikti ataskaitą, patvirtinančią, kad laikomasi šių saugumo taisyklių.

▼B

5 priedėlis

ES įslaptintos informacijos perdavimo trečiosioms šalims arba tarptautinėms organizacijoms vadovas: 3 lygio bendradarbiavimas

TVARKA

1. Kai kada Komisija tam tikromis ypatingomis aplinkybėmis gali pageidauti bendradarbiauti su valstybėmis arba organizacijomis, kurios negali suteikti pagal šias saugumo taisykles reikalaujamų garantijų, bet bendradarbiaujant gali prireikti perduoti ES įslaptintą informaciją.

2. Teisė perduoti ES įslaptintą informaciją trečiosioms šalims arba tarptautinėms organizacijoms, kurių saugumo politika ir nuostatos gerokai skiriasi nuo ES politikos ir nuostatų, priklauso tos informacijos autoriui. Teisė perduoti Komisijos sukurtą ESĮI priklauso Komisijai kaip kolegialiai institucijai.

   Iš esmės gali būti perduodama ne aukštesnio kaip ►**M1** SECRET UE ◄ laipsnio slaptumo žyma pažymėta informacija. Neperduodama informacija, saugoma specialiomis slaptumo žymos galiojimo žymomis ir kvalifikacinėmis žymomis.

3. Komisija apsvarsto įslaptintos informacijos perdavimo tikslingumą, įvertina, ar naudos gavėjui taikytinas „būtina žinoti“ principas, ir nusprendžia, kokio pobūdžio įslaptinta informacija gali būti perduodama.

4. Jei Komisijos sprendimas yra teigiamas, už saugumą atsakingas Komisijos narys:

   — stengiasi gauti perduotinos ESĮI autorių nuomonę,

   — surengia Komisijos Saugumo politikos patarėjų grupės posėdį arba prireikus supaprastinta rašytine (nutylėjimo) procedūra paprašo valstybių narių nacionalinių saugumo institucijų patikrinti Komisijos Saugumo politikos patarėjų grupės išvadas.

5. Komisijos Saugumo politikos patarėjų grupė pateikia savo nuomonę apie:

   a) ES arba valstybėms narėms egzistuojančios saugumo rizikos įvertinimą;

   b) perduotinos informacijos slaptumo žymos laipsnį;

   c) informacijos slaptumo žymos laipsnio sumažinimą arba jos išslaptinimą iki perdavimo;

   d) perduodamų dokumentų tvarkymo procedūrą (žr. 6 punktą);

   e) galimus perdavimo būdus (viešojo pašto paslaugos, viešosios arba saugios telekomunikacijos sistemos, diplomatinis paštas, patikimumo pažymėjimus turintys kurjeriai ir t. t.).

6. Šiame priedėlyje aptariami valstybei arba organizacijoms perduodami dokumentai iš esmės yra parengiami be nuorodos į šaltinį arba ES įslaptintą informaciją. Komisijos Saugumo politikos patarėjų grupė gali rekomenduoti:

   — naudoti specialias kvalifikacines žymas arba kodinius pavadinimus,

   — naudoti specialią įslaptinimo sistemą, susiejančią informacijos slaptumą su kontrolės priemonėmis, reikalingomis atsižvelgiant į gavėjo taikomus dokumentų perdavimo būdus.

▼B

7. ►M2 Už saugumą atsakingas Komisijos narys ◄ pateikia Komisijos Saugumo patarėjų grupės nuomonę Komisijai sprendimui priimti.

8. Komisijai patvirtinus ES įslaptintos informacijos perdavimą ir praktines jo įgyvendinimo procedūras, ►M2 Komisijos Saugumo direktoratas ◄ užmezga reikalingus ryšius su atitinkamos valstybės arba organizacijos saugumo įstaiga, kad padėtų pritaikyti numatytas saugumo priemones.

9. Už saugumą atsakingas Komisijos narys informuoja valstybes nares apie informacijos pobūdį bei slaptumo žymas ir apie organizacijas bei valstybes, kurioms ta informacija Komisijos sprendimu gali būti perduodama.

10. ►M2 Komisijos Saugumo direktoratas ◄ imasi visų reikiamų priemonių, kad padėtų įvertinti būsimą žalą ir iš naujo įvertinti procedūras.

Pasikeitus bendradarbiavimo sąlygoms, Komisija šį klausimą persvarsto.

SAUGUMO TAISYKLĖS, KURIAS TURI TAIKYTI GAVĖJAI

11. Už saugumą atsakingas Komisijos narys informuoja informaciją gaunančias valstybes arba tarptautines organizacijas apie Komisijos sprendimą leisti perduoti ES įslaptintą informaciją bei apie Komisijos Saugumo politikos patarėjų grupės pasiūlytas ir Komisijos patvirtintas išsamias jos apsaugos taisykles.

12. Sprendimas įsigalioja tik po to, kai naudos gavėjai raštu patvirtina, kad jie:

— naudos informaciją tik bendradarbiavimo, dėl kurio yra nusprendusi Komisija, tikslams,

— saugos informaciją taip, kaip reikalauja Komisija.

13. Dokumentų perdavimas

a) Dėl praktinės dokumentų perdavimo tvarkos susitaria ►M2 Komisijos Saugumo direktoratas ◄ ir informaciją gaunančių valstybių arba tarptautinių organizacijų saugumo įstaigos. Jie tiksliai nurodo adresus, kuriais reikia siųsti dokumentus.

b) Dokumentai su ►M1 CONFIDENTIEL UE ◄ ir aukštesnio laipsnio slaptumo žyma perduodami dvigubame voke. Vidinis vokas pažymimas specialiu spaudu arba patvirtintu kodiniu pavadinimu bei šiam dokumentui patvirtinta specialia slaptumo žyma. Kiekvienam įslaptintam dokumentui pridedamas kvitas. Kvite, kuris nežymimas slaptumo žyma, nurodoma tik dokumentui identifikuoti svarbi informacija (registracijos numeris, data, kopijos numeris) ir kalba, kuria jis parašytas, bet ne jo pavadinimas.

c) Vidinis vokas įdedamas į išorinį voką, ant kurio gavėjui nurodomas paketo numeris. Ant išorinio voko slaptumo žyma nenurodoma.

d) Kurjeris visada turi kvitą, kuriame nurodomas paketo numeris.

▼B

14. Gautų dokumentų registravimas

Adresato valstybės NSI arba ją atitinkanti institucija, savo Vyriausybės vardu priimanti Komisijos persiunčiamą įslaptintą informaciją, arba informaciją gaunančios tarptautinės organizacijos saugumo biuras užveda specialų registrą, kuriame registruoja gautą ES įslaptintą informaciją. Registre yra skiltys, kuriose įrašoma dokumento gavimo data, informacija apie dokumentą (data, registracijos numeris ir kopijos numeris), jo slaptumo žyma, pavadinimas, gavėjo pavardė arba pareigos, kvito grąžinimo data ir dokumento grąžinimo ES arba jo sunaikinimo data.

15. Naudojimasis įslaptinta informacija, kuria pasikeičiama, ir jos apsauga

a) Su informacija, pažymėta slaptumo žyma ►M1 SECRET UE ◄, dirba specialiai paskirti pareigūnai, turintys leidimą naudotis tokio slaptumo žymos laipsnio informacija. Ji saugoma kokybiškose apsaugos spintose, kurias gali atidaryti tik pareigūnai, turintys leidimą naudotis jose laikoma informacija. Zonos, kuriose tokios spintos yra, nuolat saugomos, be to, įrengiama tikrinimo sistema, užtikrinanti, kad į jas patektų tik tinkamus leidimus turintys asmenys. Slaptumo žyma ►M1 SECRET UE ◄ pažymėta informacija siunčiama diplomatiniu paštu, per saugaus pašto tarnybas arba saugiomis telekomunikacijos priemonėmis. Slaptumo žyma ►M1 SECRET UE ◄ pažymėtų dokumentų kopijos daromos tik turint to dokumento autoriaus raštišką sutikimą. Visos kopijos registruojamos ir kontroliuojamos. Visoms operacijoms, susijusioms su dokumentais, pažymėtais slaptumo žyma ►M1 SECRET UE ◄, išrašomi kvitai.

b) Slaptumo žyma ►M1 CONFIDENTIEL UE ◄ pažymėtus dokumentus tvarko tinkamai įgalioti susipažinti su atitinkamu klausimu pareigūnai. Dokumentai saugojami saugomose zonose esančiose užrakinamose apsaugos spintose.

Slaptumo žyma ►M1 CONFIDENTIEL UE ◄ pažymėta informacija siunčiama diplomatiniu paštu, per karinę pašto tarnybą ir saugiomis telekomunikacijos priemonėmis. Kopijas daro gaunančioji įstaiga, jų kiekis ir platinimo adresatai įrašomi specialiuose registruose.

c) Su slaptumo žyma ►M1 RESTREINT UE ◄ pažymėta informacija dirbama patalpose, į kurias negali patekti leidimų neturintis personalas; ji saugojama užrakintuose konteineriuose. Dokumentai registruotu paštu dvigubuose vokuose gali būti siunčiami pasinaudojant viešojo pašto paslaugomis, o nenumatytais atvejais operacijų metu – neapsaugotomis viešųjų telekomunikacijų sistemomis. Gavėjai gali daryti jų kopijas.

d) Neįslaptintai informacijai nereikalaujama specialių apsaugos priemonių, ją galima siųsti paštu ir viešųjų telekomunikacijų sistemomis. Gavėjai gali daryti jos kopijas.

16. Naikinimas

Nebereikalingi dokumentai yra naikinami. Dėl ►M1 RESTREINT UE ◄ ir ►M1 CONFIDENTIEL UE ◄ slaptumo žymomis pažymėtų dokumentų specialiuose registruose įrašoma atitinkama pastaba. ►M1 SECRET UE ◄ slaptumo žyma pažymėtiems dokumentams išrašomos naikinimo pažymos, kurias pasirašo du jų sunaikinimą stebintys asmenys.

17. Saugumo pažeidimai

Jei ►M1 CONFIDENTIEL UE ◄ arba ►M1 SECRET UE ◄ slaptumo žymomis pažymėta informacija pasinaudoja leidimo tam neturintys asmenys arba įtariama, kad tai padaryta, valstybės NSI arba organizacijos saugumo vadovas atlieka neteisėto pasinaudojimo informacija aplinkybių tyrimą. Rezultatai pranešami ►M2 Komisijos Saugumo direktoratui ◄. Imamasi veiksmų, reikalingų netinkamoms procedūroms arba saugojimo būdams patobulinti, jei dėl jų buvo neteisėtai pasinaudota informacija.

▼B

6 priedėlis

SANTRUMPOS

ACPC	Patariamasis pirkimų ir kontraktų komitetas (PPKK)
CrA	Šifravimo institucija (ŠI)
CISO	Centrinis informatikos saugumo pareigūnas (CISP)
COMPUSEC	Kompiuterių saugumas (KS)
COMSEC	Ryšių saugumas (RS)
CSO	►M2 Komisijos Saugumo direktoratas ◄ (KSB)
ESDP	Europos saugumo ir gynybos politika (ESGP)
EUCI	Europos Sąjungos įslaptinta informacija (ESĮI)
IA	Infosaugumo institucija (II)
INFOSEC	Informacijos saugumas (INFOSAUGA)
IO	Informacijos savininkas (IS)
ISO	Tarptautinė standartizacijos organizacija (TSO)
IT	Informacinės technologijos (IT)
LISO	Vietos informatikos saugumo pareigūnas (VISP)
LSO	Vietos saugumo pareigūnas (VSP)
MSO	Posėdžių apsaugos pareigūnas (PAP)
NSA	Nacionalinė saugumo institucija (NSI)
PC	Asmeninis kompiuteris (AK)
RCO	Registro kontrolės pareigūnas (RKP)
SAA	Saugumo akreditavimo institucija (SAI)
SecOPS	Saugumo operacijų tvarka (SOT)
SSRS	Sistemai pritaikyta saugumo reikalavimų suvestinė (SSRS)
TA	TEMPEST institucija (TI)
TSO	Techninių sistemų valdytojas (TSV)

▼M3

DSA	paskirtoji saugumo institucija (Designated Security Authority)
FSC	patalpų saugumo patikrinimas (Facility Security Clearance)
FSO	patalpų saugumo pareigūnas (Facility Security Officer)
PSC	personalo patikimumo patikrinimas (Personnel Security Clearance)
SAL	saugumo aspektų paaiškinimas (Security Aspects Letter)
SCG	įslaptinimo vadovas (Security Classification Guide)