II

(Įstatymo galios neturintys teisės aktai)

SPRENDIMAI

TARYBOS SPRENDIMAS

2011 m. kovo 31 d.

dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių

(2011/292/ES)

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 240 straipsnio 3 dalį,

atsižvelgdama į 2009 m. gruodžio 1 d. Tarybos sprendimą 2009/937/ES, patvirtinantį Tarybos darbo tvarkos taisykles [1], ypač į jo 24 straipsnį,

kadangi:

(1) Siekiant plėtoti Tarybos veiklą visose srityse, kuriose reikia tvarkyti įslaptintą informaciją, tikslinga sukurti Tarybą, jos generalinį sekretoriatą ir valstybes nares apimančią įslaptintos informacijos apsaugą užtikrinančią visapusišką saugumo sistemą.

(2) Šis sprendimas turėtų būti taikomas tais atvejais, kai Taryba, jos parengiamieji organai ir Tarybos generalinis sekretoriatas (TGS) tvarko ES įslaptintą informaciją (ESĮI).

(3) Vadovaudamosi savo nacionaliniais įstatymais ir kitais teisės aktais ir tiek, kiek reikia Tarybos veiklai užtikrinti, valstybės narės turėtų laikytis šio sprendimo, kai jų kompetentingos institucijos, personalas ir rangovai tvarko ESĮI, kad visi būtų tikri, jog yra užtikrinta lygiavertė ESĮI apsauga.

(4) Taryba ir Komisija yra įsipareigojusios taikyti lygiaverčius ESĮI apsaugą užtikrinančius saugumo standartus.

(5) Taryba pabrėžia, jog svarbu, kad Europos Parlamentas ir kitos ES institucijos, agentūros, įstaigos ar tarnybos atitinkamais atvejais prisidėtų prie įslaptintos informacijos apsaugos principų, standartų ir taisyklių, būtinų siekiant apsaugoti Sąjungos ir jos valstybių narių interesus, įgyvendinimo.

(6) Pagal Europos Sąjungos sutarties V antraštines dalies 2 skyrių įsteigtos ES agentūros ir įstaigos, Europolas ir Eurojustas vykdydami savo vidaus darbo organizavimą, taiko šiame sprendime nustatytus ESĮI apsaugai užtikrinti skirtus pagrindinius principus ir būtiniausius standartus, kaip numatyta atitinkamuose jų įsteigimo teisės aktuose.

(7) Pagal ES sutarties V antraštinės dalies 2 skyrių vykdomų krizių valdymo operacijų metu taikomos Tarybos patvirtintos ESĮI apsaugai užtikrinti skirtos saugumo taisyklės, jas taiko ir jose dalyvaujantis personalas.

(8) ES specialieji įgaliotiniai ir jų darbuotojų grupių nariai taiko Tarybos patvirtintas ESĮI apsaugai užtikrinti skirtas saugumo taisykles.

(9) Šis sprendimas priimamas nepažeidžiant Sutarties dėl Europos Sąjungos veikimo (SESV) 15 ir 16 straipsnių ir jų įgyvendinamųjų aktų.

(10) Šis sprendimas priimamas nedarant poveikio dabartinei valstybių narių praktikai, susijusiai su nacionalinių parlamentų informavimu apie Sąjungos veiklą,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Tikslas, taikymo sritis ir sąvokų apibrėžtys

1. Šis sprendimas nustato pagrindinius ESĮI apsaugai užtikrinti skirtus saugumo principus ir būtiniausius standartus.

[1] OL L 325, 2009 12 11, p. 35.

2. Šie pagrindiniai saugumo principai ir būtiniausi standartai taikomi Tarybai bei TGS ir jų privalo laikytis valstybės narės, vadovaudamosi savo atitinkamais nacionaliniais įstatymais ir kitais teisės aktais, kad visi būtų tikri, jog yra užtikrinta lygiavertė ESĮI apsauga.

3. Šio sprendimo taikymo tikslais, taikomos A priedėlyje pateiktos sąvokų apibrėžtys.

2 straipsnis

ESĮI sąvokos apibrėžtis, slaptumo žymos ir kitos žymos

1. ES įslaptinta informacija (ESĮI) – bet kuri informacija arba medžiaga, kuriai suteikta ES slaptumo žyma ir kurią neteisėtai atskleidus galėtų būti padaryta tam tikro dydžio žala Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

2. ESĮI žymima viena iš šių slaptumo žymų:

a) TRÉS SECRET UE/EU TOP SECRET: informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti padaryta ypatingai didelė žala Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

b) SECRET UE/EU SECRET: informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti rimtai pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

c) CONFIDENTIEL UE/EU CONFIDENTIAL: informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;

d) RESTREINT UE/EU RESTRICTED: informacija ir medžiaga, kurios neteisėtas atskleidimas galėtų būti nepalankus Europos Sąjungos arba vienos ar kelių valstybių narių interesams.

3. ESĮI žymima slaptumo žyma pagal 2 dalį. Ji gali būti pažymėta papildoma žyma, skirta nurodyti veiklos sritį, su kuria ji yra susijusi, nurodyti įslaptintos informacijos rengėją, apriboti jos platinimą, naudojimą ar suteikimą.

3 straipsnis

Įslaptinimo administravimas

1. Kompetentingos institucijos užtikrina, kad ESĮI būtų žymima tinkama slaptumo žyma, būtų aiškiai nurodoma, kad tai yra įslaptinta informacija, ir jai būtų suteikta slaptumo žyma tik tokiam laikotarpiui, kuris yra būtinas.

2. ESĮI slaptumo žymos laipsnis nesumažinamas arba ji neišslaptinama ir nekeičiamos arba nepanaikinamos 2 straipsnio 3 dalyje nurodytos žymos be išankstinio įslaptintos informacijos rengėjo rašytinio sutikimo.

3. Taryba patvirtina ESĮI rengimo saugumo politiką, kuri apima praktinį žymų vadovą.

4 straipsnis

Įslaptintos informacijos apsauga

1. ESĮI apsaugoma laikantis šio sprendimo.

2. Bet kokios ESĮI turėtojas yra atsakingas už jos apsaugą pagal šį sprendimą.

3. Valstybėms narėms nacionaline slaptumo žyma pažymėtą įslaptintą informaciją įtraukus į Europos Sąjungos struktūras ar tinklus Taryba ir TGS tą informaciją apsaugo laikydamasi reikalavimų, taikomų lygiaverčio slaptumo žymos laipsnio ESĮI, kaip nustatyta B priedėlyje pateiktoje slaptumo žymų atitikmenų lentelėje.

4. Didelio ESĮI kiekio ar ESĮI rinkinio atveju gali būti reikalaujama užtikrinti tokio lygio apsaugą, kuri taikoma aukštesnio laipsnio slaptumo žyma pažymėtai informacijai.

5 straipsnis

Saugumo rizikos valdymas

1. ESĮI kylančios rizikos valdymas yra procesas. Šio proceso tikslas – nustatyti žinomą saugumo riziką, apibrėžti saugumo priemones tokiai rizikai sumažinti iki priimtino lygio pagal šiame sprendime išdėstytus pagrindinius principus ir būtiniausius standartus ir taikyti šias priemones laikantis nuodugnios apsaugos sąvokos, kaip apibrėžta A priedėlyje. Reguliariai atliekamas tokių priemonių efektyvumo vertinimas.

2. ESĮI apsaugai užtikrinti skirtos saugumo priemonės visą savo gyvavimo ciklą turi atitikti jos slaptumo žymos laipsnį, informacijos ar medžiagos formą ir kiekį, patalpų, kuriose laikoma ESĮI, vietos ir konstrukcijos reikalavimus ir turi būti parenkamos atsižvelgiant į vietos lygiu įvertintą piktavališkos ir (arba) nusikalstamos veiklos, įskaitant šnipinėjimą, sabotažą ar terorizmą, keliamą grėsmę.

3. Nenumatytų atvejų planuose turi būti atsižvelgiama į poreikį apsaugoti ESĮI nepaprastosios padėties atvejais siekiant užkirsti kelią galimybei neteisėtai susipažinti su šia informacija, ją atskleisti ar prarasti jos vientisumą arba galimybę ja naudotis.

4. Veiklos tęstinumo planuose numatomos prevencinės ir atstatymo priemonės siekiant sumažinti didelių klaidų ar incidentų poveikį ESĮI administravimui ir saugojimui.

6 straipsnis

Šio sprendimo įgyvendinimas

1. Remdamasi Saugumo komiteto rekomendacija, Taryba prireikus patvirtina saugumo politiką, kuria nustatomos šio sprendimo įgyvendinimo priemonės.

2. Saugumo komitetas savo lygiu gali susitarti dėl saugumo gairių, kurios skirtos papildyti ar sustiprinti šį sprendimą, ir pritarti Tarybos patvirtintai saugumo politikai.

7 straipsnis

Personalo patikimumas

1. Personalo patikimumas – priemonių taikymas, siekiant užtikrinti, kad galimybė susipažinti su ESĮI, būtų suteikta tik asmenims, kurie:

— atitinka principą „būtina žinoti“,

— atitinkamais atvejais turi atitinkamo slaptumo žymos laipsnio asmens patikimumo pažymėjimus, ir

— informuoti apie jų pareigas.

2. Personalo patikimumo tikrinimo procedūrų tikslas – nustatyti, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ESĮI.

3. Prieš TGS dirbantiems asmenims, kuriems dėl jų pareigų gali reikėti susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ESĮI, leidžiant susipažinti su tokia ESĮI, jų visų patikimumas turi būti patikrintas atitinkamu lygiu. Asmens patikimumo pažymėjimo išdavimo tvarka, taikoma TGS pareigūnams ir kitiems tarnautojams, išdėstyta I priede.

4. Prieš 14 straipsnio 3 dalyje nurodytiems valstybių narių darbuotojams, kuriems dėl jų pareigų gali reikėti susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ESĮI, leidžiant susipažinti su tokia ESĮI, jų patikimumas turi būti patikrintas atitinkamu lygiu arba jie turi turėti kitus tinkamus leidimus atsižvelgiant į jų atliekamas funkcijas pagal nacionalinius įstatymus ir kitus teisės aktus.

5. Visi asmenys, prieš jiems suteikiant leidimą susipažinti su ESĮI, o vėliau – reguliariai, informuojami apie pareigą saugoti ESĮI pagal šį sprendimą ir jie ją patvirtina.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos I priede.

8 straipsnis

Fizinis saugumas

1. Fizinis saugumas yra fizinių ir techninių apsaugos priemonių taikymas siekiant užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI.

2. Fizinės saugumo priemonės skirtos sutrukdyti įsibrauti slaptai arba įsiveržti jėga, atgrasyti nuo neteisėtų veiksmų, sutrukdyti jiems bei juos nustatyti, ir sudaryti sąlygas suskirstyti personalą pagal tai, kas gali susipažinti su ESĮI, vadovaujantis principu „būtina žinoti“. Tokios priemonės grindžiamos rizikos valdymo procesu.

3. Fizinio saugumo priemonės taikomos visose patalpose, pastatuose, kabinetuose, salėse ir kitose zonose, kuriose tvarkoma arba saugoma ESĮI, įskaitant zonas, kuriose įrengtos ryšių ir informacinės sistemos, kaip apibrėžta 10 straipsnio 2 dalyje.

4. Zonos, kuriose saugoma CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ESĮI, įrengiamos kaip saugumo zonos pagal II priedo nuostatas ir patvirtinamos kompetentingos saugumo institucijos.

5. CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėtos ESĮI apsaugai naudojama tik patvirtinta įranga ar prietaisai.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos II priede.

9 straipsnis

Įslaptintos informacijos administravimas

1. Įslaptintos informacijos administravimas – administracinių ESĮI kontrolės visą jos gyvavimo ciklą priemonių taikymas siekiant papildyti 7, 8 ir 10 straipsniuose numatytas priemones ir tokiu būdu atgrasyti nuo tokios informacijos sąmoningo ar tikslingo atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius. Tokios priemonės visų pirma yra susijusios su ESĮI rengimu, registravimu, kopijavimu, vertimu, gabenimu ir naikinimu.

2. CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija saugumo tikslais registruojama prieš ją platinant ir ją gavus. TGS kompetentingos tarnybos ir valstybių narių kompetentingos institucijos šiuo tikslu sukuria registratūrų sistemą. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija registruojama tam skirtuose registruose.

3. Tarnybas ir patalpas, kuriose ESĮI tvarkoma arba saugoma, reguliariai tikrina kompetentinga saugumo institucija.

4. Už fiziškai apsaugotų zonų ribų ESĮI iš vienos tarnybos į kitą ir iš vienų patalpų į kitas perduodama šiais būdais:

a) paprastai ESĮI perduodama elektroninėmis priemonėmis apsaugant informaciją pagal 10 straipsnio 6 dalį patvirtintomis šifravimo priemonėmis;

b) kai nenaudojamos a punkte nurodytos priemonės, ESĮI gabenama:

i) elektroninėse laikmenose (pvz., USB atmintinėse, kompaktiniuose diskuose, kietuosiuose diskuose), informaciją apsaugant pagal 10 straipsnio 6 dalį patvirtintomis šifravimo priemonėmis; arba

ii) visais kitais atvejais, kompetentingos saugumo institucijos nurodytu būdu, laikantis atitinkamų III priede nustatytų apsaugos priemonių.

5. Šio straipsnio įgyvendinimo nuostatos išdėstytos III priede.

10 straipsnis

ESĮI, tvarkomos naudojantis ryšių ir informacinėmis sistemomis, apsauga

1. Informacijos saugumo užtikrinimas (ISU) ryšių ir informacinių sistemų srityje – užtikrinimas, kad tokiose sistemose tvarkoma informacija bus apsaugota ir kad, valdant teisėtiems naudotojams, jos veiks taip, kaip turi veikti, ir tada, kada turi veikti. Veiksmingas ISU užtikrina tinkamą konfidencialumo, vientisumo, prieinamumo, atsakomybės už veiksmus prisiėmimo ir autentiškumo lygį. ISU grindžiamas rizikos valdymo procesu.

2. Ryšių ir informacinė sistema – tai sistema, sudaranti sąlygas tvarkyti informaciją elektroniniu būdu. Ryšių ir informacinė sistema apima visas sistemos dalis, kurių reikia jos veikimui, įskaitant infrastruktūrą, organizavimą, personalą ir informacijos šaltinius. Šis sprendimas taikomas ryšių ir informacinėmis sistemoms, kuriose tvarkoma ESĮI (RIS).

3. ESĮI RIS tvarkoma laikantis ISU principo.

4. Visa RIS turi būti akredituojama. Akreditavimo tikslas – įsitikinti, kad įgyvendintos visos atitinkamos saugumo priemonės ir kad pasiektas pakankamas ESĮI ir RIS apsaugos lygis, vadovaujantis šiuo sprendimu. Pareiškime dėl akreditavimo nurodomas aukščiausias informacijos, kuri gali būti tvarkoma RIS, slaptumo žymos laipsnis ir atitinkami reikalavimai bei sąlygos.

5. RIS, kurioje tvarkoma CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, apsaugoma tokiu būdu, kad informacija negalėtų būti neteisėtai atskleista dėl netyčinio elektromagnetinio spinduliavimo (TEMPEST apsaugos priemonės).

6. Kai ESĮI apsauga užtikrinama šifravimo priemonėmis, tokios priemonės patvirtinamos taip:

a) SECRET UE/EU SECRET ir aukštesnio laipsnio slaptumo žyma pažymėtos informacijos konfidencialumas užtikrinamas taikant šifravimo priemones, kurias remdamasi Saugumo komiteto rekomendacija patvirtina Taryba, vykdydama Kriptografijos patvirtinimo institucijos (KPI) funkcijas;

b) CONFIDENTIEL UE/EU CONFIDENTIAL arba RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtos informacijos konfidencialumas užtikrinamas taikant šifravimo priemones, kurias remdamasis Saugumo komiteto rekomendacija patvirtina Tarybos generalinis sekretorius (toliau – generalinis sekretorius), vykdydamas KPI funkcijas.

Nepažeidžiant b punkto, valstybių narių nacionalinėse sistemose CONFIDENTIEL UE/EU CONFIDENTIAL arba RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtos ESĮI konfidencialumas gali būti apsaugomas taikant šifravimo priemones, kurias patvirtina valstybės narės KPI.

7. Perduodant ESĮI elektroninėmis priemonėmis naudojamos patvirtintos šifravimo priemonės. Nepaisant šio reikalavimo, esant nepaprastosios padėties sąlygoms arba specifinių techninių konfigūracijų atvejais, kaip nurodyta IV priede, gali būti taikomos specialios procedūros.

8. TGS kompetentingos tarnybos ir valstybių narių kompetentingos institucijos atitinkamai nustato šias ISU funkcijas vykdančias struktūras:

a) ISU instituciją (ISUI);

b) TEMPEST instituciją (TEI);

c) Kriptografijos patvirtinimo instituciją (KPI);

d) Kriptografijos platinimo instituciją (KPLI).

9. TGS kompetentingos tarnybos ir valstybių narių kompetentingos institucijos kiekvienai sistemai atitinkamai nustato:

a) Saugumo akreditavimo instituciją (SAI);

b) ISU operacinę instituciją.

10. Šio straipsnio įgyvendinimo nuostatos išdėstytos IV priede.

11 straipsnis

Pramoninis saugumas

1. Pramoninis saugumas – priemonių, kurias rangovai arba subrangovai taiko derybų dėl sutarčių sudarymo metu ir visą įslaptintų sutarčių gyvavimo ciklą siekdami užtikrinti ESĮI apsaugą, taikymas. Tokiose sutartyse nenumatoma galimybė susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija.

2. TGS sutartimi gali patikėti pramonės arba kitiems subjektams, registruotiems valstybėje narėje arba trečiojoje valstybėje, kuri yra sudariusi susitarimą arba administracinį susitarimą pagal 12 straipsnio 2 dalies a arba b punktą, užduotis, kurioms atlikti reikia arba reikės susipažinti su ESĮI arba ją tvarkyti ar laikyti.

3. TGS, kaip perkančioji institucija, užtikrina, kad sudarant įslaptintas sutartis su pramonės ar kitais subjektais būtų laikomasi šiame sprendime išdėstytų ir sutartyje nurodytų būtiniausių pramoninio saugumo standartų.

4. Kiekvienos valstybės narės nacionalinė saugumo institucija (NSI), paskirtoji saugumo institucija (PSI) ar bet kuri kita kompetentinga institucija, kiek tai įmanoma pagal nacionalinius įstatymus ir kitus teisės aktus, užtikrina, kad jų teritorijoje įregistruoti rangovai ir subrangovai derybų dėl sutarčių sudarymo metu arba vykdydami įslaptintą sutartį imtųsi visų tinkamų ESĮI apsaugos priemonių.

5. Kiekvienos valstybės narės NSI, PSI ar kita kompetentinga saugumo institucija, laikydamosi nacionalinių įstatymų ir kitų teisės aktų, užtikrina, kad minėtoje valstybėje narėje įregistruoti rangovai ar subrangovai, dalyvaujantys įslaptintose sutartyse arba subrangos sutartyse, pagal kurias jas vykdant arba prieš jas sudarant turi būti suteikta galimybė savo patalpose susipažinti su įslaptinta informacija, pažymėta slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET, turėtų reikiamą slaptumo žymos laipsnį atitinkantį Įmonės patikimumą patvirtinantį pažymėjimą (ĮPPP).

6. Rangovo ar subrangovo darbuotojams, kuriems vykdant įslaptintą sutartį reikia susipažinti su slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija, atitinkama NSI, PSI ar kita kompetentinga saugumo institucija laikydamasi nacionalinių įstatymų ir kitų teisės aktų bei I priede nustatytų būtiniausių saugumo standartų suteikia asmens patikimumo pažymėjimą (APP).

7. Šio straipsnio įgyvendinimo nuostatos išdėstytos V priede.

12 straipsnis

Keitimasis įslaptinta informacija su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

1. Tarybai nusprendus, kad reikia keistis ESĮI su trečiąja valstybe arba tarptautine organizacija, šiuo tikslu nustatoma tinkama tvarka.

2. Siekdama nustatyti tokią tvarką ir apibrėžti abipusiškumo taisykles dėl įslaptintos informacijos, kuria keičiamasi, apsaugos

a) Taryba sudaro susitarimus dėl keitimuisi ESĮI ir jos apsaugai užtikrinti skirtų saugumo procedūrų (toliau – susitarimai dėl informacijos saugumo); arba

b) generalinis sekretorius gali pagal VI priedo 17 punktą sudaryti administracinius susitarimus tuomet, kai ESĮI, kuri turi būti suteikta, slaptumo žymos laipsnis paprastai nėra aukštesnis nei RESTREINT UE/EU RESTRICTED.

3. 2 dalyje nurodytuose susitarimuose dėl informacijos saugumo arba administraciniuose susitarimuose numatomos nuostatos, kuriomis užtikrinama, jog trečiosioms valstybėms arba tarptautinėms organizacijoms gavus ESĮI tai informacijai užtikrinama jos slaptumo žymos laipsnį atitinkanti apsauga, remiantis būtiniausiais standartais, kurie yra ne mažiau griežti nei šiame sprendime nustatyti standartai.

4. Sprendimą suteikti Tarybos parengtą ESĮI trečiajai valstybei arba tarptautinei organizacijai priima Taryba atskirai kiekvienu konkrečiu atveju atsižvelgdama į tokios informacijos pobūdį ir turinį bei gavėjo atitiktį principui „būtina žinoti“ ir įvertinusi naudą ES. Jeigu Taryba nėra įslaptintos informacijos, kurią prašoma suteikti, rengėja, TGS pirmiausia bando gauti jos įslaptintos informacijos rengėjo raštišką sutikimą suteikti tą informaciją. Jei įslaptintos informacijos rengėjo neįmanoma nustatyti, jo pareigą prisiima Taryba.

5. Įvertinimo vizitai rengiami siekiant įsitikinti, kad trečiojoje valstybėje arba tarptautinėje organizacijoje taikomos ESĮI arba įslaptintos informacijos, kuri suteikta ar kuria keičiamasi, apsaugos priemonės yra veiksmingos.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos VI priede.

13 straipsnis

ESĮI saugumo pažeidimai ir neteisėtas atskleidimas

1. Saugumo pažeidimu laikomas šiame sprendime nustatytoms saugumo taisyklėms priešingas asmens veiksmas arba neveikimas.

2. Laikoma, kad ESĮI neteisėtai atskleista, jeigu pažeidus saugumo taisykles ji visa arba jos dalis yra atskleista leidimo neturintiems asmenims.

3. Apie visus saugumo pažeidimus arba įtariamus saugumo pažeidimus nedelsiant pranešama kompetentingai saugumo institucijai.

4. Tai atvejais, kai žinoma arba yra pagrįstų priežasčių manyti, kad ESĮI buvo neteisėtai atskleista arba prarasta, kompetentinga saugumo institucija, vadovaudamasi atitinkamais įstatymais ir kitais teisės aktais, imasi visų atitinkamų priemonių:

a) informuoti įslaptintos informacijos rengėją;

b) užtikrinti, kad siekiant nustatyti faktus tokį atvejį nagrinėtų su pažeidimu tiesiogiai nesusijęs personalas;

c) įvertinti galimą ES ar valstybių narių interesams padarytą žalą;

d) imtis atitinkamų priemonių, kad būtų užkirstas kelias pažeidimui pasikartoti; ir

e) kad atitinkamos institucijos būtų informuotos apie atliktus veiksmus.

5. Bet kuriam asmeniui, kuris pažeidė šiame sprendime nustatytas saugumo taisykles, gali būti taikomos drausminės priemonės vadovaujantis taikomomis taisyklėmis. Asmeniui, kuris neteisėtai atskleidė ar pametė ESĮI, taikomos drausminės ir (arba) teisinės priemonės vadovaujantis taikomais įstatymais, taisyklėmis ir kitais teisės aktais.

14 straipsnis

Atsakomybė už įgyvendinimą

1. Taryba imasi visų priemonių, būtinų siekiant užtikrinti bendrą šio sprendimo taikymo nuoseklumą.

2. Generalinis sekretorius imasi visų priemonių, būtinų užtikrinti, kad TGS pareigūnai ir kiti tarnautojai, į TGS komandiruoti darbuotojai ir TGS samdyti rangovai, tvarkydami arba saugodami ESĮI arba kitą įslaptintą informaciją Tarybos naudojamose patalpose ir TGS, įskaitant trečiosiose valstybėse esančias ryšių palaikymo tarnybas, laikytųsi šio sprendimo.

3. Vadovaudamosi savo atitinkamais nacionaliniais įstatymais ir kitais teisės aktais, valstybės narės imasi visų atitinkamų priemonių siekdamos užtikrinti, kad tvarkydami ar saugodami ESĮI šio sprendimo laikytųsi:

a) valstybių narių nuolatinių atstovybių Europos Sąjungoje darbuotojai ir Tarybos arba jos parengiamųjų organų posėdžiuose ar kitoje Tarybos veikloje dalyvaujantys nacionalinių delegacijų nariai;

b) kiti valstybių narių nacionalinių administracinių įstaigų darbuotojai, įskaitant į tas administracines įstaigas komandiruotus darbuotojus, dirbantys tiek valstybėse narėse, tiek užsienyje;

c) kiti asmenys, kuriems valstybėse narėse dėl jų funkcijų yra suteiktas tinkamas leidimas susipažinti su ESĮI; ir

d) valstybių narių rangovai, dirbantys tiek valstybėse narėse, tiek užsienyje.

15 straipsnis

Saugumo organizavimas Taryboje

1. Atlikdama savo vaidmenį užtikrinti bendrą šio sprendimo taikymo nuoseklumą, Taryba tvirtina:

a) 12 straipsnio 2 dalies a punkte nurodytus susitarimus;

b) sprendimus dėl ESĮI suteikimo trečiosioms valstybėms ir tarptautinėms organizacijoms;

c) metinę tikrinimo programą, kurią siūlo generalinis sekretorius bei rekomenduoja Saugumo komitetas ir kuri yra skirta valstybių narių tarnybų bei patalpų ir ES agentūrų bei įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, taip pat ir Europolo ir Eurojusto tikrinimams ir įvertinimo vizitams į trečiąsias valstybes bei tarptautines organizacijas siekiant įsitikinti priemonių, įgyvendintų siekiant apsaugoti ESĮI, veiksmingumu; ir

d) saugumo politiką, kaip numatyta 6 straipsnio 1 dalyje.

2. Generalinis sekretorius vykdo TGS saugumo tarnybos funkcijas. Vykdydamas tas funkcijas generalinis sekretorius:

a) įgyvendina Tarybos saugumo politiką ir ją nuolat peržiūri;

b) bendradarbiauja su valstybių narių NSI visais su Tarybos veikla susijusiais saugumo klausimais dėl įslaptintos informacijos apsaugos;

c) išduoda ES APP TGS pareigūnams ir kitiems tarnautojams pagal 7 straipsnio 3 dalį, prieš jiems suteikiant leidimą susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija;

d) atitinkamais atvejais nurodo ištirti Tarybos turimos ar parengtos įslaptintos informacijos faktinio ar įtariamo neteisėto atskleidimo arba praradimo atvejus ir prašo atitinkamų saugumo institucijų padėti atlikti šiuos tyrimus;

e) reguliariai tikrina įslaptintos informacijos apsaugai užtikrinti skirtas saugumo priemones TGS patalpose;

f) reguliariai tikrina ESĮI apsaugai užtikrinti skirtas ES agentūrose ir įstaigose, įsteigtose pagal ES sutarties V antraštinės dalies 2 skyrių, Europole ir Eurojuste, taip pat ir pagal ES sutarties V antraštinės dalies 2 skyrių vykdomų krizių valdymo operacijų metu ir ES specialiųjų įgaliotinių (ESSĮ) bei jų darbuotojų grupių narių taikomas saugumo priemones;

g) kartu su atitinkama NSI ir suderinęs su ja reguliariai tikrina ESĮI apsaugai užtikrinti skirtas saugumo priemones valstybių narių tarnybose ir patalpose;

h) derina saugumo priemones su valstybių narių kompetentingomis institucijomis, kurios yra atsakingos už įslaptintos informacijos apsaugą, ir atitinkamai su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis, įskaitant dėl grėsmių ESĮI saugumui pobūdžio ir apsaugos nuo jų priemonių;

i) sudaro administracinius susitarimus, nurodytus 12 straipsnio 2 dalies b punkte; ir

j) rengia pradinį ir reguliarius įvertinimo vizitus į trečiąsias valstybes bei tarptautines organizacijas siekdamas įsitikinti priemonių, įgyvendintų siekiant apsaugoti ESĮI, kuri teikiama arba kuria keičiamasi, veiksmingumu.

TGS saugumo tarnyba padeda generaliniam sekretoriui vykdyti šias užduotis.

3. Įgyvendindamos 14 straipsnio 3 dalį valstybės narės turėtų:

a) paskirti už ESĮI apsaugai užtikrinti skirtas saugumo priemones atsakingą NSI tam, kad:

i) viešosiose ar privačiose nacionalinėse institucijose, įstaigose ar agentūrose, esančiose valstybės teritorijoje arba užsienyje, laikoma ESĮI būtų apsaugota pagal šį sprendimą;

ii) būtų užtikrintas ESĮI apsaugai skirtų saugumo priemonių reguliarus tikrinimas;

iii) dėl jų atliekamų funkcijų visų nacionalinėse administracinėse įstaigose dirbančių asmenų ir rangovo pasamdytų asmenų, kuriems gali būti leista susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, patikimumas būtų tinkamai patikrintas arba jie turėtų kitus tinkamus leidimus pagal nacionalinius įstatymus ir kitus teisės aktus;

iv) siekiant iki minimumo sumažinti ESĮI neteisėto atskleidimo ar praradimo pavojų būtų įdiegtos būtinos saugumo programos;

v) su ESĮI apsauga susijusių saugumo klausimų derinimą su kitomis kompetentingomis nacionalinėmis institucijomis, įskaitant su nurodytąsias šiame sprendime; ir

vi) būtų atsakyta į atitinkamus ES agentūrų ir įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, Europolo ir Eurojusto, taip pat pagal ES sutarties V antraštinės dalies 2 skyrių vykdomų krizių valdymo operacijų personalo bei ESSĮ ir jų darbuotojų grupių narių prašymus išduoti asmens patikimumo pažymėjimus.

NSI yra išvardytos C priedėlyje;

b) užtikrinti, kad jų kompetentingos institucijos vyriausybėms, o per jas Tarybai, teiktų informaciją apie ESĮI saugumui kylančių grėsmių pobūdį ir apsaugos nuo jų priemones bei patarti šiais klausimais.

16 straipsnis

Saugumo komitetas

1. Įsteigiamas Saugumo komitetas. Jis nagrinėja ir vertina saugumo klausimus, kuriems taikomas šis sprendimas, ir atitinkamai teikia rekomendacijas Tarybai.

2. Saugumo komitetą sudaro valstybių narių NSI atstovai, o jo posėdžiuose dalyvauja Komisijos ir Europos išorės veiksmų tarnybos atstovas. Jam pirmininkauja generalinis sekretorius arba jo paskirtas atstovas. Jo posėdžiai rengiami pagal Tarybos nurodymus arba generalinio sekretoriaus ar NSI prašymu.

ES agentūrų ir įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, taip pat ir Europolo ir Eurojusto atstovai gali būti kviečiami dalyvauti posėdžiuose svarstant jiems svarbius klausimus.

3. Saugumo komitetas savo veiklą organizuoja taip, kad galėtų teikti rekomendacijas konkrečių saugumo sričių klausimais. Jis įsteigia ekspertų pogrupį ISU klausimais ir prireikus kitus ekspertų pogrupius. Šis komitetas parengia tokių ekspertų pogrupių įgaliojimus, o šie pogrupiai teikia jam savo veiklos ataskaitas, įskaitant prireikus bet kurias rekomendacijas Tarybai.

17 straipsnis

Ankstesnio sprendimo pakeitimas

1. Šis sprendimas panaikina ir pakeičia 2001 m. kovo 19 d. Tarybos sprendimą 2001/264/EB dėl Tarybos saugumo nuostatų patvirtinimo ([1]).

2. Visa ESĮI, įslaptinta pagal Sprendimą 2001/264/EB, toliau saugoma pagal šio sprendimo atitinkamas nuostatas.

18 straipsnis

Įsigaliojimas

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

Priimta Briuselyje 2011 m. kovo 31 d.

Tarybos vardu

Pirmininkas

VÖLNER P.

([1]) OL L 101, 2001 4 11, p. 1.

PRIEDAI

I PRIEDAS

Personalo patikimumas

II PRIEDAS

Fizinis saugumas

III PRIEDAS

Įslaptintos informacijos administravimas

IV PRIEDAS

RIS tvarkomos ESĮI apsauga

V PRIEDAS

Pramoninis saugumas

VI PRIEDAS

Keitimasis įslaptinta informacija su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

I PRIEDAS

PERSONALO PATIKIMUMAS

I. ĮVADAS

1. Šiame priede nustatytos 7 straipsnio įgyvendinimo nuostatos. Jame nustatomi kriterijai, kuriais remiantis nustatoma, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ESĮI, ir šiuo tikslu taikytinos tikrinimo bei administracinės procedūros.

2. Šiame priede, išskyrus atvejus, kai yra svarbu atskirti, terminas „asmens patikimumo pažymėjimas" reiškia nacionalinį asmens patikimumo pažymėjimą (nacionalinį APP) ir (arba) ES asmens patikimumo pažymėjimą (ES APP), kaip apibrėžta A priedėlyje.

II. LEIDIMAS SUSIPAŽINTI SU ESĮI

3. Asmeniui leidžiama susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ES įslaptinta informacija tik tuo atveju, kai:

   a) nustatoma, kad jis atitinka principą „būtina žinoti";

   b) dėl jo atliekamų funkcijų jam buvo išduotas atitinkamo slaptumo žymos laipsnio APP arba kiti tinkami leidimai pagal nacionalinius įstatymus ir kitus teisės aktus; ir

   c) jis buvo informuotas apie ESĮI apsaugai užtikrinti skirtas saugumo taisykles bei procedūras ir patvirtino savo pareigą saugoti tokią informaciją.

4. Kiekviena valstybė narė ir TGS savo struktūrose nustato tas pareigybes, kurias užimantiems asmenims reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija ir todėl jie turi turėti atitinkamo slaptumo žymos laipsnio APP.

III. ASMENS PATIKIMUMO PAŽYMĖJIMUI TAIKOMI REIKALAVIMAI

5. NSI ir kitos kompetentingos nacionalinės institucijos, gavusios pagal tinkamus įgaliojimus pateiktą prašymą, privalo užtikrinti, kad būtų vykdomas jų piliečių, kuriems turi būti sudaryta galimybė susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, patikimumo tikrinimas. Tikrinimo standartai turi atitikti nacionalinius įstatymus ir kitus teisės aktus.

6. Jeigu atitinkamas asmuo nuolat gyvena kitos valstybės narės ar trečiosios valstybės teritorijoje, kompetentingos nacionalinės institucijos prašo gyvenamosios vietos valstybės kompetentingos institucijos pagalbos laikydamosi nacionalinių įstatymų ir kitų teisės aktų. Valstybės narės padeda viena kitai vykdyti patikimumo tikrinimą pagal nacionalinius įstatymus ir kitus teisės aktus.

7. Jei leidžiama pagal nacionalinius įstatymus ir kitus teisės aktus, NSI arba kitos kompetentingos nacionalinės institucijos gali vykdyti asmenų, kurie nėra jų šalies piliečiai ir kuriems reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, patikimo tikrinimą. Tikrinimo standartai turi atitikti nacionalinius įstatymus ir kitus teisės aktus.

Patikimumo tikrinimo kriterijai

8. Asmens lojalumas ir patikimumas, kad jam būtų galima išduoti APP susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, nustatomas vykdant patikimumo tikrinimą. Kompetentinga nacionalinė institucija atlieka bendrą vertinimą, remdamasi tokio patikimumo tikrinimo išvadomis. Nepalanki išvada nebūtinai reiškia, kad bus atsisakyta išduoti APP. Šiuo tikslu taikomi pagrindiniai kriterijai turėtų apimti, atsižvelgiant į nacionalinius įstatymus ir kitus teisės aktus, nagrinėjimą, ar asmuo:

   a) įvykdė ar bandė, susitarė su kitais asmenimis arba padėjo kitiems asmenims įvykdyti šnipinėjimo, terorizmo, sabotažo, išdavystės ar kurstymo aktą;

   b) yra ar buvo šnipų, teroristų, sabotuotojų ar asmenų, pagrįstai tuo įtariamų, bendrininkas arba yra ar buvo organizacijų ar užsienio valstybių, įskaitant užsienio valstybių žvalgybos tarnybas, kurios gali kelti grėsmę ES ir (arba) valstybių narių saugumui, atstovų bendrininkas, išskyrus atvejus, kai tokiam bendrininkavimui buvo suteiktas leidimas jam vykdant oficialias pareigas;

c) yra ar buvo bet kurios organizacijos, kuri smurtinėmis, ardomosiomis ar kitomis neteisėtomis priemonėmis siekia, *inter alia*, nuversti valstybės narės vyriausybę, pakeisti valstybės narės konstitucinę tvarką arba pakeisti jos valdymo formą ar politiką, narys;

d) yra ar buvo c punkte apibūdintos bet kurios organizacijos rėmėjas arba yra ar buvo glaudžiai susijęs su tokių organizacijų nariais;

e) tyčia nuslėpė, iškreipė ar suklastojo svarbią, ypač susijusią su saugumo aspektais, informaciją arba tyčia melavo pildydamas asmens patikimumo tikrinimo klausimyną ar dalyvaudamas patikimumo tikrinimo pokalbyje;

f) buvo nuteistas už nusikalstamą veiką ar nusikalstamas veikas;

g) piktnaudžiauja alkoholiu, vartoja nelegalius narkotikus ir (arba) piktnaudžiauja legaliomis narkotinėmis medžiagomis;

h) atlieka ar atliko veiksmus, dėl kurių jį galima šantažuoti ar daryti jam spaudimą;

i) savo elgesiu ar žodžiais pasirodė esąs nesąžiningas, nelojalus ar nepatikimas;

j) rimtai ar pakartotinai pažeidė saugumo nuostatus; arba bandė atlikti ar sėkmingai atliko neteisėtus veiksmus, susijusius su ryšių ir informacinėmis sistemomis;

k) gali patirti spaudimą (pvz., dėl vienos ar kelių ne ES pilietybių turėjimo arba dėl giminaičių ar artimų asmenų, kurie galėtų būti pažeidžiami dėl užsienio žvalgybos tarnybų, teroristų grupių ar kitų ardomojo pobūdžio organizacijų ar asmenų, kurių siekiai gali kelti grėsmę ES ir (arba) valstybių narių saugumo interesams, poveikio).

9. Vykdant patikimumo tikrinimą, atitinkamais atvejais, vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, taip pat gali būti svarbi informacija apie asmens finansinę padėtį ir sveikatą.

10. Vykdant patikimumo tikrinimą, atitinkamais atvejais, vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, taip pat gali būti svarbūs sutuoktinio, sugyventinio ar artimo šeimos nario charakteris, elgesys ir gyvenimo aplinkybės.

Susipažinimui su ESĮI taikomi tikrinimo reikalavimai

APP išdavimas pirmą kartą

11. Pradinis APP, leidžiantis susipažinti su slaptumo žymomis CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET pažymėta informacija, grindžiamas patikimumo patikrinimu, apimančiu bent 5 paskutinių metų laikotarpį arba laikotarpį nuo 18 metų amžiaus iki patikrinimo datos, pasirenkant trumpesnį laikotarpį; patikrinimas apima šiuos aspektus:

a) užpildomas nacionalinis asmens patikimumo tikrinimo klausimynas, atsižvelgiant į ESĮI, su kuria asmeniui gali reikėti susipažinti, slaptumo žymos laipsnį; užpildytas klausimynas perduodamas kompetentingai saugumo institucijai;

b) patikrinta asmens tapatybė / pilietybė / nacionalinė priklausomybė – tikrinama asmens gimimo data bei vieta ir jo tapatybė. Nustatoma buvusi ir dabartinė asmens pilietybė / nacionalinė priklausomybė; taip pat įvertinamas bet kuris asmens pažeidžiamumas, susijęs su galimu užsienio subjektų spaudimu, pavyzdžiui, dėl ankstesnės gyvenamosios vietos ar buvusių ryšių atsirandantis pažeidžiamumas; ir

c) patikrinami nacionaliniai ir vietiniai duomenys – tikrinamas nacionalinio saugumo registras ir centrinis nuosprendžių registras, jei tokie egzistuoja, ir (arba) kiti palyginami vyriausybės ir policijos registrai. Tikrinami teisėsaugos įstaigų, kurių teisinei jurisdikcijai priklausė asmens gyvenamoji arba darbo vieta registrai.

12. Pradinis APP, leidžiantis susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija, grindžiamas patikimumo patikrinimu, apimančiu bent dešimt paskutinių metų laikotarpį arba laikotarpį nuo 18 metų amžiaus iki patikrinimo datos, pasirenkant trumpesnį laikotarpį. Jei organizuojami pokalbiai, kaip toliau nurodyta e punkte, patikrinimas apima bent septynių paskutinių metų laikotarpį arba laikotarpį nuo 18 metų amžiaus iki patikrinimo datos, pasirenkant trumpesnį laikotarpį. Patikimumo pažymėjimų, leidžiančių susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija, išdavimui, atsižvelgiant į nacionalinius įstatymus ir kitus teisės aktus, taikomi ne tik pirmiau 8 punkte nurodyti kriterijai, bet ir tikrinami toliau išvardyti aspektai; jie taip pat gali būti tikrinami prieš išduodant asmens patikimumo pažymėjimus, leidžiančius susipažinti su slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija, jei tai privaloma pagal nacionalinius įstatymus ir kitus teisės aktus:

a) finansinė padėtis – renkama informacija apie asmens finansinę padėtį, kad būtų galima įvertinti dėl rimtų finansinių sunkumų galintį atsirasti pažeidžiamumą užsienio ar šalies vidaus subjektų spaudimo atveju arba kad būtų nustatytas nepaaiškinamas turto padidėjimas;

b) išsilavinimas – renkama informacija siekiant sužinoti apie asmens įgytą išsilavinimą mokyklose, universitetuose ir kitose švietimo įstaigose nuo jo aštuonioliktojo gimtadienio ar per kitą, patikimumo tikrinimą atliekančios institucijos manymu, tinkamą laikotarpį;

c) darbovietės – renkama informacija apie dabartinę ir ankstesnes darbovietes, remiantis tokiais šaltiniais kaip darbo charakteristika, veiklos ar efektyvumo ataskaitos, taip pat darbdavių ar viršininkų informacija;

d) karo tarnyba – jei taikoma, tikrinama, ar asmuo tarnavo ginkluotosiose pajėgose ir kokiu būdu buvo išleistas į atsargą; ir

e) pokalbiai – kai tai numatyta ir leidžiama pagal nacionalinę teisę, organizuojamas (-i) pokalbis (-iai) su asmeniu. Į pokalbį taip pat kviečiami kiti asmenys, kurie gali nešališkai įvertinti asmens biografijos faktus, veiklą, lojalumą ir patikimumą. Kai pagal nacionalinę praktiką tikrinamo asmens prašoma pateikti rekomendacijas, turi būti apklausiami rekomendacijas pateikę asmenys, išskyrus atvejus, kai yra pagrįstų priežasčių to nedaryti.

13. Prireikus vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais gali būti atliekami papildomi patikrinimai, kad būtų surinkta visa svarbi informacija apie asmenį ir kad būtų pagrįsta arba paneigta nepalanki informacija.

APP atnaujinimas

14. Po to, kai pirmą kartą išduotas APP ir jeigu asmuo nuolat dirbo nacionalinėje administracinėje įstaigoje ar TGS bei jam nuolat reikia dirbti su ESĮI, APP peržiūrimas siekiant jį atnaujinti ne rečiau kaip kas penkerius metus pažymėjimų, leidžiančių susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija, atveju ir ne rečiau kaip kas dešimt metų pažymėjimų, leidžiančių susipažinti su slaptumo žymomis SECRET UE/EU SECRET ir CONFIDENTIEL UE/EU CONFIDENTIAL pažymėta informacija, atveju, skaičiuojant nuo paskutinio patikimumo patikrinimo, kuriuo remiantis buvo išduotas pažymėjimas, rezultatų pranešimo datos. Visuose dėl APP atnaujinimo atliekamuose patikimumo patikrinimuose tikrinamas laikotarpis nuo ankstesnio tikrinimo datos.

15. Siekiant atnaujinti APP tikrinami 11 ir 12 punktuose apibūdinti aspektai.

16. Prašymai dėl atnaujinimo teikiami laiku, atsižvelgiant į tokiam patikimumo tikrinimui atlikti reikiamą laiką. Tačiau atitinkamai NSI ar kitai kompetentingai nacionalinei institucijai gavus atitinkamą prašymą dėl atnaujinimo ir atitinkamą asmens patikimumo tikrinimo klausimyną nepasibaigus APP galiojimo laikotarpiui ir dar neužbaigus būtino patikimumo patikrinimo, kompetentinga nacionalinė institucija gali pratęsti turimo APP galiojimo laikotarpį ne ilgiau kaip 12 mėnesių, jeigu leidžia nacionaliniai įstatymai ir kiti teisės aktai. Jeigu pasibaigus šiam 12 mėnesių laikotarpiui patikimumo patikrinimas dar nebaigtas, asmeniui skiriamos tokios užduotys, kurioms atlikti nereikia turėti APP.

TGS taikoma APP išdavimo procedūra

17. TGS pareigūnų ir kitų tarnautojų atveju TGS saugumo tarnyba nusiunčia užpildytą asmens patikimumo tikrinimo klausimyną valstybės narės, kurios pilietis asmuo yra, NSI, prašydama atlikti patikimumo patikrinimą, skirtą gauti leidimą naudotis tam tikro slaptumo žymos laipsnio ESĮI, su kuria asmeniui reikės susipažinti.

18. Jei TGS sužino patikimumo patikrinimui svarbios informacijos apie asmenį, kuris pateikė prašymą dėl ES APP, TGS, laikydamasis atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai NSI.

19. Užbaigusi patikimumo patikrinimą atitinkama NSI praneša TGS saugumo tarnybai tokio patikrinimo rezultatus, naudodama Saugumo komiteto nustatytą korespondencijai skirtą standartinę formą.

a) Jei patikimumo tikrinimo rezultatai užtikrinamai rodo, kad neturima jokios nepalankios informacijos, kuri leistų abejoti asmens lojalumu ir patikimumu, TGS paskyrimų tarnyba gali asmeniui išduoti ES APP ir leisti susipažinti su iki tam tikro laipsnio slaptumo žyma pažymėta ESĮI iki nustatytos datos;

b) Jei patikimumo tikrinimo rezultatai nėra tokie užtikrinantys, TGS paskyrimų tarnyba apie tai praneša atitinkamam asmeniui, kuris gali prašyti, kad Paskyrimų tarnyba jį išklausytų. Paskyrimų tarnyba gali prašyti kompetentingos NSI pateikti daugiau paaiškinimų, kuriuos ji gali pateikti pagal savo nacionalinius įstatymus ir kitus teisės aktus. Jei rezultatai pasitvirtina, ES APP neišduodamas.

20. Patikimumo tikrinimui bei gautiems rezultatams taikomi atitinkamoje valstybėje narėje galiojantys įstatymai ir kiti teisės aktai, įskaitant su apskundimu susijusius įstatymus ir kitus teisės aktus. TGS paskyrimų tarnybos sprendimai gali būtų apskųsti pagal Europos Sąjungos pareigūnų tarnybos nuostatus ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygas, nustatytus Reglamente (EEB, Euratomas, EAPB) Nr. 259/68 ([1]) (toliau – Tarnybos nuostatai ir įdarbinimo sąlygos).

21. ES APP galioja visoms užduotims, kurias tas asmuo vykdo TGS ar Europos Komisijoje, su sąlyga, kad tebegalioja jo išdavimą pagrindžiančios aplinkybės.

22. Jeigu asmens tarnyba neprasideda per 12 mėnesių nuo patikimumo patikrinimo rezultatų pranešimo TGS paskyrimų tarnybai arba jeigu asmens tarnyboje daroma 12 mėnesių pertrauka ir tuo laikotarpiu jis nėra priimtas į pareigybę TGS ar valstybės narės nacionalinėje administracinėje įstaigoje, atitinkamos NSI prašoma patvirtinti, kad rezultatai tebegalioja bei yra tinkami.

23. Jei TGS sužino informacijos apie tai, kad galiojantį ES APP turintis asmuo kelia pavojų saugumui, TGS, laikydamasis atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai NSI. Kai NSI informuoja TGS apie tai, kad pagal 19 punkto a papunktį suteiktas užtikrinimas dėl galiojantį ES APP turinčio asmens panaikinamas, TGS paskyrimų tarnyba gali paprašyti pateikti paaiškinimą, kurį NSI gali pateikti pagal nacionalinius įstatymus ir kitus teisės aktus. Jei nepalanki informacija patvirtinama, ES APP panaikinamas, o asmeniui neleidžiama susipažinti su ESĮI ir eiti pareigų, kurias einant jis galėtų susipažinti su ta informacija arba sukelti pavojų saugumui.

24. Apie bet kurį sprendimą panaikinti TGS pareigūno ar kito tarnautojo ES APP ir, atitinkamais atvejais, tokio panaikinimo priežastis pranešama atitinkamam pareigūnui, kuris gali prašyti, kad TGS paskyrimų tarnyba jį išklausytų. NSI teikiamą informaciją reglamentuoja atitinkamoje valstybėje narėje galiojantys įstatymai ir kiti teisės aktai, įskaitant su apeliacijomis susijusius įstatymus ir kitus teisės aktus. TGS paskyrimų tarnybos sprendimai gali būtų apskųsti pagal Tarnybos nuostatus ir įdarbinimo sąlygas.

25. Į TGS komandiruoti nacionaliniai ekspertai, siekiantys eiti pareigas, kurioms reikia ES APP, TGS saugumo tarnybai prieš pradėdami tarnybą pateikia galiojantį nacionalinį APP, leidžiantį susipažinti su ESĮI.

APP registrai

26. Nacionalinių APP ir ES APP, leidžiančių susipažinti su ESĮI, registrus tvarko atitinkamai kiekviena valstybė narė ir TGS. Šiuose registruose bent jau nurodoma ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos laipsnis (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma), APP išdavimo data ir jo galiojimo laikas.

27. Kompetentinga saugumo institucija gali išduoti asmens patikimumo pažymėjimą patvirtinančią pažymą (APPP), kurioje nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos laipsnis (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma), atitinkamo nacionalinio APP, leidžiančio susipažinti su ESĮI, ar ES APP galiojimo laikas ir pačios pažymos galiojimo laikas.

Reikalavimo turėti APP taikymo išimtys

28. Teisė susipažinti su ESĮI asmenims, kuriems dėl jų atliekamų funkcijų suteiktas tinkamas leidimas, valstybėse narėse nustatoma pagal nacionalinius įstatymus ir kitus teisės aktus; tokie asmenys informuojami apie jų saugumo įsipareigojimus ESĮI apsaugos srityje.

IV. ŠVIETIMAS SAUGUMO KLAUSIMAIS IR SAUGUMO SUPRATIMAS

29. Visi asmenys, kuriems išduotas APP, raštu patvirtina, kad jie supranta savo įsipareigojimus saugoti ESSĮ ir padarinius, jei ESĮI būtų neteisėtai atskleista. Atitinkamai valstybė narė ir TGS registruoja tokius rašytinius patvirtinimus.

30. Visi asmenys, kuriems leidžiama susipažinti su ESĮI arba kurie turi dirbti su ESĮI, yra iš pat pradžių informuojami ir paskui reguliariai informuojami apie grėsmes saugumui ir jie turi nedelsdami pranešti atitinkamoms saugumo tarnyboms apie bet kokius bandymus užmegzti kontaktą ar veiklą, kurie, jų nuomone, yra įtartini ar neįprasti.

31. Visi asmenys, kurie nebeeina pareigų, kurias einant jiems reikia susipažinti su ESĮI, yra informuojami apie jų įsipareigojimus toliau saugoti ESĮI slaptumą ir atitinkamais atvejais jie tai patvirtina raštu.

([1]) OL L 56, 1968 3 4, p. 1.

V. IŠSKIRTINĖS APLINKYBĖS

32. Kai leidžia nacionaliniai įstatymai ir kiti teisės aktai, valstybės narės kompetentingos nacionalinės institucijos išduotas asmens patikimumo pažymėjimas, kuriuo leidžiama susipažinti su nacionaliniu lygiu įslaptinta informacija, gali laikinai, kol bus išduotas nacionalinis APP susipažinti su ESĮI, suteikti teisę nacionaliniams pareigūnams susipažinti su ne aukštesne nei lygiaverčio slaptumo žymos laipsnio ESĮI, kaip nustatyta B priedėlyje pateiktoje atitikmenų lentelėje, kai ES interesais būtina suteikti tokią laikiną teisę susipažinti su informacija. NSI informuoja Saugumo komitetą, kai pagal nacionalinius įstatymus ir kitus teisės aktus tokia laikina teisės susipažinti su ESĮI negali būti suteikta.

33. Dėl skubos priežasčių, kurios pagrįstos tarnybos interesais, laukiant išsamaus patikimumo patikrinimo pabaigos, TGS paskyrimų tarnyba, pasikonsultavusi su valstybės narės, kurios pilietis yra atitinkamas asmuo, NSI ir atsižvelgusi į preliminaraus patikrinimo, skirto patikrinti, ar nėra žinomos nepalankios informacijos apie asmenį, rezultatus, gali TGS pareigūnams ir kitiems tarnautojams išduoti laikiną leidimą susipažinti su ESĮI konkrečiai funkcijai atlikti. Tokie laikini leidimai galioja ne ilgiau kaip šešis mėnesius ir nesuteikia teisės susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija. Visi asmenys, kuriems išduotas laikinas leidimas, raštu patvirtina, kad jie supranta savo įsipareigojimus saugoti ESSĮ ir ESĮI neteisėto atskleidimo pasekmes. TGS registruoja tokius rašytinius patvirtinimus.

34. Kai asmuo turi būti paskirtas į pareigybę, kuriai užimti reikalingas vienu laipsniu aukštesnis nei turimas APP, jis gali būti paskirtas į tą pareigybę laikinai, jeigu:

a) asmens vadovas raštu įtikinamai pagrindžia, kad būtina susipažinti su aukštesnio laipsnio ESĮI;

b) suteikiama teisė susipažinti tik su konkrečia ESĮI, kurios reikia užduočiai atlikti;

c) asmeniui išduotas nacionalinis APP arba ES APP tebegalioja;

d) imtasi veiksmų pareigybei reikiamo laipsnio leidimui gauti;

e) kompetentinga institucija atliko pakankamus patikrinimus, kad asmuo nėra rimtai ar pakartotinai pažeidęs saugumo nuostatų;

f) asmens paskyrimą patvirtino kompetentinga institucija; ir

g) išimtys, įskaitant informacijos, su kuria leista susipažinti, aprašymą, registruojamos atsakingame registre ar subregistre.

35. Pirmiau nurodytos procedūros laikomasi, kai reikia suteikti leidimą vieną kartą susipažinti su vienu laipsniu aukštesne slaptumo žyma pažymėta ESĮI nei ta, su kuria susipažinti jiems buvo leista atlikus patikimumo patikrinimą. Tokia procedūra neturi būti naudojama pakartotinai.

36. Itin išskirtinėmis aplinkybėmis, tokiomis kaip vykdant užduotis priešiškoje aplinkoje arba kylant tarptautinei įtampai, kai to reikia imantis neatidėliotinų priemonių, visų pirma siekiant išsaugoti žmonių gyvybes, valstybės narės ir generalinis sekretorius arba generalinio sekretoriaus pavaduotojas gali, kai įmanoma – raštu, suteikti galimybę susipažinti su slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija asmenims, kuriems nėra išduotas reikiamas APP, jeigu tokio leidimo tikrai reikia ir jeigu nėra pagrįstų abejonių dėl atitinkamo asmens lojalumo ir patikimumo. Toks leidimas registruojamas, kartu aprašant informaciją, su kuria leista susipažinti.

37. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtos informacijos atveju toks leidimo suteikimas skubos tvarka taikomas tik tiems asmenims, kuriems buvo leista susipažinti su nacionaline informacija, atitinkančia TRES SECRET UE/EU TOP SECRET slaptumo laipsnį, arba su slaptumo žyma SECRET UE/EU SECRET pažymėta informacija.

38. Saugumo komitetas informuojamas apie atvejus, kai naudojamasi 36 ir 37 punktuose išdėstyta procedūra.

39. Kai valstybės narės nacionaliniai įstatymai ir kiti teisės aktai nustato griežtesnes taisykles dėl laikinų leidimų, laikinų paskyrimų, asmenims susipažinti su įslaptinta informacija vieną kartą ar skubos tvarka leidžiama ir šiame skirsnyje numatytos procedūros taikomos tik nepažeidžiant atitinkamuose įstatymuose ir kituose teisės aktuose nustatytų apribojimų.

40. Saugumo komitetui pateikiama šiame skirsnyje numatytų procedūrų taikymo metinė ataskaita.

VI. DALYVAVIMAS TARYBOJE VYKSTANČIUOSE POSĖDŽIUOSE

41. Vadovaujantis 28 punktu, asmenys, paskirti dalyvauti Tarybos arba Tarybos parengiamųjų organų posėdžiuose, kuriuose aptariama CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, gali tai daryti tik patvirtinus jų APP turėtojo statusą. Deleguotų asmenų APPPP ar kitus asmens patikimumo patikrinimo įrodymus atitinkamos institucijos siunčia TGS saugumo tarnybai arba išimtiniais atvejais ją pateikia atitinkamas deleguotas asmuo. Jei taikoma, gali būti naudojamas suvestinis pavardžių sąrašas, kuriame pateikiami atitinkami įrodymai apie APP.

42. Kai asmens, kuris eidamas savo pareigas turi dalyvauti Tarybos ir Tarybos parengiamųjų organų posėdžiuose, nacionalinis APP susipažinti su ESĮI panaikinamas saugumo sumetimais, kompetentinga institucija apie tai informuoja TGS.

VII. GALIMA PRIEIGA PRIE ESĮI

43. Kai asmenys turi būti įdarbinti tokioje aplinkoje, kurioje jie gali turėti prieigą prie CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėtos informacijos, jų patikimumas turi būti tinkamai patikrintas arba jie turi būti visą laiką lydimi.

44. Kurjerių, apsaugos darbuotojų ir lydinčių asmenų patikimumas turi būti patikrintas atitinkamu lygiu, arba jie turi būti kitaip deramai patikrinti vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, jie yra supažindinami su ESĮI apsaugai užtikrinti skirtomis saugumo procedūromis ir jiems išdėstomos jų pareigos jiems patikėtos tokios informacijos apsaugos srityje.

II PRIEDAS

FIZINIS SAUGUMAS

I. ĮVADAS

1. Šiame priede nustatytos 8 straipsnio įgyvendinimo nuostatos. Jame išdėstyti būtiniausi reikalavimai, taikomi patalpų, pastatų, kabinetų, salių ir kitų zonų, kuriose tvarkoma ir saugoma ESĮI, įskaitant zonas, kuriose yra RIS, fizinei apsaugai.

2. Fizinio saugumo priemonės yra skirtos užkirsti kelią leidimo neturintiems asmenims susipažinti su ESĮI:

   a) užtikrinant, kad ESĮI būtų tinkamai tvarkoma ir saugoma;

   b) sudarant sąlygas suskirstyti personalą pagal tai, kas gali susipažinti su ESĮI, remiantis principu „būtina žinoti“ ir atitinkamais atvejais – personalo narių patikimumo pažymėjimais;

   c) atgrasant nuo neteisėtų veiksmų, sutrukdant jiems bei juos nustatant; ir

   d) sutrukdant asmenims įsibrauti slaptai arba įsiveržti jėga arba juos užlaikant.

II. FIZINIO SAUGUMO REIKALAVIMAI IR PRIEMONĖS

3. Fizinio saugumo priemonės parenkamos remiantis grėsmių įvertinimu, kurį atlieka kompetentingos institucijos. ESĮI apsaugai užtikrinti savo patalpose TGS ir valstybės narės taiko rizikos valdymo procesą, kad užtikrintų, jog, atsižvelgiant į įvertintą riziką, būtų taikoma atitinkamo lygio fizinė apsauga. Rizikos valdymo procese atsižvelgiama į visus svarbius veiksnius, visų pirma:

   a) ESĮI slaptumo žymos laipsnį;

   b) ESĮI formą ir kiekį, atsižvelgiant į tai, kad dideliam ESĮI kiekiui ar rinkiniui apsaugoti gali reikėti taikyti griežtesnes apsaugos priemones;

   c) pastatus ar zonas, kuriose laikoma ESĮI, supančią aplinką ir jų struktūrą; ir

   d) įvertintą žvalgybos tarnybų, kurių veikla nukreipta prieš ES arba jos valstybes nares, keliamą grėsmę ir grėsmę dėl sabotažo, terorizmo, ardomosios arba kitų rūšių nusikalstamos veiklos.

4. Kompetentinga saugumo tarnyba, taikydama nuodugnios apsaugos sąvoką, nustato tinkamas įgyvendintinas fizinio saugumo priemones. Tai gali būti viena (ar daugiau) iš šių priemonių:

   a) perimetro barjeras: fizinis barjeras, kuris skirtas zonos, kurioje reikalinga apsauga, ribos apsaugai užtikrinti;

   b) įsibrovimo aptikimo sistemos (ĮAS): ĮAS gali būti naudojama siekiant padidinti perimetro barjero teikiamo saugumo lygį arba patalpose ir pastatuose vietoj apsaugos personalo ar jam padėti;

   c) patekimo kontrolė: gali būti kontroliuojamas patekimas į objektą, pastatą ar pastatus objekte arba į zonas ar patalpas pastate. Kontrolė gali būti vykdoma elektroninėmis arba elektroninėmis-mechaninėmis priemonėmis, ją gali vykdyti apsaugos personalas ir (arba) priimamojo darbuotojas, arba ji gali būti vykdoma kitomis fizinėmis priemonėmis;

   d) apsaugos personalas: siekiant atgrasyti slaptą įsibrovimą planuojančius asmenis, galima įdarbinti apmokytą ir prižiūrimą apsaugos personalą, *inter alia*, prireikus tinkamai patikrinant jų patikimumą;

   e) apsauginės vaizdo stebėjimo sistemos (AVSS): apsaugos personalas gali naudotis AVSS, kad patikrintų incidentus ir ĮAS pavojaus signalus dideliuose objektuose ar ties perimetru;

   f) apsauginis apšvietimas: apsauginis apšvietimas ne tik skleidžia šviesą, būtiną veiksmingam stebėjimui, kurį tiesiogiai atlieka apsaugos personalas arba kuris netiesiogiai atliekamas per AVSS sistemą, bet jį taip pat galima naudoti siekiant atgrasyti potencialų įsibrovėlį; ir

   g) kitos tinkamos fizinės priemonės, skirtos atgrasyti asmenis be leidimo naudotis ESĮI, nustatyti tokio naudojimo atvejus, arba užkirsti kelią tam, kad ESĮI būtų prarasta ar jai būtų padaryta žala.

5. Kompetentinga institucija gali būti įgaliojama apieškoti įeinančius ir išeinančius asmenis siekiant atgrasyti nuo neleistino medžiagos įnešimo arba neleistino ESĮI išnešimo iš patalpų ar pastatų.

6. Iškilus pavojui, kad ESĮI bus pamatyta, netgi atsitiktinai, imamasi tinkamų priemonių siekiant išvengti šio pavojaus.

7. Naujos infrastruktūros atveju infrastruktūros planavimo ir projektavimo metu apibrėžiami fizinio saugumo reikalavimai ir jos funkcinės specifikacijos. Esamos infrastruktūros atveju kiek įmanoma įgyvendinami fizinio saugumo reikalavimai.

III. ESĮI FIZINEI APSAUGAI SKIRTA ĮRANGA

8. Įsigydama ESĮI fizinei apsaugai užtikrinti skirtą įrangą (pavyzdžiui, apsaugines talpyklas, naikiklius, durų užraktus, elektronines patekimo kontrolės sistemas, įsibrovimo aptikimo sistemas, signalizacijos sistemas), kompetentinga saugumo institucija užtikrina, kad įranga atitiktų patvirtintus techninius standartus ir būtiniausius reikalavimus.

9. ESĮI fizinei apsaugai užtikrinti naudotinos įrangos techninės specifikacijos išdėstomos saugumo gairėse, kurias turi patvirtinti Saugumo komitetas.

10. Saugumo sistemos reguliariai tikrinamos ir reguliariai atliekama įrangos priežiūra. Atliekant priežiūrą atsižvelgiama į patikrinimų rezultatus, kad būtų užtikrinta, jog įrenginiai toliau veiktų optimaliai.

11. Kiekvieno patikrinimo metu iš naujo vertinamas individualių saugumo priemonių ir visos saugumo sistemos veiksmingumas.

IV. FIZIŠKAI APSAUGOTOS ZONOS

12. ESĮI fizinės apsaugos tikslais nustatomos dviejų tipų fiziškai apsaugotos zonos arba nacionalinės lygiavertės zonos:

a) administracinės zonos; ir

b) saugumo zonos (įskaitant techniniu požiūriu saugias saugumo zonas).

Šiame sprendime visos nuorodos į administracines zonas ir saugumo zonas, įskaitant techniniu požiūriu saugias saugumo zonas, laikomos ir nuorodomis į nacionalines lygiavertes zonas.

13. Kompetentinga saugumo institucija nustato, kad zona atitinka reikalavimus, jog būtų klasifikuojama kaip administracinė zona, saugumo zona ar techniniu požiūriu saugi saugumo zona.

14. Administracinių zonų atveju:

a) nustatoma aiškiai apibrėžta išorinė riba, kad būtų galima tikrinti asmenis ir, jei įmanoma, transporto priemones;

b) į šias zonas įeiti nelydimiems leidžiama tik tiems asmenims, kuriems kompetentinga institucija suteikė tinkamą leidimą; ir

c) visi kiti asmenys turi būti visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

15. Saugumo zonų atveju:

a) nustatoma aiškiai apibrėžta ir saugoma išorinė riba, per kurią kiekvienas įėjimas ir išėjimas yra kontroliuojamas naudojantis leidimų arba asmens atpažinimo sistema;

b) į zoną įeiti nelydimiems leidžiama tik tiems asmenims, kurių patikimumas patikrintas ir kurie turi specialų leidimą įeiti į zoną, vadovaujantis principu „būtina žinoti“;

c) visi kiti asmenys turi būti visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

16. Tais atvejais, kai įėjus į saugumo zoną galima visais praktiniais tikslais tiesiogiai susipažinti su joje laikoma įslaptinta informacija, taikomi tokie papildomi reikalavimai:

a) turi būti aiškiai nurodyta paprastai zonoje laikomos informacijos aukščiausio slaptumo žymos laipsnio specifikacija;

b) visi lankytojai privalo turėti specialų leidimą, suteikiantį teisę įeiti į zoną, turi būti visą laiką lydimi ir jų patikimumas turi būti tinkamai patikrintas, nebent imtasi priemonių užtikrinti, kad nebūtų įmanoma susipažinti su ESĮI.

17. Saugumo zonos, kurios turi būti apsaugotos nuo pasiklausymo, klasifikuojamos kaip techniniu požiūriu saugios saugumo zonos. Taikomi šie papildomi reikalavimai:

a) tokiose zonose turi būti įdiegta ĮAS, ir kai jose nedirbama, jos turi būti rakinamos, o kai dirbama – saugomos. Visi raktai apskaitomi ir saugomi vadovaujantis VI skirsniu;

b) visi į tokias zonas įeinantys asmenys ar įnešamos medžiagos turi būti kontroliuojami;

c) tokios zonos reguliariai fiziškai ir (arba) techniškai tikrinamos, kaip reikalauja kompetentinga saugumo institucija. Tokie patikrinimai atliekami, kai į zoną buvo įeita be leidimo ar įtariama apie tokį patekimą; ir

d) tokiose zonose negali būti ryšių linijų, kurioms nesuteiktas leidimas, telefonų, kuriems nesuteiktas leidimas, ar kitų ryšių prietaisų bei elektros ar elektroninės įrangos, kuriems nesuteiktas leidimas.

18. Nepaisant 17 punkto d papunkčio, prieš naudojantis ryšių prietaisais ir elektros ar elektronine įranga zonose, kuriose rengiami susitikimai ar atliekamas darbas, susijęs su SECRET UE/EU SECRET arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, taip pat, kai grėsmė ESĮI vertinama kaip didelė, tokius prietaisus ir įrangą visų pirma ištiria kompetentinga saugumo institucija, siekdama užtikrinti, kad naudojantis šia įranga nebūtų galima perduoti jokios suprantamos informacijos per neapdairumą ar neteisėtai už saugumo zonos perimetro.

19. Saugumo zonos, kuriose nėra visą parą budinčio personalo, atitinkamais atvejais tikrinamos pasibaigus įprastai darbo dienai ir atsitiktiniais intervalais ne įprastomis darbo valandomis, išskyrus atvejus, kai įdiegta ĮAS.

20. Siekiant surengti susitikimą, kuriame naudojama įslaptinta informacija arba bet kokiu kitu panašiu tikslu administracinėje zonoje gali būti laikinai įrengtos saugumo zonos ir techniniu požiūriu saugios saugumo zonos.

21. Saugios eksploatacijos taisyklės rengiamos kiekvienai saugumo zonai ir jose nustatoma:

a) ESĮI, kuri gali būti tvarkoma ir saugoma toje zonoje, slaptumo žymos laipsnis;

b) įdiegtinos stebėjimo ir apsaugos priemonės;

c) kokie asmenys turi leidimą nelydimi patekti į zoną, vadovaujantis principu „būtina žinoti“ ir asmens patikimumo pažymėjimu;

d) atitinkamais atvejais, palydos tvarka ir ESĮI apsaugos tvarka, kai kitiems asmenims leidžiama patekti į zoną;

e) bet kurios kitos atitinkamos priemonės ir procedūros.

22. Saugumo zonose įrengiamos saugyklos. Sienos, grindys, lubos, langai ir durys su užraktais turi būti kompetentingos saugumo institucijos patvirtintos ir užtikrinti apsaugą, kurią užtikrina apsauginės talpyklos, patvirtintos to paties laipsnio slaptumo žymos ESĮI saugoti.

V. FIZINĖS APSAUGOS PRIEMONĖS TVARKANT IR SAUGANT ESĮI

23. Slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėta ESĮI gali būti tvarkoma:

a) saugumo zonose;

b) administracinėse zonose, jeigu ta ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys; arba

c) ne saugumo zonose ar administracinėse zonose, jeigu turėtojas gabena ESĮI pagal III priedo 28–40 punktus ir yra įsipareigojęs taikyti kompensacines priemones, nustatytas kompetentingos saugumo institucijos parengtose saugumo instrukcijose, kad būtų užtikrinta, jog ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys.

24. Slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėta ESĮI saugoma tinkamuose rakinamuose biuro balduose administracinėse zonose arba saugumo zonose. Laikinai ji gali būti saugoma ne saugumo zonose ar administracinėse zonose, jeigu turėtojas yra įsipareigojęs taikyti kompensacines priemones, nustatytas kompetentingos saugumo institucijos parengtose saugumo instrukcijose.

25. Slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta ESĮI gali būti tvarkoma:

a) saugumo zonose;

b) administracinėse zonose, jeigu ta ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys; arba

c) ne saugumo zonose ar administracinėse zonose, jeigu turėtojas:

i) gabena ESĮI pagal III priedo 28–40 punktus;

ii) yra įsipareigojęs taikyti kompensacines priemones, nustatytas kompetentingos saugumo institucijos parengtose saugumo instrukcijose, kad būtų užtikrinta, jog ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;

iii) visą laiką asmeniškai kontroliuoja šią ESĮI; ir

iv) jei dokumentai yra popieriniu pavidalu, apie tai pranešė atitinkamai registratūrai.

26. Slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET pažymėta ESĮI saugoma saugumo zonose esančiose apsauginėse talpyklose arba saugyklose.

27. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta ESĮI tvarkoma saugumo zonose.

28. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta ESĮI saugoma saugumo zonose laikantis kurios nors iš toliau nurodytų sąlygų:

a) apsauginėje talpykloje laikantis 8 punkto reikalavimų, taikant vieną ar kelias iš toliau nurodytų kontrolės priemonių:

i) nuolatinė apsauga arba tikrinimas, kurį vykdo apsaugos personalas arba budintis personalas, kurio patikimumas patikrintas;

ii) patvirtinta ĮAS kartu veikiant reagavimo apsaugos personalui;

arba

b) saugykloje su įrengta ĮAS kartu veikiant reagavimo apsaugos personalui.

29. ESĮI gabenimą už fiziškai apsaugotų zonų ribų reglamentuojančios taisyklės išdėstytos III priede.

VI. ESĮI APSAUGAI UŽTIKRINTI NAUDOJAMŲ RAKTŲ IR KODŲ KONTROLĖ

30. Kompetentinga saugumo institucija nustato kabinetų, patalpų, saugyklų ir apsauginių talpyklų raktų bei kodų valdymo procedūras. Tokios procedūros apsaugo nuo neleistino susipažinimo su informacija.

31. Kodai patikimi kuo mažesniam asmenų skaičiui ir tik tiems asmenims, kuriems reikia juos naudoti; šie asmenys kodus įsimena. Apsauginių talpyklų ir saugyklų, kuriose saugoma ESĮI, kodai keičiami:

a) pasikeitus kodus žinančiam personalui;

b) iškilus pavojui ar įtarimui;

c) po spynos techninio patikrinimo ar remonto; ir

d) bent kas 12 mėnesių.

III PRIEDAS

ĮSLAPTINTOS INFORMACIJOS ADMINISTRAVIMAS

I. ĮVADAS

1. Šiame priede nustatytos 9 straipsnio įgyvendinimo nuostatos. Jame išdėstytos administracinės ESĮI kontrolės visą jos gyvavimo ciklą priemonės siekiant atgrasyti nuo tokios informacijos sąmoningo ar atsitiktinio neteisėto atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius.

II. ĮSLAPTINIMO ADMINISTRAVIMAS

Slaptumo žymos ir kitos žymos

2. Informacija įslaptinama tuo atveju, jei dėl jos konfidencialumo reikia ją apsaugoti.

3. ESĮI rengėjas atsako už slaptumo žymos laipsnio nustatymą pagal atitinkamas įslaptinimo gaires ir už pirminį informacijos platinimą.

4. ESĮI slaptumo žymos laipsnis nustatomas vadovaujantis 2 straipsnio 2 dalimi ir remiantis saugumo politika, kuri turi būti tvirtinama pagal 3 straipsnio 3 dalį.

5. Slaptumo žyma nurodoma aiškiai ir teisingai, neatsižvelgiant į tai, ar ESĮI yra pateikiama popieriuje, žodžiu, elektronine ar bet kuria kita forma.

6. Atskiroms dokumento dalims (t. y. puslapiams, dalims, skirsniams, priedams ir priedėliams) gali būti suteikiamos skirtingos slaptumo žymos ir jos atitinkamai pažymimos, taip pat tais atvejais, kai jos saugomos elektronine forma.

7. Dokumento ar dokumentų bylos bendras slaptumo žymos laipsnis nustatomas pagal aukščiausią slaptumo žymos laipsnį turinčią jo dalį. Kai renkama informacija iš įvairių šaltinių, galutinis dokumentas peržiūrimas siekiant nustatyti jo bendrą slaptumo žymos laipsnį, nes gali paaiškėti, kad jam turi būti suteiktas aukštesnis slaptumo žymos laipsnis nei jo dalims.

8. Kiek įmanoma, dokumentams, kurių dalys pažymėtos skirtingo laipsnio slaptumo žymomis, suteikiama tokia struktūra, kad skirtingo laipsnio slaptumo žymomis pažymėtas dalis būtų galima lengvai nustatyti ir prireikus atskirti.

9. Pridedamų dokumentų lydinčiųjų dokumentų slaptumo žymos laipsnis atitinka priedų aukščiausio laipsnio slaptumo žymas. Jei tokie dokumentai pateikiami atskirai nuo priedų, įslaptintos informacijos rengėjas turi aiškiai nurodyti, koks slaptumo žymos laipsnis jiems suteikiamas, naudodamas atitinkamą žymą, pavyzdžiui:

CONFIDENTIEL UE/EU CONFIDENTIAL

Be priedo (-ų) RESTREINT UE/EU RESTRICTED

Žymos

10. Be vienos iš slaptumo žymų, nurodytų 2 straipsnio 2 dalyje, ESĮI gali būti pažymėta papildomomis žymomis, pavyzdžiui:

a) identifikatoriumi, kuriuo nurodomas įslaptintos informacijos rengėjas;

b) bet kuriais apribojimais, kodiniais žodžiais ar santrumpomis, kuriais nurodoma veiklos sritis, su kuria dokumentas yra susijęs, jo specialus platinimas vadovaujantis principu „būtina žinoti“ arba naudojimo apribojimai;

c) paskirstymo žymomis;

d) jei taikoma, nurodant datą ar konkretų įvykį, po kurio informacijos slaptumo žymos laipsnis gali būti sumažintas arba ji gali būti išslaptinta.

Žymų santrumpos

11. Siekiant nurodyti atskirų teksto pastraipų slaptumo žymos laipsnį, gali būti naudojamos standartinės slaptumo žymų santrumpos. Santrumpos nepakeičia pilnų slaptumo žymų.

12. ES įslaptintuose dokumentuose gali būti naudojamos šios standartinės santrumpos, kuriomis nurodomas skirsnių arba teksto dalių, užimančių mažiau nei vieną puslapį, slaptumo žymos laipsnis:

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

ESĮI rengimas

13. Rengiant ES įslaptintą dokumentą:

a) kiekvienas puslapis aiškiai pažymimas slaptumo žyma;

b) kiekvienas puslapis numeruojamas;

c) dokumente nurodomas jo numeris ir dalykas, kurie nėra įslaptinta informacija, išskyrus tuo atveju, kai jie pažymėti kaip įslaptinta informacija;

d) dokumente nurodoma data;

e) jei platinamos kelios dokumentų, pažymėtų SECRET UE/EU SECRET ir aukštesnio laipsnio slaptumo žyma, kopijos, kiekvienos iš jų kiekviename puslapyje nurodomas kopijos numeris.

14. Kai rengiant ESĮI neįmanoma taikyti 13 punkte išdėstytų reikalavimų, taikomos kitos atitinkamos priemonės vadovaujantis saugumo gairėmis, parengtomis remiantis 6 straipsnio 2 dalimi.

ESĮI slaptumo žymos laipsnio sumažinimas ir ESĮI išslaptinimas

15. Įslaptintos informacijos rengėjas, kai įmanoma, rengdamas ESĮI, ypač RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtą informaciją, nurodo, ar tam tikrą dieną arba po tam tikro įvykio galima sumažinti ESĮI slaptumo žymos laipsnį arba ją išslaptinti.

16. TGS reguliariai peržiūri jo turimą ESĮI, siekdamas įsitikinti, ar slaptumo žymos lygis vis dar taikomas. TGS sukuria sistemą, skirtą peržiūrėti registruotos ESĮI, kurią jis parengė, slaptumo žymos laipsnį ne rečiau kaip kas penkeri metai. Tokia peržiūra nėra reikalinga, jeigu įslaptintos informacijos rengėjas iš pat pradžių nurodo, kad informacijos slaptumo žymos laipsnis bus sumažintas arba informacija išslaptinta automatiškai, o informacija buvo atitinkamai pažymėta.

III. ESĮI REGISTRAVIMAS SAUGUMO TIKSLAIS

17. Kiekviename TGS ir valstybių narių nacionalinių administracinių įstaigų organizaciniame vienete, kuriame tvarkoma ESĮI, steigiamos atsakingos registratūros, siekiant užtikrinti, kad ESĮI būtų administruojama pagal šį sprendimą. Registratūros steigiamos kaip II priede apibrėžtos saugumo zonos.

18. Šiame sprendime registravimas saugumo tikslais (toliau – registravimas) – procedūrų, kuriomis užregistruojamas dokumento gyvavimo ciklas, įskaitant jo platinimą ir sunaikinimą, taikymas.

19. Kai organizacinis vienetas gauna CONFIDENTIEL UE/EU CONFIDENTIAL ir aukštesnio laipsnio slaptumo žyma pažymėtą medžiagą ir kai ją išsiunčia, visa ši medžiaga registruojama tam skirtose registratūrose.

20. Centrinis TGS registratūra registruoja visą įslaptintą informaciją, kurią Taryba ir TGS suteikė trečiosioms valstybėms ir tarptautinėms organizacijoms, bei visą įslaptintą informaciją, gautą iš trečiųjų valstybių ir tarptautinių organizacijų.

21. RIS atveju registravimo procedūros gali būti atliekamos vykdant procesus pačioje RIS.

22. Taryba patvirtina ESĮI registravimo saugumo tikslais saugumo politiką.

TRES SECRET UE/EU TOP SECRET registratūros

23. Valstybėse narėse ir TGS paskiriama registratūra, kuri veikia kaip centrinė slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtą informaciją gaunanti ir siunčianti tarnyba. Prireikus gali būti paskirtos antrinės registratūros, kurios tvarko tokią informaciją jos registravimo tikslais.

24. Tokios antrinės registratūros negali perduoti slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtų dokumentų tiesiogiai kitoms tos pačios centrinės TRES SECRET UE/EU TOP SECRET registratūros antrinėms registratūroms arba į išorę be aiškaus rašytinio tos registratūros leidimo.

IV. ES ĮSLAPTINTŲ DOKUMENTŲ KOPIJAVIMAS IR VERTIMAS

25. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėti dokumentai kopijuojami arba verčiami tik gavus išankstinį rašytinį įslaptintos informacijos rengėjo sutikimą.

26. Jeigu SECRET UE/EU SECRET arba žemesnio laipsnio slaptumo žyma pažymėtų dokumentų įslaptintos informacijos rengėjas nenustatė apribojimų dėl jų kopijavimo ar vertimo, dokumento turėtojo nurodymu tokius dokumentus galima kopijuoti arba versti.

27. Dokumento kopijoms ir vertimams taikomos tos pačios saugumo priemonės, kaip ir dokumento originalui.

V. ESĮI GABENIMAS

28. Gabenant ESĮI taikomos 30–40 punktuose išdėstytos apsaugos priemonės. Kai ESĮI gabenama elektroninėje laikmenoje ir nepaisant 9 straipsnio 4 dalies, toliau išvardytas apsaugos priemones gali papildyti kompetentingos saugumo institucijos nurodytos atitinkamos techninės kontrpriemonės, kad būtų sumažinta rizika, jog informacija bus prarasta ar atskleista.

29. TGS ir valstybių narių kompetentingos saugumo institucijos parengia ESĮI gabenimo instrukcijas remdamosi šiuo sprendimu.

Pastate arba uždaroje pastatų grupėje

30. Pastate arba uždaroje pastatų grupėje gabenama informacija turi būti uždengta, kad nebūtų galima stebėti jos turinio.

31. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija pastate arba uždaroje pastatų grupėje turi būti gabenama apsaugotame voke, ant kurio nurodytas tik gavėjo vardas ir pavardė.

Europos Sąjungoje

32. ESĮI, gabenama iš vieno pastato ar patalpos į kitą Europos Sąjungoje, turi būti supakuota taip, kad ji būtų apsaugota nuo neteisėto atskleidimo.

33. SECRET UE/EU SECRET ir žemesnio laipsnio slaptumo žyma pažymėtą informaciją Europos Sąjungoje gabena:

a) atitinkamai karinis, vyriausybinis ar diplomatinis kurjeris;

b) kurjeris su sąlyga, kad:

i) ESĮI nepaliekama be ją gabenančio asmens priežiūros, išskyrus tuo atveju, kai ji saugoma laikantis II priede nustatytų reikalavimų;

ii) paketas su ESĮI neatidaromas gabenimo metu, o ESĮI neskaitoma viešose vietose;

iii) asmenys informuojami apie jų pareigas, susijusias su saugumu;

iv) prireikus asmenims suteikiamas kurjerio pažymėjimas;

c) pašto tarnybos arba komercinės kurjerių pašto tarnybos su sąlyga, kad:

i) jos yra patvirtintos atitinkamos NSI vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais;

ii) jos taiko atitinkamas apsaugos priemones laikydamosi būtiniausių reikalavimų, kurie turi būti nustatyti saugumo gairėse pagal 6 straipsnio 2 dalį.

Gabenimo iš vienos valstybės narės į kitą atveju c punkto nuostatos taikomos tik gabenant informaciją, pažymėtą slaptumo žyma iki CONFIDENTIEL UE/EU CONFIDENTIAL.

34. CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET slaptumo žyma pažymėtą medžiagą (pavyzdžiui, įrangą ar įrenginius), kurios negalima gabenti 33 punkte nurodytomis priemonėmis, kaip krovinį pagal V priedą gabena komercinės vežėjų bendrovės.

35. TRES SECRET UE/EU TOP SECRET slaptumo žyma pažymėtą informaciją iš vieno pastato ar patalpos į kitą Europos Sąjungoje gabena atitinkamai karinis, vyriausybinis ar diplomatinis kurjeris.

Iš ES į trečiosios valstybės teritoriją

36. ESĮI, gabenama iš ES į trečiosios valstybės teritoriją, turi būti supakuota taip, kad ji būtų apsaugota nuo neteisėto atskleidimo.

37. CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET slaptumo žyma pažymėtą informaciją iš ES į trečiosios valstybės teritoriją gabena:

a) karinis ar diplomatinis kurjeris;

b) kurjeris su sąlyga, kad:

i) ant paketo yra oficialus spaudas arba ESĮI supakuota aiškiai nurodant, kad tai yra oficiali siunta ir jai neturėtų būti taikomas muitinės ar saugumo patikrinimas;

ii) asmenys turi kurjerio pažymėjimą, kuriame nurodytas paketas ir kuris suteikia jiems teisę gabenti paketą;

iii) ESĮI nepaliekama be ją gabenančio asmens priežiūros, išskyrus tuo atveju, kai ji saugoma laikantis II priede nustatytų reikalavimų;

iv) paketas su ESĮI neatidaromas gabenimo metu arba ESĮI neskaitoma viešose vietose; ir

v) asmenys informuojami apie jų pareigas, susijusias su saugumu.

38. Gabenant ES parengtą trečiajai šaliai ar tarptautinei organizacijai skirtą slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET pažymėtą informaciją laikomasi atitinkamų nuostatų, numatytų susitarime dėl informacijos saugumo arba administraciniame susitarime pagal 12 straipsnio 2 dalies a arba b punktus.

39. Slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėtą informaciją taip pat gali gabenti pašto tarnybos ar komercinės kurjerių pašto tarnybos.

40. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtą informaciją iš ES į trečiosios šalies teritoriją gabena karinis ar diplomatinis kurjeris.

VI. ESĮI NAIKINIMAS

41. Nebereikalingi ES įslaptinti dokumentai gali būti sunaikinti nepažeidžiant atitinkamų taisyklių ir nuostatų dėl archyvavimo.

42. Dokumentus, kurie turi būti registruojami pagal 9 straipsnio 2 dalį, turėtojo arba kompetentingos institucijos nurodymu sunaikina atsakinga registratūra. Registracijos knygos ir kita registravimo informacija atitinkamai atnaujinama.

43. Dokumentai, pažymėti SECRET UE/EU SECRET arba TRES SECRET UE/EU TOP SECRET slaptumo žyma, naikinami dalyvaujant liudytojui, kuris turi leidimą susipažinti su ne žemesnio už naikinamo dokumento slaptumo žymos laipsnio įslaptinta informacija.

44. Atsakingas registratūros darbuotojas ir liudytojas, kai pastarojo dalyvavimas privalomas, pasirašo sunaikinimo aktą, kuris registruojamas atitinkamame registre. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtų dokumentų sunaikinimo aktai registre saugomi bent dešimt metų, o CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET slaptumo žyma pažymėtų dokumentų – bent penkerius metus.

45. Įslaptinti dokumentai, įskaitant pažymėtus slaptumo žyma RESTREINT UE/EU RESTRICTED, sunaikinami tokiais būdais, kurie atitinka atitinkamus ES arba lygiaverčius standartus arba kuriuos valstybės narės patvirtino laikydamosi nacionalinių techninių standartų, kad jų nebūtų galima visiškai ar iš dalies atkurti.

46. Kompiuterinių duomenų saugojimo laikmenos, naudotos ESĮI, sunaikinamos vadovaujantis IV priedo 36 punkto nuostatomis.

VII. PATIKRINIMAI IR ĮVERTINIMO VIZITAI

47. Sąvoka „patikrinimas“ toliau vartojama nurodant

a) patikrinimą pagal 9 straipsnio 3 dalį, 15 straipsnio 2 dalies e, f ir g punktus; arba

b) įvertinimo vizitą pagal 12 straipsnio 5 dalį,

kurių metu vertinamas priemonių, įgyvendintų siekiant apsaugoti ESĮI, veiksmingumas.

48. Patikrinimai atliekami, *inter alia*, siekiant:

a) užtikrinti, kad būtų laikomasi šiame sprendime nustatytų būtiniausių ESĮI apsaugos standartų;

b) tikrinamuose subjektuose pabrėžti saugumo ir veiksmingo rizikos valdymo svarbą;

c) rekomenduoti atsakomąsias priemones konkrečiam įslaptintos informacijos konfidencialumo praradimo, jos vientisumo ar prieinamumo netekimo poveikiui sušvelninti; ir

d) sustiprinti saugumo institucijų vykdomas švietimo saugumo klausimais ir sąmoningumo ugdymo programas.

49. Iki kiekvienų kalendorinių metų pabaigos Taryba patvirtina kitų metų tikrinimo programą, kaip numatyta 15 straipsnio 1 dalies c punkte. Faktinės kiekvieno patikrinimo datos nustatomos suderinus su ES agentūra ar įstaiga, valstybe nare, trečiąja valstybe ar atitinkama tarptautine organizacija.

Patikrinimų vykdymas

50. Patikrinimai atliekami siekiant patikrinti tikrinamo subjekto atitinkamas taisykles, reglamentus ir procedūras, taip pat patikrinti, ar subjekto praktika atitinka šiame sprendime nustatytus pagrindinius principus ir būtiniausius standartus ir keitimąsi įslaptinta informacija su tuo subjektu reglamentuojančias nuostatas.

51. Patikrinimai atliekami dviem etapais. Prieš patikrinimą prireikus organizuojamas parengiamasis susitikimas su atitinkamu subjektu. Po šio parengiamojo susitikimo patikrinimo grupė, suderinusi su minėtu subjektu, sudaro išsamią tikrinimo programą, apimančią visas saugumo sritis. Patikrinimo grupei leidžiama patekti į visas vietas, kuriose tvarkoma ESĮI, visų pirma registratūras ir RIS įrengimo vietas.

52. Už valstybių narių nacionalinėse administracinėse įstaigose atliekamus patikrinimus atsako bendra TGS ir Komisijos patikrinimo grupė, visapusiškai bendradarbiaudama su tikrinamo subjekto pareigūnais.

53. Už trečiųjų valstybių ir tarptautinių organizacijų patikrinimus atsako bendra TGS ir Komisijos patikrinimo grupė, visapusiškai bendradarbiaudama su trečiosios valstybės ar tarptautinės organizacijos pareigūnais.

54. ES agentūrų ir įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, taip pat Europolo ir Eurojusto patikrinimus atlieka TGS saugumo tarnyba, padedama NSI, kurios teritorijoje yra įsikūrusi agentūra ar įstaiga, ekspertų. Gali dalyvauti Europos Komisijos saugumo direktoratas (EKSD), jei jis reguliariai keičiasi ESĮI su atitinkama agentūra ar įstaiga.

55. ES agentūrų bei įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, taip pat Europolo ir Eurojusto ir trečiųjų valstybių bei tarptautinių organizacijų patikrinimų atveju NSI ekspertų pagalbos prašoma laikantis išsamios tvarkos, dėl kurios turi susitarti Saugumo komitetas.

Patikrinimo ataskaitos

56. Pabaigus patikrinimą tikrinamam subjektui pateikiamos pagrindinės išvados ir rekomendacijos. Po to parengiama patikrinimo ataskaita, už kurios parengimą atsako TGS saugumo tarnyba. Jei buvo pasiūlyti taisomieji veiksmai ir pateiktos rekomendacijos, ataskaitoje padarytos išvados turėtų būti pakankamai išsamiai pagrįstos. Ataskaita pateikiama atitinkamai patikrinto subjekto tarnybai.

57. Jei patikrinimai atliekami valstybių narių nacionalinėse administracinėse įstaigose:

a) patikrinimo ataskaitos projektas nusiunčiamas atitinkamai NSI, kad ši patikrintų jame pateikiamų faktų teisingumą, taip pat ar jame nėra jokios informacijos, pažymėtos aukštesnio laipsnio nei RESTREINT UE/EU RESTRICTED slaptumo žyma;

b) išskyrus atvejus, kai atitinkamos valstybės narės NSI paprašo, kad patikrinimų ataskaitos nebūtų platinamos, jos išplatinamos Saugumo komiteto nariams ir EKSD; ataskaita įslaptinama pažymint slaptumo žyma RESTREINT UE/EU RESTRICTED;

TGS saugumo tarnyba atsako už tai, kad būtų rengiama reguliari ataskaita, kurioje būtų akcentuojama nurodytu laikotarpiu valstybėse narėse atliktų patikrinimų metu įgyta patirtis ir kurią išnagrinėtų Saugumo komitetas.

58. Trečiųjų valstybių ir tarptautinių organizacijų įvertinimo vizitų atveju ataskaita išplatinama Saugumo komitetui ir EKSD. Ataskaita pažymima ne žemesnio laipsnio nei RESTREINT UE/EU RESTRICTED slaptumo žyma. Taisomieji veiksmai patikrinami kito vizito metu ir apie juos pranešama Saugumo komitetui.

59. ES agentūrų ir įstaigų, įsteigtų pagal ES sutarties V antraštinės dalies 2 skyrių, taip pat Europolo ir Eurojusto patikrinimo vizitų atveju patikrinimo ataskaitos išplatinamos Saugumo komiteto nariams ir EKSD. Patikrinimo ataskaitos projektas nusiunčiamas atitinkamai agentūrai ar įstaigai, kad ši patikrintų jame pateikiamų faktų teisingumą, taip pat ar jame nėra jokios informacijos, pažymėtos aukštesnio laipsnio nei RESTREINT UE/EU RESTRICTED slaptumo žyma. Taisomieji veiksmai patikrinami kito vizito metu ir apie juos pranešama Saugumo komitetui.

60. TGS saugumo tarnyba vykdo reguliarius TGS organizacinių vienetų patikrinimus 48 punkte nustatytais tikslais.

Patikrinimų kontrolinis sąrašas

61. TGS saugumo tarnyba parengia ir atnaujina dalykų, tikrintinų vykdant patikrinimą, saugumo patikrinimo kontrolinį sąrašą. Šis kontrolinis sąrašas pateikiamas Saugumo komitetui.

62. Kontroliniam sąrašui užpildyti būtina informacija gaunama visų pirma patikrinimo metu iš tikrinamo subjekto saugumo valdymo tarnybų. Išsamiai užpildžius kontrolinį sąrašą, susitarus su tikrinamu subjektu, sąrašas įslaptinamas. Jis negali būti patikrinimo ataskaitos sudedamoji dalis.

IV PRIEDAS

RIS TVARKOMOS ESĮI APSAUGA

I. ĮVADAS

1. Šiame priede nustatytos 10 straipsnio įgyvendinimo nuostatos.

2. Toliau išdėstytos ISU savybės ir sąvokos yra būtinos saugumui ir tinkamam RIS operacijų vykdymui užtikrinti:

Autentiškumas:	užtikrinimas, kad informacija yra tikra ir gauta iš *bona fide* šaltinių;
Prieinamumas:	galimybė leidimą turinčiam subjektui pateikus prašymą gauti informaciją ir ja naudotis;
Konfidencialumas:	savybė, kuri reiškia, kad informacija nėra atskleidžiama neturintiems leidimo asmenims, subjektams ar procesams;
Vientisumas:	savybė, kuri reiškia, kad apsaugomas informacijos tikslumas ir išsamumas bei turtas;
Atsakomybės už veiksmus prisiėmimas:	galimybė įrodyti, kad veiksmas buvo atliktas ar įvykis įvyko, kad šio įvykio ar veiksmo po to negalima būtų išsižadėti.

II. INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI

3. Toliau išdėstytos nuostatos yra RIS, kurioje tvarkoma ESĮI, saugumo užtikrinimo pagrindas. Išsamūs šių nuostatų įgyvendinimo reikalavimai nustatyti ISU saugumo politikoje ir saugumo gairėse.

Saugumo rizikos valdymas

4. Saugumo rizikos valdymas yra neatsiejama RIS apibrėžties, kūrimo, veikimo ir priežiūros dalis. Rizikos valdymą (įvertinimą, traktavimą, pripažinimą ir informavimą) kaip kartotinį procesą kartu vykdo sistemos savininkų, projekto institucijų, vykdančiųjų institucijų ir saugumo patvirtinimo institucijų atstovai, taikydami pavirtintą, skaidrų ir visiškai suprantamą rizikos įvertinimo procesą. RIS ir jos turinio taikymo sritis aiškiai apibrėžiama rizikos valdymo proceso pradžioje.

5. Kompetentingos institucijos peržiūri pavojus, kurie gali kilti RIS, ir nuolat vykdo naujausiais duomenimis grindžiamus ir tikslius pavojų įvertinimus, kurie atspindi esamą sistemos operacinę aplinką. Jos nuolat atnaujina savo žinias pažeidžiamumo klausimais ir reguliariai peržiūri pažeidžiamumo įvertinimą, neatsilikdamos nuo informacinių technologijų (IT) aplinkos pokyčių.

6. Tvarkant saugumo riziką siekiama taikyti apsaugos priemonių rinkinį, kuris užtikrina tinkamą vartotojų reikalavimų, sąnaudų ir likutinės rizikos, susijusios su saugumu, pusiausvyrą.

7. RIS akreditavimui taikomi konkretūs reikalavimai, reikalavimai dėl informacijos apimties ir išsamumo, kuriuos nustato atitinkama SAI, turi atitikti įvertintą riziką, atsižvelgiant į visus svarbius veiksnius, įskaitant ESĮI, kuri tvarkoma RIS, slaptumo žymos laipsnį. Akreditavimas apima atsakingos institucijos oficialų pareiškimą dėl likutinės rizikos ir likutinės rizikos pripažinimą.

Saugumas viso RIS gyvavimo ciklo metu

8. Saugumas turi būti užtikrintas viso RIS gyvavimo ciklo metu – nuo pradžios iki naudojimosi pabaigos.

9. Kiekvienu gyvavimo ciklo etapu nustatomas kiekvieno RIS dalyvio ir jo sąveikos su kitais dalyviais vaidmuo saugumo požiūriu.

10. RIS, įskaitant technines ir netechnines saugumo priemones, bandomos saugumo požiūriu akreditavimo proceso metu siekiant užtikrinti tinkamą saugumo užtikrinimo lygį ir patikrinti, ar jos teisingai įdiegtos, integruotos ir sukonfigūruotos.

11. Saugumo įvertinimai, patikrinimai ir peržiūros atliekami reguliariai RIS veikimo ir techninės priežiūros metu bei susidarius išskirtinėms aplinkybėms.

12. RIS saugumo dokumentų atnaujinimas viso jos gyvavimo ciklo metu vykdomas kaip neatsiejama pakeitimų atlikimo ir konfigūracijos tvarkymo proceso dalis.

Geriausios praktikos pavyzdžiai

13. TGS ir valstybės narės bendradarbiauja rengdami geriausios praktikos pavyzdžius RIS tvarkomai ESĮI apsaugoti. Geriausios praktikos gairėse išdėstomos RIS skirtos techninės, fizinės, organizacinės ir procedūrinės saugumo priemonės, kurių veiksmingumas apsisaugant nuo konkrečių grėsmių ir pažeidžiamumo buvo įrodytas.

14. RIS tvarkomos ESĮI apsauga grindžiama ir ES, ir už jos ribų ISU srityje dirbančių subjektų įgyta patirtimi.

15. Geriausios praktikos pavyzdžių platinimu ir jų įgyvendinimu prisidedama prie siekio užtikrinti lygiavertį įvairių TGS ir valstybių narių naudojamų RIS, kuriose tvarkoma ESĮI, saugumo užtikrinimo lygį.

Nuodugni apsauga

16. Siekiant sušvelninti pavojų RIS, įgyvendinama daug techninių ir netechninių saugumo priemonių, kurios grupuojamos kaip kelios gynybinės linijos. Jos apima:

a) *atgrasymą:* saugumo priemones, skirtas įtikinti nerengti priešiškų planų pulti RIS;

b) *prevenciją:* saugumo priemones, skirtas apsunkinti RIS puolimą arba jam sutrukdyti;

c) *aptikimą:* saugumo priemones, skirtas aptikti RIS puolimo atvejį;

d) *atsparumą:* saugumo priemones, skirtas apriboti puolimo poveikį iki mažiausio informacijos rinkinio ar RIS dalių grupės bei užkirsti kelią tolesnei žalai; ir

e) *atstatymą:* saugumo priemones, skirtas RIS saugiai padėčiai atkurti.

Tokių saugumo priemonių griežtumo lygis nustatomas atsižvelgiant į rizikos įvertinimą.

17. Kompetentingos institucijos užtikrina savo gebėjimus reaguoti į incidentus, kurie gali apimti kelias organizacijas ar valstybes, kad galėtų derinti reagavimo veiksmus ir dalytis informacija apie šiuos incidentus bei susijusią riziką (kompiuterinių incidentų tyrimo gebėjimai).

Minimalumo ir mažiausių privilegijų principas

18. Įdiegiamos tik atsižvelgiant į operacinius reikalavimus būtinos funkcijos, prietaisai ir paslaugos siekiant išvengti bereikalingos rizikos.

19. RIS naudotojams ir automatizuotiems procesams suteikiama tik tokia prieiga, privilegijos ar leidimai, kokios jiems reikia savo užduotims atlikti siekiant apriboti žalą, kuri padaroma dėl avarijų, klaidų ar RIS išteklių naudojimo be leidimo.

20. RIS atliekamos registravimo procedūros prireikus patikrinamos akreditavimo proceso metu.

Informuotumas informacijos saugumo užtikrinimo srityje

21. Informuotumas apie riziką ir turimas saugumo priemones yra pirmoji RIS saugumo gynybos linija. Visų pirma visi personalo nariai, susiję su RIS gyvavimo ciklu, įskaitant naudotojus, suvokia:

a) kad saugumo spragos gali labai pakenkti RIS;

b) galimą žalą kitiems, kuri gali kilti dėl tarpusavio sujungimo ir tarpusavio priklausomybės; ir

c) savo asmeninę atsakomybę ir atsakingumą už RIS saugumą atsižvelgdami į savo vaidmenį naudojant sistemas ir procesus.

22. Siekiant užtikrinti, kad būtų suvokiama atsakomybė už saugumą visam dalyvaujančiam personalui, įskaitant aukštesniąją vadovybę ir RIS naudotojus, yra privalomi ISU švietimo ir informuotumo mokymai.

IT saugumo priemonių vertinimas ir patvirtinimas

23. Reikiamas saugumo priemonių patikimumo lygis, apibrėžiamas kaip saugumo užtikrinimo lygis, nustatomas remiantis rizikos valdymo proceso rezultatais ir laikantis atitinkamos saugumo politikos bei saugumo gairių.

24. Saugumo užtikrinimo lygis patikrinamas naudojant tarptautiniu arba nacionaliniu lygiu patvirtintus procesus ir metodus. Tai apima pirminį įvertinimą, kontrolę ir auditą.

25. ESĮI apsaugai skirtas šifravimo priemones įvertina ir patvirtina valstybės narės nacionalinė KPI.

26. Prieš rekomenduojant, kad pagal 10 straipsnio 6 dalį jas pavirtintų Taryba arba generalinis sekretorius, tokias šifravimo priemones turi būti įvertinusi antra šalis, t. y. valstybės narės Tinkamos kvalifikacijos institucija (TKI), kuri nesusijusi su įrangos projektavimu arba gamyba. Reikalaujamas antros šalies įvertinimo išsamumo lygis priklauso nuo numatomo didžiausio ESĮI, kuri bus apsaugoma šiomis priemonėmis, slaptumo žymos laipsnio. Taryba patvirtina šifravimo priemonių vertinimo ir patvirtinimo saugumo politiką.

27. Atitinkamai Taryba arba generalinis sekretorius, remdamiesi Saugumo komiteto rekomendacija, gali netaikyti 25 arba 26 punkte nustatytų reikalavimų ir tam tikram laikotarpiui suteikti laikiną patvirtinimą laikydamiesi 10 straipsnio 6 dalyje nustatytos tvarkos, kai tai pateisinama dėl konkrečių su veikla susijusių priežasčių.

28. TKI yra valstybės narės KPI, kuri buvo akredituota remiantis Tarybos nustatytais kriterijais antram ESĮI apsaugai skirtų šifravimo priemonių įvertinimui atlikti.

29. Taryba patvirtina ne šifravimo IT saugumo priemonių reikalavimų atitikimo ir patvirtinimo saugumo politiką.

Perdavimas saugumo zonose

30. Nepaisant šio sprendimo nuostatų, kai ESĮI perdavimas vykdomas saugumo zonose, remiantis rizikos valdymo proceso rezultatais ir SAI pritarus gali būti naudojamas nešifruotas platinimas arba šifravimas žemesniu lygiu.

Saugus RIS tarpusavio sujungimas

31. Šiame sprendime sistemų tarpusavio sujungimas reiškia tiesioginį dviejų ar daugiau IT sistemų sujungimą siekiant dalytis duomenimis ir kitais informacijos šaltiniais (pavyzdžiui, ryšiais) vienakrypčiu arba daugiakrypčiu būdu.

32. RIS kiekviena tarpusavyje sujungta IT sistema pirmiausia yra traktuojama kaip nepatikima ir sistemoje įdiegiamos apsaugos priemonės keitimuisi įslaptinta informacija kontroliuoti.

33. Bet kokio RIS ir kitos IT sistemos tarpusavio sujungimo atveju laikomasi toliau išdėstytų pagrindinių reikalavimų:

a) tokiems tarpusavio sujungimams taikomus veiklos arba operacinius reikalavimus nurodo ir patvirtina atsakingos institucijos;

b) tarpusavio sujungimui taikomas rizikos valdymas ir akreditavimo procesas bei yra reikalingas kompetentingų SAI pavirtinimas; ir

c) ribų apsaugos priemonės (RAP) įdiegiamos visų RIS perimetre.

34. Akredituota RIS ir neapsaugotas arba viešas tinklas negali būti tarpusavyje sujungiami, išskyrus atvejus, kai tarp RIS ir neapsaugoto arba viešo tinklo yra šiuo tikslu įdiegtos patvirtintos ribų apsaugos priemonės. Tokiems tarpusavio sujungimams taikytinas saugumo priemones peržiūri kompetentinga ISUI ir patvirtina kompetentinga SAI.

Kai duomenys, perduodami neapsaugotu arba viešu tinklu, yra užšifruojami pagal 10 straipsnį patvirtinta šifravimo priemone, toks sujungimas nelaikomas tarpusavio sujungimu.

35. Draudžiamas tiesioginis arba pakopinis RIS, akredituotos tvarkyti slaptumo žyma TRES SECFRET UE/EU TOP SECRET pažymėtą informaciją, ir neapsaugoto arba viešo tinklo tarpusavio sujungimas.

Kompiuterinių duomenų saugojimo laikmenos

36. Kompiuterinių duomenų saugojimo laikmenos sunaikinamos laikantis kompetentingos saugumo institucijos patvirtintų procedūrų.

37. Kompiuterinių duomenų saugojimo laikmenos gali būti naudojamos pakartotinai, gali būti sumažintas jų slaptumo žymos laipsnis arba jos gali būti išslaptinamos laikantis saugumo politikos, kuri turi būti nustatyta pagal 6 straipsnio 1 dalį.

Nepaprastosios padėties sąlygos

38. Nepaisant šio sprendimo nuostatų, toliau apibūdintos specialios procedūros gali būti taikomos esant nepaprastajai padėčiai, pavyzdžiui, gresiant ar esant krizei, konfliktui ar karinei padėčiai arba susidarius išskirtinėms su eksploatavimu susijusioms sąlygoms.

39. ESĮI gali būti perduodama naudojant šifravimo priemones, kurios buvo patvirtintos žemesnio įslaptinimo laipsnio informacijai, arba nešifruota kompetentingai institucijai pritarus, jei vėlavimas padarytų aiškiai didesnę žalą, negu įslaptintos medžiagos atskleidimas, ir jei:

a) siuntėjas ir gavėjas neturi reikiamos šifravimo įrangos arba jokios šifravimo įrangos; ir

b) įslaptinta medžiaga negali būti laiku perduota kitomis priemonėmis.

40. 38 punkte išdėstytomis aplinkybėmis perduodama įslaptinta informacija nėra pažymėta jokiomis žymomis arba nuorodomis, kurios sudarytų sąlygas ją atskirti nuo neįslaptintos informacijos arba kurią galima apsaugoti naudojant turimas šifravimo priemones. Gavėjams kitomis priemonėmis nedelsiant pranešama apie informacijos slaptumo laipsnį.

41. Jeigu taikomas 38 punktas, kompetentingai institucijai ir Saugumo komitetui vėliau pateikiama ataskaita.

III. SU INFORMACIJOS SAUGUMO UŽTIKRINIMU SUSIJUSIOS FUNKCIJOS IR INSTITUCIJOS

42. Valstybėse narėse ir TGS nustatomos toliau išdėstytos su informacijos saugumo užtikrinimu susijusios funkcijos. Šioms funkcijoms nereikalingas vienas bendras organizacinis subjektas. Joms suteikiami atskiri įgaliojimai. Tačiau šios funkcijos ir su jomis susijusi atsakomybė gali būti sujungtos arba integruotos viename organizaciniame vienete arba padalytos skirtingiems organizaciniams vienetams, jei išvengiama vidaus interesų arba užduočių konfliktų.

Informacijos saugumo užtikrinimo institucija

43. ISUI atsako už šias sritis:

a) ISU srities saugumo politikos formavimą ir saugumo gairių rengimą bei jų veiksmingumo bei tinkamumo stebėseną;

b) su šifravimo priemonėmis susijusios techninės informacijos apsaugą ir administravimą;

c) užtikrinimą, kad ESĮI apsaugai parinktos ISU priemonės atitiktų atitinkamą jų tinkamumo nustatymo ir atrankos politiką;

d) užtikrinimą, kad šifravimo priemonės būtų pasirenkamos laikantis jų tinkamumo nustatymo ir atrankos politikos;

e) mokymo ir informuotumo ISU srityje derinimą;

f) konsultavimąsi su sistemos tiekėju, saugumo srities subjektais ir vartotojų atstovais ISU saugumo politikos ir saugumo gairių klausimais; ir

g) užtikrinimą, kad Saugumo komiteto ISU klausimais ekspertų pogrupis turėtų atitinkamas žinias.

TEI

44. TEI užtikrina, kad RIS atitiktų TEMPEST politiką ir gaires. Ji patvirtina TEMPEST kontrpriemones, skirtas įrenginiams ir priemonėms, siekiant apsaugoti ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje.

Kriptografijos patvirtinimo institucija

45. Kriptografijos patvirtinimo institucijos (KPI) pareiga – užtikrinti, kad šifravimo priemonės atitiktų nacionalinę šifravimo politiką arba Tarybos šifravimo politiką. Ji suteikia leidimą naudoti šifravimo priemonę siekiant apsaugoti ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje. Valstybėse narėse KPI papildomai atsako už šifravimo priemonių įvertinimą.

Kriptografijos platinimo institucija

46. Kriptografijos platinimo institucija (KPI) atsako už šias sritis:

a) ES šifravimo medžiagos valdymą ir apskaitą;

b) užtikrinimą, kad visos ES šifravimo medžiagos apskaitai, saugiam tvarkymui, saugojimui ir platinimui būtų taikomos tinkamos procedūros ir nustatyti tinkami kanalai; ir

c) ES šifravimo medžiagos perdavimo ją naudojantiems asmenims ir tarnyboms arba priėmimo iš jų užtikrinimą.

Saugumo akreditavimo institucija

47. Kiekvienai sistemai skirta SAI atsako už šias sritis:

a) užtikrinimą, kad RIS atitiktų atitinkamą saugumo politiką ir saugumo gaires, pareiškimo dėl RIS patvirtinimo, leidžiant jas naudoti tvarkant ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje, pateikimą, nurodant akreditavimo reikalavimus ir sąlygas bei kriterijus, kuriais remiantis sprendžiama, kad reikia iš naujo patvirtinti arba akredituoti RIS;

b) saugumo akreditavimo proceso nustatymą vadovaujantis atitinkama politika, aiškiai nurodant patvirtinimo sąlygas, nustatytas jos priežiūrai pavestoms RIS;

c) saugumo akreditavimo strategijos, kurioje išdėstytas akreditavimo proceso išsamumo lygis, atitinkantis reikiamą saugumo užtikrinimo lygį, nustatymą;

d) su saugumu susijusių dokumentų, įskaitant pareiškimus dėl rizikos valdymo ir likutinės rizikos, sistemos saugumo reikmių aktus (toliau – SSRA), saugumo įgyvendinimo patikrinimo dokumentus ir saugios eksploatacijos taisykles (toliau – SecOPs), nagrinėjimą ir patvirtinimą bei užtikrinimą, kad jie atitiktų Tarybos saugumo taisykles ir politiką;

e) su RIS susijusių saugumo priemonių įgyvendinimo patikrinimą vykdant saugumo įvertinimus, patikrinimus ar peržiūras arba juos finansuojant;

f) saugumo reikalavimų (pavyzdžiui, susijusių su personalo patikimumo laipsniais), taikomų svarbiausioms, susijusioms su RIS apsauga pareigybėms, nustatymą;

g) patvirtintų šifravimo ir TEMPEST priemonių, naudojamų siekiant užtikrinti RIS saugumą, parinkimo patvirtinimą;

h) RIS tarpusavio sujungimo su kitomis RIS patvirtinimą arba prireikus dalyvavimą bendrame patvirtinime; ir

i) sistemos tiekėjo, saugumo srities subjektų ir vartotojų atstovų konsultavimą saugumo rizikos valdymo, visų pirma likutinės rizikos, ir pareiškimo dėl patvirtinimo reikalavimų ir sąlygų klausimais.

48. TGS SAI atsako už visų TGS kompetencijai priklausančių RIS akreditavimą.

49. Atitinkama valstybės narės SAI atsako už tos valstybės narės kompetencijai priklausančių RIS ir jų sisteminių komponentų akreditavimą.

50. Jungtinė saugumo akreditacijos valdyba (SAV) yra atsakinga tiek už TGS SAI žinioje, tiek už valstybių narių SAI žinioje esančių RIS akreditavimą. Ją sudaro po vieną kiekvienos valstybės narės SAI atstovą, o jos posėdžiuose dalyvauja Europos Komisijos atstovas SAI klausimais. Kiti subjektai, turintys prijungimo prie RIS mazgus, kviečiami dalyvauti posėdžiuose, kai svarstomi su ta sistema susiję klausimai.

SAV pirmininkauja TGS SAI atstovas. Ji sprendimus priima institucijų, valstybių narių ir kitų subjektų, turinčių prijungimo prie RIS mazgus, SAI atstovų sutarimu. SAV reguliariai teikia savo veiklos ataskaitas Saugumo komitetui ir jam praneša apie visus pareiškimus dėl akreditavimo.

Informacijos saugumo užtikrinimo operacinė institucija

51. Kiekvienai sistemai skirta ISU operacinė institucija atsako už šias sritis:

a) saugumo dokumentų, atitinkančių saugumo politiką ir saugumo gaires, rengimą, visų pirma SSRA, įskaitant pareiškimą dėl likutinės rizikos, SecOPs ir šifravimo planą vykdant RIS akreditavimo procesą, rengimą;

b) dalyvavimą atrenkant ir bandant konkrečioms sistemoms skirtas techninio saugumo priemones, prietaisus ir programinę įrangą, jų įgyvendinimo priežiūrą ir užtikrinimą, kad jie būtų saugiai įdiegti, sukonfigūruoti bei eksploatuojami pagal atitinkamus saugumo dokumentus;

c) dalyvavimą parenkant TEMPEST saugumo priemones ir prietaisus, jei reikia pagal SSRA, ir užtikrinimą, kad jie būtų saugiai įdiegti ir eksploatuojami bendradarbiaujant su TEI;

d) SecOps įgyvendinimo ir taikymo stebėseną; prireikus atsakomybę už eksploatavimo saugumą deleguojant sistemos savininkui;

e) šifravimo priemonių valdymą ir tvarkymą užtikrinant šifravimo ir kontroliuojamų objektų saugojimą ir prireikus užtikrinant šifravimo kintamųjų generavimą;

f) saugumo analizės peržiūros ir bandymų atlikimą, visų pirma siekiant parengti atitinkamas rizikos ataskaitas, kurių reikalauja SAI;

g) mokymo konkrečioms RIS skirto ISU klausimais rengimą;

h) konkrečioms RIS skirtų apsaugos priemonių įgyvendinimą ir vykdymą.

V PRIEDAS

PRAMONINIS SAUGUMAS

I. ĮVADAS

1. Šiame priede nustatytos 11 straipsnio įgyvendinimo nuostatos. Jame išdėstytos bendros saugumo nuostatos, taikomos pramonės ar kitiems subjektams derybų dėl sutarčių sudarymo metu arba visą TGS sudarytų įslaptintų sutarčių gyvavimo ciklą.

2. Taryba patvirtina pramoninio saugumo politiką, kurioje visų pirma apibrėžiami išsamūs reikalavimai susiję su ĮPPP, saugumo aspektų paaiškinimais (SAP), vizitais, ESĮI perdavimu ir gabenimu.

II. SAUGUMO ASPEKTAI ĮSLAPTINTOSE SUTARTYSE

Slaptumo žymų vadovas (SŽV)

3. Prieš paskelbdamas kvietimą teikti pasiūlymus įslaptintai sutarčiai sudaryti arba prieš sudarydamas įslaptintą sutartį, TGS, kaip perkančioji institucija, nustato visos informacijos, kuri turi būti suteikta konkurso dalyviams ir rangovams, slaptumo žymą, taip pat visos informacijos, kurią turi parengti rangovas, slaptumo žymą. Šiuo tikslu TGS parengia SŽV, kuris turi būti naudojamas vykdant sutartį.

4. Siekiant nustatyti skirtingų įslaptintos sutarties dalių slaptumo žymą, taikomi toliau nurodyti principai:

a) rengdamas SŽV, TGS atsižvelgia į visus svarbius saugumo aspektus, įskaitant slaptumo žymą, kurią informacijai priskyrė jos įslaptintos informacijos rengėjas ir kurią jis patvirtino kaip naudotiną tai sutarčiai;

b) bendras sutarties slaptumo žymos laipsnis negali būti žemesnis nei aukščiausia bet kurios jos dalies slaptumo žyma; ir

c) atitinkamais atvejais, jei daromi pakeitimai, susiję su slaptumo žymų suteikimu informacijai, parengtai rangovų ar jiems suteiktai vykdant sutartį, ir jei daromi vėlesni SŽV pakeitimai, TGS palaiko ryšius su valstybių narių NSI/PSI ar kitomis atitinkamomis kompetentingomis saugumo institucijomis.

Saugumo aspektų paaiškinimas (SAP)

5. Konkrečioms sutartims skirti saugumo reikalavimai aprašomi SAP. Prireikus į SAP įtraukiamas SŽV; SAP yra neatsiejama įslaptintos sutarties ar subrangos sutarties dalis.

6. SAP nustatomos nuostatos, pagal kurias reikalaujama, kad rangovas ir (arba) subrangovas laikytųsi būtiniausių šiame sprendime nustatytų standartų. Šių būtiniausių standartų nesilaikymas gali būti pakankamas pagrindas sutarčiai nutraukti.

Programos / projekto saugumo instrukcijos (PSI)

7. Atsižvelgiant į programų ar projektų, kuriuos vykdant reikia susipažinti su ESĮI arba ją tvarkyti ar saugoti, apimtį, programą ar projektą valdyti paskirta perkančioji institucija gali parengti konkrečios programos / projekto saugumo instrukcijas (PSI). PSI turi patvirtinti valstybių narių NSI/PSI ar kita programoje / projekte dalyvaujanti kompetentinga saugumo institucija; jose gali būti nustatyti papildomi saugumo reikalavimai.

III. ĮMONĖS PATIKIMUMĄ PATVIRTINANTIS PAŽYMĖJIMAS (ĮPPP)

8. ĮPPP išduoda valstybės narės NSI arba PSI ar kita kompetentinga saugumo institucija ir jame pagal nacionalinius įstatymus ir kitus teisės aktus nurodoma, kad pramonės arba kitas subjektas savo patalpose gali apsaugoti atitinkamo slaptumo žymos (CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET) laipsnio ESĮI. Prieš rangovui ar subrangovui arba potencialiam rangovui ar subrangovui suteikiant ESĮI arba galimybę susipažinti su ESĮI, TGS, kaip perkančiajai institucijai, turi būti pateikiamas ĮPPP.

9. Išduodama ĮPPP atitinkama NSI ar PSI, mažų mažiausiai:

a) įvertina pramonės ar kitų subjektų patikimumą;

b) įvertina nuosavybę, kontrolę ar nederamos įtakos tikimybę, kurie gali būti laikomi saugumo rizika;

c) įsitikina, kad pramonės arba kitas subjektas patalpose yra sukūręs saugumo sistemą, kuri apima visas atitinkamas saugumo priemones, būtinas, kad būtų apsaugota informacija ar medžiaga, pažymėta CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma, laikantis šiame sprendime nustatytų reikalavimų;

d) įsitikina, kad vadovybės, savininkų ir darbuotojų, kurie turi turėti galimybę susipažinti su informacija, pažymėta CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma, asmens patikimumo statusas yra nustatytas laikantis šiame sprendime nustatytų reikalavimų;

e) įsitikina, kad pramonės arba kitas subjektas yra paskyręs patalpų saugumo pareigūną, kuris yra atsakingas vadovybei už saugumo įsipareigojimų tokiame subjekte vykdymo užtikrinimą.

10. Atitinkamais atvejais TGS, kaip perkančioji institucija, praneša atitinkamai NSI/PSI ar kitai kompetentingai saugumo institucijai, kad prieš sudarant sutartį arba sutarties vykdymui reikalingas ĮPPP. ĮPPP arba APP reikalaujama prieš sudarant sutartį, tais atvejais, kai ESĮI, pažymėta CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma, turi būti suteikta paraiškų teikimo proceso metu.

11. Perkančioji institucija nesudaro įslaptintos sutarties su pasirinktu dalyviu prieš tai negavusi valstybės narės, kurioje yra registruotas atitinkamas rangovas ar subrangovas, NSI/PSI ar kitos kompetentingos saugumo institucijos patvirtinimo, kad reikiamais atvejais yra išduotas tinkamas ĮPPP.

12. ĮPPP išdavusi NSI/PSI ar kita kompetentinga saugumo institucija praneša TGS, kaip perkančiajai institucijai, apie pasikeitimus, turinčius įtakos ĮPPP. Subrangos sutarties atveju atitinkamai informuojama NSI/PSI ar kita kompetentinga saugumo institucija.

13. Jeigu atitinkama NSI/PSI ar kita kompetentinga saugumo institucija panaikina ĮPPP, tai yra pakankamas pagrindas TGS, kaip perkančiajai institucijai, nutraukti įslaptintą sutartį arba pašalinti dalyvį iš konkurso.

IV. ĮSLAPTINTOS SUTARTYS IR SUBRANGOS SUTARTYS

14. Tais atvejais, kai ESĮI suteikiama dalyviui prieš sudarant sutartį, kvietime teikti paraiškas numatoma nuostata, kuria paraiškos nepateikęs dalyvis arba dalyvis, kuris nebuvo atrinktas, įpareigojamas per nurodytą laiką grąžinti visus įslaptintus dokumentus.

15. Sudarius įslaptintą sutartį ar subrangos sutartį, TGS, kaip perkančioji institucija, praneša rangovo ar subrangovo NSI/PSI ar kitai kompetentingai saugumo institucijai tos įslaptintos sutarties saugumo nuostatas.

16. Nutraukus tokią sutartį, TGS, kaip perkančioji institucija (ir (arba) atitinkamai NSI/PSI ar kita kompetentinga saugumo institucija subrangos sutarties atveju) skubiai apie tai praneša valstybės narės, kurioje registruotas rangovas arba subrangovas, NSI/PSI ar kitai kompetentingai saugumo institucijai.

17. Paprastai reikalaujama, kad nutraukus įslaptintą sutartį ar subrangos sutartį rangovas arba subrangovas perkančiajai institucijai grąžintų visą turimą ESĮI.

18. Konkrečios nuostatos dėl ESĮI sunaikinimo vykdant sutartį arba ją nutraukus nustatomos SAP.

19. Tais atvejais, kai rangovui arba subrangovui duotas leidimas nutraukus sutartį pasilikti ESĮI, rangovas ir subrangovas toliau laikosi šiame sprendime nustatytų būtiniausių standartų bei užtikrina ESĮI konfidencialumą.

20. Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, nurodomos kvietime teikti paraiškas ir sutartyje.

21. Prieš sudarydamas subrangos sutartis dėl įslaptintos sutarties dalių, rangovas turi gauti TGS, kaip perkančiosios institucijos, leidimą. Su pramonės arba kitais subjektais, registruotais valstybėje, kuri nėra ES valstybė narė ir nėra sudariusi susitarimo dėl informacijos saugumo su ES, subrangos sutartys negali būti sudaromos.

22. Rangovas atsako už tai, kad visa subrangos veikla būtų vykdoma laikantis šiame sprendime nustatytų būtiniausių standartų, ir negali suteikti subrangovui ESĮI be išankstinio rašytinio perkančiosios institucijos sutikimo.

23. ESĮI, kurią parengė ar tvarko rangovas arba subrangovas, atžvilgiu įslaptintos informacijos rengėjo teisėmis naudojasi perkančioji institucija.

V. SU ĮSLAPTINTOMIS SUTARTIMIS SUSIJĘ VIZITAI

24. Jei TGS, rangovams ar subrangovams vykdant įslaptintą sutartį jiems priklausančiose patalpose reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma pažymėta informacija, dėl jų vizitų susitariama palaikant ryšius su NSI/PSI arba kita susijusia kompetentinga saugumo institucija. Tačiau atsižvelgiant į tam tikrus projektus NSI/PSI gali taip pat susitarti dėl tvarkos, pagal kurią dėl tokių vizitų gali būti susitariama tiesiogiai.

25. Tam, kad būtų leista susipažinti su ESĮI, susijusia su TGS sutartimi, visi lankytojai turi turėti atitinkamą APP ir turi būti vadovaujamasi principu „būtina žinoti“.

26. Lankytojams leidžiama susipažinti tik su ta ESĮI, kuri yra susijusi su vizito tikslu.

VI. ESĮI PERDAVIMAS IR GABENIMAS

27. Perduodant ESĮI elektroninėmis priemonėmis taikomos atitinkamos 10 straipsnio ir IV priedo nuostatos.

28. Gabenant ESĮI taikomos atitinkamos III priedo nuostatos, laikantis nacionalinių įstatymų ir kitų teisės aktų.

29. Nustatant įslaptintos medžiagos kaip krovinio gabenimui taikomą saugumo tvarką taikomi toliau nurodyti principai:

a) saugumas užtikrinamas visuose gabenimo etapuose nuo gabenimo pradžios vietos iki galutinės paskirties vietos;

b) siuntai suteikiamas apsaugos lygis nustatomas pagal joje esančios medžiagos aukščiausią slaptumo žymos laipsnį;

c) gabenimą užtikrinančios bendrovės turi gauti atitinkamos slaptumo žymos ĮPPP. Tokiais atvejais laikantis I priedo turi būti patikrintas siuntą gabenančio personalo patikimumas;

d) prieš gabenant per valstybių sienas medžiagą, pažymėtą CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET slaptumo žyma, siuntėjas parengia, o atitinkamos NSI/PSI ar kitos kompetentingos saugumo institucijos patvirtina gabenimo planą;

e) stengiamasi, kad kelionės vyktų be sustojimo ir būtų užbaigtos kuo greičiau, atsižvelgiant į aplinkybes;

f) kai galima, turėtų būti pasirenkami maršrutai tik per valstybių narių teritorijas. Maršrutais per valstybes, kurios nėra valstybės narės, turėtų būti gabenama tik gavus siuntėjo ir gavėjo valstybių NSI/PSI ar kitos kompetentingos saugumo institucijos leidimą.

VII. ESĮI PERDAVIMAS TREČIOSIOSE VALSTYBĖSE ĮSIKŪRUSIEMS RANGOVAMS

30. ESĮI trečiosiose valstybėse įsikūrusiems rangovams ir subrangovams perduodama laikantis saugumo priemonių, dėl kurių susitarė TGS, kaip perkančioji institucija, ir atitinkamos trečiosios valstybės, kurioje registruotas rangovas, NSI/PSI.

VIII. RESTREINT UE/EU RESTRICTED SLAPTUMO ŽYMA PAŽYMĖTOS INFORMACIJOS TVARKYMAS IR SAUGOJIMAS

31. Palaikydamas ryšius su valstybės narės NSI/PSI TGS, kaip perkančioji institucija, prireikus turi teisę remiantis sutarties nuostatomis rengti vizitus į rangovo / subrangovo patalpas, kad patikrintų, ar įgyvendintos pagal sutartį reikalaujamos tinkamos saugumo priemonės, skirtos apsaugoti RESTREINT UE/EU RESTRICTED laipsnio slaptumo žyma pažymėtą ESĮI.

32. Kiek būtina pagal nacionalinius įstatymus ir kitus teisės aktus, NSI/PSI ar kitoms kompetentingoms saugumo institucijoms TGS, kaip perkančioji institucija, praneša apie sutartis arba subrangos sutartis, kuriose yra RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtos informacijos.

33. TGS sudarytų sutarčių, kuriose yra RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėtos informacijos, atveju rangovai ar subrangovai ir jų personalas neprivalo turėti ĮPPP ar APP.

34. TGS, kaip perkančioji institucija, išnagrinėja atsakymus į kvietimus dalyvauti konkurse dėl sutarčių, pagal kurias turi būti suteikta galimybė susipažinti su RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėta informacija, neatsižvelgdama į reikalavimus, susijusius su ĮPPP ar APP, kurie gali būti numatyti nacionaliniuose įstatymuose ir kituose teisės aktuose.

35. Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, turi atitikti 21 punkto reikalavimus.

36. Kai pagal sutartį numatytas informacijos, pažymėtos RESTREINT UE/EU RESTRICTED slaptumo žyma, tvarkymas rangovo naudojamoje RIS, TGS, kaip perkančioji institucija, užtikrina, kad sutartyje arba subrangos sutartyje būtų nustatyti su RIS akreditavimu susiję būtini techniniai ir administraciniai reikalavimai, kurie atitiktų įvertintą riziką, atsižvelgiant į visus svarbius veiksnius. Perkančioji institucija ir atitinkama NSI/PSI susitaria dėl tokio RIS akreditavimo masto.

VI PRIEDAS

KEITIMASIS ĮSLAPTINTA INFORMACIJA SU TREČIOSIOMIS ŠALIMIS IR TARPTAUTINĖMIS ORGANIZACIJOMIS

I. ĮVADAS

1. Šiame priede nustatytos 12 straipsnio įgyvendinimo nuostatos.

II. TVARKA, REGLAMENTUOJANTI KEITIMĄSI ĮSLAPTINTA INFORMACIJA

2. Tarybai nustačius, kad yra ilgalaikis poreikis keistis įslaptinta informacija, sudaromas

— susitarimas dėl informacijos saugumo, arba

— administracinis susitarimas,

vadovaujantis 12 straipsnio 2 dalimi ir III bei IV skirsniais bei remiantis saugumo komiteto rekomendacija.

3. Tais atvejais, kai BSGP operacijos vykdymui surinkta ESĮI gali būti suteikiama tokioje operacijoje dalyvaujančioms trečiosioms valstybėms ar tarptautinėms organizacijoms, ir jeigu nėra nustatyta 2 dalyje nurodyta tvarka, keitimasis ESĮI su dalyvaujančiąja trečiąja valstybe arba tarptautine organizacija vadovaujantis V skirsniu reglamentuojamas:

— susitarimu dėl dalyvavimo bendrųjų sąlygų,

— *ad hoc* susitarimu dėl dalyvavimo, arba

— jeigu nėra sudarytas nė vienas iš pirmiau nurodytų susitarimų – *ad hoc* administraciniu susitarimu.

4. Jeigu nėra nustatyta 2 ir 3 dalyse nurodyta tvarka ir jeigu priimamas sprendimas vadovaujantis VI skirsniu suteikti ESĮI trečiajai valstybei ar tarptautinei organizacijai išimtine *ad hoc* tvarka, iš atitinkamos trečiosios valstybės ar tarptautinės organizacijos turi būti gautas raštiškas patvirtinimas, kad ji saugos bet kokią jai suteiktą ESĮI laikydamasi šiame sprendime nustatytų pagrindinių principų ir būtiniausių standartų.

III. SUSITARIMAI DĖL INFORMACIJOS SAUGUMO

5. Susitarimais dėl informacijos saugumo nustatomi pagrindiniai principai ir būtiniausi standartai, reglamentuojantys ES ir trečiosios valstybės ar tarptautinės organizacijos keitimąsi įslaptinta informacija.

6. Susitarimuose dėl informacijos saugumo numatomi techniniai įgyvendinimo susitarimai, dėl kurių turi susitarti TGS saugumo tarnyba, EKSD ir kompetentinga atitinkamos trečiosios valstybės ar tarptautinės organizacijos saugumo institucija. Tokiuose susitarimuose atsižvelgiama į atitinkamoje trečiojoje valstybėje ar tarptautinėje organizacijoje galiojančiais saugumo nuostatais ir esamomis struktūromis bei procedūromis užtikrinamą apsaugos lygį. Šiuos susitarimus patvirtina Saugumo komitetas.

7. Keistis ESĮI elektroninėmis priemonėmis neleidžiama, jei tai nėra aiškiai numatyta susitarime dėl informacijos saugumo arba techniniuose įgyvendinimo susitarimuose.

8. Susitarimuose dėl informacijos saugumo numatoma, kad prieš keičiantis įslaptinta informacija pagal susitarimą, TGS saugumo tarnyba ir EKSD susitaria, kad gaunančioji šalis atitinkamu būdu gali apsaugoti ir saugoti jai teikiamą informaciją.

9. Kai Taryba sudaro susitarimą dėl informacijos saugumo, kiekvienoje šalyje paskiriama po vieną registratūrą, kuri yra pagrindinis įslaptintos informacijos gavimo ir išsiuntimo punktas.

10. Siekiant įvertinti atitinkamos trečiosios valstybės ar tarptautinės organizacijos saugumo nuostatus, struktūras ir procedūras, abipusiu susitarimu su atitinkama trečiąja valstybe ar tarptautine organizacija TGS Saugumo tarnyba kartu su EKSD rengia įvertinimo vizitus. Tokie įvertinimo vizitai rengiami laikantis atitinkamų III priedo nuostatų ir jų metu įvertinama:

a) įslaptintai informacijai apsaugoti taikoma reglamentavimo sistema;

b) bet kurie konkretūs saugumo politikos ypatumai ir saugumo organizavimo tvarka trečiojoje valstybėje arba tarptautinėje organizacijoje, kurie galėtų daryti poveikį įslaptintos informacijos, kuria gali būti keičiamasi, slaptumo žymos laipsniui;

c) faktiškai taikomos saugumo priemonės ir procedūros; ir

d) patikimumo patikrinimo procedūros, susijusios su numatomos suteikti ESĮI slaptumo žymos laipsniu.

11. ES vardu įvertinimo vizitą atliekanti grupė įvertina, ar atitinkamoje trečiojoje valstybėje arba tarptautinėje organizacijoje saugumo nuostatai ir procedūros yra tinkami, kad būtų apsaugota atitinkamo slaptumo žymos laipsnio ESĮI.

12. Šių vizitų rezultatai pateikiami ataskaitoje, kuria remdamasis Saugumo komitetas nustato, koks gali būti aukščiausias ESĮI, kuria gali būti keičiamasi su atitinkama trečiąja šalimi popieriuje ir prireikus elektroninėmis priemonėmis, slaptumo žymos laipsnis, bei konkrečias sąlygas, reglamentuojančias keitimąsi šia informacija su ta šalimi.

13. Būtina dėti visas pastangas, kad būtų surengtas vizitas į atitinkamą trečiąją valstybę arba tarptautinę organizaciją saugumui visapusiškai įvertinti prieš tai, kai Saugumo komitetas patvirtina įgyvendinamuosius susitarimus, siekiant nustatyti taikomos saugumo sistemos pobūdį ir veiksmingumą. Tačiau jei tai nėra įmanoma, TGS saugumo tarnyba Saugumo komitetui pateikia kuo išsamesnę ataskaitą, pagrįstą turima informacija, informuodama Saugumo komitetą apie taikomus saugumo nuostatus ir saugumo organizavimo tvarką atitinkamoje trečiojoje valstybėje arba tarptautinėje organizacijoje.

14. Saugumo komitetas gali nuspręsti, kad laukiant įvertinimo vizito rezultatų negalima suteikti ESĮI arba galima suteikti ESĮI, kurios slaptumo žymos laipsnis ne aukštesnis nei nurodytas, arba jis gali nustatyti kitas specialias sąlygas, kurios taikomos ESĮI suteikimui atitinkamai trečiajai valstybei arba tarptautinei organizacijai. Apie tai TGS saugumo tarnyba praneša atitinkamai trečiajai valstybei arba tarptautinei organizacijai.

15. Remdamasi tarpusavio susitarimu su atitinkama trečiąja valstybe arba tarptautine organizacija, TGS saugumo tarnyba reguliariai rengia tolesnius įvertinimo vizitus, siekdama patikrinti, ar įdiegtos priemonės ir toliau atitinka iš pradžių sutartus būtiniausius standartus.

16. Kai susitarimas dėl informacijos saugumo įsigalioja ir keičiamasi įslaptinta informacija su atitinkama trečiąja valstybe ar tarptautine organizacija, Saugumo komitetas gali nuspręsti pakeisti ESĮI, kuria gali būti keičiamasi popieriniu pavidalu ar elektroninėmis priemonėmis, aukščiausią slaptumo žymos laipsnį, visų pirma atsižvelgdamas į tolesnių įvertinimo vizitų rezultatus.

IV. ADMINISTRACINIAI SUSITARIMAI

17. Esant ilgalaikiam poreikiui su trečiąja valstybe ar tarptautine organizacija keistis įslaptinta informacija, kurios slaptumo žymos laipsnis paprastai nėra aukštesnis nei RESTREINT UE/EU RESTRICTED, ir Saugumo komitetui nustačius, kad atitinkama šalis neturi pakankamai išplėtotos tokiai informacijai skirtos saugumo sistemos, kad ta šalis galėtų sudaryti susitarimą dėl informacijos saugumo, generalinis sekretorius gali, pritarus Tarybai, sudaryti administracinį susitarimą su atitinkamos trečiosios valstybės ar tarptautinės organizacijos atitinkamomis institucijomis.

18. Tais atvejais, kai dėl skubių operatyvinių priežasčių reikia greitai nustatyti keitimosi įslaptinta informacija tvarką, tik Taryba gali nuspręsti, kad būtų sudarytas administracinis susitarimas siekiant keistis aukštesnio slaptumo žymos laipsnio informacija.

19. Administraciniai susitarimai paprastai sudaromi pasikeičiant laiškais.

20. Prieš faktiškai suteikiant ESĮI atitinkamai trečiajai valstybei ar tarptautinei organizacijai rengiamas 10 punkte nurodytas įvertinimo vizitas, o šio vizito ataskaita siunčiama Saugumo komitetui ir jo tvirtinama kaip patenkinama. Tačiau, jei esama išskirtinių priežasčių skubiai pasikeisti įslaptinta informacija, apie kurias pranešta Tarybai, ESĮI gali būti suteikta, su sąlyga, kad dedamos visos pastangos kuo greičiau surengti tokį įvertinimo vizitą.

21. Keistis ESĮI elektroninėmis priemonėmis neleidžiama, jei tai nėra aiškiai numatyta administraciniame susitarime.

V. KEITIMASIS ĮSLAPTINTA INFORMACIJA VYKDANT BSGP OPERACIJAS

22. Trečiųjų valstybių ar tarptautinių organizacijų dalyvavimą BSGP operacijose reglamentuoja susitarimai dėl dalyvavimo bendrųjų sąlygų. Tokiuose susitarimuose nustatomos nuostatos dėl BSGP operacijų vykdymui surinktos ESĮI suteikimo jose dalyvaujančiosioms trečiosioms valstybėms ar tarptautinėms organizacijoms. Aukščiausias ESĮI, kuria gali būti keičiamasi, slaptumo žymos laipsnis yra RESTREINT UE/EU RESTRICTED BSGP civilinėms operacijoms ir CONFIDENTIEL UE/EU CONFIDENTIAL BSGP karinėms operacijoms, išskyrus atvejus, kai nustatyta kitaip sprendime, kuriuo įsteigiama kiekviena BSGP operacija.

23. *Ad hoc* susitarimuose dėl dalyvavimo, sudarytuose dėl konkrečios BSGP operacijos, nustatomos nuostatos dėl tos operacijos vykdymui surinktos ESĮI suteikimo joje dalyvaujančiajai trečiajai valstybei ar tarptautinei organizacijai. Aukščiausias ESĮI, kuria gali būti keičiamasi, slaptumo žymos laipsnis yra RESTREINT UE/EU RESTRICTED BSGP civilinėms operacijoms ir CONFIDENTIEL UE/EU CONFIDENTIAL BSGP karinėms operacijoms, išskyrus atvejus, kai nustatyta kitaip sprendime, kuriuo įsteigiama kiekviena BSGP operacija.

24. *Ad hoc* administraciniuose susitarimuose dėl trečiosios valstybės ar tarptautinės organizacijos dalyvavimo konkrečioje BSGP operacijoje gali būti numatytas, *inter alia*, operacijos vykdymui surinktos ESĮI suteikimas tai trečiajai valstybei ar tarptautinei organizacijai. Tokie *ad hoc* administraciniai susitarimai sudaromi vadovaujantis IV skirsnio 17 ir 18 punktuose nustatyta tvarka. Aukščiausias ESĮI, kuria gali būti keičiamasi, slaptumo žymos laipsnis yra RESTREINT UE/EU RESTRICTED BSGP civilinėms operacijoms ir CONFIDENTIEL UE/EU CONFIDENTIAL BSGP karinėms operacijoms, išskyrus atvejus, kai nustatyta kitaip sprendime, kuriuo įsteigiama kiekviena BSGP operacija.

25. Prieš įgyvendinant nuostatas dėl ESĮI suteikimo pagal 22, 23 ir 24 punktus, nėra būtina sudaryti įgyvendinimo susitarimus ar rengti įvertinimo vizitus.

26. Jei priimančioji valstybė, kurios teritorijoje vykdoma BSGP operacija, nėra sudariusi su ES susitarimo dėl informacijos saugumo arba administracinio susitarimo dėl keitimosi įslaptinta informacija, iškilus konkrečiai neatidėliotinai su operatyvine veikla susijusiai būtinybei gali būti sudarytas *ad hoc* administracinis susitarimas. Ši galimybė numatoma sprendime, kuriuo įsteigiama BSGP operacija. Tokiomis aplinkybėmis suteikiama tik ta ESĮI, kuri buvo surinkta BSGP operacijai vykdyti ir kurios slaptumo žymos laipsnis nėra aukštesnis nei RESTREINT UE/EU RESTRICTED. Pagal tokį *ad hoc* administracinį susitarimą priimančioji valstybė įsipareigoja saugoti ESĮI laikydamasi būtiniausių standartų, kurie turi būti ne mažiau griežti nei yra nustatyti šiame sprendime.

27. Nuostatose dėl įslaptintos informacijos, kurios turi būti įtrauktos į susitarimus dėl dalyvavimo bendrųjų sąlygų ir į 22–24 punktuose nurodytus *ad hoc* administracinius susitarimus, nustatoma, kad atitinkama trečioji valstybė ar tarptautinė organizacija užtikrina, kad jos personalas, komandiruotas į bet kokią operaciją, saugos ESĮI pagal Tarybos saugumo taisykles ir vadovaudamasis tolesniais kompetentingų institucijų, įskaitant operacijos vadovavimo grandinės pareigūnus, pateiktais nurodymais.

28. Jeigu vėliau sudaromas ES ir dalyvaujančiosios trečiosios valstybės ar tarptautinės organizacijos susitarimas dėl informacijos saugumo, šio susitarimo dėl informacijos saugumo nuostatos yra viršesnės už bet kokių susitarimų dėl dalyvavimo bendrųjų sąlygų, *ad hoc* susitarimų dėl dalyvavimo ir *ad hoc* administracinių susitarimų nuostatas dėl keitimosi ESĮI bei jos apdorojimo.

29. Keistis ESĮI elektroninėmis priemonėmis pagal susitarimą dėl dalyvavimo bendrųjų sąlygų, *ad hoc* susitarimą dėl dalyvavimo ar *ad hoc* administracinį susitarimą su trečiąja valstybe ar tarptautine organizacija neleidžiama, jei tai nėra aiškiai numatyta atitinkamame susitarime arba administraciniame susitarime.

30. BSGP operacijos vykdymui surinkta ESĮI gali būti atskleidžiama trečiųjų valstybių ar tarptautinių organizacijų į tą operaciją komandiruotam personalui, vadovaujantis 22–29 punktų nuostatomis. Kai tokiam personalui leidžiama susipažinti su ESĮI BSGP operacijos patalpose ar RIS, turi būti imamasi priemonių (įskaitant atskleistos ESĮI registravimą), kad būtų sumažinta rizika, jog informacija bus prarasta ar atskleista. Tokios priemonės nurodomos atitinkamuose planavimo ar misijos dokumentuose.

VI. ESĮI *AD HOC* SUTEIKIMAS IŠIMTINE TVARKA

31. Jei nėra nustatyta galiojančios tvarkos pagal III–V skirsnius, ir Tarybai ar vienam iš jos parengiamųjų organų nusprendus, kad išimtiniu atveju reikia suteikti ESĮI trečiajai valstybei ar tarptautinei organizacijai, TGS:

a) kiek įmanoma, patikrina atitinkamas trečiosios valstybės ar tarptautinės organizacijos saugumo institucijas, ar jų saugumo nuostatai, struktūros bei procedūros yra pakankami, kad užtikrintų, jog joms suteikta ESĮI būtų apsaugota pagal ne mažiau griežtus standartus nei yra nustatyti šiame sprendime;

b) prašo Saugumo komiteto, remiantis turima informacija, pateikti rekomendaciją, kiek galima pasitikėti atitinkamos trečiosios valstybės ar tarptautinės organizacijos, kuriai bus suteikta ESĮI, saugumo nuostatais, struktūromis bei procedūromis.

32. Jeigu Saugumo komitetas pateikia rekomendaciją, kuria pritaria ESĮI suteikimui, klausimas perduodamas Nuolatinių atstovų komitetui (COREPER), kuris priima sprendimą dėl šios ESĮI suteikimo.

33. Jeigu Saugumo komiteto rekomendacijoje nepritariama ESĮI suteikimui:

a) su BUSP/BSGP susijusiose srityse Politinis ir saugumo komitetas aptaria šį klausimą ir suformuluoja rekomendaciją dėl Nuolatinių atstovų komiteto sprendimo;

b) visose kitose srityse Nuolatinių atstovų komitetas aptarią šį klausimą ir priima sprendimą.

34. Jei manoma, kad tikslinga, ir iš anksto gavus rašytinį įslaptintos informacijos rengėjo sutikimą, Nuolatinių atstovų komitetas gali nuspręsti, kad įslaptinta informacija gali būti suteikta tik iš dalies ir tik tuo atveju, jei prieš tai jos slaptumo žymos laipsnis sumažinamas arba ji išslaptinama, arba kad informacija, kurią suteikti numatyta, turi būti parengta nenurodant šaltinio ar pirminio ES slaptumo žymos laipsnio.

35. Priėmus sprendimą suteikti ESĮI, TGS perduoda atitinkamą dokumentą, pažymėtą leidimo suteikti informaciją žyma, nurodant trečiąją valstybę ar tarptautinę organizaciją, kuriai ji buvo suteikta. Prieš suteikiant tokią informaciją arba faktinio jos suteikimo metu atitinkama trečioji šalis raštu įsipareigoja apsaugoti ESĮI, kurią ji gauna, pagal šiame sprendime nustatytus pagrindinius principus ir būtiniausius standartus.

VII. LEIDIMAS SUTEIKTI ESĮI TREČIOSIOMS VALSTYBĖMS ARBA TARPTAUTINĖMS ORGANIZACIJOMS

36. Kai yra nustatyta 2 dalyje nurodyta tvarka, reglamentuojanti keitimąsi įslaptinta informacija su trečiąja valstybe ar tarptautine organizacija, Taryba priima sprendimą suteikti leidimą generaliniam sekretoriui suteikti ESĮI atitinkamai trečiajai valstybei ar tarptautinei organizacijai, laikantis principo, kad su tuo turi sutikti įslaptintos informacijos rengėjas.

37. Kai yra nustatyta 3 dalyje nurodyta tvarka, reglamentuojanti keitimąsi įslaptinta informacija su trečiąja valstybe ar tarptautine organizacija, generaliniam sekretoriui suteikiamas leidimas suteikti ESĮI, vadovaujantis tuo sprendimu, kuriuo įsteigiama BSGP operacija, ir laikantis principo, kad su tuo turi sutikti įslaptintos informacijos rengėjas.

38. Generalinis sekretorius gali perduoti šią teisę vyresniesiems TGS pareigūnams ar kitiems jam pavaldiems asmenims.

Priedėliai

A Priedėlis

Sąvokų apibrėžtys

B Priedėlis

Slaptumo žymų atitikmenys

C Priedėlis

Nacionalinių saugumo institucijų (NSI) sąrašas

D Priedėlis

Santrumpų sąrašas

A priedėlis

SĄVOKŲ APIBRĖŽTYS

Šiame sprendime vartojamos tokios sąvokų apibrėžtys:

akreditavimas – procesas, po kurio Saugumo akreditavimo institucija (SAI) pateikia oficialų pareiškimą, patvirtinantį kad sistemai yra leista veikti taikant nustatytą slaptumo žymos laipsnį, konkrečiu slaptumo režimu jos operacinėje aplinkoje ir priimtinu rizikos lygiu, laikantis prielaidos, kad įgyvendintas patvirtintas techninių, fizinių, organizacinių ir procedūrinių saugumo priemonių rinkinys;

asmens patikimumo pažymėjimas (APP) – viena iš dviejų arba abi apibrėžtys:

— ES asmens patikimumo pažymėjimas (ES APP) – TGS paskyrimo tarnybos leidimas susipažinti su ESĮI, išduodamas pagal šį sprendimą valstybės narės kompetentingoms institucijoms užbaigus patikimumo tikrinimo procedūras ir patvirtinantis, kad asmeniui gali būti leidžiama susipažinti su iki tam tikro laipsnio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma) pažymėta ESĮI iki nustatytos datos, jei nustatyta, kad asmuo atitinka principą „būtina žinoti“; taigi laikoma, kad nurodyto asmens patikimumas yra patikrintas,

— „nacionalinis asmens patikimumo pažymėjimas“ (nacionalinis APP) – valstybės narės kompetentingos institucijos pažyma, leidžianti susipažinti su ESĮI ir išduota valstybės narės kompetentingoms institucijoms užbaigus patikimumo tikrinimo procedūras ir patvirtinanti, kad asmeniui gali būti leidžiama susipažinti su iki tam tikro laipsnio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma) pažymėta ESĮI iki nustatytos datos, jei nustatyta, kad asmuo atitinka principą „būtina žinoti“; taigi laikoma, kad nurodyto asmens patikimumas yra patikrintas,

asmens patikimumo pažymėjimą patvirtinanti pažyma (APPPP) – kompetentingos institucijos išduota pažyma, kurioje nurodoma, kad asmens patikimumas yra patikrintas ir kad jis turi galiojantį nacionalinį arba ES APP, ir nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos laipsnis (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma), atitinkamo APP galiojimo laikas ir pačios pažymos galiojimo laikas;

BSGP operacija – karinio ar civilinio krizių valdymo operacija vadovaujantis ES sutarties V antraštinės dalies 2 skyriumi;

darbo saugumo režimas – sąlygų, kuriomis veikia RIS, apibrėžtis, pagrįsta apdorojamos informacijos slaptumo žyma ir patikimumo laipsniais, oficialiais prieigos patvirtinimais ir naudotojams taikomu principu „būtina žinoti“. Įslaptintos informacijos apdorojimui arba perdavimui gali būti taikomi keturi darbo režimai: skirtinis režimas, aukšto lygio sistemos režimas, patalpų atskyrimo pertvaromis režimas ir daugialaipsnis režimas;

— skirtinis režimas – toks darbo režimas, kai visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo žymos laipsnio informacija ir pagal bendrą principą „būtina žinoti“ turi susipažinti su visa RIS tvarkoma informacija,

— aukšto lygio sistemos režimas – toks darbo režimas, kai visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo žymos laipsnio informacija, tačiau ne visi galintys naudotis RIS asmenys turi pagal bendrą principą „būtina žinoti“ susipažinti su RIS tvarkoma informacija; patvirtinimas apie teisės susipažinti su informacija suteikimą gali būti išduodamas asmens,

— patalpų atskyrimo pertvaromis režimas – toks darbo režimas, kai visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo žymos laipsnio informacija, tačiau ne visi galintys naudotis RIS asmenys turi oficialų leidimą susipažinti su visa RIS tvarkoma informacija; oficialus leidimas reiškia oficialų patekimo į objektą centrinį valdymą, kuris yra atskirtas nuo leidimo asmeniui savo nuožiūra suteikti prieigą,

— daugialaipsnis režimas – toks darbo režimas, kai ne visi galintys naudotis RIS asmenys turi leidimą naudotis RIS tvarkoma aukščiausio slaptumo žymos laipsnio informacija ir ne visi galintys naudotis RIS asmenys turi pagal bendrą principą „būtina žinoti“ susipažinti su RIS tvarkoma informacija;

dokumentas – fiksuota informacija, neatsižvelgiant į jos fizinę formą ar charakteristikas;

ES įslaptinta informacija (ESĮI) – žr. 2 straipsnio 1 dalį;

ESĮI administravimas – visi galimi veiksmai, kurie gali būti atliekami su ESĮI per visą jos gyvavimo ciklą. Tai apima ESĮI parengimą, apdorojimą, gabenimą, slaptumo žymos laipsnio sumažinimą, išslaptinimą ir sunaikinimą. RIS atžvilgiu tai taip pat apima ESĮI rinkimą, skelbimą, perdavimą ir saugojimą;

fizinis saugumas – žr. 8 straipsnio 1 dalį;

grėsmė – galimas nepageidaujamas atvejis, dėl kurio gali būti padaryta žala organizacijai ar jos naudojamoms sistemoms; tokios grėsmės gali būti atsitiktinės arba tyčinės (piktybinės); jas apibūdina pavojingi elementai, galimi taikiniai ir puolimo būdai;

Įmonės patikimumą patvirtinantis pažymėjimas (ĮPPP) – NSI ar PSI administracinis patvirtinimas, kad saugumo požiūriu patalpose gali būti užtikrinta nurodyto slaptumo žymos laipsnio ESĮI tinkamo lygio apsauga ir kad buvo tinkamai patikrintas jose dirbančio personalo narių, kuriems reikia susipažinti su ESĮI, patikimumas bei jie buvo informuoti apie atitinkamus saugumo reikalavimus, būtinus norint susipažinti su ESĮI ir ją apsaugoti;

informacijos saugumo užtikrinimas – žr. 10 straipsnio 1 dalį;

įslaptintos informacijos administravimas – žr. 9 straipsnio 1 dalį;

įslaptintos informacijos rengėjas – ES institucija, agentūra ar įstaiga, valstybė narė, trečioji valstybė ar tarptautinė organizacija, kurios atsakomybe įslaptinta informacija buvo parengta ir (arba) pateikta naudoti ES struktūrose;

įslaptinta subrangos sutartis – TGS rangovo ir kito rangovo (t. y. subrangovo) sudaryta prekių tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia susipažinti su ESĮI ar ją rengti arba suteikiama galimybė su ja susipažinti ar ją rengti;

įslaptinta sutartis – TGS ir rangovo sudaryta prekių tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdant reikia susipažinti su ESĮI ar ją rengti arba suteikiama galimybė su ja susipažinti ar ją rengti;

išslaptinimas – bet kokios slaptumo žymos panaikinimas;

likutinė rizika – rizika, kuri lieka po to, kai buvo įgyvendintos saugumo priemonės, atsižvelgiant į tai, kad ne nuo visų grėsmių apsisaugoma ir ne visi pažeidžiamumo aspektai gali būti pašalinti;

medžiaga – dokumentas arba bet kokie pagaminti ar gaminami įrenginiai ar įranga;

nuodugni apsauga – saugumo priemonių, kurios grupuojamos į kelis apsaugos lygius, taikymas;

paskirtoji saugumo institucija (PSI) – valstybės narės nacionalinei saugumo institucijai (NSI) atsakinga institucija, kuri atsako už pramonės ir kitų subjektų informavimą apie nacionalinę politiką visais pramoninio saugumo klausimais ir duoda nurodymus bei padeda ją įgyvendinti. PSI funkciją gali vykdyti NSI arba kita kompetentinga institucija;

patikimumo tikrinimas – tikrinimo procedūros, kurias, vadovaudamasi valstybėje narėje galiojančiais įstatymais ir kitais teisės aktais, atlieka kompetentinga institucija siekdama gauti užtikrinimą, kad nėra jokios nepalankios informacijos, kuri neleistų asmeniui išduoti nacionalinio arba ES asmens patikimumo pažymėjimo, suteikiančio galimybę susipažinti su tam tikro lygio ESĮI (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija);

pažeidžiamumas – bet kokio pobūdžio silpnumas, kuriuo gali būti naudojamasi vienos ar daugiau grėsmių atveju. Pažeidžiamumas gali atsirasti dėl neveikimo arba gali būti susijęs su kontrolės stiprumo, išsamumo ar nuoseklumo trūkumu ir gali būti techninio, procedūrinio, fizinio, organizacinio ar veiklos pobūdžio;

personalo patikimumas – žr. 7 straipsnio 1 dalį;

pramonės arba kitas subjektas – subjektas, tiekiantis prekes, vykdantis darbus arba teikiantis paslaugas; tai gali būti pramonės, prekybos, paslaugų, mokslo, mokslinių tyrimų, švietimo ar vystymo subjektas arba savarankiškai dirbantis asmuo;

pramoninis saugumas – žr. 11 straipsnio 1 dalį;

programos / projekto saugumo instrukcijos (PSI) – saugumo procedūrų, kurios yra taikomos konkrečiai programai / projektui siekiant standartizuoti saugumo procedūras, sąrašas. Jos gali būti tikslinamos įgyvendinant programą / projektą;

rangovas – fizinis arba juridinis asmuo, turintis teisnumą ir veiksnumą sudaryti sutartis;

registravimas – žr. III priedo 18 punktą;

RIS gyvavimo ciklas – visa RIS egzistavimo trukmė, įskaitant inicijavimą, koncepciją, planavimą, reikalavimų analizę, projektavimą, sukūrimą, bandymą, įdiegimą, veikimą ir priežiūrą bei naudojimo nutraukimą;

ryšių ir informacinė sistema (RIS) – žr. 10 straipsnio 2 dalį;

rizika – galimybė, kad tam tikros grėsmės atveju bus pasinaudota organizacijos ar sistemų vidiniu ir išoriniu pažeidžiamumu ir taip bus padaryta žala organizacijai ir jos materialiajam ar nematerialiajam turtui. Ji įvertinama atsižvelgiant į kylančios grėsmės tikimybę ir į jos poveikį;

— rizikos pripažinimas – sprendimas atlikus rizikos tvarkymą pripažinti, kad vis dar yra likutinė rizika,

— rizikos įvertinimas – grėsmių ir pažeidžiamų sričių nustatymas bei susijusios rizikos analizės, t. y. galimumo ir poveikio analizės, atlikimas,

— informavimas apie riziką – RIS vartotojų bendruomenės informuotumo apie riziką didinimas, patvirtinimo institucijų informavimas apie tokią riziką ir pranešimų vykdančiosioms institucijoms teikimas;

rizikos tvarkymas – rizikos silpninimas, šalinimas, mažinimas (taikant tinkamas technines, fizines, valdymo ar procedūrines priemones), perkėlimas arba stebėsena;

saugumo aspektų paaiškinimas (SAP) – specialių sutartinių sąlygų rinkinys, kurį parengia perkančioji institucija ir kuris yra įslaptintos sutarties, pagal kurią gali būti susipažįstama su ESĮI arba tokia informacija gali būti rengiama, sudėtinė dalis – jame nurodomi saugumo reikalavimai arba sutarties dalys, kurių saugumą būtina užtikrinti;

saugumo rizikos valdymo procesas – visas nebūtinai galinčių įvykti atvejų, kurie gali paveikti organizacijos arba jos naudojamų sistemų saugumą, nustatymo, kontrolės ir mažinimo procesas. Jis apima visą su rizika susijusią veiklą, įskaitant jos įvertinimą, tvarkymą, pripažinimą ir informavimą apie ją;

slaptumo žymos laipsnio sumažinimas – slaptumo žymos lygio sumažinimas;

slaptumo žymų vadovas (SŽV) – dokumentas, kuriame aprašomi programos arba sutarties įslaptintos dalys, nurodant taikomus slaptumo žymų laipsnius. SŽV gali būti papildomas programos arba sutarties vykdymo laikotarpiu, o informacijos dalims gali būti suteiktos naujos slaptumo žymos arba jų slaptumo žymos laipsnis gali būti sumažintas; tais atvejais, kai yra parengtas SŽV, jis yra SAP dalis;

šifravimo priemonės – šifravimo algoritmai, šifravimo techninės ir programinės įrangos moduliai, priemonės, apimančios vykdymo informaciją bei susijusius dokumentus ir raktų duomenis;

tarpusavio sujungimas – žr. IV priedo 31 punktą;

TEMPEST – elektromagnetinio spinduliavimo, dėl kurio neteisėtai atskleidžiama informacija, tikrinimas, tyrimas bei kontrolė ir jo šalinimo priemonės;

turėtojas – tinkamą leidimą turintis asmuo, kuris atitinka principą „būtina žinoti“ ir turi ESĮI dalį bei yra atitinkamai atsakingas už jos apsaugą;

turtas – viskas, kas turi tam tikrą vertę organizacijai, jos veiklos operacijoms bei jų tęstinumui, įskaitant informacijos išteklius, padedančius vykdyti organizacijos misiją.

B priedėlis

SLAPTUMO ŽYMŲ ATITIKMENYS

ES	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Belgija	Très Secret (Loi 11.12.1998) Zeer Geheim (Wet 11.12.1998)	Secret (Loi 11.12.1998) Geheim (Wet 11.12.1998)	Confidentiel (Loi 11.12.1998) Vertrouwelijk (Wet 11.12.1998)	(1) pastaba
Bulgarija	Строго секретно	Секретно	Поверително	За служебно ползване
Čekija	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danija	Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
Vokietija	STRENG GEHEIM	GEHEIM	VS (2) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Airija	Top Secret	Secret	Confidential	Restricted
Graikija	Άκρως Απόρρητο Santrumpa: ΑΑΠ	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Ispanija	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Prancūzija	Très Secret Défense	Secret Défense	Confidentiel Défense	(3) pastaba
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipras	Άκρως Απόρρητο Santrumpa: (ΑΑΠ)	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Latvija	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lietuva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Liuksemburgas	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Vengrija	Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
Malta	L-Oghla Segretezza	Sigriet	Kunfidenzjali	Ristrett
Nyderlandai	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Lenkija	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalija	Muito Secreto	Secreto	Confidencial	Reservado
Rumunija	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu

ES	TRES SECRET UE/EU TOP SECRET	SECRET UE/EU SECRET	CONFIDENTIEL UE/EU CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
Slovėnija	Strogo tajno	Tajno	Zaupno	Interno
Slovakija	Prísne tajné	Tajné	Dôverné	Vyhradené
Suomija	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švedija ([4])	HEMLIG/TOP SECRET HEMLIG AV SYNNERLIG BETYDELSE FÖR RIKETS SÄKERHET	HEMLIG/SECRET HEMLIG	HEMLIG/CONFIDENTIAL HEMLIG	HEMLIG/RESTRICTED HEMLIG
Jungtinė Karalystė	Top Secret	Secret	Confidential	Restricted

([1]) *Diffusion Restreinte/Beperkte Verspreiding* nėra slaptumo žyma Belgijoje. Žyma „RESTREINT UE/EU RESTRICTED“ pažymėtą informaciją Belgija tvarko ir saugo taip pat griežtai, kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

([2]) Vokietija: VS = *Verschlusssache*.

([3]) Prancūzijos nacionalinėje sistemoje slaptumo žyma „RESTREINT“ nenaudojama. Žyma „RESTREINT UE/EU RESTRICTED“ pažymėtą informaciją Prancūzija tvarko ir saugo taip pat griežtai, kaip taikant nustatytus Europos Sąjungos Tarybos saugumo taisyklėse aprašytus standartus ir procedūras.

([4]) Švedija: viršutinėje eilutėje nurodytas slaptumo žymas naudoja gynybos institucijos, o nurodytas apatinėje eilutėje – kitos institucijos.

C Priedėlis

NACIONALINIŲ SAUGUMO INSTITUCIJŲ (NSI) SĄRAŠAS

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

Sekretoriato telefonas: + 32/2/501 45 42
Faksas: + 32/2/501 45 96
El. paštas: nvo-ans@diplobel.fed.be

BULGARIJA
State Commission on Information Security
90 Cherkovna Str.
BG-1505 Sofia

Telefonas: + 359/2/921 5911
Faksas: + 359/2/987 3750
El. paštas: dksi@government.bg
Tinklavietė: www.dksi.bg

ČEKIJA
Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
CZ-150 06 Praha 56

Telefonas: + 420/257 28 33 35
Faksas: + 420/257 28 31 10
El. paštas: czech.nsa@nbu.cz
Tinklavietė: www.nbu.cz

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

Telefonas: + 353/1/ 478 08 22
Faksas: + 353/1/ 408 29 59

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

Τηλέφωνα: + 30/210/657 20 45 (ώρες γραφείου)
+ 30/210/657 20 09 (ώρες γραφείου)
Φαξ: + 30/210/653 62 79
+ 30/210/657 76 12

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

Telefonas: + 30/210/657 20 45
+ 30/210/657 20 09
Faksas: + 30/210/653 62 79
+ 30/210/657 76 12

DANIJA
Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg

Telefonas: + 45/33/14 88 88
Faksas: + 45/33/43 01 90

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

Telefonas: + 45/33/32 55 66
Faksas: + 45/33/93 13 20

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

Telefonas: + 49/30/18 681 0
Faksas: + 49/30/18 681 1441
El. paštas: oesIII3@bmi.bund.de

ESTIJA
National Security Authority Department
Estonian Ministry of Defence
Sakala 1
EE-15094 Tallinn

Telefonas: +372/7170 113, +372/7170 117
Faksas: +372/7170 213
El. paštas: nsa@kmin.ee

ISPANIJA
Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
E-28023 Madrid

Telefonas: + 34/91/372 50 00
Faksas: + 34/91/372 58 08
El. paštas: nsa-sp@areatec.com

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

Telefonas: + 33/1/71 75 81 77
Faksas: + 33/1/71 75 82 00

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

Telefonas: + 39/06/611 742 66
Faksas: + 39/06/488 52 73

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

Τηλέφωνα: + 357/22/80 75 69, + 357/22/80 76 43, + 357/22/80 77 64
Τηλεομοιότυπο: + 357/22/30 23 51

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

Telefonas: + 357/22/80 75 69, + 357/22/80 76 43, +357 /22/80 77 64
Faksas: + 357/22/30 23 51
El. paštas: cynsa@mod.gov.cy

LIUKSEMBURGAS
Autorité nationale de Sécurité
Boîte postale 2379
L-1023 Luxembourg

Telefonas: + 352/2478 22 10 centrinis
+ 352/2478 22 53 tiesioginis
Faksas: + 352/2478 22 43

VENGRIJA
Nemzeti Biztonsági Felügyelet
(National Security Authority)
P.O. Box 2
HU-1357 Budapest

Telefonas: + 361/346 96 52
Faksas: + 361/346 96 58
El. paštas: nbf@nbf.hu
Tinklavietė: www.nbf.hu

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

Telefonas: + 356/21 24 98 44
Faksas: + 356/25 69 53 21

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

Telefonas: +371/6702 54 18
Faksas: +371/6702 54 54
El. paštas: ndi@sab.gov.lv

LIETUVA
Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija
(*The Commission for Secrets Protection Coordination of the Republic of Lithuania*
National Security Authority)
Gedimino pr. 40/1
LT-01110 Vilnius

Telefonai: +370 52663201,
+370 5266 32 02
Faksas + 370 52663200
El. paštas nsa@vsd.lt

NYDERLANDAI
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
NL-2500 EA Den Haag

Telefonas: + 31/70/320 44 00
Faksas: + 31/70/320 07 33

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
NL-2500 ES Den Haag

Telefonas: + 31/70/318 70 60
Faksas: + 31/70/318 75 22

AUSTRIJA
Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
A-1014 Wien

Telefonas: + 43/1/531 15 25 94
Faksas: + 43/1/531 15 26 15
El. paštas: ISK@bka.gv.at

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

Telefonas: + 48/22/585 73 60
Faksas: + 48/22/585 85 09
El. paštas: nsa@abw.gov.pl
Tinklavietė: www.abw.gov.pl

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

Telefonas: + 48/22/684 12 47
Faksas: + 48/22/684 10 76
El. paštas: skw@skw.gov.pl

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

Telefonas: + 40/21/ 224 58 30
Faksas: + 40/21/ 224 07 14
El. paštas: nsa.romania@nsa.ro
Tinklavietė: www.orniss.ro

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

Telefonas: +351/ 213 031 710
Faksas: +351/ 213 031 711

SLOVĖNIJA
Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
SVN-1000 Ljubljana

Telefonas: + 386/1/478 13 90
Faksas: + 386/1/478 13 99

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

Telefonas: + 421/2/68 69 23 14
Faksas: + 421/2/63 82 40 05
Tinklavietė: www.nbusr.sk

ŠVEDIJA
Utrikesdepartementet
(Ministry of Foreign Affairs)
SSSB
S-103 39 Stockholm

Telefonas: + 46/8/405 10 00
Faksas: + 46/8/723 11 76
El. paštas: ud-nsa@foreign.ministry.se

SUOMIJA
National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government

Telefonas 1: + 358/9/160 56487
Telefonas 2: +358/9/160 56484
Faksas: + 358/9/160 55140
El. paštas: NSA@formin.fi

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

Telefonas 1: + 44/20/7276 5649
Telefonas 2: + 44/20/7276 5497
Faksas: + 44/20/7276 5651
El. paštas: UK-NSA@cabinet-office.x.gsi.gov.uk

D priedėlis

SANTRUMPŲ SĄRAŠAS

Santrumpa	Reikšmė
APP	Asmens patikimumo pažymėjimas
APPPP	Asmens patikimumo pažymėjimą patvirtinanti pažyma
AVSS	Apsauginės vaizdo stebėjimo sistemos
BSGP	Bendra saugumo ir gynybos politika
BUSP	Bendra užsienio ir saugumo politika
COREPER	Nuolatinių atstovų komitetas
EKSD	Komisijos saugumo direktoratas
ESĮI	ES įslaptinta informacija
ESSĮ	ES specialusis įgaliotinis
ĮAS	Įsibrovimo aptikimo sistemos
ĮPPP	Įmonės patikimumą patvirtinantis pažymėjimas
ISU	Informacijos saugumo užtikrinimas
ISUI	ISU institucija
IT	Informacinės technologijos
KPI	Kriptografijos patvirtinimo institucijos
KPI	Kriptografijos platinimo institucija
NSI	Nacionalinė saugumo institucija
PSI	Paskirtoji saugumo institucija
PSI	Programos / projekto saugumo instrukcijos
RAP	Ribų apsaugos priemonės
RIS	Ryšių ir informacinės sistemos, kuriose tvarkoma ESĮI
SAI	Saugumo akreditavimo institucija
SAP	Saugumo aspektų paaiškinimai
SAV	Jungtinė saugumo akreditacijos valdyba
SecOPs	Saugumo įgyvendinimo patikrinimo dokumentai ir saugios eksploatacijos taisyklės
SSRA	Sistemos saugumo reikmių aktai
SŽV	Slaptumo žymų vadovas
TEI	TEMPEST institucija
TGS	Tarybos generalinis sekretoriatas
TKI	Tinkamos kvalifikacijos institucija