

KOMISIJOS SPRENDIMAS (ES, Euratomas) 2015/444**2015 m. kovo 13 d.****dėl ES įslaptintos informacijos apsaugai užtikrinti skirtų saugumo taisyklių**

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 249 straipsnį,

atsižvelgdama į Europos atominės energijos bendrijos steigimo sutartį, ypač į jos 106 straipsnį,

atsižvelgdama į Protokolą Nr. 7 dėl Europos Sąjungos privilegijų ir imunitetų, pridėtą prie Sutarčių, ypač į jo 18 straipsnį,

kadangi:

- (1) atsižvelgiant į institucinius, organizacinius, veiklos ir technologinius pokyčius, reikia peržiūrėti ir atnaujinti Komisijos taikomas saugumo nuostatas, kurių tikslas – apsaugoti Europos Sąjungos įslaptintą informaciją (ESI);
- (2) Europos Komisija su Belgijos, Liuksemburgo ir Italijos Vyriausybėmis sudarė susitarimus ⁽¹⁾ dėl pagrindinių jos darbo vietų saugumo;
- (3) Komisija, Taryba ir Europos išorės veiksmų tarnyba yra įsipareigojusios taikyti lygiaverčius ESI apsaugą užtikrinančius saugumo standartus;
- (4) svarbu, kad Europos Parlamentas ir kitos Sąjungos institucijos, agentūros, įstaigos ar organai atitinkamais atvejais prisidėtų prie įslaptintos informacijos apsaugos principų, standartų ir taisyklių, būtinų siekiant apsaugoti Sąjungos ir jos valstybių narių interesus, taikymo;
- (5) ESI 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. Periodiškai atliekamas tokių priemonių efektyvumo vertinimas;
- (6) fizinis saugumas, skirtas įslaptintai informacijai apsaugoti Komisijoje – tai fizinių ir techninių apsaugos priemonių taikymas siekiant užkirsti kelią leidimo neturintiems asmenims susipažinti su ESI;
- (7) ESI valdymas – administracinių ESI kontrolės visą jos gyvavimo ciklą priemonių taikymas siekiant papildyti šio sprendimo 2, 3 ir 5 skyriuose numatytas priemones ir tokiu būdu atgrasyti nuo sąmoningo ar atsitiktinio tokios informacijos neteisėto atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius. Tokios priemonės visų pirma yra susijusios su ESI rengimu, saugojimu, registravimu, kopijavimu, vertimu, slaptumo mažinimu, išslaptinimu, gabenimu ir sunaikinimu ir papildo bendrąsias Komisijos dokumentų tvarkymo taisykles (Sprendimai 2002/47/EB, EAPB, Euratomas ⁽²⁾ ir 2004/563/EB, Euratomas ⁽³⁾);

⁽¹⁾ Žr. 2004 m. gruodžio 31 d. „Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité“, 2007 m. sausio 20 d. „Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois“ ir 1959 m. liepos 22 d. „Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratomas) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale“.

⁽²⁾ 2002 m. sausio 23 d. Komisijos sprendimas 2002/47/EB, EAPB, Euratomas, iš dalies keičiantis jos darbo tvarkos taisykles (OL L 21, 2002 I 24, p. 23).

⁽³⁾ 2004 m. liepos 7 d. Komisijos sprendimas 2004/563/EB, Euratomas, iš dalies keičiantis jos darbo tvarkos taisykles (OL L 251, 2004 7 27, p. 9).

- (8) šio sprendimo nuostatos nedaro poveikio:
- a) Reglamentui (Euratomas) Nr. 3 ⁽¹⁾;
 - b) Europos Parlamento ir Tarybos reglamentui (EB) Nr. 1049/2001 ⁽²⁾;
 - c) Europos Parlamento ir Tarybos reglamentui (EB) Nr. 45/2001 ⁽³⁾;
 - d) Tarybos reglamentui (EEB, Euratomas) Nr. 354/83 ⁽⁴⁾,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 SKYRIUS

PAGRINDINIAI PRINCIPAI IR BŪTINIAUSI STANDARTAI

1 straipsnis

Apibrėžtys

Šiame sprendime vartojamų terminų apibrėžtys:

- 1) Komisijos padalinys – Komisijos generalinis direktoratas, tarnyba arba Komisijos nario kabinetas;
- 2) kriptografinė medžiaga – kriptografiniai algoritmai, techninės ir programinės kriptografinės įrangos moduliai, priemonės, apimančios vykdymo informaciją bei susijusius dokumentus ir raktų duomenis;
- 3) Išslaptinimas – bet kokios saugumo žymos panaikinimas;
- 4) nuodugni apsauga – saugumo priemonių, kurios grupuojamos į kelis apsaugos lygius, taikymas;
- 5) Dokumentas – bet kokios fizinės formos ir charakteristikų užregistruota informacija;
- 6) slaptumo mažinimas – aukštesnio slaptumo lygio keitimas žemesniu slaptumo lygiu;
- 7) ESĮI tvarkymas – visi galimi veiksmai, kurie gali būti atliekami su ESĮI per visą jos gyvavimo ciklą. Tai apima ESĮI rengimą, registravimą, apdorojimą, gabenimą, slaptumo mažinimą, išslaptinimą ir sunaikinimą. Ryšių ir informacinių sistemų (RIS) atžvilgiu tai taip pat apima ESĮI rinkimą, skelbimą, perdavimą ir saugojimą;
- 8) Turėtojas – tinkamą leidimą turintis asmuo, kuriam „būtina žinoti“ ir kuris turi ESĮI dalį bei yra atitinkamai atsakingas už jos apsaugą;
- 9) įgyvendinimo taisyklės – taisyklės arba saugumo pranešimai, priimti pagal Komisijos sprendimo (ES, Euratomas) 2015/443 ⁽⁵⁾ 5 skyrių;
- 10) Medžiaga – terpė, duomenų laikmena arba pagaminti ar gaminami įrenginiai ar įranga;
- 11) Rengėjas – Sąjungos institucija, agentūra ar įstaiga, valstybė narė, trečioji valstybė ar tarptautinė organizacija, kurios atsakomybe išslaptinta informacija buvo parengta ir (arba) pateikta naudoti Sąjungos struktūrose;
- 12) Patalpos – bet koks nekilnojamas ar panašus Komisijos turtas ir nuosavybė;

⁽¹⁾ 1958 m. liepos 31 d. Reglamentas (Euratomas) Nr. 3, įgyvendinantis Europos atominės energijos bendrijos steigimo sutarties 24 straipsnį (OL L 17, 1958 10 6, p. 406/58).

⁽²⁾ 2001 m. gegužės 30 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 1049/2001 dėl galimybės visuomenei susipažinti su Europos Parlamento, Tarybos ir Komisijos dokumentais (OL L 145, 2001 5 31, p. 43).

⁽³⁾ 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo (OL L 8, 2001 1 12, p. 1).

⁽⁴⁾ 1983 m. vasario 1 d. Tarybos reglamentas (EEB, Euratomas) Nr. 354/83 dėl Europos ekonominės bendrijos ir Europos atominės energijos bendrijos istorinių archyvų atvėrimo visuomenei (OL L 43, 1983 2 15, p. 1).

⁽⁵⁾ 2015 m. kovo 13 d. Komisijos sprendimas (ES, Euratomas) 2015/443 dėl Komisijos saugumo (žr. šio Oficialiojo leidinio p. 41).

- 13) saugumo rizikos valdymo procesas – visas nebūtinai galinčių įvykti įvykių, kurie gali paveikti organizacijos arba jos naudojamų sistemų saugumą, nustatymo, kontrolės ir padarinių mažinimo procesas. Jis apima visą su rizika susijusią veiklą, įskaitant jos įvertinimą, valdymą, pripažinimą ir informavimą apie ją;
- 14) Tarnybos nuostatai – Europos Sąjungos pareigūnų tarnybos nuostatai ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygos, nustatyti Tarybos reglamentu (EEB, Euratomas, EAPB) Nr. 259/68 ⁽¹⁾;
- 15) Grėsmė – galima nepageidaujamo incidento, dėl kurio gali būti padaryta žala organizacijai ar jos naudojamoms sistemoms, priežastis. Tokios grėsmės gali būti atsitiktinės arba tyčinės (piktybinės); jas apibūdina pavojingi elementai, galimi taikiniai ir puolimo būdai;
- 16) Pažeidžiamumas – bet kokio pobūdžio trūkumas, kuriuo gali būti naudojamos vienos ar daugiau grėsmių atveju. Pažeidžiamumas gali atsirasti dėl neveikimo arba gali būti susijęs su negriežta, neišsamia arba nenuoseklia kontrole ir gali būti techninio, procedūrinio, fizinio, organizacinio ar veiklos pobūdžio.

2 straipsnis

Dalykas ir taikymo sritis

1. Šis sprendimas nustato pagrindinius ESII apsaugai užtikrinti skirtus saugumo principus ir būtiniausius standartus.
2. Šis sprendimas taikomas visiems Komisijos padaliniais ir visose Komisijos patalpose.
3. Nepaisant konkrečių nuorodų dėl tam tikrų darbuotojų grupių, šis sprendimas taikomas Komisijos nariams, Komisijos darbuotojams pagal Tarnybos nuostatus ir kitų Europos Bendrijų tarnautojų įdarbinimo sąlygas, į Komisiją deleguotiems nacionaliniams ekspertams (SNE), paslaugų teikėjams ir jų darbuotojams, stažuotojams ir bet kuriam asmeniui, galinčiam patekti į Komisijos pastatus ar naudotis kitu turtu, arba informacijai, kurią tvarko Komisija.
4. Šio sprendimo nuostatos nedaro poveikio Sprendimui 2002/47/EB, EAPB, Euratomas ir Sprendimui 2004/563/EB, Euratomas.

3 straipsnis

ESII, slaptumo žymų ir kitų žymų apibrėžtis

1. Europos Sąjungos išslaptinta informacija (ESII) – 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. ESII žymima viena iš šių slaptumo žymų:
 - a) TRES SECRET UE/ES TOP SECRET – informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti padaryta ypač didelė žala Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;
 - b) SECRET UE/ES SECRET – informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti rimtai pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;
 - c) CONFIDENTIEL UE/ES CONFIDENTIAL – informacija ir medžiaga, kurią neteisėtai atskleidus galėtų būti pakenkta Europos Sąjungos arba vienos ar kelių valstybių narių esminiams interesams;
 - d) RESTREINT UE/ES RESTRICTED – informacija ir medžiaga, kurios neteisėtas atskleidimas galėtų būti nepalankus Europos Sąjungos arba vienos ar kelių valstybių narių interesams.
3. ESII žymima slaptumo žyma pagal 2 dalį. Ji gali būti žymima papildoma žyma, kuri yra ne slaptumo žyma, bet skirta veiklos sričiai, su kuria ji yra susijusi, nurodyti, išslaptintos informacijos rengėjui įvardyti, jos platinimui ir naudojimui apriboti ar suteikimui nurodyti.

⁽¹⁾ 1968 m. vasario 29 d. Tarybos reglamentas (EEB, Euratomas, EAPB) Nr. 259/68, nustatantis Europos Bendrijų pareigūnų tarnybos nuostatus ir kitų Europos Bendrijų tarnautojų įdarbinimo sąlygas bei Komisijos pareigūnams laikinai taikomas specialias priemones (Kitų tarnautojų įdarbinimo sąlygos) (OL L 56, 1968 3 4, p. 1).

4 straipsnis

Įslaptinimo valdymas

1. Kiekvienas Komisijos narys arba kiekviena Komisijos tarnyba užtikrina, kad jos parengta ESII būtų žymima tinkama slaptumo žyma, būtų aiškiai nurodoma, kad tai yra ESII, ir jai būtų suteikta slaptumo žyma tik tokiam laikotarpiui, kuris yra būtinas.
2. Nedarant poveikio 26 straipsniui, be išankstinio įslaptintos informacijos rengėjo raštiško sutikimo ESII slaptumas nemažinamas arba ji neišslaptinama, o 3 straipsnio 2 dalyje nurodytos žymos nekeičiamos arba nepanaikinamos.
3. Jei reikia, remiantis 60 straipsniu nustatomos ESII tvarkymo įgyvendinimo taisyklės, įskaitant praktinį slaptumo žymų vadovą.

5 straipsnis

Įslaptintos informacijos apsauga

1. ESII saugoma laikantis šio sprendimo ir jo įgyvendinimo taisyklių.
2. Bet kokios ESII turėtojas yra atsakingas už jos apsaugą pagal šį sprendimą ir jo įgyvendinimo taisykles, laikantis 4 skyriuje nustatytų taisyklių.
3. Valstybėms narėms nacionaline slaptumo žyma pažymėtą įslaptintą informaciją perdavus į Komisijos struktūras ar tinklus, Komisija tą informaciją saugo laikydamasi reikalavimų, taikomų lygiaverčio slaptumo žymos lygio ESII, kaip nustatyta I priede pateiktoje slaptumo žymų atitikmenų lentelėje.
4. ESII visumos atveju gali būti reikalaujama užtikrinti apsaugos lygį, atitinkantį aukštesnį slaptumo žymos lygį nei jos atskirų komponentų slaptumo žymos.

6 straipsnis

Saugumo rizikos valdymas

1. ESII apsaugai užtikrinti skirtos saugumo priemonės visą savo gyvavimo ciklą turi atitikti jos slaptumo žymos lygį, informacijos ar medžiagos formą ir kiekį, patalpų, kuriose laikoma ESII, vietos ir konstrukcijos reikalavimus ir turi būti parenkamos atsižvelgiant į vietos lygiu įvertintą piktavališkos ir (arba) nusikalstamos veiklos, įskaitant šnipinėjimą, sabotажą ar terorizmą, keliamą grėsmę.
2. Nenumatytų atvejų planuose turi būti atsižvelgiama į poreikį apsaugoti ESII ekstremaliosios padėties atvejais siekiant užkirsti kelią galimybei neteisėtai susipažinti su šia informacija, ją atskleisti ar prarasti jos vientisumą arba galimybę ja naudotis.
3. Visų tarnybų veiklos tęstinumo planuose numatomos prevencinės ir atstatymo priemonės siekiant sumažinti didelių klaidų ar incidentų poveikį ESII administravimui ir saugojimui.

7 straipsnis

Šio sprendimo įgyvendinimas

1. Jei reikia, remiantis 60 straipsniu nustatomos įgyvendinimo taisyklės, skirtos šiam sprendimui papildyti ar sustiprinti.
2. Komisijos tarnybos imasi visų būtinų jų atsakomybės sričiai priklausančių priemonių, siekdamos užtikrinti, kad tvarkant arba saugant ESII ar kitą įslaptintą informaciją būtų laikomasi šio sprendimo ir atitinkamų įgyvendinimo taisyklių.
3. Saugumo priemonės, kurių imamasi įgyvendinant šį sprendimą, turi atitikti Komisijos saugumo principus, nustatytus Sprendimo (ES, Euratomas) 2015/443 3 straipsnyje.

4. Žmogiškųjų išteklių ir saugumo generalinio direktorato generalinis direktorius Žmogiškųjų išteklių ir saugumo generaliniame direktorate įsteigia Komisijos saugumo instituciją. Komisijos saugumo institucija atlieka pareigas, jai paskirtas šiuo sprendimu ir jo įgyvendinimo taisyklėmis.

5. Kiekvieno Komisijos padalinio vietos saugumo pareigūnas (VSP), nurodytas Sprendimo (ES, Euratomas) 2015/443 20 straipsnyje, yra bendrai atsakingas už ESĮI apsaugą pagal šį sprendimą ir, glaudžiai bendradarbiaudamas su Žmogiškųjų išteklių ir saugumo generaliniu direktoratu, atlieka šias užduotis:

- a) administruoja prašymus darbuotojams išduoti saugumo leidimus;
- b) prisideda prie saugumo mokymų ir teikia informaciją;
- c) prižiūri padalinio registracijos kontrolės pareigūno (RKP) veiklą;
- d) praneša apie saugumo pažeidimus ir neteisėto ESĮI atskleidimo atvejus;
- e) saugo atsarginius raktus ir visų kodų sąrašą;
- f) atlieka kitas su ESĮI apsauga susijusias arba įgyvendinimo taisyklėse nustatytas užduotis.

8 straipsnis

ESĮI saugumo pažeidimai ir neteisėtas atskleidimas

1. Saugumo pažeidimu laikomas šiame sprendime ir jo įgyvendinimo taisyklėse nustatytoms saugumo taisyklėms priešingas asmens veikimas arba neveikimas.
2. Laikoma, kad ESĮI neteisėtai atskleista, jeigu pažeidus saugumo taisykles ji visa arba jos dalis yra atskleista susipažinti su ja leidimo neturintiems asmenims.
3. Apie visus saugumo pažeidimus arba įtariamus saugumo pažeidimus nedelsiant pranešama Komisijos saugumo institucijai.
4. Tais atvejais, kai žinoma arba yra pagrįstų priežasčių manyti, kad ESĮI buvo neteisėtai atskleista arba prarasta, remiantis Sprendimo (ES, Euratomas) 2015/443 13 straipsniu atliekamas saugumo tyrimas.
5. Imamasi visų tinkamų priemonių, siekiant:
 - a) informuoti įslaptintos informacijos rengėją;
 - b) užtikrinti, kad siekiant nustatyti faktus tokį atvejį nagrinėtų su pažeidimu tiesiogiai nesusijęs personalas;
 - c) įvertinti galimą Sąjungos ar valstybių narių interesams padarytą žalą;
 - d) imtis atitinkamų priemonių, kad būtų užkirstas kelias pažeidimui pasikartoti ir
 - e) atitinkamas institucijas informuoti apie atliktus veiksmus.
6. Bet kuriam asmeniui, kuris pažeidė šiame sprendime nustatytas saugumo taisykles, gali būti taikomos drausminės priemonės vadovaujantis Tarnybos nuostatais. Asmeniui, kuris atsakingas už ESĮI neteisėtą atskleidimą ar praradimą, taikomos drausminės ir (arba) teisinės priemonės pagal taikomus įstatymus, taisykles ir kitus teisės aktus.

2 SKYRIUS

PERSONALO SAUGUMAS

9 straipsnis

Apibrėžtys

Šiame skyriuje vartojamų terminų apibrėžtys:

- 1) Leidimas susipažinti su ESĮI – remiantis valstybės narės kompetentingos institucijos patvirtinimu Komisijos priimtas saugumo institucijos sprendimas, kad Komisijos pareigūnui, kitam tarnautojui arba deleguotajam nacionaliniam ekspertui iki nustatytos datos gali būti leidžiama susipažinti su ESĮI, pažymėta nurodyto lygio slaptumo žyma (iki CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma), jei nustatyta, kad asmeniui „būtina žinoti“ ir jis buvo tinkamai informuotas apie savo atsakomybę; laikoma, kad asmuo, kuriam taikoma ši apibrėžtis, yra asmuo, turintis leidimą susipažinti su įslaptinta informacija.

- 2) Darbuotojo saugumo leidimas – priemonių taikymas, siekiant užtikrinti, kad galimybė susipažinti su ESII būtų suteikta tik asmenims:
 - a) kuriems „būtina žinoti“;
 - b) kurie atitinkamai atvejais turi leidimus susipažinti su tam tikro lygio slaptumo žyma pažymėta išlaptinta informacija ir
 - c) kurie yra informuoti apie savo pareigas.
- 3) Asmens patikimumo pažymėjimas (APT) – valstybės narės kompetentingos institucijos patvirtinimas, kuris pateikiamas valstybės narės kompetentingoms institucijoms baigus patikimumo patikrinimą ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jam „būtina žinoti“ ir jis buvo tinkamai informuotas apie savo atsakomybę, gali būti suteikiamas leidimas iki nurodytos datos susipažinti su nurodyto lygio slaptumo žyma (iki CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma) pažymėta ESII.
- 4) Asmens patikimumo pažymėjimą patvirtinanti pažyma (APPPP) – kompetentingos institucijos išduota pažyma, kurioje nurodoma, kad asmuo turi galiojantį patikimumo pažymėjimą arba Komisijos saugumo institucijos išduotą saugumo leidimą, ir nurodomas ESII, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos lygis (CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnis), atitinkamo asmens patikimumo pažymėjimo arba leidimo galiojimo laikas ir pačios pažymos galiojimo laikas;
- 5) Patikimumo patikrinimas – tyrimo 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 jo patikimumo pažymėjimo, suteikiančio galimybę susipažinti su nurodyto lygio (iki CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio) ESII.

10 straipsnis

Pagrindiniai principai

1. Leidimas susipažinti su ESII asmeniui suteikiamas tik po to, kai:
 - 1) nustatoma, kad jam „būtina žinoti“;
 - 2) jis buvo informuotas apie ESII apsaugai užtikrinti skirtas saugumo taisykles bei atitinkamus saugumo standartus ir gaires ir patvirtino savo pareigą saugoti tokią informaciją;
 - 3) jam dėl jo atliekamų funkcijų išduotas atitinkamo lygio saugumo leidimas susipažinti su išlaptinta informacija, pažymėta CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma, arba jam išduoti kiti tinkami leidimai pagal nacionalinius įstatymus ir kitus teisės aktus.
2. Visi asmenys, kuriems dėl jų pareigų gali reikėti susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta ESII, prieš susipažindami su tokia ESII gauna atitinkamo lygio saugumo leidimus. Atitinkamas asmuo raštu sutinka dalyvauti jo patikimumo pažymėjimo išdavimo procedūroje. To nepadaręs asmuo negali būti paskirtas į pareigas, jam negali būti patikėtos funkcijos arba užduotys, kurias vykdant reikėtų susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta išlaptinta informacija.
3. Asmens patikimumo pažymėjimo išdavimo procedūrų tikslas – nustatyti, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ESII.
4. Asmens lojalumas ir patikimumas, prieš suteikiant jam asmens patikimumo pažymėjimą, leisiantį susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, nustatomas vykdant patikimumo patikrinimą, kurį atlieka valstybės narės kompetentingos tarnybos, laikydamosi nacionalinių įstatymų ir kitų teisės aktų.
5. Komisijos saugumo institucija yra atsakinga tik už ryšių palaikymą su nacionalinėmis saugumo institucijomis (toliau – NSI) arba kitomis kompetentingomis nacionalinėmis institucijomis visais patikimumo tikrinimo klausimais. Visus Komisijos tarnybų ir jų darbuotojų ryšius su NSI ir kitomis kompetentingomis institucijomis palaiko Komisijos saugumo institucija.

11 straipsnis

Saugumo leidimų išdavimo tvarka

1. Kiekvienas Komisijos generalinis direktorius arba tarnybos vadovas nustato, kurias pareigybes užimantys jo padalinio darbuotojai atlikdami savo pareigas privalo susipažinti su išlaptinta informacija, pažymėta CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma, ir kuriems reikia išduoti saugumo leidimą.

2. Kai žinoma, kad asmuo bus paskirtas į pareigas, kurias atliekant reikės turėti galimybę susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta išlaptinta informacija, atitinkamo Komisijos padalinio VSP praneša apie tai Komisijos saugumo institucijai, o ji tam asmeniui perduoda patikimumo pažymėjimo klausimyną, parengtą tos valstybės narės, kurios pilietis yra paskirtasis Europos Sąjungos institucijų darbuotojas, nacionalinės saugumo institucijos. Asmuo raštu sutinka dalyvauti patikimumo pažymėjimo išdavimo procedūroje ir kuo greičiau grąžinti užpildytą klausimyną Komisijos saugumo institucijai.
3. Komisijos saugumo institucija nusiunčia užpildytą asmens patikimumo pažymėjimo klausimyną valstybės narės, kurios pilietis yra paskirtasis Europos Sąjungos institucijų darbuotojas, NSI, prašydama atlikti patikimumo patikrinimą, skirtą gauti leidimui naudotis tam tikro slaptumo žymos lygio ESII, su kuria asmeniui reikės susipažinti.
4. Jei Komisijos saugumo institucija sužino patikimumui patikrinti svarbios informacijos apie asmenį, kuris pateikė prašymą išduoti patikimumo pažymėjimą, laikydamosi atitinkamų taisyklių ir teisės aktų, ji apie tai praneša atitinkamai NSI.
5. Užbaigusi patikimumo patikrinimą ir kaip įmanoma greičiau po to, kai gauna atitinkamos NSI patikimumo patikrinimo bendro vertinimo išvadas, Komisijos saugumo institucija:
 - a) atitinkamam asmeniui gali suteikti leidimą susipažinti su ESII ir leisti susipažinti su iki atitinkamo lygio slaptumo žyma pažymėta ESII iki nustatytos datos, bet ne ilgiau kaip 5 metus, jei patikimumo patikrinimo rezultatai užtikrintai rodo, kad neturima jokios nepalankios informacijos, kuri leistų abejoti asmens lojalumu ir patikimumu;
 - b) jei patikimumo patikrinimo rezultatai nėra tokie užtikrinantys, laikydamosi atitinkamų taisyklių ir teisės aktų apie tai praneša atitinkamam asmeniui, kuris gali prašyti, kad Komisijos saugumo institucija jį išklaustytų; Komisijos saugumo institucija gali prašyti kompetentingos NSI pateikti daugiau paaiškinimų, kuriuos ji gali pateikti pagal savo nacionalinius įstatymus ir kitus teisės aktus. Jei patikimumo patikrinimo rezultatai pasitvirtina, leidimas susipažinti su ESII neišduodamas.
6. Patikimumo patikrinimui bei gautiems rezultatams taikomi atitinkamoje valstybėje narėje galiojantys įstatymai ir kiti teisės aktai, įskaitant su apskundimu susijusius įstatymus ir kitus teisės aktus. Komisijos saugumo institucijos sprendimai gali būti apskūsti pagal Tarnybos nuostatus.
7. Komisija pripažįsta kitos Sąjungos institucijos, įstaigos ar agentūros išduotą leidimą susipažinti su ESII, su sąlyga, kad jis tebegalioja. Leidimas galioja visoms užduotims, kurias tas asmuo vykdo Komisijoje Sąjungos institucija, įstaiga ar agentūra, kurioje asmuo pradeda dirbti, praneša atitinkamai NSI apie darbdavio pasikeitimą.
8. Jeigu asmens tarnyba neprasideda per 12 mėnesių nuo patikimumo patikrinimo rezultatų pranešimo Komisijos saugumo institucijai arba jeigu asmens tarnyboje daroma 12 mėnesių pertrauka ir tuo laikotarpiu jis nedirba Komisijoje arba kitoje Sąjungos institucijoje, įstaigoje ar agentūroje arba valstybės narės nacionalinėje administracinėje įstaigoje, Komisijos saugumo institucija apie tai praneša atitinkamai NSI ir prašo patvirtinti, kad patikimumo pažymėjimas tebegalioja ir yra tinkamas.
9. Jei Komisijos saugumo institucija sužino, kad galiojantį saugumo leidimą turintis asmuo kelia saugumo riziką, Saugumo institucija, laikydamosi atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai NSI.
10. Kai NSI informuoja Komisijos saugumo instituciją apie tai, kad pagal 5 dalies a punktą suteiktas užtikrinimas dėl asmens, turinčio leidimą susipažinti su ESII, panaikinamas, Komisijos saugumo institucija gali paprašyti pateikti paaiškinimą, kurį NSI gali pateikti pagal nacionalinius įstatymus ir kitus teisės aktus. Jei atitinkama NSI patvirtina nepalankią informaciją, saugumo leidimas panaikinamas, o asmeniui neleidžiama susipažinti su ESII ir užimti pareigų, kurias eidamas jis galėtų susipažinti su ta informacija arba sukelti pavojų saugumui.
11. Apie sprendimą panaikinti arba sustabdyti asmens, kuriam taikomas šis sprendimas, leidimą susipažinti su ESII ir atitinkamais atvejais tokio panaikinimo arba sustabdymo priežastis pranešama atitinkamam asmeniui, kuris gali prašyti, kad Komisijos saugumo institucija jį išklaustytų. NSI teikiama informacija reglamentuojama atitinkamoje valstybėje narėje galiojančiais įstatymais ir kitais teisės aktais. Komisijos saugumo institucijos šiuo klausimu priimti sprendimai gali būti apskūsti pagal Tarnybos nuostatus.

12. Komisijos padaliniai užtikrina, kad į juos deleguoti nacionaliniai ekspertai, siekiantys eiti pareigas, kurioms reikia turėti saugumo leidimą susipažinti su ESII, prieš pradėdami tarnybą Komisijos saugumo institucijai pateiktą pagal nacionalinius įstatymus ir kitus teisės aktus galiojantį asmens patikimumo pažymėjimą (APP) arba asmens patikimumo pažymėjimą patvirtinančią pažymą (APPPP), kuria remdamasi Komisijos saugumo institucija išduoda saugumo leidimą susipažinti su tokio slaptumo laipsnio ESII, koks nurodytas nacionaliniame patikimumo pažymėjime; toks leidimas galioja ne ilgiau nei jų paskyrimo laikotarpis.

Asmenų, kuriems dėl jų atliekamų funkcijų suteiktas tinkamas leidimas, teisė susipažinti su ESII

13. Komisijos nariai, kurie dėl savo atliekamų pareigų pagal Sutartį gali susipažinti su ESII, informuojami apie jų saugumo įsipareigojimus ESII apsaugos srityje.

Patikimumo pažymėjimų ir saugumo leidimų registrai

14. Remiantis šiuo sprendimu, patikimumo pažymėjimų ir leidimų susipažinti su ESII registrai saugomi Komisijos saugumo institucijoje. Šiuose registruose nurodomas bent jau ESII, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos lygis, patikimumo pažymėjimo išdavimo data ir jo galiojimo laikas.

15. Komisijos saugumo institucija gali išduoti APPPP, kurioje nurodomas ESII, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos lygis (CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma), atitinkamo leidimo susipažinti su ESII galiojimo laikas ir pačios pažymos galiojimo laikas.

Saugumo leidimų atnaujinimas

16. Po to, kai patikimumo pažymėjimas suteiktas pirmą kartą, ir jeigu asmuo nuolat dirbo Europos Komisijoje arba kitoje Sąjungos institucijoje, įstaigoje ar agentūroje bei jam reikia nuolat dirbti su ESII, saugumo leidimas susipažinti su ESII peržiūrimas siekiant jį atnaujinti paprastai kas penkerius metus skaičiuojant nuo paskutinio patikimumo patikrinimo, kuriuo remiantis buvo išduotas pažymėjimas, rezultatų pranešimo datos.

17. Komisijos saugumo institucija gali pratęsti turimo saugumo leidimo galiojimo laikotarpį ne ilgiau kaip 12 mėnesių, jeigu per du mėnesius nuo prašymo atnaujinti leidimą ir su juo susijusio asmens patikimumo pažymėjimo klausimyno pateikimo dienos iš atitinkamos NSI ar kitos kompetentingos nacionalinės institucijos negauta nepalankios informacijos. Jeigu pasibaigus šiam 12 mėnesių laikotarpiui atitinkama NSI ar kita kompetentinga nacionalinė institucija Komisijos saugumo institucijai nepraneša apie savo nuomonę, asmeniui skiriamos tokios užduotys, kurioms atlikti saugumo leidimas nereikalingas.

12 straipsnis

Saugumo leidimo informaciniai susitikimai

1. Visi asmenys, kuriems išduoti leidimai susipažinti su įslaptinta informacija, dalyvauja Komisijos saugumo institucijos rengiamame saugumo leidimo informaciniame susitikime, po kurio raštu patvirtina suprantantys savo įsipareigojimus saugoti ESII ir ESII neteisėto atskleidimo pasekmes. Komisijos saugumo institucija užregistruoja tokius rašytinius patvirtinimus.

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

3. Visi asmenys, nebeeinantys pareigų, kurias einant jiems reikia susipažinti su ESII, yra informuojami apie jų įsipareigojimus toliau saugoti ESII slaptumą ir atitinkamais atvejais jie tai patvirtina raštu.

13 straipsnis

Laikini saugumo leidimai

1. Esant išskirtinėms aplinkybėms, kurios tinkamai pagrįstos tarnybos interesais, ir laukiant išsamaus patikimumo patikrinimo pabaigos, Komisijos saugumo institucija, pasikonsultavusi su valstybės narės, kurios pilietis yra atitinkamas asmuo, NSI ir atsižvelgusi į preliminarų patikrinimą, ar nėra žinomos ir susijusios nepalankios informacijos apie asmenį, rezultatus, gali jam išduoti laikiną leidimą susipažinti su ESII konkrečiai funkcijai atlikti, nepažeisdama asmens patikimumo pažymėjimų pratęsimo nuostatų. Tokie laikini leidimai susipažinti su ESII galioja vieną ne ilgesnį kaip šešių mėnesių laikotarpį ir nesuteikia teisės susipažinti su slaptumo žyma TRES SECRET UE / EU TOP SECRET pažymėta informacija

2. Pagal 12 straipsnio 1 dalies nuostatas susipažinę su informacija, visi asmenys, kuriems išduotas laikinas leidimas, raštu patvirtina, kad jie supranta išpareigojimus saugoti ESSĮ ir ESĮI neteisėto atskleidimo pasekmes. Komisijos saugumo institucija užregistruoja tokius rašytinius patvirtinimus.

14 straipsnis

Dalyvavimas Komisijos rengiamuose susitikimuose, kuriuose naudojama įslaptinta informacija

1. Komisijos padaliniai, atsakingi už susitikimų, kuriuose naudojama CONFIDENTIEL UE/ES CONFIDENTIAL ar aukštesnio lygio slaptumo žyma pažymėta įslaptinta informacija, rengimą, per savo VSP arba per susitikimo rengėją iš anksto praneša Komisijos saugumo institucijai apie tokių susitikimų datas, laiką, vietą ir dalyvius.

2. Laikantis 11 straipsnio 13 dalies nuostatų, asmenys, paskirti dalyvauti Komisijos rengiamuose susitikimuose, kuriuose naudojama CONFIDENTIEL UE/ES CONFIDENTIAL ar aukštesnio lygio slaptumo žyma pažymėta informacija, dalyvauti gali tik tuomet, jei patvirtinama, kad jų patikimumas patikrintas arba jie turi saugumo leidimą. Tokiuose susitikimuose, kuriuose naudojama įslaptinta informacija, neleidžiama dalyvauti asmenims, kurie Komisijos saugumo institucijai nepateikia APPPP arba kito patikimumo pažymėjimo įrodymo, taip pat saugumo leidimų neturintiems Komisijos darbuotojams.

3. Prieš rengdamas susitikimą, kuriame naudojama įslaptinta informacija, susitikimo rengėjas arba susitikimą rengiančio Komisijos padalinio VSP paprašo, kad išorės dalyviai Komisijos saugumo institucijai pateiktų APPPP ar kitą patikimumo pažymėjimo įrodymą. Komisijos saugumo institucija informuoja VSP arba susitikimo rengėją apie gautus APPPP ar kitus patikimumo pažymėjimų įrodymus. Jei taikoma, gali būti naudojamas suvestinis pavardžių sąrašas, kuriame pateikiami atitinkami įrodymai apie patikimumo pažymėjimą.

4. Jei kompetentingos institucijos praneša Komisijos saugumo institucijai, kad asmuo, kuris eidamas savo pareigas turi dalyvauti Komisijos rengiamuose susitikimuose, neturi asmens patikimumo pažymėjimo, Komisijos saugumo institucija apie tai praneša Komisijos padalinio, atsakingo už rengiamą susitikimą, VSP.

15 straipsnis

Galima prieiga prie ESĮI

Kurjeriams, apsaugos darbuotojams ir lydintiems asmenims išduodamas atitinkamo lygio saugumo leidimas arba jie yra kitaip deramai patikrinami vadovaujantis nacionaliniais įstatymais ir kitais teisės aktais, informuojami apie ESĮI apsaugai užtikrinti skirtas saugumo procedūras ir jiems išdėstomos jų pareigos, susijusios su jiems patikėtos tokios informacijos apsauga.

3 SKYRIUS

FIZINIS SAUGUMAS, SKIRTAS ĮSLAPTINTAI INFORMACIJAI APSAUGOTI

16 straipsnis

Pagrindiniai principai

1. Fizinio saugumo priemonės skirtos sutrukdyti įsibrauti slapčiai 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 nustatomos remiantis rizikos valdymo procesu ir laikantis šio sprendimo bei jo įgyvendinimo taisyklių.

2. Visų pirma fizinio saugumo priemonėmis siekiama 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 – darbuotojų saugumo leidimais;
- c) atgrasant nuo neteisėtų veiksmų, sutrukdant jiems bei juos nustatant ir
- d) sutrukdant asmenims įsibrauti slapčiai ar įsiveržti jėga arba juos užlaikant.

3. Fizinio saugumo priemonės taikomos visose patalpose, pastatuose, kabinetuose, salėse ir kitose zonose, kuriose tvarkoma arba saugoma ESII, įskaitant zonas, kuriose įrengtos 5 skyriuje nurodytos ryšių ir informacinės sistemos.
4. Zonos, kuriose saugoma CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta ESII, įrengiamos kaip saugumo zonos laikantis šio skyriaus nuostatų ir patvirtinamos Komisijos saugumo akreditavimo institucijos.
5. CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėtos ESII apsaugai naudojama tik Komisijos saugumo institucijos patvirtinta įranga ar prietaisai.

17 straipsnis

Fizinio saugumo reikalavimai ir priemonės

1. Fizinio saugumo priemonės nustatomos remiantis grėsmių įvertinimu, kurį atlieka Komisijos saugumo institucija, prireikus konsultuodamasi su kitais Komisijos padaliniais, kitomis ES institucijomis, agentūromis arba įstaigomis ir (arba) kompetentingoms valstybių narių institucijoms. ESII apsaugai užtikrinti savo patalpose Komisija 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) ESII slaptumo žymos lygį;
 - b) ESII formą ir kiekį, atsižvelgiant į tai, kad dideliame ESII kiekiui ar rinkiniui apsaugoti gali reikėti taikyti griežtesnes apsaugos priemones;
 - c) pastatus ar zonas, kuriose laikoma ESII, supančią aplinką ir jų struktūrą ir
 - d) įvertintą žvalgybos tarnybų, kurių veikla nukreipta prieš Sąjungą, jos institucijas, įstaigas ar agentūras arba prieš valstybes nares, keliamą grėsmę ir grėsmę dėl sabotažo, terorizmo, ardomosios arba kitų rūšių nusikalstamos veikos.
2. Komisijos saugumo institucija, taikydama nuodugnios apsaugos sąvoką, nustato tinkamas įgyvendintinas fizinio saugumo priemones. Tuo tikslu Komisijos saugumo institucija parengia būtiniausius standartus, normas ir kriterijus, nustatytus įgyvendinimo taisyklėse.
3. Komisijos saugumo institucijai leidžiama apieškoti įeinančius ir išeinančius asmenis siekiant atgrasyti, kad į patalpas arba pastatus be leidimo nebūtų įnešama medžiaga arba iš jų be leidimo nebūtų išnešama ESII.
4. Iškilus pavojui, kad ESII bus pamatyta, netgi atsitiktinai, atitinkami Komisijos padaliniai imasi tinkamų Komisijos saugumo institucijos nustatytų priemonių siekiant išvengti šio pavojaus.
5. Naujos infrastruktūros atveju fizinio saugumo reikalavimai ir jos funkcinės specifikacijos apibrėžiami infrastruktūros planavimo ir projektavimo metu konsultuojantis su Komisijos saugumo institucija. Esamų infrastruktūrų fizinio saugumo reikalavimai įgyvendinami laikantis įgyvendinimo taisyklėse nustatytų būtiniausių standartų, normų ir kriterijų.

18 straipsnis

ESII fizinei apsaugai skirta įranga

1. ESII fizinės apsaugos tikslais nustatomos dviejų tipų fiziškai apsaugotos zonos:
 - a) administracinės zonos ir
 - b) saugios zonos (įskaitant techniniu požiūriu saugias zonas).
2. Komisijos saugumo akreditavimo institucija nustato, ar zona atitinka reikalavimus, kad būtų laikoma administracine zona, saugia zona ar techniniu požiūriu saugia zona.
3. Administracinių zonų atveju:
 - a) nustatomas aiškiai apribotas plotas, kad būtų galima tikrinti asmenis ir, jei įmanoma, transporto priemones;
 - b) į šias zonas įeiti nelydimiems leidžiama tik tiems asmenims, kuriems Komisijos saugumo institucija ar bet kuri kita kompetentinga institucija suteikė tinkamą leidimą, ir
 - c) visi kiti asmenys visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

4. Saugių zonų atveju:

- a) nustatomas aiškiai apribotas ir saugomas plotas, 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, nes jiems „būtina žinoti“;
- c) visi kiti asmenys turi būti visą laiką lydimi arba jiems turi būti taikomos lygiavertės kontrolės priemonės.

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

- a) aiškiai nurodomas paprastai zonoje laikomos informacijos aukščiausio slaptumo žymos lygis;
- b) visi lankytojai privalo turėti specialų leidimą, suteikiantį teisę įeiti į zoną, turi būti visą laiką lydimi ir jų patikimumas turi būti tinkamai patikrinamas, nebent imtasi priemonių užtikrinti, kad nebūtų įmanoma susipažinti su ESII.

6. Nuo pasiklausymo apsaugotos saugios zonos klasifikuojamos kaip techniniu požiūriu saugios zonos. Taikomi šie papildomi reikalavimai:

- a) tokiose zonose įdiegiama įsibrovimo aptikimo sistema (IAS) ir, kai jose nedirbama, jos turi būti rakinamos, o kai dirbama – saugomos. Visi raktai valdomi vadovaujantis 20 straipsniu;
- b) visi į tokias zonas įeinantys asmenys ar įnešamos medžiagos kontroliuojami;
- c) tokios zonos reguliariai fiziškai ir (arba) techniškai tikrinamos Komisijos saugumo institucijos. Be to, tokie patikrinimai atliekami, kai į zoną buvo įeita be leidimo ar įtariama apie tokį įėjimą, 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.

7. Nepaisant 6 punkto d papunkčio, prieš naudojantis ryšių prietaisais ir elektros ar elektronine įranga zonose, kuriose rengiami susitikimai ar atliekamas darbas, susijęs su SECRET UE/ES SECRET arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, taip pat kai grėsmė ESII vertinama kaip didelė, tokius prietaisus ir įrangą visų pirma ištiria Komisijos saugumo institucija, siekdama užtikrinti, kad naudojantis šia įranga nebūtų galima perduoti jokios suprantamos informacijos per neapdairumą ar neteisėtai už saugios zonos ploto.

8. Saugios zonos, kuriose nėra visą parą budinčio personalo, atitinkamais atvejais tikrinamos pasibaigus įprastoms darbo valandoms ir atsitiktiniais intervalais ne įprastomis darbo valandomis, išskyrus atvejus, kai įdiegta IAS.

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

10. Atitinkamo Komisijos padalinio VSP parengia kiekvienos saugios zonos, už kurią jis atsakingas, saugios eksploatacijos taisykles (SET), kuriose, laikantis šio sprendimo ir jo įgyvendinimo taisyklių, nurodoma:

- a) ESII, kuri gali būti tvarkoma ir saugoma toje zonoje, slaptumo žymos lygis;
- b) įdiegtinos stebėjimo ir apsaugos priemonės;
- c) kokiems asmenims leidžiama nelydimiems įeiti į zoną, vadovaujantis principu, kad jiems „būtina žinoti“, ir jų saugumo leidimais;
- d) atitinkamais atvejais palydos tvarka ir ESII apsaugos tvarka, kai kitiems asmenims leidžiama įeiti į zoną;
- e) bet kurios kitos atitinkamos priemonės ir procedūros.

11. Saugiose zonose įrengiamos saugyklos. Sienos, grindys, lubos, langai ir durys su užraktais patvirtinamos Komisijos saugumo institucijos ir užtikrina apsaugą, kurią užtikrina apsauginės talpyklos, patvirtintos to paties lygio slaptumo žymos ESII saugoti.

19 straipsnis

Fizinės apsaugos priemonės tvarkant ir saugant ESĮ

1. Slaptumo žyma RESTREINT UE/ES RESTRICTED pažymėta ESĮ gali būti tvarkoma:
 - a) saugiose zonose;
 - b) administracinėse zonose, jeigu ESĮ yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys, arba
 - c) ne saugiose zonose ar administracinėse zonose, jeigu turėtojas gabena ESĮ pagal 31 straipsnį ir yra įsipareigojęs taikyti kompensacines priemones, nustatytas įgyvendinimo priemonėse, kad būtų užtikrinta, jog ESĮ yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys.
2. Slaptumo žyma RESTREINT UE/ES RESTRICTED pažymėta ESĮ saugoma tinkamuose rakinamuose biuro balduose administracinėse zonose arba saugiose zonose. Ji gali būti laikinai saugoma ne administracinėse zonose arba ne saugiose zonose, jeigu turėtojas yra įsipareigojęs taikyti kompensacines priemones, nustatytas įgyvendinimo priemonėse.
3. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET pažymėta ESĮ gali būti tvarkoma:
 - a) saugiose zonose;
 - b) administracinėse zonose, jeigu ESĮ yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys, arba
 - c) ne saugiose zonose ar administracinėse zonose, jeigu turėtojas:
 - i) yra įsipareigojęs taikyti kompensacines priemones, nustatytas įgyvendinimo priemonėse, kad būtų užtikrinta, jog ESĮ yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys;
 - ii) visą laiką asmeniškai kontroliuoja ESĮ ir
 - iii) jei dokumentai yra popierinio pavidalo, apie tai pranešė atitinkamai registratūrai.
4. Slaptumo žyma CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėta ESĮ saugoma saugiose zonose esančiose apsauginėse talpyklose arba saugyklose.
5. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta ESĮ tvarkoma saugiose zonose, kurias sukuria ir tvarko Komisijos saugumo institucija ir kurias Komisijos saugumo akreditavimo institucija akredituoja kaip to saugias zonas.
6. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta ESĮ saugoma Komisijos saugumo akreditavimo institucijos akredituotose tokio lygio saugiose zonose laikantis kurios nors iš toliau nurodytų sąlygų:
 - a) apsauginėje talpykloje laikantis 18 straipsnio nuostatų, taikant vieną ar kelias iš toliau nurodytų kontrolės priemonių:
 - 1) nuolatinė apsauga arba tikrinimas, kurį vykdo apsaugos arba budintis personalas, kurio patikimumas patikrintas;
 - 2) patvirtinta ĮAS kartu veikiant apsaugos reagavimo personaluiarba
 - b) saugykloje su įrengta ĮAS kartu veikiant apsaugos reagavimo personalui.

20 straipsnis

ESĮ apsaugai užtikrinti naudojamų raktų ir kodų kontrolė

1. Kabinetų, patalpų, saugyklų ir apsauginių talpyklų raktų bei kodų valdymo procedūros nustatomos įgyvendinimo taisyklėse remiantis 60 straipsniu. Tokių procedūrų tikslas – apsaugoti nuo susipažinimo su informacija neturint leidimo.
2. Kodus įsimena kuo mažesnis asmenų, kuriems būtina juos žinoti, skaičius. Apsauginių talpyklų ir saugyklų, kuriose saugoma ESĮ, kodai keičiami:
 - a) gavus naują talpyklą;
 - b) pasikeitus kodus žinančiam personalui;
 - c) neteisėtai atskleidus kodus arba įtarus jų neteisėtą atskleidimą;
 - d) po spynos techninio patikrinimo ar remonto ir
 - e) bent kas 12 mėnesių.

4 SKYRIUS

ES ĮSLAPTINTOS INFORMACIJOS VALDYMAS

21 straipsnis

Pagrindiniai principai

1. Visi ESĮ dokumentai turėtų būti tvarkomi laikantis Komisijos politikos dėl dokumentų tvarkymo, todėl jie turėtų būti užregistruojami, kataloguojami, saugomi ir galiausiai sunaikinami, atrenkami arba perduodami istoriniams archyvams laikantis bendro Europos Komisijos bylų saugojimo sąrašo.
2. CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija saugumo tikslais registruojama prieš ją platinant ir ją gavus. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija registruojama tam skirtose registratūrose.
3. Komisijos ESĮ registravimo sistema sukurama remiantis 27 straipsnio nuostatomis.
4. Komisijos padalinius ir patalpas, kuriuose ESĮ tvarkoma arba saugoma, reguliariai tikrina Komisijos saugumo institucija.
5. Už fiziškai apsaugotų zonų ribų ESĮ iš vienos tarnybos į kitą ir iš vienos patalpų į kitas perduodama šiais būdais:
 - a) paprastai ESĮ perduodama elektroninėmis priemonėmis apsaugant informaciją pagal 5 skyrių patvirtintomis kriptografinėmis priemonėmis;
 - b) kai nenaudojamos a punkte nurodytos priemonės, ESĮ gabenama:
 - i) elektroninėse laikmenose (pvz., USB atmintinėse, kompaktiniuose diskuose, kietuosiuose diskuose), informaciją apsaugant pagal 5 skyrių patvirtintomis kriptografinėmis priemonėmis, arba
 - ii) visais kitais atvejais – kaip nurodyta įgyvendinimo taisyklėse.

22 straipsnis

Slaptumo ir kitos žymos

1. Informacija įslaptinama tuo atveju, jei dėl jos konfidencialumo reikia ją apsaugoti pagal 3 straipsnio 1 dalį.
2. ESĮ rengėjas atsako už slaptumo žymos lygio nustatymą pagal atitinkamas įgyvendinimo taisykles, įslaptinimo standartus ir gaires ir už pirminį informacijos platinimą.
3. ESĮ slaptumo žymos lygis nustatomas vadovaujantis 3 straipsnio 2 dalimi ir susijusiomis įgyvendinimo nuostatomis.
4. Slaptumo žyma nurodoma aiškiai ir teisingai, neatsižvelgiant į tai, ar ESĮ yra pateikiama popieriuje, žodžiu, elektronine ar bet kuria kita forma.
5. Atskiroms dokumento dalims (t. y. puslapiams, pastraipoms, skirsniams, priedams ir priedėliams) gali būti suteikiamos skirtingos slaptumo žymos ir jos atitinkamai pažymimos, taip pat tais atvejais, kai jos saugomos elektronine forma.
6. Dokumento ar dokumentų bylos bendras slaptumo žymos lygis nustatomas bent pagal aukščiausią slaptumo žymos lygį turinčią jų dalį. Kai renkama informacija iš įvairių šaltinių, galutinis dokumentas peržiūrimas siekiant nustatyti jo bendrą slaptumo žymos lygį, nes gali prireikti jam suteikti aukštesnį slaptumo žymos lygį nei jo dalims.
7. Kiek įmanoma, dokumentams, kurių dalys pažymėtos skirtingo lygio slaptumo žymomis, suteikiama tokia struktūra, kad skirtingo lygio slaptumo žymomis pažymėtas dalis būtų galima lengvai nustatyti ir prireikus atskirti.
8. Su priedais pateikiamų dokumentų slaptumo žymos laipsnis atitinka priedų aukščiausio laipsnio slaptumo žymas. Jei tokie dokumentai pateikiami atskirai nuo priedų, įslaptintos informacijos rengėjas aiškiai nurodo, koks slaptumo žymos lygis jiems suteikiamas, naudodamas atitinkamą žymą, pavyzdžiui:

CONFIDENTIEL UE/ES CONFIDENTIAL

Be priedo (-ų) RESTREINT UE/ES RESTRICTED

23 straipsnis

Žymos

Be vienos iš slaptumo žymų, nurodytų 3 straipsnio 2 dalyje, ESĮI gali būti pažymėta papildomomis žymomis, pavyzdžiui:

- a) identifikatoriumi, kuriuo nurodomas įslaptintos informacijos rengėjas;
- b) bet kuriomis žymomis, kodiniais žodžiais ar santrumpomis, kuriais nurodoma veiklos sritis, su kuria dokumentas yra susijęs, jo specialus platinimas vadovaujantis principu „būtina žinoti“ arba naudojimo apribojimais;
- c) paskirstymo žymomis;
- d) jei taikoma, nurodant datą ar konkretų įvykį, po kurio informacijos slaptumas gali būti sumažintas arba ji gali būti išslaptinta.

24 straipsnis

Žymų santrumpos

1. Nurodant atskirų teksto pastraipų slaptumo žymos lygį gali būti naudojamos standartinės slaptumo žymų santrumpos. Santrumpos nepakeičia visais žodžiais nurodytų slaptumo žymų.
2. ES įslaptintuose dokumentuose gali būti naudojamos šios standartinės santrumpos, kuriomis nurodomas skirsnių arba teksto dalių, užimančių mažiau nei vieną puslapį, slaptumo žymos lygis:

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

25 straipsnis

ESĮI rengimas

1. Rengiant ES įslaptintą dokumentą:
 - a) kiekvienas puslapis aiškiai pažymimas slaptumo žyma;
 - b) kiekvienas puslapis numeruojamas;
 - c) dokumente nurodomas jo registracijos numeris ir tema, kurie nėra įslaptinta informacija, išskyrus tuos atvejus, kai jie pažymėti kaip įslaptinta informacija;
 - d) dokumente nurodoma data;
 - e) jei platinamos kelios dokumentų, pažymėtų SECRET UE/ES SECRET ar aukštesnio lygio slaptumo žyma, kopijos, kiekvienos iš jų kiekviename puslapyje nurodomas kopijos numeris.
2. Kai rengiant ESĮI neįmanoma taikyti 1 dalyje išdėstytų reikalavimų, remiantis įgyvendinimo taisyklėmis taikomos kitos tinkamos priemonės.

26 straipsnis

ESĮI slaptumo mažinimas ir ESĮI išslaptinimas

1. Įslaptintos informacijos rengėjas, kai įmanoma, rengdamas ESĮI nurodo, ar tam tikrą dieną arba po tam tikro įvykio galima sumažinti ESĮI slaptumą arba ją išslaptinti.
2. Kiekviena Komisijos tarnyba reguliariai peržiūri savo parengtą ESĮI, siekdama įsitikinti, ar slaptumo žymos lygis vis dar taikomas. Įgyvendinimo taisyklėse nustatoma sistema, skirta Komisijos parengtos registruotos ESĮI slaptumo žymos lygiui peržiūrėti ne rečiau kaip kas penkerius metus. Tokia peržiūra nėra reikalinga, jeigu įslaptintos informacijos rengėjas iš pat pradžių nurodo, kad informacijos slaptumas bus sumažintas arba informacija išslaptinta automatiškai, o informacija buvo atitinkamai pažymėta.

3. Komisijos parengta informacija, pažymėta slaptumo žyma RESTREINT UE/ES RESTRICTED, remiantis Reglamentu (EEB, Euratomas) Nr. 354/83 su pakeitimais, padarytais Tarybos reglamentu (EB, Euratomas) Nr. 1700/2003 ⁽¹⁾ automatiškai laikoma visiškai išslaptinta praėjus trisdešimčiai metų.

27 straipsnis

ESII registravimo sistema Komisijoje

1. Nedarant poveikio 52 straipsnio 5 daliai, kiekviename Komisijos padalinyje, kuriame tvarkoma arba saugoma ESII, pažymėta CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET slaptumo žyma, nustatoma atsakinga vietinė ESII registratūra, siekiant užtikrinti, kad ESII būtų tvarkoma pagal šį sprendimą.
2. Generalinio sekretoriato valdoma ESII registratūra yra centrinė Komisijos ESII registratūra. Ji veikia kaip:
 - vietinė Komisijos Generalinio sekretoriato ESII registratūra,
 - privačių Komisijos narių kabinetų ESII registratūra, išskyrus atvejus, kai jiems paskirta vietinė ESII registratūra,
 - generalinių direktoratų arba tarnybų, kuriose nėra vietinės ESII registratūros, ESII registratūra,
 - pagrindinis visos informacijos, pažymėtos RESTREINT UE/ES RESTRICTED ir aukštesne, įskaitant SECRET UE/ES SECRET, slaptumo žyma, kuria keičiasi Komisija ir jos tarnybos su trečiosiomis valstybėmis bei tarptautinėmis organizacijomis, bei, kai tai numatyta specialia tvarka, kitos Sąjungos institucijos, agentūros ir įstaigos, gavimo ir išsiuntimo punktas.
3. Komisijos saugumo institucija Komisijoje įsteigia centrinę registratūrą, kuri veikia kaip centrinė slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtą informaciją gaunanti ir siunčianti institucija. Prireikus gali būti paskirtos antrinės registratūros, kurios tvarko tokią informaciją jos registravimo tikslais.
4. Antrinės registratūros negali perduoti slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtų dokumentų tiesiogiai kitoms tos pačios centrinės TRES SECRET UE/ES TOP SECRET registratūros antrinėms registratūroms arba į išorę be aiškaus rašytinio centrinės registratūros leidimo.
5. ESII registratūros įrengiamos kaip 3 skyriuje nurodytos saugios zonos ir akredituojamos Komisijos saugumo akreditavimo institucijos (SAI).

28 straipsnis

Registracijos kontrolės pareigūnas

1. Kiekvieną ESII registratūrą valdo registracijos kontrolės pareigūnas (RKP).
2. RKP turi tinkamą patikimumo pažymėjimą.
3. RKP veiklą Komisijos padalinyje, susijusią su ESII dokumentų tvarkymo nuostatų taikymu ir atitinkamų saugumo taisyklių laikymusi, prižiūri vietos saugumo pareigūnas (VSP).
4. ESII registratūros, į kurią paskirtas, valdymo užduotis vykdančiam RKP pagal šį sprendimą ir atitinkamas įgyvendinimo taisykles, standartus ir gaires tenka šios bendros užduotys:
 - valdyti veiksmus, susijusius su informacijos registravimu, saugojimu, kopijavimu, vertimu, perdavimu, siuntimu ir naikinimu arba perdavimu ESII istorinių archyvų tarnybai,
 - periodiškai tikrinti, ar būtina, kad informacija išliktų išslaptinta,
 - atlikti bet kokias kitas su ESII apsauga susijusias įgyvendinimo taisyklėse nustatytas užduotis.

29 straipsnis

ESII registravimas saugumo tikslais

1. Šiame sprendime registravimas saugumo tikslais (toliau – registravimas) – procedūrų, kuriomis užregistruojamas ESII gyvavimo ciklas, įskaitant jos platinimą, taikymas.

⁽¹⁾ 2003 m. rugėjo 22 d. Tarybos reglamentas (EB, Euratomas) Nr. 1700/2003, iš dalies keičiantis Reglamentą (EEB, Euratomas) Nr. 354/83 dėl Europos ekonominės bendrijos ir Europos atominės energijos bendrijos istorinių archyvų atvėrimo visuomenei (OL L 243, 2003 9 27, p. 1).

2. Organizacinis vienetas, gavęs CONFIDENTIEL UE/ES CONFIDENTIAL ir aukštesnio lygio slaptumo žyma pažymėtą informaciją ar medžiagą arba ją išsiuntęs, ją užregistruoja tam skirtose registratūrose.
3. Kai ESII tvarkoma arba saugoma naudojant ryšių ir informacinę sistemą (RIS), registravimo procedūros gali būti atliekamos vykdamas procesus pačioje RIS.
4. Išsamesnės ESII registravimo saugumo tikslais nuostatos numatomos įgyvendinimo taisyklėse.

30 straipsnis

ES įslaptintų dokumentų kopijavimas ir vertimas

1. Slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėti dokumentai kopijuojami arba verčiami tik gavus išankstinį rašytinį įslaptintos informacijos rengėjo sutikimą.
2. Jeigu SECRET UE/ES SECRET arba žemesnio lygio slaptumo žyma pažymėtų dokumentų rengėjas nenustatė apribojimų dėl jų kopijavimo ar vertimo, dokumento turėtojo nurodymu tokius dokumentus galima kopijuoti arba versti.
3. Dokumento kopijoms ir vertimams taikomos tokios pat saugumo priemonės kaip ir dokumento originalui.

31 straipsnis

ESII gabenimas

1. ESII gabenama taip, kad pervežama būtų apsaugota nuo neteisėto atskleidimo.
2. Gabenant ESII taikomos apsaugos priemonės, kurios:
 - atitinka gabenamos ESII slaptumo žymos lygį ir
 - pritaikytos prie ypatingų jos gabenimo sąlygų, visų pirma atsižvelgiant į tai, ar ESII gabenama:
 - Komisijos pastate arba uždaroje Komisijos pastatų grupėje,
 - tarp Komisijos pastatų, esančių toje pačioje valstybėje narėje,
 - Sąjungoje,
 - iš Sąjungos į trečiosios valstybės teritoriją ir
 - pritaikytos prie ESII pobūdžio ir formos.
3. Šios apsaugos priemonės išsamiai nustatomos įgyvendinimo taisyklėse arba, kai įgyvendinami 42 straipsnyje nurodyti projektai ir programos, – yra neatsiejama atitinkamos programos ar projekto saugumo instrukcijų (PSI) dalis.
4. Į įgyvendinimo taisyklės arba PSI įtraukiamos nuostatos, atitinkančios ESII slaptumo žymos lygį, susijusios su:
 - gabenimo rūšimis, kaip antai, ar informaciją gabena kurjeris, diplomatinis arba karinis kurjeris, ar ji gabenama pašto tarnybomis arba komercinėmis kurjerių pašto tarnybomis,
 - ESII pakuotėmis,
 - techninėmis apsaugos priemonėmis, kai ESII gabenama elektroninėje laikmenoje,
 - bet kokiomis kitomis procedūrinėmis, fizinėmis arba elektroninėmis priemonėmis,
 - registravimo procedūromis,
 - saugumo leidimus turinčių darbuotojų naudojimu.
5. Kai ESII gabenama elektroninėje laikmenoje ir nepaisant 21 straipsnio 5 dalies, atitinkamose įgyvendinimo taisyklėse nustatytos apsaugos priemonės gali būti papildytos Komisijos saugumo institucijos patvirtintomis techninėmis apsaugos priemonėmis, kad būtų sumažinta informacijos praradimo arba atskleidimo rizika.

32 straipsnis

ESĮI sunaikinimas

1. Nebereikalingi ES įslaptinti dokumentai gali būti sunaikinti, laikantis teisės aktų dėl archyvų ir Komisijos dokumentų tvarkymo ir archyvavimo taisyklių bei nuostatų, visų pirma bendrojo visos Komisijos informacijos saugojimo sąrašo.
2. Informacijos turėtojo arba kompetentingos institucijos nurodymu už ESĮI registratūrą atsakingas RKP sunaikina CONFIDENTIEL UE/ES CONFIDENTIAL ir aukštesnio lygio slaptumo žyma pažymėtą ESĮI. RKP atitinkamai atnaujiną registrų knygos ir kitą registravimo informaciją.
3. Dokumentus, pažymėtus SECRET UE/ES SECRET arba TRES SECRET UE/ES TOP SECRET slaptumo žyma, RKP naikina dalyvaujant liudytojui, kuris turi leidimą susipažinti su ne žemesnio už naikinamo dokumento slaptumo žymos lygio įslaptinta informacija.
4. Už registrą atsakingas darbuotojas ir liudytojas, kai pastarojo dalyvavimas privalomas, pasirašo sunaikinimo aktą, kuris įtraukiamas į atitinkamą registrą. Už ESĮI registrą atsakingas RKP slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėtų dokumentų sunaikinimo aktus registre saugo ne trumpiau kaip dešimt metų, o CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET slaptumo žyma pažymėtų dokumentų sunaikinimo aktus – ne trumpiau kaip penkerius metus.
5. Įslaptinti dokumentai, įskaitant pažymėtus RESTREINT UE/ES RESTRICTED slaptumo žyma, sunaikinami įgyvendinimo taisyklėse nustatytais būdais, atitinkančiais atitinkamus ES arba lygiaverčius standartus.
6. Įslaptintai informacijai saugoti naudotos kompiuterinių duomenų saugojimo laikmenos sunaikinamos laikantis įgyvendinimo taisyklėse nustatytų procedūrų.

33 straipsnis

ESĮI sunaikinimas ekstremaliosios padėties atveju

1. ESĮI tvarkantys Komisijos padaliniai, atsižvelgdami į vietos sąlygas, parengia ES įslaptintos medžiagos apsaugojimo kriziniais atvejais planus, kurie prireikus gali apimti ir sunaikinimo ar evakuacijos ekstremaliosios padėties atveju planus. Juose pateikiami nurodymai, kurių reikia laikytis norint apsaugoti ESĮI nuo patekimo į leidimo ja naudotis neturinčių asmenų rankas.
2. Priemonės, skirtos slaptumo žymomis CONFIDENTIEL UE/ES CONFIDENTIAL ir SECRET UE/ES SECRET pažymėtai medžiagai apsaugoti ir (arba) sunaikinti kriziniais atvejais, jokiais aplinkybėmis neturi pakenkti medžiagos, pažymėtos slaptumo žyma TRES SECRET UE/ES TOP SECRET, apsaugai arba sutrukdyti ją, taip pat ir šifravimo įrangą sunaikinti – tai padaryti yra aukščiausio prioriteto užduotis.
3. Ekstremaliosios padėties atveju, jei gresia tiesioginis neteisėto atskleidimo pavojus, ESĮI turėtojas sunaikina ją taip, kad ji negalėtų būti atkurta visa arba iš dalies. Rengėjas ir pirminė registratūra informuojami apie registruotos ESĮI sunaikinimą dėl ekstremaliosios padėties.
4. Išsamesnės ESĮI naikinimo nuostatos numatomos įgyvendinimo taisyklėse.

5 SKYRIUS

ES ĮSLAPTINTOS INFORMACIJOS APSAUGA RYŠIŲ IR INFORMACINĖSE SISTEMOSE (RIS)

34 straipsnis

Pagrindiniai informacijos saugumo užtikrinimo principai

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.

2. Veiksmingu informacijos saugumo užtikrinimu garantuojamas tinkamas lygis:
- Autentiškumo: užtikrinimas, kad informacija yra tikra ir gauta iš *bona fide* šaltinių;
- Prieinamumo: galimybė leidimą turinčiam subjektui pateikus prašymą gauti informaciją ir ja naudotis;
- Konfidencialumo: savybė, kuri reiškia, kad informacija nėra atskleidžiama leidimo neturintiems asmenims ir subjektams arba panaudojama neteisėtiems procesams;
- Vientisumo: savybė, kuri reiškia, kad apsaugomas turto ir informacijos tikslumas ir visuma;
- Nepaneigiamumo: galimybė įrodyti, kad veiksmas buvo atliktas ar įvykis įvyko, kad šio įvykio ar veiksmo paskui to nebūtų galima užginčyti.
3. ISU grindžiamas rizikos valdymo procesu.

35 straipsnis

Apibrėžtys

Šiame skyriuje vartojamų terminų apibrėžtys:

- a) akreditavimas – saugumo akreditavimo institucijos (SAI) suteiktas oficialus leidimas ir patvirtinimas, kad ryšių ir informacinės sistemos veiklos aplinkoje galima tvarkyti ESĮ; jis suteikiamas po oficialaus saugumo plano patvirtinimo ir tinkamo jo įgyvendinimo;
- b) akreditavimo procesas – būtini veiksmai ir užduotys, kuriuos privaloma atlikti siekiant gauti saugumo akreditavimo institucijos akreditavimą. Šie veiksmai bei užduotys nurodomi akreditavimo proceso standartuose;
- c) ryšių ir informacinė sistema (RIS) – sistema, sudaranti sąlygas tvarkyti informaciją elektroniniu būdu. Ryšių ir informacinė sistema apima visas sistemos dalis, kurių reikia jos veikimui užtikrinti, įskaitant infrastruktūrą, organizavimą, personalą ir informacijos išteklius;
- d) 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;
- e) 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;
- f) rizikos pripažinimas – valdant riziką priimtas sprendimas pripažinti, kad vis dar yra likutinė rizika;
- g) rizikos įvertinimas – grėsmių ir pažeidžiamų sričių nustatymas bei susijusios rizikos analizės, t. y. galimumo ir poveikio analizės, atlikimas;
- h) informavimas apie riziką – RIS vartotojų bendruomenės informuotumo apie riziką didinimas, patvirtinimo institucijų informavimas apie tokią riziką ir pranešimų vykdančiosioms institucijoms teikimas;
- i) rizikos valdymas – rizikos silpninimas, šalinimas, mažinimas (taikant tinkamas technines, fizines, organizacines arba procedūrines priemones), perkėlimas arba stebėjimas.

36 straipsnis

RIS, kuriose tvarkoma ESĮ

1. RIS sistemose ESĮ tvarkoma laikantis ISU principo.
2. RIS sistemoms, kuriose tvarkoma ESĮ, taikoma Komisijos informacinių sistemų saugumo politika, apibrėžta Komisijos sprendime C(2006) 3602 ⁽¹⁾:
- a) įgyvendinant informacinių sistemų saugumo politiką visą informacinių sistemų gyvavimo ciklą taikomas principas „planuoti-daryti-tikrinti-veikti“;
 - b) atliekant veiklos poveikio vertinimą turi būti nustatomi saugumo poreikiai;
 - c) oficialiai klasifikuojamas informacinės sistemos inventorių ir joje kaupiami duomenys;

⁽¹⁾ 2006 m. rugpjūčio 16 d. Sprendimas C(2006) 3602 dėl Europos Komisijos naudojamų informacinių sistemų saugumo.

- d) privaloma taikyti visas privalomas saugumo priemones, nustatytas įgyvendinant informacinių sistemų saugumo politiką;
 - e) privaloma taikyti rizikos valdymo procesą, kurį sudaro šie etapai: grėsmių ir pažeidžiamumo nustatymas, rizikos vertinimas, rizikos tvarkymas, rizikos pripažinimas ir informavimas apie riziką;
 - f) rengiamas, įgyvendinamas, tikrinamas ir peržiūrimas saugumo planas, įskaitant saugumo politiką ir saugios eksploatacijos taisykles.
3. Visi darbuotojai, dalyvaujantys kuriant, plėtojant, bandant, eksploatuojant, valdant ar naudojant RIS, kuriose tvarkoma ESII, SAS praneša apie visus galimus saugumo trūkumus, incidentus, pažeidimus arba neteisėto atskleidimo atvejus, kurie gali daryti poveikį RIS ir (arba) joje tvarkomos ESII apsaugai.
4. Kai ESII apsauga užtikrinama kriptografinėmis priemonėmis, tokios priemonės patvirtinamos taip:
- a) pirmenybė teikiama priemonėms, kurias patvirtino Taryba arba Tarybos Generalinis sekretorius, vykdamas Tarybos kriptografijos patvirtinimo institucijos funkcijas, remdamiesi Komisijos saugumo ekspertų grupės rekomendacija;
 - b) kai tai pateisinama konkrečiomis su veikla susijusiomis priežastimis, Komisijos kriptografijos patvirtinimo institucija (KPI) gali, remdamasi Komisijos saugumo ekspertų grupės rekomendacija, netaikyti a punkte nurodytų reikalavimų ir suteikti laikiną patvirtinimą tam tikram laikotarpiui.
5. ESII perduodant, tvarkant ir saugant elektroninėmis priemonėmis, naudojamos patvirtintos kriptografinės priemonės. Nepaisant šio reikalavimo, esant ekstremaliajai padėčiai arba specifinių techninių konfigūracijų atvejais gali būti taikomos KPI patvirtintos specialios procedūros.
6. Įgyvendinamos saugumo priemonės, siekiant apsaugoti RIS, kuriose tvarkoma CONFIDENTIEL UE/ES CONFIDENTIAL arba aukštesnio lygio slaptumo žyma pažymėta informacija, kad tokia informacija negalėtų būti neteisėtai atskleista dėl netyčinio elektromagnetinio spinduliavimo (TEMPEST apsaugos priemonės). Tokios apsaugos priemonės turi būti proporcingos neteisėto pasinaudojimo informacija rizikai ir informacijos slaptumo žymos lygiui.
7. Komisijos saugumo institucija vykdo šias funkcijas:
- ISU institucijos (ISUI),
 - Saugumo akreditavimo institucijos (SAI),
 - TEMPEST institucijos (TEI),
 - Kriptografijos patvirtinimo institucijos (KPI),
 - Kriptografijos platinimo institucijos (KPLI).
8. Komisijos saugumo institucija paskiria kiekvienos sistemos ISU operacinę instituciją.
9. 7 ir 8 dalyse nurodytų funkcijų vykdymo pareigos bus nustatytos įgyvendinimo taisyklėse.

37 straipsnis

RIS, kuriose tvarkoma ESII, akreditavimas

1. Visų RIS, kuriose tvarkoma ESII, akreditavimo procesas vykdomas remiantis ISU principais, kurių išsamumo lygis turi atitikti reikiamą apsaugos lygį.
2. Akreditavimo procesas apima oficialų Komisijos SAS pateikiamą atitinkamos RIS saugumo plano patvirtinimą siekiant įsitikinti, kad:
 - a) buvo tinkamai atliktas 36 straipsnio 2 dalyje nurodytas rizikos valdymo procesas;
 - b) sistemos savininkas žino apie likutinės rizikos pavojų ir su tuo sutinka ir
 - c) laikantis šio sprendimo pasiektas pakankamas RIS ir joje tvarkomos ESII apsaugos lygis.

3. Komisijos SAI išduoda akreditavimo pareiškimą, kuriame nurodytas aukščiausias ESII, kuri gali būti tvarkoma RIS, slaptumo žymos lygis ir atitinkami veiklos reikalavimai bei sąlygos. Tai nedaro poveikio Saugumo akreditavimo valdybos, apibrėžtos Europos Parlamento ir Tarybos reglamento (ES) Nr. 512/2014 ⁽¹⁾ 11 straipsnyje, užduotims.
4. Jungtinė saugumo akreditavimo valdyba (SAV) atsakinga už Komisijos RIS, kuriose dalyvauja keletas šalių, akreditavimą. Valdybą sudaro po vieną kiekvienos dalyvaujančios šalies SAI atstovą, o jos posėdžiams pirmininkauja Komisijos SAI atstovas.
5. Akreditavimo procesą sudaro įvairios užduotys, kurias vykdo dalyvaujančios šalys. Už akreditavimo bylų ir dokumentų rengimą atsako tik sistemos RIS savininkas.
6. Už akreditavimą atsakinga Komisijos SAI, kuri bet kuriuo RIS gyvavimo ciklo etapu turi teisę:
 - a) reikalauti, kad būtų taikomas akreditavimo procesas;
 - b) atlikti RIS auditą arba patikrą;
 - c) jei nebesilaikoma veikimo sąlygų, reikalauti, kad per aiškiai apibrėžtą laikotarpį būtų nustatytas ir veiksmingai įgyvendinamas saugumo gerinimo planas, o jei reikia, panaikinti RIS veiklos leidimą, kol vėl bus laikomasi veikimo sąlygų.
7. Akreditavimo procesas nustatomas RIS, kuriose tvarkoma ESII, akreditavimo proceso standarte, kuris patvirtinamas remiantis Komisijos sprendimo C(2006) 3602 10 straipsnio 3 dalimi.

38 straipsnis

Ekstremalioji padėtis

1. Nepaisant šio skyriaus nuostatų, toliau apibūdintos specialios procedūros gali būti taikomos esant ekstremaliajai padėčiai, pavyzdžiui, gresiant ar esant krizei, konfliktui ar karinei padėčiai arba susidarius išskirtinėms veiklos sąlygoms.
2. ESII gali būti perduodama naudojant kriptografinės priemonės, kurios buvo patvirtintos žemesnio įslaptinimo lygio informacijai, arba nešifruota kompetentingai institucijai pritarus, jei vėlavimas padarytų aiškiai didesnę žalą nei įslaptintos medžiagos atskleidimas ir jei:
 - a) siuntėjas ir gavėjas neturi reikiamos šifravimo įrangos ir
 - b) įslaptinta medžiaga negali būti laiku perduota kitomis priemonėmis.
3. 1 dalyje išdėstytomis aplinkybėmis perduodama įslaptinta informacija nėra žymima jokiais žymomis arba nuorodomis, kurios sudarytų sąlygas ją atskirti nuo informacijos, kuri yra neįslaptinta arba kurią galima apsaugoti naudojant turimas kriptografinės priemonės. Gavėjams kitomis priemonėmis nedelsiant pranešama apie informacijos slaptumo lygį.
4. Vėliau pateikiama ataskaita kompetentingai institucijai ir Komisijos saugumo ekspertų grupei.

6 SKYRIUS

PRAMONINIS SAUGUMAS

39 straipsnis

Pagrindiniai principai

1. Pramoninis saugumas – priemonių taikymas, siekiant užtikrinti ESII apsaugą
 - a) vykdant įslaptintas sutartis:
 - i) kandidatų ar konkurso dalyvių užtikrinama apsauga pasiūlymų teikimo ir sutarčių sudarymo procedūros metu;
 - ii) rangovų arba subrangovų užtikrinama apsauga per visą įslaptintų sutarčių gyvavimo ciklą;

⁽¹⁾ 2014 m. balandžio 16 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 512/2014, kuriuo iš dalies keičiamas Reglamentas (ES) Nr. 912/2010, kuriuo įsteigiama Europos GNSS agentūra (OL L 150, 2014 5 20, p. 72).

- b) vykdamas įslaptintus dotacijos susitarimus:
 - i) pareiškėjų užtikrinama apsauga vykstant dotacijos skyrimo procedūroms;
 - ii) dotacijos gavėjų užtikrinama apsauga per visą įslaptintų dotacijos susitarimų gyvavimo ciklą.
- 2. Tokiose sutartyse arba dotacijos susitarimuose nenumatoma galimybė susipažinti su slaptumo žyma TRES SECRET UE/ES TOP SECRET pažymėta informacija.
- 3. Išskyrus atvejus, kai nustatyta kitaip, šio skyriaus nuostatos, susijusios su įslaptintomis sutartimis ar rangovais, taip pat taikomos įslaptintoms subrangos sutartims ar subrangovams.

40 straipsnis

Apibrėžtys

Šiame skyriuje vartojamų terminų apibrėžtys:

- a) įslaptinta sutartis – Komisijos arba jos padalinio su rangovu sudaryta Tarybos reglamente (EB, Euratomas) Nr. 1605/2002 ⁽¹⁾ nurodyta preliminarioji sutartis arba kilnojamąjo arba nekilnojamąjo turto tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdamas reikia rengti, tvarkyti arba saugoti ESĮI arba suteikiama galimybė ją rengti, tvarkyti arba saugoti;
- b) įslaptinta subrangos sutartis – Komisijos arba jos padalinio rangovo ir kito rangovo (t. y. subrangovo) sudaryta kilnojamąjo arba nekilnojamąjo turto tiekimo, darbų vykdymo arba paslaugų teikimo sutartis, kurią vykdamas reikia rengti, tvarkyti arba saugoti ESĮI arba suteikiama galimybė ją rengti, tvarkyti arba saugoti;
- c) įslaptintas dotacijos susitarimas – susitarimas, kuriuo Komisija skiria dotaciją, kaip nurodyta Reglamente (EB, Euratomas) Nr. 1605/2002 I dalies VI antraštinėje dalyje, kurią vykdamas reikia rengti, tvarkyti arba saugoti ESĮI arba suteikiama galimybė ją rengti, tvarkyti arba saugoti;
- d) paskirtoji saugumo institucija (PSI) – valstybės narės nacionalinei saugumo institucijai (NSI) atsakinga institucija, kuri atsako už pramonės ar 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.

41 straipsnis

Įslaptintoms sutartims arba dotacijos susitarimams taikoma procedūra

- 1. Kiekvienas Komisijos padalinys, kaip perkančioji organizacija, užtikrina, kad, sudarant įslaptintas sutartis arba dotacijos susitarimus, sutartyse būtų paminėti arba juos įtraukti šiame skyriuje nustatyti būtiniausi pramoninio saugumo standartai ir kad jų būtų laikomasi.
- 2. Taikant 1 dalį, kompetentingos Komisijos tarnybos konsultuojasi su Žmogiškųjų išteklių ir saugumo generaliniu direktoratu, visų pirma su Saugumo direktoratu, ir užtikrina, kad į pavyzdines sutartis ir subrangos sutartis bei pavyzdinius dotacijos susitarimus būtų įtraukiamos nuostatos dėl pagrindinių principų ir būtiniausių ESĮI apsaugos standartų, kurių turi laikytis rangovai ir subrangovai bei dotacijos gavėjai pagal susitarimus.
- 3. Komisija glaudžiai bendradarbiauja su NSI, PSI ar kitomis kompetentingomis atitinkamų valstybių narių institucijomis.
- 4. Kai perkančioji organizacija ketina pradėti procedūrą, kurios tikslas – sudaryti įslaptintą sutartį arba dotacijos susitarimą, visais procedūros etapais ji konsultuojasi su Komisijos saugumo institucija dėl klausimų, susijusių su įslaptintu procedūros pobūdžiu ir aspektais.
- 5. Įslaptintų sutarčių ir subrangos sutarčių ir įslaptintų dotacijos susitarimų formos ir pavyzdžiai, skelbimų apie pirkimą turinys, gairės dėl aplinkybių, kuriomis reikalaujama Įmonės patikimumą patvirtinančio pažymėjimo (IPPP), programos arba projekto saugumo instrukcijos (PSI), saugumo aspektų paaiškinimai (SAP), vizitų nuostatos, ESĮI perdavimo ir gabenimo vykdamas įslaptintas sutartis arba įslaptintus dotacijos susitarimus nuostatos pasikonsultavus su Komisijos saugumo ekspertų grupe nustatomos pramoninio saugumo įgyvendinimo taisyklėse.

⁽¹⁾ 2002 m. birželio 25 d. Tarybos reglamentas (EB, Euratomas) Nr. 1605/2002 dėl Europos Bendrijų bendrajam biudžetui taikomo Finansinio reglamento (OL L 248, 2002 9 16, p. 1).

6. Komisija gali sudaryti įslaptintas sutartis arba dotacijos susitarimus, kuriuose ekonominės veiklos vykdytojams, registruotiems valstybėje narėje arba trečiojoje valstybėje, kuri yra sudariusi susitarimą arba administracinį susitarimą pagal šio sprendimo 7 skyrių, patikimos užduotys, kurioms atlikti reikia arba gali reikėti susipažinti su ESĮI arba ją tvarkyti ar saugoti.

42 straipsnis

Įslaptintos sutarties arba įslaptinto dotacijos susitarimo saugumo aspektai

1. Į įslaptintas sutartis arba dotacijos susitarimus įtraukiami tokie saugumo aspektai:

Programos arba projekto saugumo instrukcijos

- a) Programos arba projekto saugumo instrukcijos (PSI) – saugumo procedūrų, kurios yra taikomos konkrečiai programai arba projektui siekiant standartizuoti saugumo procedūras, sąrašas. Jos gali būti tikslinamos įgyvendinant programą arba projektą;
- b) Žmogiškųjų išteklių ir saugumo generalinis direktoratas parengia bendrąsias PSI, o už programas arba projektus, kuriuose tvarkoma arba saugoma ESĮI, atsakingi Komisijos padaliniai, jei reikia, remdamiesi bendrosiomis PSI gali parengti konkrečias PSI;
- c) Konkrečios PSI visų pirma rengiamos įgyvendinant didelės svarbos, apimties arba sudėtingumo programas ir projektus, arba kai juose dalyvauja daug ir (arba) įvairių rangovų, dotacijos gavėjų ir kitų partnerių bei suinteresuotųjų šalių, pavyzdžiui, ypač dėl skirtingo jų teisinio statuso. Glaudžiai bendradarbiaudamas (-i) su Žmogiškųjų išteklių ir saugumo generaliniu direktoratu, konkrečias PSI rengia Komisijos padalinys (-iai), kuris (-ie) valdo programą ar projektą.
- d) Žmogiškųjų išteklių ir saugumo generalinis direktoratas su Komisijos saugumo ekspertų grupe konsultuojasi ir dėl bendrųjų, ir dėl konkrečių PSI.

Saugumo aspektų paaiškinimas

- a) Saugumo aspektų paaiškinimas (SAP) – specialių sutartinių sąlygų rinkinys, kurį parengia perkančioji organizacija ir kuris yra įslaptintos sutarties, pagal kurią gali būti susipažįstama su ESĮI arba tokia informacija gali būti rengiama, sudėtinė dalis; jame nurodomi saugumo reikalavimai ir tos sutarties dalys, kurių saugumą būtina užtikrinti;
- b) SAP aprašomi konkrečioms sutartims skirti saugumo reikalavimai. Prireikus į SAP įtraukiamas slaptumo žymų vadovas (SŽV). SAP yra neatsiejama įslaptintos sutarties, subrangos sutarties ar dotacijos susitarimo dalis;
- c) SAP nustatomos nuostatos, pagal kurias reikalaujama, kad rangovas arba dotacijos gavėjas laikytųsi būtiniausių šiame sprendime nustatytų standartų. Perkančioji organizacija užtikrina, kad SAP būtų nurodyta, jog šių būtiniausių standartų nesilaikymas gali būti pakankamas pagrindas sutarčiai arba dotacijos susitarimui nutraukti.

2. Į PSI ir SAP įtraukiamas privalomas saugumo aspektas – SŽV:

- a) Slaptumo žymų vadovas (SŽV) – dokumentas, kuriame aprašomi programos, projekto, sutarties arba dotacijos susitarimo įslaptinti elementai, nurodant taikomus slaptumo žymų lygius. SŽV gali būti papildomas programos, projekto, sutarties arba dotacijos susitarimo vykdymo laikotarpiu, o informacijos dalims gali būti suteiktos naujos slaptumo žymos arba jų slaptumas gali būti sumažintas; tais atvejais, kai yra parengtas SŽV, jis yra SAP dalis.
- b) Prieš paskelbdamas kvietimą teikti pasiūlymus įslaptintai sutarčiai sudaryti arba prieš sudarydamas įslaptintą sutartį, Komisijos padalinys, kaip perkančioji institucija, nustato visos informacijos, kuri turi būti suteikta kandidatams ir konkurso dalyviams arba rangovams, slaptumo žymą, taip pat visos informacijos, kurią turi parengti rangovas, slaptumo žymą. Pasikonsultavęs su Komisijos saugumo institucija, tuo tikslu jis parengia SŽV, kuris turi būti naudojamas vykdamas sutartį pagal šį sprendimą ir jo įgyvendinimo taisykles.

- c) Siekiant nustatyti skirtingų įslaptintos sutarties dalių slaptumo žymą, taikomi toliau nurodyti principai:
- i) rengdamas SŽV, Komisijos padalinys, kaip perkančioji institucija, atsižvelgia į visus svarbius saugumo aspektus, įskaitant slaptumo žymą, kurią informacijai priskyrė informacijos rengėjas ir kurią jis patvirtino kaip naudotiną tai sutarčiai;
 - ii) bendras sutarties slaptumo žymos lygis negali būti žemesnis nei aukščiausia bet kurios jos dalies slaptumo žyma ir
 - iii) atitinkamais atvejais, jei daromi pakeitimai, susiję su slaptumo žymų suteikimu informacijai, parengtai rangovų ar jiems suteiktai vykdant sutartį, ir jei daromi vėlesni SŽV pakeitimai, perkančioji institucija per Komisijos saugumo instituciją palaiko ryšius su valstybių narių NSI, PSI ar kitomis atitinkamomis kompetentingomis saugumo institucijomis.

43 straipsnis

Rangovų ir dotacijos gavėjų darbuotojų teisė susipažinti su ESĮI

Perkančioji institucija arba dotaciją skiriančioji institucija užtikrina, kad į įslaptintą sutartį arba įslaptintą dotacijos susitarimą būtų įtrauktos nuostatos, pagal kurias rangovo, subrangovo arba dotacijos gavėjo darbuotojai, kuriems vykdant įslaptintą sutartį, subrangos sutartį arba dotacijos susitarimą reikia susipažinti su ESĮI, turėtų galimybę susipažinti su tokia informacija, jei:

- a) jiems buvo išduotas atitinkamo lygio saugumo leidimas arba kitas tinkamas leidimas nustačius, kad jiems „būtina žinoti“;
- b) jie buvo informuoti apie ESĮI apsaugai užtikrinti taikomas saugumo taisykles ir patvirtino savo pareigą saugoti tokią informaciją;
- c) atitinkama NSI, PSI ar bet kuri kita kompetentinga institucija jiems išdavė atitinkamo lygmens asmens patikimumo pažymėjimus, suteikiančius teisę susipažinti su informacija, pažymėta CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma.

44 straipsnis

Įmonės patikimumą patvirtinantis pažymėjimas

1. Įmonės patikimumą patvirtinantis pažymėjimas (ĮPPP) – NSI, PSI ar kitos kompetentingos saugumo institucijos išduotas administracinis patvirtinimas, kad saugumo požiūriu patalpose gali būti užtikrinta tinkama nurodyto slaptumo žymos lygio ESĮI apsauga.
2. NSI, PSI ar kita kompetentinga valstybės narės saugumo institucija, laikydamosi nacionalinių įstatymų ir kitų teisės aktų, išduoda ĮPPP, kuriuo nurodoma, kad ekonominės veiklos vykdytojas savo patalpose gali apsaugoti atitinkamo slaptumo žyma (CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET) pažymėtą ESĮI. Šis ĮPPP pateikiamas Komisijos saugumo institucijai, o ši jį perduoda Komisijos padaliniui, veikiančiam kaip perkančioji arba dotaciją skiriančioji institucija, prieš suteikiant kandidatui, konkurso dalyviui ar rangovui arba dotacijos gavėjui ESĮI arba galimybę susipažinti su ESĮI.
3. Atitinkamais atvejais perkančioji institucija per Komisijos saugumo instituciją praneša atitinkamai NSI, PSI ar kitai kompetentingai saugumo institucijai, kad sutarčiai vykdyti reikalingas ĮPPP. ĮPPP arba APP reikalaujama turėti tais atvejais, kai viešųjų pirkimų arba dotacijos skyrimo procedūrų metu reikia suteikti ESĮI, pažymėtą CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma.
4. Perkančioji institucija arba dotaciją skiriančioji institucija nesudaro įslaptintos sutarties arba dotacijos susitarimo su konkurso laimėtoju arba 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.
5. Kai NSI, PSI ar kita kompetentinga ĮPPP išdavusi saugumo institucija Komisijos saugumo institucijai praneša apie pasikeitimus, turinčius įtakos ĮPPP, Komisijos saugumo institucija apie tai praneša Komisijos padaliniui, veikiančiam kaip perkančioji arba dotaciją skiriančioji institucija. Subrangos sutarties atveju apie tai atitinkamai informuojama NSI, PSI ar kita kompetentinga saugumo institucija.

6. Jeigu atitinkama NSI, PSI ar kita kompetentinga saugumo institucija panaikina ĮPPP, tai yra pakankamas pagrindas, kad perkančioji arba dotaciją skiriančioji institucija nutrauktų įslaptintą sutartį arba pašalintų kandidatą, konkurso dalyvį arba paraiškos teikėją iš konkurso. Tokia nuostata įtraukiama į rengiamas pavyzdines sutartis ir dotacijos susitarimus.

45 straipsnis

Įslaptintoms sutartims ir dotacijos susitarimams taikomos nuostatos

1. Tais atvejais, kai kandidatui, konkurso dalyviui arba paraiškos teikėjui ESĮI suteikiama vykstant viešųjų pirkimų, kvietimo pateikti pasiūlymus arba kvietimo teikti paraiškas procedūrai, numatoma nuostata, kuria pasiūlymo arba paraiškos nepateikęs arba neatrinktas kandidatas, konkurso dalyvis arba paraiškos teikėjas įpareigojamas per nurodytą laiką grąžinti visus įslaptintus dokumentus.
2. Perkančioji arba dotaciją skiriančioji institucija per Komisijos saugumo instituciją praneša NSI, PSI ar kitai kompetentingai saugumo institucijai, kad sudaryta įslaptinta sutartis arba dotacijos susitarimas, ir perduoda susijusius duomenis, kaip antai rangovo (-ų) arba dotacijos gavėjų pavadinimus, sutarties trukmę ir aukščiausią informacijos įslaptinimo lygį.
3. Kai tokia sutartis arba dotacijos susitarimas nutraukiami, perkančioji arba dotaciją skiriančioji institucija per Komisijos saugumo instituciją nedelsdamas praneša apie tai NSI, PSI ar kitai kompetentingai valstybės narės, kurioje yra įregistruotas rangovas arba dotacijos gavėjas, saugumo institucijai.
4. Paprastai reikalaujama, kad, nutraukus įslaptintą sutartį ar įslaptintą dotacijos susitarimą arba dotacijos gavėjui nebedalyvaujant įgyvendinant įslaptintą sutartį ar įslaptintą dotacijos susitarimą, rangovas arba dotacijos gavėjas perkančiajai arba dotaciją skiriančiajai institucijai grąžintų visą turimą ESĮI.
5. SAP nustatomos konkrečios nuostatos dėl ESĮI sunaikinimo vykdant įslaptintą sutartį arba įslaptintą dotacijos susitarimą arba juos nutraukus.
6. Tais atvejais, kai rangovui arba dotacijos gavėjui suteikiamas leidimas nutraukus įslaptintą sutartį arba įslaptintą dotacijos susitarimą negrąžinti ESĮI, rangovas arba dotacijos gavėjas toliau laikosi šiame sprendime nustatytų būtiniausių standartų ir užtikrina ESĮI konfidencialumą.

46 straipsnis

Įslaptintoms sutartims taikomos konkrečios nuostatos

1. ESĮI apsaugai svarbios sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, nurodomos kvietime teikti paraiškas ir įslaptintoje sutartyje.
2. Prieš sudarydamas subrangos sutartis dėl įslaptintos sutarties dalių, rangovas turi gauti perkančiosios institucijos leidimą. Su trečiojoje šalyje registruotais subrangovais negali būti sudaromos sutartys, kurias vykdant reikia susipažinti su ESĮI, išskyrus atvejus, kai nustatoma 7 skyriuje numatyta informacijos saugumo reglamentavimo sistema.
3. 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.
4. Komisija laikoma ESĮI, kurią parengė ar tvarko rangovas, rengėja, o rengėjo teisėmis naudojasi perkančioji institucija.

47 straipsnis

Su įslaptintomis sutartimis susiję vizitai

1. Jei vykdant įslaptintą sutartį arba dotacijos susitarimą Komisijos darbuotojui arba rangovo ar dotacijos gavėjo personalui vienas kito patalpose reikia susipažinti su CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma pažymėta informacija, dėl vizitų susitariama palaikant ryšius su NSI, PSI arba kita susijusia kompetentinga saugumo institucija. Apie tokius vizitus pranešama Komisijos saugumo institucijai. Tačiau įgyvendinant tam tikras programas arba projektus NSI, PSI arba kita kompetentinga saugumo institucija gali taip pat susitarti dėl tvarkos, pagal kurią dėl tokių vizitų gali būti susitariama tiesiogiai.

2. Tam, kad būtų leista susipažinti su ESII, kuri susijusi su įslaptinta sutartimi, visi lankytojai turi turėti atitinkamą patikimumo pažymėjimą ir jiems turi būti „būtina žinoti“.
3. Lankytojams leidžiama susipažinti tik su ta ESII, kuri yra susijusi su vizito tikslu.
4. Išsamesnės nuostatos nustatomos įgyvendinimo taisyklėse.
5. Privaloma laikytis šiame sprendime ir įgyvendinimo taisyklėse, nurodytose šio straipsnio 4 dalyje, numatytų vizitų, susijusių su įslaptintomis sutartimis, nuostatų.

48 straipsnis

ESII perdavimas ir gabenimas vykdant įslaptintas sutartis arba įslaptintus dotacijos susitarimus

1. Perduodant ESII elektroninėmis priemonėmis taikomos atitinkamos šio sprendimo 5 skyriaus nuostatos.
2. Gabenant ESII taikomos atitinkamos šio sprendimo 4 skyriaus nuostatos, laikantis nacionalinių įstatymų ir kitų teisės aktų.
3. Nustatant įslaptintos medžiagos kaip krovinio gabenimui taikomą saugumo tvarką taikomi toliau nurodyti principai:
 - a) saugumas užtikrinamas visuose gabenimo etapuose nuo išgabenimo vietos iki galutinės paskirties vietos;
 - b) siuntai suteikiamas apsaugos lygis nustatomas pagal joje esančios medžiagos aukščiausią slaptumo žymos lygį;
 - c) prieš gabenant per valstybių sienas medžiagą, pažymėtą CONFIDENTIEL UE/ES CONFIDENTIAL arba SECRET UE/ES SECRET slaptumo žyma, siuntėjas parengia, o atitinkamos NSI, PSI ar kitos kompetentingos saugumo institucijos patvirtina gabenimo planą;
 - d) stengiamasi, kad kelionės vyktų be sustojimo ir būtų užbaigtos kuo greičiau, atsižvelgiant į aplinkybes;
 - e) kai galima, turėtų būti pasirenkami maršrutai tik per valstybes nares. Maršrutais per valstybes, kurios nėra valstybės narės, turėtų būti gabenama tik gavus siuntėjo ir gavėjo valstybių NSI, PSI ar kitos kompetentingos saugumo institucijos leidimą.

49 straipsnis

ESII perdavimas trečiosiose valstybėse įsikūrusiems rangovams arba dotacijos gavėjams

Trečiosiose valstybėse įsikūrusiems rangovams ir dotacijos gavėjams ESII perduodama laikantis saugumo priemonių, dėl kurių susitarė Komisijos saugumo institucija, Komisijos padalinys, kaip perkančioji arba dotaciją skiriančioji institucija, ir atitinkamos trečiosios valstybės, kurioje registruotas rangovas arba dotacijos gavėjas, NSI, PSI ar kita kompetentinga saugumo institucija.

50 straipsnis

Informacijos, pažymėtos RESTREINT UE/ES RESTRICTED žyma, tvarkymas vykdant įslaptintas sutartis arba įslaptintus dotacijos susitarimus

1. Įslaptintos informacijos, pažymėtos RESTREINT UE/ES RESTRICTED slaptumo žyma, tvarkomos ir saugomos pagal įslaptintas sutartis arba įslaptintus dotacijos susitarimus, apsauga grindžiama proporcingumo ir ekonominio efektyvumo principais.
2. Vykdant įslaptintas sutartis arba įslaptintus dotacijos susitarimus, kai tvarkoma RESTREINT UE/ES RESTRICTED slaptumo žyma pažymėta informacija, nereikalaujama turėti IPPP arba APP.
3. Kai pagal sutartį arba dotacijos susitarimą numatytas informacijos, pažymėtos RESTREINT UE/ES RESTRICTED slaptumo žyma, tvarkymas rangovo arba dotacijos gavėjo eksploatuojamoje RIS, perkančioji arba dotaciją skiriančioji institucija, pasikonsultavusi su Komisijos saugumo institucija, užtikrina, kad sutartyje arba dotacijos susitarime būtų nustatyti su RIS akreditavimu arba patvirtinimu susiję būtini techniniai ir administraciniai reikalavimai, kurie atitiktų įvertintą riziką, atsižvelgiant į visus svarbius veiksnius. Komisijos saugumo institucija ir atitinkama NSI ar PSI susitaria dėl tokio RIS akreditavimo arba patvirtinimo masto.

7 SKYRIUS

KEITIMASIS ĮSLAPTINTA INFORMACIJA SU KITOMIS SĄJUNGOS INSTITUCIJOMIS, AGENTŪROMIS, ĮSTAIGOMIS IR ORGANAIS, SU VALSTYBĖMIS NARĖMIS IR SU TREČIOSIOMIS VALSTYBĖMIS BEI TARPTAUTINĖMIS ORGANIZACIJOMIS

51 straipsnis

Pagrindiniai principai

1. Komisijai arba vienam iš jos padalinių nusprendus, kad reikia keisti ESĮI su kita Sąjungos institucija, agentūra, įstaiga ar organu arba su trečiąja valstybe ar tarptautine organizacija, imamasi reikalingų priemonių, kad būtų nustatyta tam skirta tinkama teisinė arba administracinė sistema, į kurią gali būti įtraukiami susitarimai dėl informacijos saugumo arba administraciniai susitarimai, sudaryti laikantis atitinkamų teisės aktų.
2. Nedarant poveikio 57 straipsniui, ESĮI su kita Sąjungos institucija, agentūra, įstaiga ar organu arba su trečiąja valstybe ar tarptautine organizacija gali būti keičiamasi tik jeigu nustatyta tokia tinkama teisinė arba administracinė sistema ir jeigu pateikta pakankamai garantijų, kad Sąjungos institucija, agentūra, įstaiga ar organas arba atitinkama trečioji valstybė ar tarptautinė organizacija taiko lygiaverčius pagrindinius įslaptintos informacijos apsaugos principus ir būtiniausius standartus.

52 straipsnis

Keitimas ESĮI su kitomis Sąjungos institucijomis, agentūromis, įstaigomis ir organais

1. Prieš sudarydama administracinį susitarimą dėl keitimosi ESĮI su kita Sąjungos institucija, agentūra, įstaiga ar organu, Komisija įsitikina, kad ta Sąjungos institucija, agentūra, įstaiga ar organas:
 - a) yra nustatę ESĮI apsaugos reguliavimo sistemą, kurioje išdėstyti pagrindiniai principai ir būtiniausi standartai, lygiaverčiai nustatytiesiems šiame sprendime ir jo įgyvendinimo taisyklėse;
 - b) taiko saugumo standartus ir asmens patikimumo, fizinio saugumo, ESĮI valdymo ir ryšių ir informacinių sistemų (RIS) saugumo gaires, kuriais užtikrinamas Komisijos taikomam apsaugos lygiui lygiavertis ESĮI apsaugos lygis;
 - c) savo parengtą ESĮI žymi įslaptintos informacijos žymomis.
2. Žmogiškųjų išteklių ir saugumo generalinis direktoratas, glaudžiai bendradarbiaudamas su kitais kompetentingais Komisijos padaliniais, vadovauja Komisijai sudarant administracinius susitarimus dėl keitimosi ESĮI su kitomis Sąjungos institucijomis, agentūromis, įstaigomis ar organais.
3. Administraciniai susitarimai paprastai sudaromi pasikeičiant laiškais, kuriuos Komisijos vardu pasirašo Žmogiškųjų išteklių ir saugumo generalinis direktorius.
4. Prieš sudarant administracinį susitarimą dėl keitimosi ESĮI, Komisijos saugumo institucija surengia įvertinimo vizitą, kurio tikslas – įvertinti ESĮI apsaugai skirtą reguliavimo sistemą ir įsitikinti, kad ESĮI apsaugos priemonės įgyvendinamos veiksmingai. Administracinis susitarimas įsigalioja ir ESĮI keičiamasi tik tuo atveju, jei šio įvertinimo vizito rezultatai yra patenkinami ir buvo laikomasi po vizito pateiktų rekomendacijų. Reguliariai rengiami tolesni įvertinimo vizitai, siekiant patikrinti, ar laikomasi administracinių susitarimų ir ar apsaugos priemonės vis dar atitinka nustatytus pagrindinius principus ir būtiniausius standartus.
5. Generalinio sekretoriato valdoma Komisijos ESĮI registratūra paprastai yra pagrindinis įslaptintos informacijos, kuria keičiamasi su kitomis Sąjungos institucijomis, agentūromis, įstaigomis ir organais, gavimo ir išsiuntimo punktas. Tačiau tais atvejais, kai dėl saugumo, organizacinių arba veiklos priežasčių ESĮI apsaugai labiau tiktų vietinės ESĮI registratūros, remiantis šiuo sprendimu ir jo įgyvendinimo taisyklėmis Komisijos padaliniuose įsteigiamos tokios registratūros, kurios veikia kaip įslaptintos informacijos, susijusios su atitinkamų Komisijos padalinių kompetencijos klausimais, gavimo ir išsiuntimo punktai.
6. Komisijos Saugumo ekspertų grupė informuojama apie administracinių susitarimų pagal 2 dalį sudarymo eigą.

53 straipsnis

Keitimasis ESII su valstybėmis narėmis

1. ESII gali būti keičiamasi su valstybėmis narėmis ir ta informacija gali būti joms teikiama su sąlyga, kad valstybės narės saugos išlaptintą informaciją laikydamosi reikalavimų, taikomų lygiaverčio nacionalinės slaptumo žymos lygio ESII, kaip nustatyta I priede pateiktoje slaptumo žymų atitikmenų lentelėje.
2. Valstybės narės nacionaline slaptumo žyma pažymėtą išlaptintą informaciją perdavus į Europos Sąjungos struktūras ar tinklus, Komisija tą informaciją saugo laikydamosi reikalavimų, taikomų lygiaverčio slaptumo žymos lygio ESII, kaip nustatyta I priede pateiktoje slaptumo žymų atitikmenų lentelėje.

54 straipsnis

Keitimasis ESII su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

1. Kai Komisija nustato, kad yra ilgalaikis poreikis keisti išlaptintą informaciją su trečiosiomis valstybėmis arba tarptautinėmis organizacijomis, imamas reikalingų priemonių, kad būtų nustatyta tam skirta tinkama teisinė arba administracinė sistema, į kurią gali būti įtraukiami susitarimai dėl informacijos saugumo arba administraciniai susitarimai, sudaryti laikantis atitinkamų teisės aktų.
2. Tokiuose 1 dalyje nurodytuose susitarimuose dėl informacijos saugumo ir administraciniuose susitarimuose numatomos nuostatos, kuriomis užtikrinama, kad trečiosioms valstybėms arba tarptautinėms organizacijoms gavus ESII ta informacija būtų saugoma atsižvelgiant į jos slaptumo žymos lygį, remiantis būtiniausiais standartais, kurie atitinka šiame sprendime nustatytus standartus.
3. Komisija gali pagal 56 straipsnį sudaryti administracinius susitarimus tuomet, kai ESII slaptumo žymos lygis paprastai nėra aukštesnis nei RESTREINT UE/ES RESTRICTED.
4. 3 dalyje nurodytuose administraciniuose susitarimuose dėl keitimosi išlaptinta informacija numatomos nuostatos, kuriomis užtikrinama, kad trečiosioms valstybėms arba tarptautinėms organizacijoms gavus ESII ta informacija būtų saugoma atsižvelgiant į jos slaptumo žymos lygį, remiantis būtiniausiais standartais, kurie atitinka šiame sprendime nustatytus standartus. Dėl susitarimų dėl informacijos saugumo arba administracinių susitarimų sudarymo konsultuojamasi su Komisijos saugumo ekspertų grupe.
5. Sprendimą suteikti Komisijos parengtą ESII trečiajai valstybei arba tarptautinei organizacijai priima tą ESII parengęs Komisijos padalinys, atskirai kiekvienu konkrečiu atveju atsižvelgdamas į tokios informacijos pobūdį ir turinį bei tai, ar gavėjui „būtina žinoti“, ir įvertinęs naudą Sąjungai. Jeigu Komisija nėra išlaptintos informacijos, kurią prašoma suteikti, arba pradinės medžiagos, kuri gali būti įtraukta į tą informaciją, rengėja, išlaptintą informaciją turintis Komisijos padalinys pirmiausia prašo jos rengėjo pateikti rašytinį sutikimą suteikti šią informaciją. Jei išlaptintos informacijos rengėjo neįmanoma nustatyti, išlaptintą informaciją turintis Komisijos padalinys, pasikonsultavęs su Komisijos saugumo ekspertų grupe, prisiima rengėjo atsakomybę.

55 straipsnis

Susitarimai dėl informacijos saugumo

1. Susitarimai dėl informacijos saugumo su trečiosiomis valstybėmis arba tarptautinėmis organizacijomis sudaromi remiantis SESV 218 straipsniu.
2. Susitarimuose dėl informacijos saugumo:
 - a) nustatomi pagrindiniai principai ir būtiniausi standartai, reglamentuojantys Sąjungos ir trečiosios valstybės ar tarptautinės organizacijos keitimąsi išlaptinta informacija;
 - b) numatomi techniniai įgyvendinimo susitarimai, dėl kurių turi susitarti atitinkamų Sąjungos institucijų ir įstaigų kompetentingos saugumo tarnybos 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;
 - c) numatoma, kad prieš keičiantis išlaptinta informacija pagal susitarimą būtų užtikrinta, kad gaunančioji šalis atitinkamu būdu gali apsaugoti ir saugoti jai teikiamą išlaptintą informaciją.

3. Kai remiantis 51 straipsnio 1 dalimi nustatoma, kad yra poreikis keistis įslaptinta informacija, Komisija prirėikus konsultuojasi su Europos išorės veiksmų tarnyba, Tarybos generaliniu sekretoriatu ir kitomis Sąjungos institucijomis bei įstaigomis, kad nustatytų, ar reikia pateikti rekomendaciją pagal SESV 218 straipsnio 3 dalį.
4. Keistis ESĮ elektroninėmis priemonėmis neleidžiama, jei tai nėra aiškiai numatyta susitarime dėl informacijos saugumo arba techniniuose įgyvendinimo susitarimuose.
5. Generalinio sekretoriato valdoma Komisijos ESĮ registratūra paprastai yra pagrindinis įslaptintos informacijos, kuria keičiamasi su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis, gavimo ir išsiuntimo punktas. Tačiau tais atvejais, kai dėl saugumo, organizacinių arba veiklos priežasčių ESĮ apsaugai labiau tiktų vietinės ESĮ registratūros, remiantis šiuo sprendimu ir jo įgyvendinimo taisyklėmis Komisijos padaliniuose įsteigiamos tokios registratūros, kurios veikia kaip įslaptintos informacijos, susijusios su atitinkamų Komisijos padalinių kompetencijos klausimais, gavimo ir išsiuntimo punktai.
6. Siekiant įvertinti atitinkamos trečiosios valstybės ar tarptautinės organizacijos saugumo nuostatus, struktūras ir procedūras, Komisija, bendradarbiaudama su kitomis Sąjungos institucijomis, agentūromis arba įstaigomis, dalyvauja įvertinimo vizituose abipusiu susitarimu su atitinkama trečiąja valstybe ar tarptautine organizacija. Tokiuose įvertinimo vizituose 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 lygiui;
 - c) faktiškai taikomos saugumo priemonės ir procedūros ir
 - d) patikimumo patikrinimo procedūros, susijusios su numatomos suteikti ESĮ slaptumo žymos lygiu.

56 straipsnis

Administraciniai susitarimai

1. Kai, taikant Sąjungos politinę arba teisinę sistemą, yra ilgalaikis poreikis su trečiąja valstybe arba tarptautine organizacija keistis įslaptinta informacija, kurios slaptumo žymos lygis paprastai nebūna aukštesnis nei RESTREINT UE/ES RESTRICTED, ir kai Komisijos saugumo institucija po konsultacijų su Komisijos saugumo ekspertų grupe visų pirma nustato, kad atitinkama šalis neturi pakankamai išplėtos saugumo sistemos, kad galėtų sudaryti susitarimą dėl informacijos saugumo, Komisija gali nuspręsti su atitinkamos trečiosios valstybės ar tarptautinės organizacijos atitinkamomis institucijomis sudaryti administracinį susitarimą.
2. Tokie administraciniai susitarimai paprastai sudaromi pasikeičiant laiškais.
3. Prieš sudarant susitarimą surengiamas įvertinimo vizitas. Komisijos saugumo ekspertų grupė informuojama apie įvertinimo vizito rezultatus. Jei esama išskirtinių priežasčių skubiai pasikeisti įslaptinta informacija, ESĮ gali būti suteikta su sąlyga, kad dedamos visos pastangos įvertinimo vizitą surengti kuo greičiau.
4. Keistis ESĮ elektroninėmis priemonėmis neleidžiama, jei tai nėra aiškiai numatyta administraciniame susitarime.

57 straipsnis

ESĮ *ad hoc* suteikimas išimtinė tvarka

1. Jei nėra sudarytas susitarimas dėl informacijos saugumo arba administracinis susitarimas ir jei Komisija arba kuris nors jos padalinys nustato, kad taikant Sąjungos politinę arba teisinę sistemą išimtiniais atvejais trečiajai valstybei arba tarptautinei organizacijai reikia suteikti ESĮ, Komisijos saugumo institucija kreipiasi į atitinkamos trečiosios valstybės arba tarptautinės organizacijos saugumo institucijas ir kiek įmanoma patikrina, ar jų saugumo nuostatai, struktūros bei procedūros užtikrina, jog joms suteikta ESĮ būtų saugoma taikant ne mažiau griežtus nei šiame sprendime nustatytieji standartus.
2. Pasikonsultavusi su Komisijos saugumo ekspertų grupe, sprendimą suteikti ESĮ atitinkamai trečiajai valstybei arba tarptautinei organizacijai priima Komisija, remdamasi už saugumą klausimus atsakingo Komisijos nario pasiūlymu.

3. Komisijai priėmus sprendimą suteikti ESII ir gavus išankstinį rašytinį rengėjo, įskaitant pradinės medžiagos, kuri gali būti įtraukta į tą informaciją, rengėjus, sutikimą, kompetentingas Komisijos padalinys perduoda atitinkamą informaciją, pažymėtą leidimo suteikti informaciją žyma, kurioje nurodyta trečioji valstybė arba tarptautinė organizacija, kuriai informacija buvo suteikta. Prieš suteikiant tokią informaciją arba faktinio jos suteikimo metu atitinkama trečioji šalis raštu įsipareigoja apsaugoti ESII, kurią ji gauna, pagal šiame sprendime nustatytus pagrindinius principus ir būtiniausius standartus.

8 SKYRIUS

BAIGIAMOSIOS NUOSTATOS

58 straipsnis

Ankstesnio sprendimo pakeitimas

Šis sprendimas panaikina ir pakeičia Komisijos sprendimą 2001/844/EB, EAPB, Euratomas ⁽¹⁾.

59 straipsnis

Įslaptinta informacija, parengta iki šio sprendimo įsigaliojimo

1. Visa ESII, įslaptinta pagal Sprendimą 2001/844/EB, EAPB, Euratomas, toliau saugoma pagal šio sprendimo atitinkamas nuostatas.
2. Visa įslaptinta informacija, Komisijos turėta Sprendimo 2001/844/EB, EAPB, Euratomas įsigaliojimo dieną, išskyrus Euratomo įslaptintą informaciją:
 - a) jei ji buvo parengta Komisijos, jos slaptumo žyma ir toliau laikoma pakeista į žymą RESTREINT UE, jei iki 2002 m. sausio 31 d. jos autorius nenusprendė suteikti informacijai kitos slaptumo žymos ir apie tai nepranešė visiems atitinkamo dokumento gavėjams;
 - b) jei ji buvo parengta ne Komisijos autorių, išlaiko savo pradinę slaptumo žymą ir todėl laikoma lygiaverčio slaptumo žymos ESII, jei jos autorius nesutinka, kad informacija būtų išslaptinta arba kad jos slaptumas būtų sumažintas.

60 straipsnis

Igyvendinimo taisyklės ir saugumo pranešimai

1. Prireikus, visapusiškai laikantis vidaus darbo tvarkos taisyklių, šio sprendimo įgyvendinimo taisyklės priimamos atskiru Komisijos sprendimu dėl įgaliojimų suteikimo už saugumo reikalus atsakingam Komisijos nariui.
2. Gavęs įgaliojimus pagal pirmiau minėtą Komisijos sprendimą, už saugumo reikalus atsakingas Komisijos narys gali rengti saugumo pranešimus, kuriuose nustatomos saugumo gairės ir geriausios praktikos pavyzdžiai šio sprendimo ir jo įgyvendinimo taisyklių taikymo srityje.
3. Visapusiškai laikydamasi vidaus darbo tvarkos taisyklių, Komisija 1 ir 2 šio straipsnio dalyse minėtas užduotis atskiru sprendimu dėl įgaliojimų perdavimo gali pavesti Žmogiškųjų išteklių ir saugumo generalinio direktorato generaliniam direktoriui.

61 straipsnis

Įsigaliojimas

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

Priimta Briuselyje 2015 m. kovo 13 d.

Komisijos vardu

Pirmininkas

Jean-Claude JUNKER

⁽¹⁾ 2001 m. lapkričio 29 d. Komisijos sprendimas 2001/844/EB, EAPB, Euratomas, iš dalies keičiantis jos darbo tvarkos taisykles (OL L 317, 2001 12 3, p. 1).

I PRIEDAS

SLAPTUMO ŽYMŲ ATITIKMENYS

ES	TRES SECRET UE/ES TOP SECRET	SECRET UE/ES SECRET	CONFIDENTIEL UE/ES CONFIDENTIAL	RESTREINT UE/ES RESTRICTED
Euratomas	EURA TOP SECRET	EURA SECRET	EURA CONFIDENTIAL	EURA 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	Ακρως Απόρρητο Trumpinys: ΑΑΠ	Απόρρητο Trumpinys: (ΑΠ)	Εμπιστευτικό Trumpinys: (ΕΜ)	Περιορισμένης Χρήσης Trumpinys: (ΠΧ)
Ispanija	Secreto	Reservado	Confidencial	Difusión Limitada
Prancūzija	Très Secret Défense	Secret Défense	Confidentiel Défense	(³) pastaba
Kroatija	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipras	Ακρως Απόρρητο Trumpinys: (ΑΑΠ)	Απόρρητο Trumpinys: (ΑΠ)	Εμπιστευτικό Trumpinys: (ΕΜ)	Περιορισμένης Χρήσης Trumpinys: (ΠΧ)
Latvija	Sevišķi slēpeni	Slēpeni	Konfidenciali	Visiškai slapiai
Lietuva	Visiškai slapiai	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	Ścisłe Tajne	Tajne	Poufne	Zastrzeżone
Portugalija	Muito Secreto	Secreto	Confidencial	Reservado

ES	TRES SECRET UE/ES TOP SECRET	SECRET UE/ES SECRET	CONFIDENTIEL UE/ES CONFIDENTIAL	RESTREINT UE/ES RESTRICTED
Rumunija	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovėnija	Strogo tajno	Tajno	Zaupno	Interno
Slovakija	Prísne tajné	Tajné	Dôverné	Vyhradené
Suomija	ERITTÄIN SALAINEN YTTERST HEMLIIG	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	UK TOP SECRET	UK SECRET	Atitiktis nėra ⁽⁵⁾	UK OFFICIAL – SENSITIVE

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

⁽²⁾ Vokietijoje: VS = *Verschlusssache*.

⁽³⁾ Prancūzijos nacionalinėje sistemoje slaptumo žyma RESTREINT nenaudojama. Žyma RESTREINT UE/ES 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.

⁽⁵⁾ Žyma CONFIDENTIEL UE/ES CONFIDENTIAL pažymėtą ESĮI Jungtinė Karalystė tvarko ir saugo laikydamasi žyma UK SECRET pažymėtai informacijai taikomų apsauginių saugumo reikalavimų.

II PRIEDAS

SANTRUMPŲ SĄRAŠAS

Santrumpa	Reikšmė
KI	Kriptografijos institucija
KPI	Kriptografijos patvirtinimo institucija
AVSS	Apsauginė vaizdo stebėjimo sistema
KPLI	Kriptografijos platinimo institucija
RIS	Ryšių ir informacinės sistemos, kuriose tvarkoma ESII
PSI	Paskirtoji saugumo institucija
ESII	ES išlaptinta informacija
ĮPPP	Įmonės patikimumą patvirtinantis pažymėjimas
ISU	Informacijos saugumo užtikrinimas
ISUI	Informacijos saugumo užtikrinimo institucija
IAS	Išsibrovimo aptikimo sistema
IT	Informacinės technologijos
VSP	Vietos saugumo pareigūnas
NSI	Nacionalinė saugumo institucija
APP	Asmens patikimumo pažymėjimas
APPPP	Asmens patikimumo pažymėjimą patvirtinanti pažyma
PRSI	Programos/projekto saugumo instrukcijos
RKP	Registracijos kontrolės pareigūnas
SAI	Saugumo akreditavimo institucija
SAP	Saugumo aspektų paaiškinimas
SŽV	Slaptumo žymų vadovas
SEK	Saugios eksploatacijos taisyklės
TEI	Institucija TEMPEST
SESV	Sutartis dėl ES veikimo

III PRIEDAS

NACIONALINIŲ SAUGUMO INSTITUCIJŲ SĄRAŠAS

BELGIJA

Autorité nationale de Sécurité
SPF Affaires étrangères, Commerce extérieur et
Coopération au Développement
15, rue des Petits Carmes
1000 Bruxelles
Sekretoriato telefonas +32 25014542
Faksas +32 25014596
El. paštas nvo-ans@diplobel.fed.be

BULGARIJA

State Commission on Information Security
90 Cherkovna Str.
1505 Sofia
Telefonas +359 29333600
Faksas +359 29873750
El. paštas dksi@government.bg
Interneto svetainė www.dksi.bg

ČEKIJA

Národní bezpečnostní úřad
(National Security Authority)
Na Popelce 2/16
CZ-150 06 Praha 56
Telefonas +420 257283335
Faksas +420 257283110
El. paštas czech.nsa@nbu.cz
Interneto svetainė www.nbu.cz

DANIJA

Politiets Efterretningstjeneste
(Danish Security Intelligence Service)
Klausdalsbrovej 1
DK-2860 Søborg
Telefonas +45 33148888
Faksas +45 33430190
Forsvarets Efterretningstjeneste
(Danish Defence Intelligence Service)
Kastellet 30
DK-2100 Copenhagen Ø
Telefonas +45 33325566
Faksas +45 33931320

VOKIETIJA

Bundesministerium des Innern
Referat ÖS III 3
Alt-Moabit 101 D
11014 Berlin
Telefonas +49 30186810
Faksas +49 30186811441
El. paštas oesIII3@bmi.bund.de

ESTIJA

National Security Authority Department
Estonian Ministry of Defence
Sakala 1
EE-15094 Tallinn
Telefonai: +372 7170019, +372 7170117
Faksas +372 7170213
El. paštas nsa@mod.gov.ee

GRAIKIJA

Γενικό Επιτελείο Εθνικής Άμυνας (ΓΕΕΘΑ)
Διακλαδική Διεύθυνση Στρατιωτικών Πληροφοριών (ΔΔΣΠ)
Διεύθυνση Ασφαλείας και Αντιπληροφοριών
ΣΤΤ 1020 -Χολαργός (Αθήνα)
Ελλάδα
Telefonai: + 30/210/657 20 45 (darbo valandomis)
+ 30/210/657 20 09 (darbo valandomis)
Faksai: +30 2106536279; + 30 2106577612
Hellenic National Defence General Staff (HNDGS)
Military Intelligence Sectoral Directorate
Security Counterintelligence Directorate
GR-STG 1020 Hologoros – Athens
Telefonai: +30 2106572045
+ 30 2106572009
Faksai: +30 2106536279, +30 2106577612

ISPANIJA

Autoridad Nacional de Seguridad
Oficina Nacional de Seguridad
Avenida Padre Huidobro s/n
E-28023 Madrid
Telefonas +34 913725000
Faksas +34 913725808
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 171758177

Faksas +33 171758200

Ministry of Defence

Minister's Military Staff

National Security Authority (NSA)

4 Emanuel Roidi street

1432 Nicosia

Telefonai: +357 22807569, +357 22807643,

+357 22807764

Faksas +357 22302351

El. paštas cynsa@mod.gov.cy

KROATIJA

Office of the National Security Council

Croatian NSA

Jurjevska 34

10000 Zagrebas

Kroatija

Telefonas +385 14681222

Faksas + 385 14686049

Interneto svetainė www.uvns.hr

LATVIJA

National Security Authority

Constitution Protection Bureau of the Republic of Latvia

P.O.Box 286

LV-1001 Ryga

Telefonas +371 67025418

Faksas +371 67025454

El. paštas ndi@sab.gov.lv

AIRIJA

National Security Authority

Department of Foreign Affairs

76–78 Harcourt Street

Dublin 2

Telefonas +353 14780822

Faksas +353 14082959

LIETUVA

Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija

(Lietuvos Respublikos paslapčių apsaugos koordinavimo komisija – Nacionalinė saugumo institucija)

Gedimino pr. 40/1

LT-01110 Vilnius

Telefonai: +370 70666701, +370 70666702

Faksas +370 70666700

El. paštas nsa@vds.lt

ITALIJA

Presidenza del Consiglio dei Ministri

D.I.S. – U.C.Se.

Via di Santa Susanna, 15

IT-00187 Roma

Telefonas +39 0661174266

Faksas +39 064885273

LIUKSEMBURGAS

Autorité nationale de Sécurité

Boîte postale 2379

1023 Luxembourg

Telefonai: + 352/2478 22 10 centrinis

+ 352 24782253 tiesioginis

Faksas +352 24782243

KIPRAS

ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΑΣ

ΣΤΡΑΤΙΩΤΙΚΟ ΕΠΙΤΕΛΕΙΟ ΤΟΥ ΥΠΟΥΡΓΟΥ

Εθνική Αρχή Ασφάλειας (ΕΑΑ)

Υπουργείο Άμυνας

Λεωφόρος Εμμανουήλ Ροΐδη 4

1432 Λευκωσία, Κύπρος

Telefonai: +357 22807569, +357 22807643,

+357 22807764

Faksas +357 22302351

VENGRIJA

Nemzeti Biztonsági Felügyelet

(Vengrijos nacionalinė saugumo institucija)

H-1024 Budapest, Szilágyi Erzsébet fasor 11/B

Telefonas +36 (1) 7952303

Faksas +36 (1) 7950344

Pašto adresas:

H-1357 Budapest, PO Box 2

El. paštas nbfb@nbfb.hu

Interneto svetainė www.nbfb.hu

MALTA

Ministry for Home Affairs and National Security
P.O. Box 146
MT-Valletta
Telefonas +356 21249844
Faksas +356 25695321

1300–342 Lisboa

Telefonas +351 213031710
Faksas +351 213031711

NYDERLANDAI

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20010
NL-2500 EA Den Haag
Telefonas +31 703204400
Faksas +31 703200733

Ministerie van Defensie
Beveiligingsautoriteit
Postbus 20701
NL-2500 ES Den Haag
Telefonas +31 703187060
Faksas +31 703187522

RUMUNIJA

Oficiul Registrului Național al Informațiilor Secrete de Stat

(Rumunijos NSI – ORNISS Nacionalinis įslaptintos informacijos registro biuras)

4 Mures Street
012275 Bucharest
Telefonas +40 212245830
Faksas +40 212240714
El. paštas nsa.romania@nsa.ro
Interneto svetainė www.orniss.ro

AUSTRIJA

Informationssicherheitskommission
Bundeskanzleramt
Ballhausplatz 2
AT-1014 Wien
Telefonas +43 1531152594
Faksas +43 1531152615
El. paštas ISK@bka.gv.at

SLOVĖNIJA

Urad Vlade RS za varovanje tajnih podatkov
Gregorčičeva 27
1000 Ljubljana
Telefonas +386 14781390
Faksas +386 14781399
El. paštas gp.uvtp@gov.si

LENKIJA

Agencja Bezpieczeństwa Wewnętrzznego – ABW
(Vidaus saugumo agentūra)
2A Rakowiecka St.
00–993 Warszawa
Telefonas +48 22 58 57 944
Faksas +48 22 58 57 443
El. paštas nsa@abw.gov.pl
Interneto svetainė www.abw.gov.pl

SLOVAKIJA

Národný bezpečnostný úrad
(Nacionalinė saugumo institucija)
Budatínska 30
P.O. Box 16
850 07 Bratislava
Telefonas +421 268692314
Faksas +421 263824005
Interneto svetainė www.nbusr.sk

PORTUGALIJA

Presidência do Conselho de Ministros
Autoridade Nacional de Segurança
Rua da Junqueira, 69

SUOMIJA

National Security Authority
Ministry for Foreign Affairs
P.O. Box 453
FI-00023 Government
Telefonas 16055890
Faksas +358 916055140
El. paštas NSA@formin.fi

ŠVEDIJA

Utrikesdepartementet

(Užsienio reikalų ministerija)

SSSB

S-103 39 Stockholm

Telefonas +46 84051000

Faksas +46 87231176

El. paštas ud-nsa@foreign.ministry.se

JUNGTINĖ KARALYSTĖ

UK National Security Authority

Room 335, 3rd Floor

70 Whitehall

London

SW1A 2AS

Telefonas 1: +44 2072765649

Telefonas 2: +44 2072765497

Faksas +44 2072765651

El. paštas UK-NSA@cabinet-office.x.gsi.gov.uk