EUROPOS IŠORĖS VEIKSMŲ TARNYBA

SĄJUNGOS VYRIAUSIOJO ĮGALIOTINIO UŽSIENIO REIKALAMS IR SAUGUMO POLITIKAI SPRENDIMAS

2023 m. birželio 19 d.

dėl Europos išorės veiksmų tarnybos saugumo taisyklių

(2023/C 263/04)

SĄJUNGOS VYRIAUSIASIS ĮGALIOTINIS UŽSIENIO REIKALAMS IR SAUGUMO POLITIKAI,

atsižvelgdamas į 2010 m. liepos 26 d. Tarybos sprendimą 2010/427/ES, kuriuo nustatoma Europos išorės veiksmų tarnybos struktūra ir veikimas ([1]) (toliau – Tarybos sprendimas 2010/427/ES), ypač į jo 10 straipsnio 1 dalį,

kadangi:

(1) Europos išorės veiksmų tarnyba (toliau – EIVT), kaip funkciniu požiūriu savarankiška Europos Sąjungos (ES) įstaiga, turi turėti saugumo taisykles, kaip numatyta Tarybos sprendimo 2010/427/ES 10 straipsnio 1 dalyje;

(2) Sąjungos vyriausiasis įgaliotinis užsienio reikalams ir saugumo politikai (toliau – vyriausiasis įgaliotinis) turi nuspręsti dėl EIVT saugumo taisyklių, kurios apimtų visus saugumo aspektus, susijusius su EIVT veikimu, kad EIVT galėtų veiksmingai valdyti riziką, kylančią darbuotojams, už kuriuos atsakinga EIVT, jos materialiajam turtui, informacijai ir lankytojams, ir kad ji vykdytų rūpestingumo pareigą ir įsipareigojimus šiuo atžvilgiu;

(3) visų pirma turėtų būti užtikrintas toks darbuotojų, už kuriuos atsakinga EIVT, EIVT materialiojo turto, įskaitant ryšių ir informacines sistemas, informacijos ir lankytojų apsaugos lygis, kuris atitiktų Tarybos, Komisijos, valstybių narių ir atitinkamai tarptautinių organizacijų geriausią praktiką;

(4) EIVT saugumo taisyklės turėtų padėti užtikrinti labiau suderintą visapusišką bendrą sistemą Europos Sąjungoje, skirtą ES įslaptintos informacijos (toliau – ESĮI) apsaugai, remiantis Europos Sąjungos Tarybos (toliau – Taryba) saugumo taisyklėmis ir Europos Komisijos saugumo nuostatomis ir išlaikant kuo didesnį suderinamumą su jomis;

(5) EIVT, Taryba ir Komisija yra įsipareigojusios taikyti lygiaverčius ESĮI apsaugą užtikrinančius saugumo standartus;

(6) šis sprendimas nedaro poveikio Sutarties dėl Europos Sąjungos veikimo (SESV) 15 bei 16 straipsniams ir jų įgyvendinamiesiems aktams;

(7) būtina nustatyti saugumo organizavimą EIVT ir paskirstyti saugumo užduotis EIVT struktūrose;

(8) vyriausiasis įgaliotinis reikiamu mastu turėtų atsižvelgti į atitinkamą valstybių narių, Tarybos generalinio sekretoriato ir Komisijos patirtį;

(9) vyriausiasis įgaliotinis turėtų imtis visų tinkamų priemonių, būtinų, kad šios taisyklės būtų įgyvendintos, padedamas valstybių narių, Tarybos generalinio sekretoriato ir Komisijos;

([1]) OL L 201, 2010 8 3, p. 30.

(10) net jei EIVT Saugumo institucija yra EIVT generalinis sekretorius, tikslinga peržiūrėti EIVT saugumo taisykles, visų pirma siekiant atsižvelgti į Reagavimo į krizes centro įsteigimą ir tuo tikslu panaikinti ir pakeisti 2017 m. rugsėjo 19 d. Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai sprendimą ADMIN(2017) 10 ([2]);

(11) vadovaujantis 2017 m. rugsėjo 19 d. Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai sprendimo ADMIN(2017) 10 dėl Europos išorės veiksmų tarnybos saugumo taisyklių 15 straipsnio 4 dalies a punktu, dėl EIVT saugumo taisyklių numatomų pakeitimų konsultuotasi su EIVT Saugumo komitetu,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Tikslas ir taikymo sritis

Šiuo sprendimu nustatomos Europos išorės veiksmų tarnybos saugumo taisyklės (toliau – EIVT saugumo taisyklės).

Pagal Tarybos sprendimo 2010/427/ES 10 straipsnio 1 dalį jos taikomos visiems EIVT personalo nariams ir visiems darbuotojams Sąjungos delegacijose, nepaisant jų administracinio statuso ar to, kokia administracija juos paskyrė, ir jomis nustatoma bendroji reglamentavimo sistema, kad būtų veiksmingai valdoma rizika, kylanti darbuotojams, už kuriuos atsakinga EIVT, kaip nurodyta 2 straipsnyje, EIVT patalpoms, materialiajam turtui, informacijai ir lankytojams.

2 straipsnis

Apibrėžtys

Šiame sprendime vartojamų terminų apibrėžtys:

a) EIVT personalas – EIVT pareigūnai ir kiti Europos Sąjungos tarnautojai, įskaitant valstybių narių diplomatinių tarnybų darbuotojus, kurie įdarbinami kaip laikinieji darbuotojai, ir komandiruotus nacionalinius ekspertus, kaip apibrėžta Tarybos sprendimo 2010/427/ES 6 straipsnio atitinkamai 2 ir 3 dalyse;

b) darbuotojai, už kuriuos atsakinga EIVT, – būstinėje ir Sąjungos delegacijose dirbantys EIVT personalo nariai ir visi kiti darbuotojai Sąjungos delegacijose, nepaisant jų administracinio statuso ar to, kokia administracija juos paskyrė, taip pat, šio sprendimo kontekste, vyriausiasis įgaliotinis ir atitinkamai kiti darbuotojai, kurie dirba EIVT būstinės patalpose;

c) reikalavimus atitinkantys išlaikytiniai – darbuotojo, už kurį Sąjungos delegacijose atsakinga EIVT, šeimos nariai, kurie yra jo atitinkamo namų ūkio nariai, kaip pranešta priimančiosios valstybės Užsienio reikalų ministerijai, ir kurie faktiškai su juo gyvena įdarbinimo vietoje evakavimo iš šalies metu;

d) EIVT patalpos – visos EIVT įstaigos, įskaitant pastatus, biurus, kabinetus ir kitas zonas, ir zonos su įrengtomis ryšių ir informacinėmis sistemomis (įskaitant sistemas, kuriomis tvarkoma ESĮI), kuriose EIVT vykdo nuolatinę ar laikiną veiklą;

e) EIVT saugumo interesai – darbuotojai, už kuriuos atsakinga EIVT, EIVT patalpos, išlaikytiniai, materialusis turtas, įskaitant ryšių ir informacines sistemas, informacija ir lankytojai;

f) ESĮI – bet kuri informacija arba medžiaga, kuriai suteikta ES slaptumo žyma ir kurią be leidimo atskleidus galėtų būti padaryta įvairaus dydžio žala Europos Sąjungos arba vienos ar daugiau valstybių narių interesams;

g) Sąjungos delegacija – delegacijos trečiosiose šalyse bei tarptautinėse organizacijose, kaip nurodyta Tarybos sprendimo 2010/427/ES 1 straipsnio 4 dalyje, ir ES tarnybose, vadovaujantis Tarybos sprendimo 2010/427/ES 5 straipsniu.

Kitos šiame sprendime vartojamų terminų apibrėžtys pateiktos atitinkamuose prieduose ir A priedėlyje.

([2]) OL C 126, 2018 4 10, p. 1.

3 straipsnis

Rūpestingumo pareiga

1. EIVT saugumo taisyklėmis siekiama užtikrinti, kad būtų vykdoma EIVT rūpestingumo pareiga ir jos įsipareigojimai šiuo atžvilgiu.

2. EIVT rūpestingumo pareiga yra stropus visų pagrįstų veiksmų vykdymas siekiant įgyvendinti saugumo priemones, kad būtų užkirstas kelias pagrįstai numatomai žalai EIVT saugumo interesams.

Ji apima ir saugumo, ir saugos aspektus, įskaitant aspektus, susijusius su ekstremaliosiomis situacijomis ar krizėmis, kad ir koks būtų jų pobūdis.

3. Atsižvelgdama į valstybių narių, ES institucijų ar įstaigų ir kitų šalių, kurių darbuotojai dirba Sąjungos delegacijose ir (arba) Sąjungos delegacijų patalpose, rūpestingumo pareigą, taip pat EIVT rūpestingumo pareigą Sąjungos delegacijų, kurios priimamos pirmiau minėtų kitų šalių patalpose, atžvilgiu, EIVT su kiekvienu iš šių subjektų sudaro administracinius susitarimus, kuriuose nustatomos jų atitinkamos funkcijos ir pareigos, užduotys ir bendradarbiavimo mechanizmai.

4 straipsnis

Fizinis saugumas ir infrastruktūros saugumas

1. Visose EIVT patalpose EIVT nustato visas tinkamas fizinio saugumo priemones (laikinas arba nuolatines), įskaitant patekimo kontrolės priemones, kad būtų apsaugoti EIVT saugumo interesai. Į tokias priemones atsižvelgiama projektuojant ir planuojant naujas patalpas arba prieš išsinuomojant esamas patalpas.

2. Darbuotojams, už kuriuos atsakinga EIVT, ir išlaikytiniams dėl su saugumu susijusių priežasčių tam tikrą laikotarpį ir tam tikrose zonose gali būti nustatyti specialūs įpareigojimai ar apribojimai.

3. 1 ir 2 dalyse nurodytos priemonės turi atitikti įvertintą riziką.

5 straipsnis

Parengties lygiai ir krizinės situacijos

1. EIVT Saugumo institucija, kaip apibrėžta 13 straipsnio I skirsnio 1 dalyje, yra atsakinga už tai, kad būtų nustatyti parengties lygiai ir įdiegtos tinkamos parengties lygių priemonės, kad būtų numatomos grėsmės ir incidentai, darantys poveikį saugumui EIVT, arba į juos būtų reaguojama.

2. 1 dalyje nurodytos parengties lygių priemonės turi atitikti grėsmės saugumui lygį. Parengties lygius EIVT Saugumo institucija nustato glaudžiai bendradarbiaudama su kitų Sąjungos institucijų, agentūrų ir įstaigų, taip pat valstybės (-ių) narės (-ių), kurioje (-iose) yra EIVT patalpų, kompetentingomis tarnybomis.

3. EIVT Saugumo institucija yra kontaktinis punktas parengties lygių ir reagavimo į krizę klausimais. Ji gali perdeleguoti susijusias užduotis atitinkamai už išteklių valdymą atsakingam generaliniam direktoriui, kaip nurodyta Tarybos sprendimo 2010/427/ES 4 straipsnio 3 dalies a punkto antroje įtraukoje (EIVT būstinės vardu), ir Reagavimo į krizes centro (CRC) direktoriui (Sąjungos delegacijų vardu).

6 straipsnis

Įslaptintos informacijos apsauga

1. ESĮI apsauga reglamentuojama šiame sprendime, ypač jo A priede, nustatytais reikalavimais. Bet kokios ESĮI dalies turėtojas yra atsakingas už tinkamą jos apsaugą.

2. EIVT užtikrina, kad galimybė susipažinti su įslaptinta informacija būtų suteikta tik asmenims, kurie atitinka A priedo 5 straipsnyje nustatytas sąlygas.

3. Sąlygas, kuriomis vietos darbuotojai gali susipažinti su ESĮI, taip pat nustato vyriausias įgaliotinis pagal šio sprendimo A priede nustatytas ESĮI apsaugos taisykles.

4. EIVT *užtikrina* visų darbuotojų, už kuriuos atsakinga EIVT, ir visų EIVT rangovų darbuotojų patikimumo pažymėjimų statuso *administravimą*.

5. Valstybėms narėms nacionaline slaptumo žyma pažymėtą įslaptintą informaciją perdavus į EIVT struktūras ar tinklus, EIVT tą informaciją saugo laikydamasi reikalavimų, taikomų lygiaverčio slaptumo žymos laipsnio ESĮI, kaip nustatyta šio sprendimo B priedėlyje pateiktoje slaptumo žymų atitikmenų lentelėje.

6. EIVT zonos, kuriose saugoma CONFIDENTIEL UE/EU CONFIDENTIAL arba lygiaverčio ar aukštesnio laipsnio slaptumo žyma pažymėta informacija, įrengiamos kaip saugumo zonos pagal šio sprendimo A II priede nustatytas taisykles, o EIVT Saugumo institucija jas patvirtina.

7. Vyriausiojo įgaliotinio pareigų, susijusių su susitarimais ar administraciniais susitarimais su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis dėl keitimosi ESĮI, vykdymo procedūros aprašytos šio sprendimo A ir *A VI* prieduose.

8. Generalinis sekretorius nustato sąlygas, kuriomis EIVT gali dalytis savo turima ESĮI su kitomis Sąjungos institucijomis, įstaigomis, tarnybomis ar agentūromis. Tam bus sukurta atitinkama sistema, be kita ko, prireikus tuo tikslu sudarant *tarpinstitucinius* susitarimus ar kitokius susitarimus.

9. Pagal tokią sistemą užtikrinama, kad ESĮI būtų taikoma jos slaptumo žymos laipsnį atitinkanti apsauga, laikantis pagrindinių principų ir būtiniausių standartų, kurie turi būti lygiaverčiai nustatytiesiems šiame sprendime.

7 straipsnis

Reagavimas į saugumo incidentus, ekstremaliąsias situacijas ir krizes

1. Siekdama užtikrinti, kad į saugumo incidentus būtų reaguojama laiku ir veiksmingai, EIVT nustato pranešimų apie tokius incidentus ir ekstremaliąsias situacijas procedūrą, kuria turi būti galima pasinaudoti dvidešimt keturias valandas per parą, septynias dienas per savaitę ir kuri apima visus saugumo incidentus ir grėsmes EIVT saugumo interesams (pvz., avarijas, konfliktus, piktavališkus veiksmus, nusikalstamus veiksmus, žmonių grobimą bei įkaitų ėmimą, su sveikata susijusias ekstremaliąsias situacijas, ryšių ir informacinių sistemų incidentus, kibernetinius išpuolius ir kt.).

2. Tarp EIVT būstinės, Sąjungos delegacijų, Tarybos, Komisijos, ES specialiųjų įgaliotinių ir valstybių narių sukuriami ekstremaliosioms situacijoms skirti ryšių palaikymo kanalai, padedantys jiems reaguoti į su personalu susijusias krizes, saugumo incidentus bei ekstremaliąsias situacijas ir jų padarinius, įskaitant nenumatytų atvejų planavimą.

3. Reagavimas į saugumo incidentus / ekstremaliąsias situacijas / krizes, *inter alia*, apima:

— veiksmingos pagalbos priimant sprendimus dėl su personalu susijusių grėsmių, saugumo incidentų ir ekstremaliųjų situacijų, įskaitant sprendimus dėl misijos personalo išvežimo ar misijos laikino sustabdymo, procedūras ir

— darbuotojų susigrąžinimo politiką ir procedūras (pvz., darbuotojų dingimo, pagrobimo arba paėmimo įkaitais atvejais), atsižvelgiant į konkrečią valstybių narių, ES institucijų ir EIVT atsakomybę šiuo klausimu. Dėl konkrečių pajėgumų poreikio valdant tokias operacijas sprendžiama atsižvelgiant į išteklius, kuriuos galėtų suteikti valstybės narės.

4. EIVT nustato tinkamas pranešimų apie saugumo incidentus Sąjungos delegacijose teikimo procedūras. Kai tinkama, informuojamos valstybės narės, Komisija, visos kitos atitinkamos institucijos, taip pat atitinkami saugumo komitetai.

5. Reagavimo į incidentus, ekstremaliąsias situacijas ir krizes procedūros reguliariai išbandomos ir peržiūrimos.

8 straipsnis

Ryšių ir informacinių sistemų saugumas

1. EIVT saugo ryšių ir informacinėse sistemose (RIS), kaip apibrėžta šio sprendimo A priedėlyje, tvarkomą informaciją nuo grėsmių, kylančių konfidencialumui, vientisumui, prieinamumui, autentiškumui ir atsakomybės už veiksmus prisiėmimui.

2. Visų EIVT turimų ar naudojamų RIS apsaugai skirtas taisykles, saugumo gaires ir saugumo programą tvirtina EIVT Saugumo institucija.

3. Šios taisyklės, politika ir programa turi atitikti Tarybos ir Komisijos taisykles, politiką bei programą ir, kai tinkama, valstybių narių taikomą saugumo politiką, o jų įgyvendinimas turi būti glaudžiai su jomis koordinuojamas.

4. Visos RIS, kuriose tvarkoma įslaptinta informacija, turi būti akredituojamos. EIVT, konsultuodamasi su Tarybos generaliniu sekretoriatu ir Komisija, taiko saugumo akreditavimo valdymo sistemą.

5. Tais atvejais, kai EIVT tvarkomos ESĮI apsauga užtikrinama naudojant šifravimo priemones, tokias priemones tvirtina EIVT kriptografijos patvirtinimo institucija, remdamasi Tarybos Saugumo komiteto rekomendacija.

6. EIVT Saugumo institucija, tiek, kiek būtina, įsteigia šias informacijos saugumo užtikrinimo institucijas:

a) Informacijos saugumo užtikrinimo instituciją (ISUI);

b) TEMPEST instituciją (TEI);

c) Kriptografijos patvirtinimo instituciją (KPI);

d) Kriptografijos platinimo instituciją (KPLI).

7. Atitinkamoms sistemoms tvarkyti EIVT Saugumo institucija įsteigia šias institucijas:

a) Saugumo akreditavimo instituciją (SAI);

b) Informacijos saugumo užtikrinimo operacinę instituciją (ISUOI).

8. Šio straipsnio įgyvendinimo nuostatos, susijusios su ESĮI apsauga, išdėstytos A ir A IV prieduose.

9 straipsnis

Įslaptintos informacijos saugumo pažeidimai ir neteisėtas atskleidimas

1. Saugumo pažeidimu laikomas šiame sprendime nustatytoms saugumo taisyklėms ir (arba) saugumo politikai ar gairėms, kuriomis nustatytos šiam sprendimui įgyvendinti būtinos priemonės (patvirtintos pagal 21 straipsnio 1 dalį), priešingas veiksmas arba neveikimas.

2. Neteisėtas įslaptintos informacijos atskleidimas įvyksta tada, kai ji visiškai arba iš dalies atskleidžiama leidimo neturintiems asmenims ar subjektams.

3. Apie bet kokį faktinį ar įtariamą saugumo pažeidimą ir apie bet kokį faktinį ar įtariamą įslaptintos informacijos neteisėtą atskleidimą nedelsiant pranešama už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoriui, o jis imasi tinkamų priemonių, kaip nustatyta A priedo 11 straipsnyje.

4. Bet kuriam asmeniui, kuris yra atsakingas už šiame sprendime nustatytų saugumo taisyklių pažeidimą arba už neteisėtą įslaptintos informacijos atskleidimą, gali būti taikomos drausminės ir (arba) teisinės priemonės pagal taikomus įstatymus, taisykles ir kitus teisės aktus, kaip nustatyta A priedo 11 straipsnio 3 dalyje.

10 straipsnis

Saugumo incidentų, pažeidimų ir (arba) neteisėto informacijos atskleidimo atvejų tyrimas ir taisomieji veiksmai

1. Nedarant poveikio Tarnybos nuostatų ([3]) 86 straipsniui ir IX priedui, už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas gali inicijuoti ir atlikti patikimumo patikrinimus:

a) ESĮI, Euratomo įslaptintos informacijos arba neskelbtinos neįslaptintos informacijos galimo nutekėjimo, netinkamo naudojimo arba neteisėto atskleidimo atveju;

b) kai siekiama atremti priešiškų žvalgybos tarnybų išpuolius prieš EIVT ir jos personalą;

c) kai siekiama atremti teroristinius išpuolius prieš EIVT ir jos personalą;

d) kibernetinių incidentų atveju;

e) kitų incidentų, įskaitant įtariamas nusikalstamas veikas, darančių arba galinčių daryti poveikį bendram EIVT saugumui, atveju.

2. EIVT Saugumo institucija, padedama už būstinės saugumą [...] ir EIVT informacijos saugumą atsakingo direktorato, už Reagavimo į krizes centrą (CRC) atsakingo direktorato ir atitinkamai ekspertų iš valstybių narių ir (arba) kitų ES institucijų, kai tinkama ir tinkamu būdu įgyvendina tyrimų metu nustatytus reikiamus taisomuosius veiksmus.

Įgaliojimai vykdyti ir koordinuoti patikimumo patikrinimus Europos išorės veiksmų tarnyboje gali būti suteikti tik darbuotojams, turintiems leidimą pagal asmeninius įgaliojimus, kuriuos jiems suteikė EIVT Saugumo institucija, atsižvelgiant į tų darbuotojų dabartines pareigas.

3. Tyrimus vykdantys asmenys gali susipažinti su visa informacija, būtina tokiems tyrimams vykdyti, ir šioje srityje gauna visapusišką visų EIVT tarnybų ir personalo pagalbą.

Tyrimus vykdantys asmenys gali imtis tinkamų veiksmų, kad apsaugotų įrodymų pėdsakus tokiu būdu, kuris būtų proporcingas tiriamo atvejo rimtumui.

4. Jei reikia susipažinti su informacija, kuri yra susijusi su asmens duomenimis, įskaitant ryšių ir informacinėse sistemose saugomus asmens duomenis, tokia galimybė su ja susipažinti suteikiama laikantis Reglamento (ES) 2018/1725 ([4]).

5. Jei būtina sukurti tyrimų duomenų bazę, kurioje ketinama saugoti asmens duomenis, apie tai pranešama Europos duomenų apsaugos priežiūros pareigūnui (EDAPP), kaip nustatyta pirmiau nurodytame reglamente.

11 straipsnis

Saugumo rizikos valdymas

1. Siekdami nustatyti EIVT saugumo poreikius, už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas ir už Reagavimo į krizes centrą (CRC) atsakingas direktoratas, glaudžiai bendradarbiaudami su Komisijos Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratu ir, kai tinkama, su Tarybos generalinio sekretoriato Saugumo tarnyba, parengia ir nuolat atnaujina išsamią saugumo rizikos vertinimo metodiką.

2. EIVT saugumo interesams kylančios rizikos valdymas yra procesas. Šio proceso tikslai – nustatyti žinomą saugumo riziką, apibrėžti saugumo priemones tokiai rizikai sumažinti iki priimtino lygio ir taikyti tas priemones laikantis pakopinės apsaugos koncepcijos. Reguliariai atliekamas tokių priemonių efektyvumo ir rizikos lygio vertinimas.

([3]) Europos Sąjungos pareigūnų tarnybos nuostatai ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygos (toliau – Tarnybos nuostatai).

([4]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (OL L 295, 2018 11 21, p. 39).

3. Šiame sprendime nustatytos funkcijos, pareigos ir užduotys nedaro poveikio kiekvieno darbuotojo, už kuriuos atsakinga EIVT, pareigoms; ypač ES darbuotojai, esantys misijose trečiosiose šalyse, turi vadovautis sveika nuovoka ir gebėti priimti tinkamus sprendimus dėl savo saugos ir saugumo, taip pat turi laikytis visų taikomų saugumo taisyklių, kitų teisės aktų, procedūrų ir instrukcijų.

4. Kad būtų užtikrinta rizikos saugumui prevencija ir kontrolė, įgaliotieji darbuotojai gali atlikti asmenų, kurie patenka į šio sprendimo taikymo sritį, patikrinimus, kad nustatytų, ar, tokiems asmenims leidus patekti į EIVT patalpas arba suteikus prieigą prie jos informacijos, kyla grėsmė saugumui. Tuo tikslu, laikydamiesi Reglamento (ES) 2018/1725, atitinkami įgaliotieji darbuotojai gali: a) naudotis bet kokiu EIVT prieinamu informacijos šaltiniu, atsižvelgdami į to informacijos šaltinio patikimumą; b) tinkamai pagrįstais atvejais susipažinti su asmens byla arba EIVT turimais joje dirbančių ar ketinamų įdarbinti asmenų arba rangovo darbuotojų duomenimis.

5. EIVT imasi visų pagrįstų priemonių, kad užtikrintų savo saugumo interesų apsaugą ir užkirstų kelią pagrįstai numatomai žalai šiems saugumo interesams.

6. ESĮI apsaugai užtikrinti skirtos EIVT saugumo priemonės visą savo gyvavimo ciklą turi atitikti visų pirma slaptumo žymos laipsnį, informacijos ar medžiagos formą ir kiekį, patalpų, kuriose laikoma ESĮI, vietos bei konstrukcijos reikalavimus ir piktavališkos ir (arba) nusikalstamos veiklos, įskaitant šnipinėjimą, sabotažą ir terorizmą, keliamą grėsmę, įskaitant vietos lygiu įvertintą grėsmę.

12 straipsnis

Informuotumas ir mokymas saugumo klausimais

1. EIVT Saugumo institucija užtikrina, kad už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas parengtų tinkamas informuotumo ir mokymo saugumo klausimais programas. Būstinės darbuotojams rengiami būtini informuotumui saugumo klausimais skirti informaciniai susitikimai ir mokymas; juos turi rengti už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktorato informuotumo saugumo klausimais grupės. Sąjungos delegacijų darbuotojams, taip pat, kai tinkama, jų reikalavimus atitinkantiems išlaikytiniams bus rengiami būtini informuotumui saugumo klausimais skirti informaciniai susitikimai ir mokymas, atitinkantys jų darbo arba gyvenamoje vietoje kylančią riziką; juos turi rengti saugumo valdymo grupės, koordinuodamos veiksmus su direktoratu, atsakingu už Reagavimo į krizes centrą (CRC).

2. Darbuotojai, prieš jiems suteikiant galimybę susipažinti su ESĮI, o vėliau – reguliariai, informuojami apie pareigą saugoti ESĮI pagal 6 straipsnyje nustatytas taisykles ir ją patvirtina.

13 straipsnis

Saugumo organizavimas EIVT

1 skirsnis. Bendrosios nuostatos

1. EIVT Saugumo institucija yra generalinis sekretorius. Vykdydamas šias funkcijas generalinis sekretorius užtikrina, kad:

a) sprendžiant visus EIVT veiklai svarbius saugumo klausimus, įskaitant klausimus, susijusius su rizikos EIVT saugumo interesams pobūdžiu ir apsaugos nuo jos priemonėmis, saugumo priemonės būtų reikiamu mastu derinamos su valstybių narių kompetentingomis institucijomis, Tarybos generaliniu sekretoriatu ir Komisija, taip pat atitinkamai su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis;

b) į saugumo aspektus būtų visiškai atsižvelgiama bet kokioje EIVT veikloje nuo pat jos pradžios;

c) galimybė susipažinti su įslaptinta informacija būtų suteikta tik asmenims, kurie atitinka A priedo 5 straipsnyje nustatytas sąlygas;

d) būtų imtasi tinkamų priemonių, kad būtų administruojamas visų darbuotojų, už kuriuos atsakinga EIVT, ir visų EIVT rangovų darbuotojų patikimumo pažymėjimų statusas;

e) būtų sukurta registrų sistema, kuria būtų užtikrinta, kad CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija Europos išorės veiksmų taryboje ir pateikus ją ES valstybėms narėms, ES institucijoms, įstaigoms ar agentūroms arba kitiems įgaliotiesiems gavėjams būtų tvarkoma pagal šį sprendimą. Visa ESĮI, kurią EIVT pateikė trečiosioms valstybėms arba tarptautinėms organizacijoms, ir visa įslaptinta informacija, gauta iš trečiųjų valstybių arba tarptautinių organizacijų, registruojama atskirai;

f) būtų vykdomi 16 straipsnyje nurodyti saugumo patikrinimai;

g) būtų vykdomi visų faktinių ar įtariamų saugumo pažeidimų, taip pat visų EIVT turimos ar parengtos įslaptintos informacijos faktinio ar įtariamo neteisėto atskleidimo arba praradimo atvejų tyrimai ir kad vykdant tokius tyrimus būtų prašoma atitinkamų saugumo institucijų pagalbos;

h) būtų parengti tinkami incidentų ir padarinių valdymo planai ir mechanizmai, kad būtų galima laiku ir veiksmingai reaguoti į saugumo incidentus;

i) būtų imtasi tinkamų priemonių tuo atveju, jei tam tikri asmenys nesilaiko šio sprendimo;

j) būtų nustatytos tinkamos fizinės ir organizacinės priemonės, skirtos EIVT saugumo interesams apsaugoti.

Šiuo atžvilgiu EIVT Saugumo institucija:

— konsultuodamasi su Komisija nustato Sąjungos delegacijų saugumo kategoriją,

— nustato reagavimo į krizes mechanizmą ir apibrėžia jo užduotis ir pareigas;

— priima sprendimą (kai tinkama, pasikonsultavusi su vyriausiuoju įgaliotiniu), kada evakuoti Sąjungos delegacijos darbuotojus, jei tai būtina atsižvelgiant į saugumo padėtį,

— priima sprendimus dėl taikytinų reikalavimus atitinkančių išlaikytinių apsaugos priemonių, kai tinkama, atsižvelgdama į susitarimus su ES institucijomis, kaip nurodyta 3 straipsnio 3 dalyje,

— tvirtina šifruotų ryšių politiką, visų pirma šifravimo priemonių diegimo programą ir mechanizmą.

2. Pagal Tarybos sprendimo 2010/427/ES 10 straipsnio 3 dalį EIVT Saugumo institucijai šias užduotis vykdyti bendrai padeda:

i) už išteklių valdymą atsakingas generalinis direktorius, padedamas už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktoriaus,

ii) Reagavimo į krizes centro (CRC) direktorius

ir atitinkamai už taikos, saugumo ir gynybos klausimus atsakingas generalinio sekretoriaus pavaduotojas, kad būtų užtikrintas suderinamumas su saugumo priemonėmis, kurių turi būti imtasi BSGP misijų ir operacijų tikslais.

3. Generalinis sekretorius, kaip EIVT Saugumo institucija, gali atitinkamai perdeleguoti savo užduotis.

4. Kiekvienas padalinio / skyriaus vadovas yra atsakingas už tų taisyklių, taip pat šio sprendimo 21 straipsnyje nurodytų saugumo gairių ir visų kitų procedūrų ar priemonių, kuriomis siekiama apsaugoti ESĮI jo padalinyje / skyriuje, įgyvendinimo užtikrinimą.

Kiekvieno padalinio / skyriaus vadovas ne tik vykdo pirmiau nurodytas funkcijas, bet ir skiria darbuotojus į padalinio saugumo koordinatorių pareigas. Darbuotojų, vykdančių tokias funkcijas, skaičius turi būti proporcingas atitinkamo padalinio /skyriaus tvarkomos ESĮI kiekiui.

Kai tinkama ir tinkamu būdu, padalinio saugumo koordinatoriai padeda savo padalinio / skyriaus vadovui ir remia jį, vykdydami šias su saugumu susijusias užduotis:

a) rengia papildomus saugumo reikalavimus, atitinkančius konkrečius padalinio / skyriaus poreikius, konsultuodamiesi su už būstinės saugumą ir EIVT informacijos saugumą atsakingu direktoratu;

b) papildo už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktorato reguliariai rengiamus informacinius pranešimus saugumo klausimais jų padalinio / skyriaus nariams informacija apie papildomus saugumo reikalavimus, kaip nurodyta a punkte;

c) užtikrina, kad jų padalinyje / skyriuje būtų laikomasi principo „būtina žinoti“;

d) kai taikytina, tvarko ir atnaujina saugos kodų ir raktų sąrašą;

e) kai taikytina, užtikrina, kad saugumo procedūros ir saugumo priemonės būtų nuolat atnaujinamos ir veiksmingos;

f) praneša apie visus saugumo pažeidimus ir (arba) ESĮI neteisėto atskleidimo atvejus savo direktoriui ir už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui;

g) surengia informacinį susitikimą su EIVT nebedirbančiais darbuotojais;

h) per savo vadovus reguliariai teikia ataskaitas dėl padalinio / skyriaus saugumo klausimų;

i) palaiko ryšius saugumo klausimais su už būstinės saugumą ir EIVT informacijos saugumą atsakingu direktoratu.

Apie visus veiksmus ar problemas, kurie galėtų daryti poveikį saugumui, laiku pranešama už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui.

2 skirsnis. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas

1. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas administraciniu požiūriu priklauso už išteklių valdymą atsakingam generaliniam direktoratui. Jis:

a) EIVT būstinėje vykdo su rūpestingumo pareiga susijusius EIVT įsipareigojimus ir yra atsakingas už visus saugumo klausimus EIVT būstinėje, be kita ko, susijusius su ryšių ir informacinėmis sistemomis (RIS) ir Sąjungos delegacijų informacijos saugumu;

b) valdo, koordinuoja, prižiūri ir (arba) įgyvendina visas saugumo priemones visose EIVT būstinės patalpose;

c) užtikrina visų veiksmų, kurie gali daryti poveikį EIVT saugumo interesų apsaugai, nuoseklumą ir suderinamumą su šiuo sprendimu ir jo įgyvendinimo nuostatomis;

d) padeda EIVT Saugumo akreditavimo institucijai vykdydamas ryšių ir informacinių sistemų, kuriose tvarkoma ESĮI, ir visų EIVT patalpų, kuriose ketinama leisti tvarkyti ir saugoti ESĮI, bendrosios saugumo aplinkos (BSA) ir vietos saugumo aplinkos (VSA) fizinio saugumo vertinimus.

Už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui pagal Tarybos sprendimo 2010/427/ES 10 straipsnio 3 dalį padeda atitinkamos valstybių narių tarnybos.

2. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktorius yra atsakingas už:

a) bendros EIVT saugumo interesų apsaugos užtikrinimą už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktorato kompetencijos srityje;

b) saugumo taisyklių rengimą, peržiūrą ir atnaujinimą, taip pat saugumo priemonių koordinavimą su Reagavimo į krizes centro (CRC) direktoriumi, valstybių narių kompetentingomis institucijomis ir atitinkamai su trečiųjų valstybių kompetentingomis institucijomis bei tarptautinėmis organizacijomis, kurios su ES susietos saugumo sutartimis ir (arba) susitarimais;

c) vyriausiojo įgaliotinio, EIVT Saugumo institucijos ir už taikos, saugumo ir gynybos klausimus atsakingo generalinio sekretoriaus pavaduotojo pagrindinio patarėjo visais su saugumu būstinėje ir informacijos saugumu susijusiais klausimais funkcijos vykdymą;

d) visų darbuotojų, už kuriuos atsakinga EIVT, ir EIVT rangovų darbuotojų patikimumo pažymėjimo statuso administravimą;

e) pirmininkavimą EIVT Saugumo komiteto nacionalinių saugumo institucijų (NSI) sudėties posėdžiams, kaip nustatyta šio sprendimo 15 straipsnio 1 dalyje, EIVT Saugumo institucijos nurodymu, taip pat paramą jo darbui;

f) ryšių palaikymą su visais partneriais ar kitomis institucijomis, nei nurodyta b punkte, saugumo klausimais, priklausančiais už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktorato kompetencijai;

g) prioritetų nustatymą ir pasiūlymų dėl būstinės ir Sąjungos delegacijų saugumo biudžeto valdymo teikimą, pastarąjį klausimą koordinuojant su Reagavimo į krizes centro (CRC) direktoriumi;

h) užtikrinimą, kad saugumo pažeidimai ir neteisėto atskleidimo atvejai, nurodyti šio sprendimo 9 straipsnyje, būtų registruojami ir, jei ir kai reikia, būtų pradėti ir vykdomi tyrimai;

i) reguliarius ir prireikus rengiamus susitikimus bendro intereso klausimais su Tarybos generalinio sekretoriato saugumo direktoriumi ir Komisijos Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato direktoriumi.

3. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas užmezga ryšius ir glaudžiai bendradarbiauja savo kompetencijos srityje su:

— valstybių narių nacionalinėmis saugumo institucijomis (NSI) ir (arba) kitomis kompetentingomis saugumo institucijomis, kad gautų jų pagalbą dėl informacijos, kuri jam reikalinga pavojams ir grėsmėms, kurių gali iškilti EIVT, jos personalui, veiklai, turtui bei ištekliams ir jos įslaptintai informacijai įprastoje jos veiklos vietoje, įvertinti;

— trečiųjų valstybių, su kuriomis ES yra sudariusi susitarimą dėl informacijos saugumo arba kurių teritorijoje Sąjunga dislokuoja BSGP misiją ar operaciją, kompetentingomis saugumo institucijomis; Tarybos generalinio sekretoriato Saugumo tarnyba bei Komisijos Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratu ir, kai tikslinga, kitų ES institucijų, įstaigų ir agentūrų saugumo padaliniais;

— tarptautinių organizacijų, su kuriomis ES yra sudariusi susitarimą dėl informacijos saugumo, saugumo padaliniu ir

— valstybių narių NSI visais klausimais, susijusiais su ESĮI apsauga, įskaitant asmens patikimumo pažymėjimus (APP).

3 skirsnis. Už Reagavimo į krizes centrą (CRC) atsakingas direktoratas

1. Už Reagavimo į krizes centrą (CRC) atsakingas direktoratas:

a) Sąjungos delegacijose vykdo su rūpestingumo pareiga susijusius EIVT įsipareigojimus;

b) užtikrina darbuotojų Sąjungos delegacijose, už kuriuos atsakinga EIVT, saugumą, siūlo priemones, kurios turi būti patvirtintos krizės atveju, kad būtų užtikrintas Sąjungos delegacijų veiklos tęstinumas, ir įgyvendina evakavimo procedūras glaudžiai bendradarbiaudamas su už išteklių valdymą atsakingo generalinio direktorato koordinavimo skyriumi;

c) valdo, koordinuoja, prižiūri ir (arba) įgyvendina visas saugumo priemones Sąjungos delegacijų EIVT patalpose;

d) užtikrina visų veiksmų, kurie gali daryti poveikį EIVT saugumo interesams, nuoseklumą ir suderinamumą su šiuo sprendimu ir jo įgyvendinimo nuostatomis CRC kompetencijos srityje;

e) padeda EIVT Saugumo akreditavimo institucijai vykdyti Sąjungos delegacijų patalpų, kuriose ketinama leisti tvarkyti ir saugoti ESĮI, fizinio saugumo vertinimus.

2. Reagavimo į krizes centro (CRC) direktorius yra atsakingas už:

a) bendros EIVT saugumo interesų apsaugos užtikrinimą už Reagavimo į krizes centrą (CRC) atsakingo direktorato kompetencijos srityje;

b) saugumo priemonių ir procedūrų koordinavimą su priimančiųjų valstybių kompetentingomis institucijomis ir atitinkamai su tam tikromis tarptautinėmis organizacijomis;

c) EIVT reagavimo į krizes mechanizmo aktyvavimo ir valdymo užtikrinimą;

d) EIVT dislokavimo pajėgumų (dislokuojamos paramos grupės, įskaitant reikiamą įrangą) rengimą ir valdymą, taip pat jų parengties bet kuriuo metu užtikrinimą;

e) vyriausiojo įgaliotinio, EIVT Saugumo institucijos ir už taikos, saugumo ir gynybos klausimus atsakingo generalinio sekretoriaus pavaduotojo pagrindinis patarėjo visais su Sąjungos delegacijų saugumu ir reagavimu į krizes, darančias joms poveikį, susijusiais klausimais funkcijos vykdymą;

f) pirmininkavimą EIVT Saugumo komiteto užsienio reikalų ministrų (URM) sudėties posėdžiams, kaip nustatyta šio sprendimo 15 straipsnio 1 dalyje, EIVT Saugumo institucijos nurodymu, taip pat paramą jo darbui;

g) ryšių palaikymą su visais partneriais ar kitomis institucijomis, nei nurodyta b punkte, saugumo klausimais, priklausančiais už Reagavimo į krizes centrą (CRC) atsakingo direktorato kompetencijai;

h) tai, kad būtų prisidedama nustatant prioritetus ir teikiant pasiūlymus dėl Sąjungos delegacijų saugumui skirto biudžeto valdymo, veiksmus koordinuojant už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoriui;

i) užtikrinimą, kad apie saugumo pažeidimus ir neteisėto atskleidimo atvejus už Reagavimo į krizes centrą (CRC) atsakingo direktorato kompetencijos srityje būtų pranešta už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui, kad būtų imtasi tinkamų tolesnių veiksmų.

3. Už Reagavimo į krizes centrą (CRC) atsakingas direktoratas užmezga ryšius ir glaudžiai bendradarbiauja Reagavimo į krizes centro kompetencijos srityje su:

— atitinkamais valstybių narių užsienio reikalų ministerijų padaliniais;

— kiek tai yra būtina, priimančiųjų valstybių, kurių teritorijoje yra įsikūrusios ES delegacijos, kompetentingomis saugumo institucijomis, kiek tai susiję su EIVT saugumo interesais;

— Tarybos generalinio sekretoriato Saugumo tarnyba bei Komisijos Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratu ir, kai tikslinga, kitų ES institucijų, įstaigų ir agentūrų saugumo padaliniais savo kompetencijos srityje;

— tarptautinių organizacijų saugumo padaliniais, kad būtų vykdomas naudingas veiksmų koordinavimas, savo kompetencijos srityje.

4 skirsnis. Sąjungos delegacijos

1. Kiekvienas delegacijos vadovas yra atsakingas už visų priemonių, susijusių su EIVT saugumo interesų, priklausančių Sąjungos delegacijų kompetencijai, apsauga Sąjungos delegacijų patalpose, įgyvendinimą vietoje ir valdymą.

Vadovaudamasis Reagavimo į krizes centro (CRC) gairėmis ir prireikus konsultuodamasis su priimančiosios valstybės kompetentingomis institucijomis, jis imasi visų praktiškai įmanomų priemonių užtikrinti, kad būtų įdiegtos tinkamos fizinės ir organizacinės priemonės jo su rūpestingumo pareiga susijusiems įsipareigojimams vykdyti.

Delegacijos vadovas nustato saugumo procedūras, skirtas reikalavimus atitinkantiems išlaikytiniams, kaip apibrėžta 2 straipsnio c punkte, apsaugoti, kai tinkama, atsižvelgdamas į visus administracinius susitarimus, nurodytus 3 straipsnio 3 dalyje.

Delegacijos vadovas visais savo kompetencijai priklausančiais klausimais, susijusiais su rūpestingumo pareiga, teikia ataskaitas Reagavimo į krizes centro (CRC) direktoriui, o kitais su saugumu susijusiais klausimais – už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktorato direktoriui.

Jam padeda už Reagavimo į krizes centrą (CRC) atsakingas direktoratas, Sąjungos delegacijos saugumo valdymo grupė, kurią sudaro saugumo užduotis ir funkcijas vykdantys darbuotojai, o prireikus – ir saugumo darbuotojai. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas padeda savo kompetencijos srityje.

Sąjungos delegacija užmezga reguliarius ryšius ir glaudžiai bendradarbiauja saugumo klausimais su valstybių narių diplomatinėmis atstovybėmis.

2. Be to, delegacijos vadovas:

— koordinuodamas veiksmus su Reagavimo į krizes centru (CRC), remdamasis bendrosiomis standartinėmis veiklos procedūromis, nustato išsamius Sąjungos delegacijos saugumo ir nenumatytų atvejų planus;

— Sąjungos delegacijos veikloje taiko veiksmingą, 24 valandas per parą ir 7 dienas per savaitę veikiančią saugumo incidentų ir ekstremaliųjų situacijų valdymo sistemą,

— užtikrina, kad visi Sąjungos delegacijos darbuotojai būtų apdrausti atsižvelgiant į sąlygas atitinkamoje vietovėje;

— užtikrina, kad į Sąjungos delegacijos pradinį mokymą, kuris teikiamas visiems Sąjungos delegacijos darbuotojams jiems atvykus į Sąjungos delegaciją, būtų įtrauktas saugumo aspektas, ir

— užtikrina, kad būtų įgyvendintos visos rekomendacijos, pateiktos atlikus saugumo vertinimus, ir reguliariai teikia rašytines ataskaitas dėl jų įgyvendinimo Reagavimo į krizes centro (CRC) direktoriui ir už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoriui.

3. Delegacijos vadovas išlieka atsakingas ir atskaitingas už saugumo valdymo ir organizacijos atsparumo užtikrinimą, tačiau gali deleguoti vykdyti savo saugumo užduočių vykdymą delegacijos saugumo koordinatoriui, kuris yra ir delegacijos vadovo pavaduotojas, arba, jei toks nepaskirtas, – atitinkamam pakaitiniam darbuotojui.

Visų pirma gali būti deleguojamos šios pareigos:

— saugumo funkcijų koordinavimas Sąjungos delegacijoje;

— ryšių palaikymas saugumo klausimais su priimančiosios valstybės kompetentingomis institucijomis ir atitinkamais valstybių narių ambasadų ir diplomatinių atstovybių darbuotojais, einančiais analogiškas pareigas;

— tinkamų saugumo valdymo procedūrų, susijusių su EIVT saugumo interesais, įskaitant ESĮI apsaugą, įgyvendinimas;

— užtikrinimas, kad būtų laikomasi saugumo taisyklių ir nurodymų;

— darbuotojų informavimas apie jiems taikomas saugumo taisykles ir apie konkrečius pavojus priimančiojoje valstybėje;

— užklausų dėl patikimumo patikrinimo ir postų, kuriuos užimantiems darbuotojams reikalingas asmens patikimumo pažymėjimas (APP), teikimas už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui ir

— nuolatinis delegacijos vadovo, regiono saugumo pareigūno (RSP) ir už Reagavimo į krizes centrą (CRC) atsakingo direktorato informavimas apie incidentus ar su saugumu susijusius pokyčius atitinkamoje vietovėje, susijusius su EIVT saugumo interesų apsauga.

4. Delegacijos vadovas gali deleguoti administracinio ar techninio pobūdžio saugumo užduotis administracijos vadovui ir kitiems Sąjungos delegacijos darbuotojams.

5. Sąjungos delegacijai padeda regiono saugumo pareigūnas (RSP). RSP Sąjungos delegacijose, atitinkančiose geografinius regionus, už kuriuos jie atsakingi, vykdo toliau nurodytas funkcijas.

Tam tikromis aplinkybėmis, kai tai būtina dėl esamos saugumo padėties, specialus RSP gali būti paskirtas į konkrečią Sąjungos delegaciją kaip nuolatinis darbuotojas.

Už Reagavimo į krizes centrą (CRC) atsakingo direktorato sprendimu RSP gali būti paskirtas į vietovę, kuri yra ne jo atsakomybės zonoje, įskaitant būstinę, arba, atsižvelgiant į esamą saugumo padėtį, netgi į bet kokią šalį eiti nuolatines pareigas.

6. RSP veiklą tiesiogiai kontroliuoja EIVT būstinės tarnyba, atsakinga už saugumą vietoje, tačiau administracinę kontrolę dalijasi jų įdarbinimo vietos delegacijos vadovas ir už saugumą vietoje atsakinga būstinės tarnyba. RSP konsultuoja delegacijos vadovą ir Sąjungos delegacijos darbuotojus ir padeda jiems rengiant ir įgyvendinant visas fizines, organizacines ir procedūrines priemones, susijusias su Sąjungos delegacijos saugumu.

7. RSP konsultuoja delegacijos vadovą ir Sąjungos delegacijos darbuotojus ir jiems padeda. Kai tikslinga, visų pirma tais atvejais, kai RSP yra nuolatinis darbuotojas, jis [...] turėtų padėti Sąjungos delegacijai vykdyti saugumo valdymo ir įgyvendinimo funkcijas, įskaitant saugumo sutarčių parengimą, akreditacijų ir patikimumo pažymėjimų tvarkymą.

14 straipsnis

BSGP operacijos ir ES specialieji įgaliotiniai

Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktorius ir Reagavimo į krizes centro (CRC) direktorius atitinkamose jų direktoratų kompetencijos srityse prireikus konsultuoja už bendrą saugumo ir gynybos politiką (BSGP) atsakingą valdantįjį direktorių, Europos Sąjungos karinio štabo (EUMS) generalinį direktorių, taip pat jam einant Karinių misijų planavimo ir vykdymo centro (MPCC) direktoriaus pareigas, ir už Civilinių operacijų planavimo ir vykdymo centrą (CPCC) atsakingą valdantįjį direktorių dėl BSGP misijų ir operacijų planavimo ir vykdymo saugumo aspektų, o ES specialiuosius įgaliotinius – dėl su jų įgaliojimais susijusių saugumo aspektų; šios nuostatos papildo šioje srityje galiojančias specialias Tarybos patvirtintos atitinkamos politikos nuostatas.

15 straipsnis

EIVT Saugumo komitetas

1. Įsteigiamas EIVT Saugumo komitetas.

Jam pirmininkauja EIVT Saugumo institucija arba paskirtasis delegatas; Saugumo komitetas posėdžiauja pirmininko nurodymu arba bet kurio komiteto nario prašymu. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas ir už Reagavimo į krizes centrą (CRC) atsakingas direktoratas atitinkamose jų kompetencijos srityse padeda pirmininkui vykdyti šią funkciją ir reikiamu mastu teikia administracinę pagalbą Komiteto darbui.

2. EIVT Saugumo komitetą sudaro šių subjektų atstovai:

— visų valstybių narių;

— Tarybos generalinio sekretoriato Saugumo tarnybos;

— Komisijos Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktorato.

Valstybės narės delegaciją EIVT Saugumo komitete gali sudaryti šių subjektų atstovai:

— nacionalinės saugumo institucijos (NSI) ir (arba) paskirtosios saugumo institucijos (PSI);

— už saugumą atsakingų užsienio reikalų ministerijų (URM) padalinių.

3. Prireikus komiteto atstovai gali dirbti kartu su ekspertais ir naudotis jų konsultacijomis. Gali būti pakviesti dalyvauti kitų ES institucijų, agentūrų ar įstaigų atstovai, nagrinėjant šių institucijų saugumo požiūriu svarbius klausimus.

4. Nedarant poveikio 5 daliai, EIVT Saugumo komitetas teikia pagalbą EIVT konsultuodamas visais saugumo klausimais, kurie svarbūs EIVT veiklai, būstinei ir Sąjungos delegacijoms.

Nedarant poveikio 5 daliai, su EIVT Saugumo komitetu visų pirma:

a) konsultuojamasi šiais klausimais:

— saugumo politikos, gairių, koncepcijų ar kitų su saugumu susijusių metodikos dokumentų, ypač dokumentų, susijusių su įslaptintos informacijos apsauga ir priemonėmis, kurių reikia imtis, jei EIVT personalo nariai nesilaiko saugumo taisyklių;

— techninių saugumo aspektų, kurie gali daryti poveikį vyriausiojo įgaliotinio sprendimui teikti rekomendaciją Tarybai dėl derybų dėl susitarimų dėl informacijos saugumo, kurie nurodyti A priedo 10 straipsnio 1 dalies a punkte, pradžios;

— šio sprendimo pakeitimų;

b) gali būti konsultuojamasi klausimais, susijusiais su EIVT būstinės ir Sąjungos delegacijų darbuotojų bei turto saugumu, arba jis gali būti atitinkamai informuojamas apie šiuos klausimus nedarant poveikio 3 straipsnio 3 daliai;

c) jis informuojamas apie visus EIVT įvykusius ESĮI neteisėto atskleidimo ar praradimo atvejus.

5. Šiame sprendime ir jo A priede pateiktų ESĮI apsaugos taisyklių pakeitimams turi vieningai pritarti valstybės narės, atstovaujamos EIVT Saugumo komitete. Tokia vieninga palanki nuomonė taip pat reikalinga prieš:

— pradedant derybas dėl administracinių susitarimų, nurodytų A priedo 10 straipsnio 1 dalies b punkte;

— išskirtinėmis aplinkybėmis, nurodytomis A VI priedo 9, 11 ir 12 dalyse, suteikiant įslaptintą informaciją;

— aplinkybėmis, nurodytomis A priedo 10 straipsnio 6 dalies paskutiniame sakinyje, prisiimant informacijos rengėjo atsakomybę.

Kai reikalinga vieninga palanki nuomonė, ši sąlyga bus laikoma įvykdyta, jei valstybių narių delegacijos per komiteto posėdžius nepateiks jokių prieštaravimų.

6. EIVT Saugumo komitetas visiškai atsižvelgia į galiojančią Tarybos ir Komisijos saugumo politiką ir gaires.

7. EIVT Saugumo komitetas gauna metinių EIVT patikrinimų sąrašą ir atliktų patikrinimų ataskaitas.

8. Posėdžių organizavimas

— EIVT Saugumo komitetas posėdžiauja bent du kartus per metus. Papildomus posėdžius gali sušaukti pirmininkas arba juos sušaukti gali paprašyti komiteto nariai; tai gali būti visos sudėties arba NSI/PSI ar MFA saugumo sudėties posėdžiai.

— EIVT Saugumo komitetas savo veiklą organizuoja taip, kad galėtų teikti rekomendacijas konkrečių saugumo sričių klausimais. Prireikus jis gali įsteigti kitus ekspertų pogrupius. Komitetas apibrėžia tokių ekspertų pogrupių įgaliojimus, o šie pogrupiai teikia jam savo veiklos ataskaitas.

— Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas ir už Reagavimo į krizes centrą (CRC) atsakingas direktoratas yra atsakingi už jų atitinkamai kompetencijai priklausančių klausimų, kurie bus svarstomi, parengimą. Kiekvienam posėdžiui pirmininkas parengia preliminarią darbotvarkę. Komiteto nariai gali siūlyti aptarti ir kitus klausimus.

16 straipsnis

Saugumo patikrinimai

1. EIVT Saugumo institucija užtikrina, kad EIVT būstinėje ir Sąjungos delegacijose būtų reguliariai vykdomi saugumo patikrinimai, siekiant įvertinti, ar tinkamai įgyvendinamos saugumo priemonės, ir patikrinti, ar jos atitinka šį sprendimą. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas, bendradarbiaudamas su už Reagavimo į krizes centrą (CRC) atsakingu direktoratu, gali, kai tikslinga, paskirti papildomus ekspertus, kurie dalyvautų saugumo patikrinimuose, vykdomuose pagal ES sutarties V antraštinės dalies 2 skyrių įsteigtose ES agentūrose ir įstaigose.

2. EIVT saugumo patikrinimai vykdomi vadovaujant už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui, kai tikslinga, padedant EIVT Reagavimo į krizes centrui (CRC) ir, 3 straipsnio 3 dalyje nurodytų susitarimų atžvilgiu, padedant kitų ES institucijų ar valstybių narių saugumo ekspertams.

3. Prireikus EIVT gali remtis valstybių narių, Tarybos generalinio sekretoriato ir Europos Komisijos patirtimi.

Kai būtina, dalyvauti Sąjungos delegacijos saugumo patikrinime gali būti pakviesti atitinkami valstybių narių misijų trečiosiose valstybėse saugumo ekspertai ir (arba) valstybių narių diplomatinių atstovybių saugumo padalinių atstovai.

4. Šio straipsnio įgyvendinimo nuostatos, susijusios su ESĮI apsauga, išdėstytos A III priede.

17 straipsnis

Įvertinimo vizitai

Siekiant įsitikinti, kad trečiojoje valstybėje arba tarptautinėje organizacijoje taikomos ESĮI, kuria keičiamasi pagal A priedo 10 straipsnio 1 dalies b punkte nurodytą administracinį susitarimą, apsaugos priemonės yra veiksmingos, rengiami įvertinimo vizitai.

Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas gali paskirti papildomus ekspertus, kurie dalyvautų įvertinimo vizituose trečiosiose valstybėse ar tarptautinėse organizacijose, su kuriomis ES yra sudariusi susitarimus dėl informacijos saugumo, nurodytus A priedo 10 straipsnio 1 dalies a punkte.

18 straipsnis

Veiklos tęstinumo planavimas

Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas ir už Reagavimo į krizes centrą (CRC) atsakingas direktoratas padeda EIVT Saugumo institucijai valdant su saugumu susijusius EIVT veiklos tęstinumo procesų aspektus, kurie yra bendro EIVT veiklos tęstinumo planavimo dalis.

19 straipsnis

Rekomendacijos dėl kelionių, skirtos misijoms, kurios vykdomos ne ES

Už Reagavimo į krizes centrą (CRC) atsakingas direktoratas užtikrina, kad būtų teikiamos rekomendacijos dėl kelionių, susijusios su darbuotojų, už kuriuos atsakinga EIVT, misijomis į ne ES šalis, remdamasis visų atitinkamų EIVT tarnybų, ypač INTCEN, už išteklių valdymą atsakingo generalinio direktorato kontržvalgybos grupės, geografinių padalinių ir Sąjungos delegacijų, ištekliais.

Už Reagavimo į krizes centrą (CRC) atsakingas direktoratas, gavęs prašymą ir remdamasis pirmiau nurodytais ištekliais, teikia konkrečias rekomendacijas dėl kelionių, susijusias su darbuotojų, už kuriuos atsakinga EIVT, misijomis į trečiąsias valstybes, kuriose rizikos lygis yra labai didelis arba padidėjęs.

20 straipsnis

Sveikata ir sauga

EIVT saugumo taisyklės papildo vyriausiojo įgaliotinio patvirtintas EIVT sveikatos ir saugos užtikrinimo taisykles.

21 straipsnis

Įgyvendinimas ir peržiūra

1. EIVT Saugumo institucija, atitinkamai pasikonsultavusi su EIVT Saugumo komitetu, tvirtina saugumo gaires, kuriose nustatomos priemonės, būtinos šių taisyklių įgyvendinimui EIVT, taip pat, glaudžiai bendradarbiaudama su valstybių narių kompetentingomis saugumo institucijomis ir padedama ES institucijų atitinkamų tarnybų, rengia pajėgumus, būtinus visiems saugumo aspektams užtikrinti.

2. Pagal Tarybos sprendimo 2010/427/ES 4 straipsnio 5 dalį prireikus EIVT gali sudaryti tarnybų lygio susitarimus su atitinkamomis Tarybos generalinio sekretoriato ir Komisijos tarnybomis.

3. Vyriausiasis įgaliotinis užtikrina bendrą šio sprendimo taikymo nuoseklumą ir nuolat peržiūri šias saugumo taisykles.

4. EIVT saugumo taisyklės turi būti įgyvendinamos glaudžiai bendradarbiaujant su valstybių narių kompetentingomis saugumo institucijomis.

5. EIVT užtikrina, kad EIVT reagavimo į krizes sistemoje būtų atsižvelgta į visus saugumo proceso aspektus.

6. Šio sprendimo įgyvendinimą užtikrina generalinis sekretorius, kaip Saugumo institucija, už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktorato direktorius ir Reagavimo į krizes centro (CRC)direktorius.

22 straipsnis

Ankstesnių sprendimų pakeitimas

Šiuo sprendimu panaikinamas ir pakeičiamas 2017 m. rugsėjo 19 d. Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai sprendimas ADMIN (2017)10 dėl Europos išorės veiksmų tarnybos saugumo taisyklių ([5]).

23 straipsnis

Baigiamosios nuostatos

Šis sprendimas įsigalioja jo pasirašymo dieną.

Jis skelbiamas *Europos Sąjungos oficialiajame leidinyje*.

EIVT Saugumo institucija visiems darbuotojams, kurie patenka į šio sprendimo ir jo priedų taikymo sritį, tinkamai ir laiku praneša apie jų turinį, įsigaliojimą ir visus tolesnius pakeitimus.

Priimta Briuselyje, 2023 m. birželio 19 d.

Josep BORRELL FONTELLES
Sąjungos vyriausiasis įgaliotinis
užsienio reikalams ir saugumo politikai

([5]) OL C 126, 2018 4 10, p. 1.

A PRIEDAS

ESĮI APSAUGOS PRINCIPAI IR STANDARTAI

1 straipsnis

Tikslas, taikymo sritis ir apibrėžtys

1. Šiame priede nustatyti pagrindiniai ESĮI apsaugai užtikrinti skirti saugumo principai ir būtiniausi standartai.

2. Šie pagrindiniai principai ir būtiniausi standartai taikomi EIVT ir darbuotojams, už kuriuos atsakinga EIVT, kaip nurodyta ir apibrėžta atitinkamai šio sprendimo 1 ir 2 straipsniuose.

2 straipsnis

ESĮI sąvokos apibrėžtis, slaptumo žymos ir kitos žymos

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

2. ESĮI žymima viena iš šių slaptumo žymų:

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

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

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

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

3 straipsnis

Įslaptinimo administravimas

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

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

3. EIVT Saugumo institucija, pasikonsultavusi su EIVT Saugumo komitetu pagal šio sprendimo 15 straipsnio 5 dalį, patvirtina ESĮI rengimo saugumo gaires, kurios apima praktinį žymų vadovą.

4 straipsnis

Įslaptintos informacijos apsauga

1. ESĮI apsaugoma laikantis šio sprendimo.

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

3. Valstybėms narėms nacionaline slaptumo žyma pažymėtą įslaptintą informaciją perdavus į EIVT struktūras ar tinklus, EIVT tą informaciją saugo laikydamasi reikalavimų, taikomų lygiaverčio slaptumo žymos laipsnio ESĮI, kaip nustatyta B priedėlyje pateiktoje slaptumo žymų atitikmenų lentelėje.

EIVT nustato tinkamas procedūras, skirtas tiksliam registravimui užtikrinti, kurios taikomos tokios informacijos rengėjams:

— įslaptintos informacijos, kurią gauna EIVT, ir

— pradinės medžiagos, kuri yra EIVT parengtos įslaptintos informacijos dalis.

Apie šias procedūras pranešama EIVT Saugumo komitetui.

4. Didelio ESĮI kiekio ar ESĮI rinkinio atveju gali būti reikalaujama užtikrinti tokio lygio apsaugą, kuri žymima aukštesnio laipsnio slaptumo žyma nei šios informacijos sudedamosios dalys.

5 straipsnis

Personalo patikimumo užtikrinimo priemonės, taikomos tvarkant ES įslaptintą informaciją

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

— kurie atitinka principą „būtina žinoti“,

— kurių patikimumas patikrintas atitinkamu lygiu ir kuriems suteikta teisė susipažinti su informacija, pažymėta CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio saugumo žyma, arba kiti tinkami leidimai pagal nacionalinius įstatymus ir teisės aktus, ir

— kurie yra informuoti apie jų pareigas.

2. Taikant asmens patikimumo pažymėjimo (APP) išdavimo procedūras, nustatoma, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ESĮI.

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

4. Šio straipsnio įgyvendinimo nuostatos išdėstytos A I priede.

6 straipsnis

ES įslaptintos informacijos fizinis saugumas

1. Fizinis saugumas yra fizinių ir techninių apsaugos priemonių taikymas siekiant atgrasyti nuo neteisėtos prieigos prie ESĮI.

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

3. Fizinio saugumo priemonės taikomos visose patalpose, pastatuose, kabinetuose, salėse ir kitose zonose, kuriose tvarkoma arba saugoma ESĮI, įskaitant zonas, kuriose įrengtos ryšių ir informacinės sistemos, kaip apibrėžta šio sprendimo A priedėlyje.

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

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

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos A II priede.

7 straipsnis

Įslaptintos informacijos administravimas

1. Įslaptintos informacijos administravimas – administracinių ESĮI kontrolės visą jos gyvavimo ciklą priemonių taikymas siekiant papildyti 5, 6 ir 8 straipsniuose numatytas priemones ir tokiu būdu atgrasyti nuo tokios informacijos sąmoningo ar atsitiktinio neteisėto atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius. Tokios priemonės visų pirma yra susijusios su ESĮI rengimu, registravimu, kopijavimu, vertimu, gabenimu, tvarkymu, saugojimu ir naikinimu.

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

3. Tarnybas ir patalpas, kuriose ESĮI tvarkoma arba saugoma, reguliariai tikrina EIVT Saugumo institucija.

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

a) paprastai ESĮI perduodama elektroninėmis priemonėmis, apsaugant informaciją šifravimo priemonėmis, patvirtintomis pagal šio sprendimo 7 straipsnio 5 dalį ir aiškiai apibrėžtas saugios eksploatacijos taisykles (SecOPs);

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

   i) elektroninėse laikmenose (pvz., USB atmintinėse, kompaktiniuose diskuose, kietuosiuose diskuose), informaciją apsaugant pagal šio sprendimo 8 straipsnio 5 dalį patvirtintomis šifravimo priemonėmis arba

   ii) visais kitais atvejais – EIVT Saugumo institucijos nurodytu būdu, laikantis atitinkamų A III priedo V skirsnyje nustatytų apsaugos priemonių.

5. Šio straipsnio įgyvendinimo nuostatos išdėstytos A III priede.

8 straipsnis

Ryšių ir informacinėse sistemose tvarkomos ESĮI apsauga

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

2. ESĮI RIS tvarkoma laikantis ISU koncepcijos.

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

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

5. Tais atvejais, kai ESĮI apsauga užtikrinama šifravimo priemonėmis, tokios priemonės patvirtinamos pagal šio sprendimo 8 straipsnio 5 dalį.

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

7. Pagal šio sprendimo 8 straipsnio 6 dalį, tiek, kiek būtina, įsteigiamos šios ISU institucijos:

a) ISU institucija (ISUI);

b) TEMPEST institucija (TEI);

c) Kriptografijos patvirtinimo institucija (KPI);

d) Kriptografijos platinimo institucija (KPLI).

8. Pagal šio sprendimo 8 straipsnio 7 dalį kiekvienoje sistemoje įsteigiamos šios institucijos:

a) Saugumo akreditavimo institucija (SAI);

b) ISU operacinė institucija.

9. Šio straipsnio įgyvendinimo nuostatos išdėstytos A IV priede.

9 straipsnis

Pramoninis saugumas

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

2. EIVT sutartimi gali patikėti pramonės arba kitiems subjektams, registruotiems valstybėje narėje arba trečiojoje valstybėje, kuri yra sudariusi susitarimą dėl informacijos saugumo arba administracinį susitarimą pagal A priedo 10 straipsnio 1 dalį, užduotis, kurioms atlikti reikia arba reikės susipažinti su ESĮI arba ją tvarkyti ar saugoti.

3. EIVT, kaip perkančioji organizacija, užtikrina, kad skiriant įslaptintas sutartis pramonės ar kitiems subjektams būtų laikomasi šiame sprendime išdėstytų ir sutartyje nurodytų būtiniausių pramoninio saugumo standartų. Ji, pasitelkdama atitinkamas NSI/PSI, užtikrina atitiktį būtiniausiems standartams.

4. Valstybėje narėje įregistruoti rangovai ar subrangovai, dalyvaujantys įslaptintose sutartyse arba subrangos sutartyse, pagal kurias jas vykdant arba prieš jas sudarant šių subjektų patalpose tvarkoma ir saugoma įslaptinta informacija, pažymėta slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET, turi turėti reikiamą slaptumo žymos laipsnį atitinkantį Įmonės patikimumą patvirtinantį pažymėjimą (ĮPPP), išduotą atitinkamos valstybės narės NSI, PSI ar kitos kompetentingos saugumo institucijos.

5. Rangovo ar subrangovo darbuotojai, kuriems vykdant įslaptintą sutartį reikia susipažinti su slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija, turi turėti asmens patikimumo pažymėjimą (APP), išduotą atitinkamos nacionalinės saugumo institucijos (NSI), paskirtosios saugumo institucijos (PSI) ar kitos kompetentingos saugumo institucijos pagal nacionalinius įstatymus ir teisės aktus bei A I priede nustatytus būtiniausius saugumo standartus.

6. Šio straipsnio įgyvendinimo nuostatos išdėstytos A V priede.

10 straipsnis

Keitimasis įslaptinta informacija su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis

1. EIVT gali keistis ESĮI su trečiąja valstybe ar tarptautine organizacija, tik jei:

a) galioja ES ir atitinkamos trečiosios valstybės ar tarptautinės organizacijos susitarimas dėl informacijos saugumo, sudarytas pagal ES sutarties 37 straipsnį ir SESV 218 straipsnį, arba

b) įsigaliojo vyriausiojo įgaliotinio ir atitinkamos trečiosios valstybės ar tarptautinės organizacijos kompetentingų saugumo institucijų administracinis susitarimas dėl keitimosi iš principo ne aukštesnio lygio nei RESTREINT UE/EU RESTRICTED slaptumo žyma pažymėta informacija, sudarytas pagal procedūrą, nustatytą šio sprendimo 15 straipsnio 5 dalyje, arba

c) taikytinas ES ir atitinkamos trečiosios valstybės bendrasis arba *ad hoc* dalyvavimo susitarimas BSGP krizių valdymo operacijos kontekste, sudarytas pagal ES sutarties 37 straipsnį ir SESV veikimo 218 straipsnį,

ir įvykdytos tame dokumente nustatytos sąlygos.

Pirmiau nurodytų pagrindinių taisyklių išimtys išdėstytos A VI priedo V skirsnyje.

2. Į 1 dalies b punkte nurodytus administracinius susitarimus įtraukiamos nuostatos, kuriomis užtikrinama, jog trečiosioms valstybėms arba tarptautinėms organizacijoms gavus ESĮI, tai informacijai užtikrinama jos slaptumo žymos laipsnį atitinkanti apsauga, remiantis būtiniausiais standartais, kurie yra ne mažiau griežti nei šiame sprendime nustatyti standartai.

Informacija, kuria keičiamasi pagal 1 dalies c punkte sudarytus susitarimus, gali būti tik informacija, susijusi su BSGP operacijomis, kuriose atitinkama trečioji valstybė dalyvauja remiantis šiais susitarimais ir pagal jų nuostatas.

3. Jeigu vėliau sudaromas Sąjungos ir dalyvaujančiosios trečiosios valstybės ar tarptautinės organizacijos susitarimas dėl informacijos saugumo, šio susitarimo dėl informacijos saugumo nuostatos yra viršesnės už bet kokiuose susitarimuose dėl dalyvavimo bendrųjų sąlygų, *ad hoc* susitarimuose dėl dalyvavimo arba *ad hoc* administraciniuose susitarimuose išdėstytas nuostatas dėl keitimosi įslaptinta informacija, kiek tai susiję su keitimusi ESĮI ir jos tvarkymu.

4. BSGP operacijos vykdymui surinkta ESĮI gali būti suteikiama trečiųjų valstybių ar tarptautinių organizacijų į tą operaciją komandiruotam personalui, vadovaujantis 1–3 dalių ir A VI priedo nuostatomis. Kai tokiam personalui leidžiama susipažinti su ESĮI BSGP operacijos patalpose ar RIS, turi būti imamasi priemonių (įskaitant suteiktos ESĮI registravimą), kad būtų sumažinta rizika, jog informacija bus prarasta ar neteisėtai atskleista. Tokios priemonės apibrėžiamos atitinkamuose planavimo ar misijos dokumentuose.

5. Šio sprendimo 17 straipsnyje nurodyti įvertinimo vizitai į trečiąsias valstybes ar tarptautines organizacijas rengiami siekiant įsitikinti, kad ten taikomos bet kokios ESĮI, kuria keičiamasi, apsaugos priemonės yra veiksmingos.

6. Sprendimą suteikti EIVT turimą ESĮI trečiajai valstybei ar tarptautinei organizacijai EIVT priima atskirai kiekvienu konkrečiu atveju, atsižvelgdama į tokios informacijos pobūdį ir turinį bei gavėjo atitiktį principui „būtina žinoti“ ir įvertinusi naudą ES.

EIVT prašo subjekto, pateikusio įslaptintą informaciją, kuri buvo panaudota kaip pradinė medžiaga ESĮI, kurią parengė EIVT, pateikti rašytinį sutikimą, patvirtinantį, kad subjektas neprieštarauja šios informacijos suteikimui.

Jeigu EIVT nėra įslaptintos informacijos, kurią prašoma suteikti, rengėja, EIVT pirmiausia prašo jos įslaptintos informacijos rengėjo pateikti rašytinį sutikimą suteikti šią informaciją.

Tačiau, jei EIVT negali nustatyti atitinkamos informacijos rengėjo, EIVT Saugumo institucija, gavusi vieningą valstybių narių, atstovaujamų EIVT Saugumo komitete, pritarimą, perima rengėjo atsakomybę.

7. Šio straipsnio įgyvendinimo nuostatos išdėstytos A VI priede.

11 straipsnis

Įslaptintos informacijos saugumo pažeidimai ir neteisėtas atskleidimas

1. Apie bet kokį faktinį ar įtariamą saugumo pažeidimą ir apie bet kokį faktinį ar įtariamą įslaptintos informacijos neteisėtą atskleidimą nedelsiant pranešama už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui, kuris, prireikus, informuoja atitinkamą (-as) valstybę (-es) narę (-es) ar kitus atitinkamus subjektus.

2. Tais atvejais, kai žinoma arba yra pagrįstų priežasčių įtarti, kad įslaptinta informacija buvo neteisėtai atskleista arba prarasta, už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas informuoja atitinkamos (-ų) valstybės (-ių) narės (-ių) NSI ir, vadovaudamasis atitinkamais įstatymais ir teisės aktais, imasi visų atitinkamų priemonių:

a) išsaugoti įrodymus;

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

c) nedelsiant informuoti informacijos rengėją arba kitą atitinkamą subjektą;

d) imtis atitinkamų priemonių, kad būtų užkirstas kelias pažeidimui ar neteisėtam atskleidimui pasikartoti;

e) įvertinti galimą ES ar valstybių narių interesams padarytą žalą; ir

f) pranešti atitinkamoms institucijoms apie faktinio ar įtariamo neteisėto informacijos atskleidimo padarinius ir veiksmus, kurių imtasi.

3. Bet kuriam darbuotojui, už kurio įdarbinimą atsakinga EIVT, kuris pažeidė šiame sprendime nustatytas saugumo taisykles, gali būti taikomos drausminės priemonės pagal taikytinas taisykles ir teisės aktus.

Asmeniui, kuris atsakingas už įslaptintos informacijos neteisėtą atskleidimą ar praradimą, taikomos drausminės priemonės ir (arba) imamasi teisinių veiksmų pagal taikomus įstatymus, taisykles ir kitus teisės aktus.

4. Vykdant tyrimą dėl pažeidimo ir (arba) informacijos neteisėto atskleidimo, už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktorato vadovas gali laikinai sustabdyti asmens leidimą susipažinti su ESĮI ir patekti į EIVT patalpas. Apie šį sprendimą nedelsiant pranešama Komisijos Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratui, Tarybos generalinio sekretoriato Saugumo tarnybai ir valstybės (-ių) narės (-ių) NSI ar kitiems atitinkamiems subjektams.

A I PRIEDAS

PERSONALO PATIKIMUMAS

I. ĮVADAS

1. Šiame priede pateiktos A priedo 5 straipsnio įgyvendinimo nuostatos. Jame visų pirma nustatomi kriterijai, kuriais remdamasi EIVT nustato, ar asmeniui, atsižvelgiant į jo lojalumą ir patikimumą, gali būti leidžiama susipažinti su ESĮI, ir šiuo tikslu taikytinos tikrinimo bei administracinės procedūros.

2. Asmens patikimumo pažymėjimas (APP), kuriuo suteikiama teisė susipažinti su ESĮI, yra valstybės narės kompetentingos institucijos patvirtinimas, kuris pateikiamas valstybės narės kompetentingoms institucijoms baigus patikimumo tyrimą ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jis atitinka principą „būtina žinoti“, suteikiamas leidimas iki nurodytos datos susipažinti su iki tam tikro laipsnio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma) pažymėta ESĮI. Laikoma, kad asmens, kuriam taikoma ši apibrėžtis, patikimumas patikrintas.

3. Asmens patikimumo pažymėjimą patvirtinanti pažyma (APPPP) yra EIVT Saugumo institucijos išduota pažyma, kurioje nurodoma, kad asmens patikimumas yra patikrintas, ir nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos laipsnis, atitinkamo APP galiojimo laikas ir pačios pažymos galiojimo laikas.

4. Leidimas susipažinti su ESĮI yra EIVT Saugumo institucijos leidimas, kuris suteikiamas pagal šį sprendimą, po to, kai valstybės narės kompetentingos institucijos suteikia APP, ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jis atitinka principą „būtina žinoti“, suteikiamas leidimas iki nurodytos datos susipažinti su iki tam tikro laipsnio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma) pažymėta ESĮI. Laikoma, kad asmens, kuriam taikoma ši apibrėžtis, patikimumas patikrintas.

II. LEIDIMAS SUSIPAŽINTI SU ESĮI

5. Siekiant įgyti galimybę susipažinti su informacija, pažymėta slaptumo žyma RESTREINT UE/EU RESTRICTED, patikimumo pažymėjimas nebūtinas. Ši galimybė suteikiama, kai:

   a) atsiranda asmens sąsaja su EIVT, pagrįsta teisės aktais ar sutartimi;

   b) nustatoma, kad asmuo atitinka principą „būtina žinoti“;

   c) asmeniui pateikiama informacija apie ESĮI apsaugai užtikrinti skirtas saugumo taisykles bei procedūras ir jis raštu patvirtina savo pareigą saugoti ESĮI pagal šį sprendimą.

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

   a) atsiranda asmens sąsaja su EIVT, pagrįsta teisės aktais ar sutartimi;

   b) nustatoma, kad jis atitinka principą „būtina žinoti“;

   c) dėl jo atliekamų funkcijų jam suteiktas APP, pagal kurį jis gali susipažinti su iki atitinkamo laipsnio slaptumo žyma pažymėta informacija, arba jam buvo išduoti kiti tinkami leidimai pagal nacionalinius įstatymus ir teisės aktus ir

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

7. EIVT savo struktūrose nustato tas pareigas, kurias einantiems asmenims reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija ir todėl jie turi turėti iki atitinkamo slaptumo žymos laipsnio APP, kaip nustatyta pirmiau pateiktoje 4 dalyje.

8. EIVT personalo nariai nurodo, ar jie turi daugiau kaip vienos šalies pilietybę.

EIVT taikoma prašymo dėl APP pateikimo procedūra

9. EIVT personalo atveju EIVT Saugumo institucija nusiunčia užpildytą asmens patikimumo tikrinimo klausimyną valstybės narės, kurios pilietis asmuo yra, NSI, prašydama atlikti patikimumo tyrimą, skirtą gauti leidimui naudotis tam tikro laipsnio slaptumo žyma pažymėta ESĮI, su kuria asmeniui reikės susipažinti.

10. Jei asmuo turi daugiau kaip vienos šalies pilietybę, prašymas patikrinti patikimumą siunčiamas šalies, kurios pilietybė nurodyta asmenį įdarbinant, NSI.

11. Jei EIVT sužino patikimumo tyrimui svarbios informacijos apie asmenį, kuris pateikė prašymą dėl APP, EIVT, laikydamasi atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai NSI.

12. Užbaigusi patikimumo tyrimą, atitinkama NSI praneša už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui tokio patikrinimo rezultatus.

    a) Jei patikimumo tyrimo rezultatai užtikrintai rodo, kad neturima jokios nepalankios informacijos, kuri leistų abejoti asmens lojalumu ir patikimumu, EIVT Saugumo institucija gali atitinkamam asmeniui suteikti leidimą susipažinti su iki tam tikro laipsnio slaptumo žyma pažymėta ESĮI iki nurodytos datos.

    b) EIVT imasi visų tinkamų priemonių, kad užtikrintų, kad NSI taikomos sąlygos ar apribojimai būtų tinkamai įgyvendinami. NSI pranešama apie įgyvendinimo rezultatus.

    c) Jei patikimumo tyrimo rezultatai nėra tokie užtikrinantys, EIVT Saugumo institucija apie tai praneša atitinkamam asmeniui, kuris gali prašyti, kad EIVT Saugumo institucija jį išklausytų. EIVT Saugumo institucija gali prašyti kompetentingos NSI pateikti daugiau paaiškinimų, kuriuos ji gali pateikti pagal savo nacionalinius įstatymus ir teisės aktus. Jei rezultatai pasitvirtina, leidimas susipažinti su ESĮI neišduodamas. Tokiu atveju EIVT imasi visų tinkamų priemonių, kad užtikrintų, kad prašymo pateikėjui nebūtų suteikta galimybė susipažinti su ESĮI.

13. Patikimumo tyrimui bei gautiems rezultatams, kuriais EIVT Saugumo institucija grindžia savo sprendimą suteikti leidimą susipažinti su ESĮI ar jo nesuteikti, taikomi atitinkamoje valstybėje narėje galiojantys įstatymai ir teisės aktai, įskaitant su apskundimu susijusius įstatymus ir teisės aktus. EIVT Saugumo institucijos sprendimus galima apskųsti Tarnybos nuostatų 90 ir 91 straipsniuose numatytomis sąlygomis.

14. APP galioja visoms užduotims, kurias tas asmuo vykdo EIVT, Tarybos generaliniame sekretoriate ar Komisijoje, su sąlyga, kad tebegalioja jo išdavimą pagrindžiančios aplinkybės.

15. EIVT pripažįsta kitos Sąjungos institucijos, įstaigos ar agentūros išduotą leidimą susipažinti su ESĮI, su sąlyga, kad jis tebegalioja. Leidimai galioja visoms užduotims, kurias tas asmuo vykdo EIVT. Sąjungos institucija, įstaiga ar agentūra, kurioje asmuo pradeda dirbti, praneša atitinkamai NSI apie darbdavio pasikeitimą.

16. Jeigu asmens tarnyba neprasideda per 12 mėnesių nuo patikimumo tyrimo rezultatų pranešimo EIVT Saugumo institucijai arba jeigu asmens tarnyboje daroma 12 mėnesių pertrauka ir tuo laikotarpiu jis nėra priimtas į pareigas EIVT, kitoje ES institucijoje, agentūroje ar įstaigoje arba valstybės narės nacionalinėje administracinėje įstaigoje, kurias einant reikia susipažinti su įslaptinta informacija, atitinkamos NSI prašoma patvirtinti, kad rezultatai tebegalioja bei yra tinkami.

17. Jei EIVT sužino informacijos apie tai, kad asmuo, turintis galiojantį APP, kelia pavojų saugumui, EIVT, laikydamasi atitinkamų taisyklių ir teisės aktų, apie tai praneša atitinkamai NSI ir gali asmeniui laikinai nesuteikti galimybės susipažinti su ESĮI arba panaikinti leidimą susipažinti su ESĮI. Tais atvejais, kai NSI informuoja EIVT apie tai, kad pagal 12 dalies a punktą suteiktas užtikrinimas dėl galiojantį leidimą susipažinti su ESĮI turinčio asmens panaikinamas, EIVT Saugumo institucija gali paprašyti pateikti paaiškinimą, kurį NSI gali pateikti pagal nacionalinius įstatymus ir teisės aktus. Jei nepalanki informacija patvirtinama, pirmiau nurodytas leidimas panaikinamas, o asmeniui neleidžiama susipažinti su ESĮI ir eiti pareigų, kurias einant jis galėtų susipažinti su ta informacija arba sukelti pavojų saugumui.

18. Apie bet kokį sprendimą panaikinti EIVT personalo nario leidimą susipažinti su ESĮI ir, kai tinkama, tokio panaikinimo priežastis pranešama atitinkamam asmeniui, o jis gali prašyti, kad EIVT Saugumo institucija jį išklausytų. NSI teikiamą informaciją reglamentuoja atitinkamoje valstybėje narėje galiojantys įstatymai ir teisės aktai, įskaitant su apskundimu susijusius įstatymus ir teisės aktus. EIVT Saugumo institucijos sprendimus galima apskųsti Tarnybos nuostatų 90 ir 91 straipsniuose numatytomis sąlygomis.

19. Į EIVT komandiruoti nacionaliniai ekspertai, siekiantys eiti pareigas, kurias einant reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta įslaptinta informacija, EIVT Saugumo institucijai prieš pradėdami tarnybą pateikia galiojantį APP, leidžiantį susipažinti su atitinkamo laipsnio slaptumo žyma pažymėta ESĮI. Pirmiau minėtą procesą administruoja siunčiančioji valstybė narė.

Įrašai apie APP

20. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas EIVT direktoratas tvarko visų darbuotojų, už kuriuos atsakinga EIVT, ir EIVT rangovų darbuotojų patikimumo pažymėjimo statuso duomenų bazę. Šiuose įrašuose nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos laipsnis (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma), APP išdavimo data ir jo galiojimo laikas.

21. Valstybės narės ir kitos ES institucijos, agentūros ir įstaigos, siekdamos užtikrinti, kad EIVT turėtų tikslius ir išsamius visų darbuotojų, už kuriuos atsakinga EIVT, ir įrašus apie EIVT rangovų darbuotojų patikimumo pažymėjimo statusą, nustato atitinkamas koordinavimo procedūras.

22. EIVT Saugumo institucija gali išduoti asmens patikimumo pažymėjimą patvirtinančią pažymą (APPPP), kurioje nurodomas ESĮI, su kuria tam asmeniui gali būti leista susipažinti, slaptumo žymos laipsnis (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma), atitinkamo APP arba leidimo galiojimo laikas ir pačios pažymos galiojimo laikas.

Reikalavimo turėti APP taikymo išimtys

23. Jei reikia, už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas informuoja asmenis, kuriems dėl jų atliekamų funkcijų pagal nacionalinius įstatymus ir teisės aktus suteikta teisė susipažinti su ESĮI, apie jų saugumo pareigas ESĮI apsaugos srityje.

III. ŠVIETIMAS IR INFORMUOTUMAS SAUGUMO KLAUSIMAIS

24. Prieš asmenims suteikiant leidimą susipažinti su ESĮI, jie raštu patvirtina, kad supranta savo pareigas saugoti ESĮI ir ESĮI neteisėto atskleidimo padarinius. Įrašą apie tokį rašytinį patvirtinimą saugo už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas.

25. Visi asmenys, kuriems leidžiama susipažinti su ESĮI arba kurie turi dirbti su ESĮI, yra iš pat pradžių informuojami ir paskui reguliariai informuojami apie grėsmes saugumui ir jie turi nedelsdami pranešti atitinkamo padalinio / delegacijos saugumo koordinatoriams ir už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui apie bet kokius bandymus užmegzti kontaktą ar veiklą, kurie, jų nuomone, yra įtartini ar neįprasti.

26. Visiems asmenims, kuriems leidžiama susipažinti su ESĮI, laikotarpį, kurį jie tvarko ESĮI, taikomos nuolatinės asmens patikimumo užtikrinimo priemonės (t. y. priežiūra). Už nuolatinį asmens patikimumą atsakingi:

    a) asmenys, kuriems suteikta teisė susipažinti su ESĮI: jie yra asmeniškai atsakingi už savo patikimumą ir turi nedelsdami pranešti atitinkamoms saugumo institucijoms apie bet kokius bandymus užmegzti kontaktą ar veiklą, kuri, jų nuomone, yra įtartina ar neįprasta, ir visus jų asmeninių aplinkybių pokyčius, kurie gali turėti poveikį jų APP ar leidimui susipažinti su ESĮI;

b) tiesioginiai vadovai: jie atsakingi už nustatymą, ar asmuo atitinka principą „būtina žinoti“ ir už savo darbuotojų informavimą apie saugumo priemones ir pareigą apsaugoti ESĮI, darbuotojų patikimumo stebėjimą, problemiškų saugumo klausimų pateikimą patiems darbuotojams ir bet kokios neigiamos informacijos, kuri gali turėti poveikį jų darbuotojų APP ar leidimams susipažinti su ESĮI, pranešimą atitinkamoms saugumo institucijoms;

c) EIVT saugumo organizacijos saugumo srities subjektai, nurodyti šio sprendimo 12 straipsnyje: jie atsakingi už informuotumui saugumo klausimais skirtų informacinių susitikimų rengimą siekiant užtikrinti reguliarų jų atsakomybės srityje dirbančių darbuotojų informavimą, stiprios darbo kultūros skatinimą jų atsakomybės srityje, priemonių, skirtų darbuotojų patikimumui stebėti, nustatymą ir bet kokios neigiamos informacijos, kuri gali turėti poveikį asmens APP, pranešimą atitinkamoms saugumo institucijoms;

d) EIVT ir valstybės narės: jos nustato reikalingus informacijos, kuri gali turėti poveikį bet kokio asmens APP ar leidimui susipažinti su ESĮI, perdavimo kanalus.

27. Visi asmenys, nebeeinantys pareigų, kurias einant jiems reikia susipažinti su ESĮI, yra informuojami apie jų pareigas toliau saugoti ESĮI slaptumą ir, kai tinkama, jie tai patvirtina raštu.

IV. IŠSKIRTINĖS APLINKYBĖS

28. Dėl skubos priežasčių, kurios pagrįstos EIVT interesais, laukiant išsamaus patikimumo tyrimo pabaigos, EIVT Saugumo institucija, pasikonsultavusi su valstybės narės, kurios pilietis yra atitinkamas asmuo, NSI ir atsižvelgusi į preliminaraus patikrinimo, skirto patikrinti, ar nėra žinomos nepalankios informacijos apie asmenį, rezultatus, gali EIVT pareigūnams ir kitiems tarnautojams išduoti laikiną leidimą susipažinti su ESĮI konkrečiai funkcijai atlikti. Išsamus patikimumo tyrimas turi būti baigtas kuo greičiau. Tokie laikini leidimai galioja ne ilgiau kaip šešis mėnesius ir nesuteikia teisės susipažinti su slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija. Visi asmenys, kuriems išduotas laikinas leidimas, raštu patvirtina, kad jie supranta savo pareigas saugoti ESĮI ir ESĮI neteisėto atskleidimo pasekmes. Įrašą apie tokį rašytinį patvirtinimą saugo už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas.

29. Kai asmuo turi būti paskirtas į pareigas, kurioms eiti reikalingas vienu laipsniu aukštesnis nei turimas APP, jis gali būti paskirtas į tas pareigas laikinai, jeigu:

a) atitinkamas asmens vadovas atitinkamai direktoriaus / valdančiojo direktoriaus / delegacijos vadovo lygmeniu raštu įtikinamai pagrindžia, kad būtina susipažinti su aukštesnio laipsnio ESĮI;

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

c) asmuo turi galiojantį APP;

d) imtasi veiksmų pareigoms reikiamo laipsnio leidimui gauti;

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

f) asmens paskyrimą patvirtino kompetentinga EIVT institucija;

g) pasikonsultuota su atitinkama NSI/PSI, kuri asmeniui išdavė APP, ir negauta jokių prieštaravimų; ir

h) išimtis, įskaitant informacijos, su kuria leista susipažinti, aprašymą, registruoja atsakingas registras ar antrinis registras.

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

31. Itin išskirtinėmis aplinkybėmis, pvz., vykdant užduotis priešiškoje aplinkoje arba kylant tarptautinei įtampai, kai to reikia imantis neatidėliotinų priemonių, visų pirma siekiant išsaugoti žmonių gyvybes, vyriausiasis įgaliotinis, EIVT Saugumo institucija arba už išteklių valdymą atsakingas generalinis direktorius gali, kai įmanoma – raštu, suteikti galimybę susipažinti su slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija asmenims, kuriems nėra išduotas reikiamas APP, jeigu tokio leidimo tikrai reikia. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas registruoja šį leidimą, kuriame aprašoma informacija, su kuria leista susipažinti.

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

33. EIVT Saugumo komitetas informuojamas apie atvejus, kai naudojamasi 31 ir 32 punktuose išdėstyta procedūra.

34. EIVT Saugumo komitetui pateikiama metinė ataskaita dėl naudojimosi šiame skirsnyje numatytomis procedūromis.

V. DALYVAVIMAS EIVT BŪSTINĖJE IR SĄJUNGOS DELEGACIJOSE VYKSTANČIUOSE POSĖDŽIUOSE

35. Asmenys, paskirti dalyvauti EIVT būstinėje ir Sąjungos delegacijose vykstančiuose posėdžiuose, kuriuose aptariama CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, gali tai daryti tik patvirtinus jų APP turėtojo statusą. Valstybių narių atstovų, Tarybos generalinio sekretoriato bei Komisijos pareigūnų APPPP ar kitus APP įrodymus atitinkamos institucijos siunčia už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui, Sąjungos delegacijos saugumo koordinatoriui arba išimtiniais atvejais ją pateikia atitinkamas asmuo. Kai taikytina, gali būti naudojamas suvestinis pavardžių sąrašas, kuriame pateikiami atitinkami APP įrodymai.

36. Jei panaikinamas asmens, kuris eidamas savo pareigas turi dalyvauti EIVT būstinėje ir Sąjungos delegacijose vykstančiuose posėdžiuose, kuriuose aptariama CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, APP, leidžiantis susipažinti su ESĮI, kompetentinga institucija apie tai praneša už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui.

VI. GALIMA PRIEIGA PRIE ESĮI

37. Kai asmenys turi būti įdarbinti tokiomis aplinkybėmis, kuriomis jie potencialiai gali turėti prieigą prie CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėtos informacijos, jų patikimumas turi būti tinkamai patikrintas arba jie turi būti visą laiką lydimi.

38. Kurjerių, apsaugos darbuotojų ir lydinčių asmenų patikimumas turi būti patikrintas tinkamu lygiu, arba jie turi būti kitaip deramai patikrinti vadovaujantis nacionaliniais įstatymais ir teisės aktais, jie turi būti reguliariai supažindinami su ESĮI apsaugai užtikrinti skirtomis saugumo procedūromis ir jiems išdėstomos jų pareigos, jiems patikėtos tokios informacijos arba informacijos, su kuria jie gali susipažinti per neapdairumą, apsaugos srityje.

A II PRIEDAS

ES ĮSLAPTINTOS INFORMACIJOS FIZINIS SAUGUMAS

I. ĮVADAS

1. Šiame priede pateiktos A priedo 6 straipsnio įgyvendinimo nuostatos. Jame išdėstyti būtiniausi reikalavimai, taikomi patalpų, pastatų, kabinetų, salių ir kitų zonų, kuriose tvarkoma ir saugoma ESĮI, įskaitant zonas, kuriose yra RIS, fizinei apsaugai.

2. Fizinio saugumo priemonės turi būti parengtos taip, kad užkirstų 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, kai tinkama – personalo narių patikimumo pažymėjimais;

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

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

II FIZINIO SAUGUMO REIKALAVIMAI IR PRIEMONĖS

3. ESĮI apsaugai užtikrinti savo patalpose EIVT taiko rizikos valdymo procesą, kad užtikrintų, jog, atsižvelgiant į įvertintą riziką, būtų taikoma tinkamo lygio fizinė apsauga. Rizikos valdymo procese atsižvelgiama į visus svarbius veiksnius, visų pirma:

   a) ESĮI slaptumo žymos laipsnį;

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

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

   d) trečiųjų šalių grėsmės įvertinimą, parengtą INTCEN – už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktorato kontržvalgybos grupės, ir parengtą remiantis visų pirma Sąjungos delegacijų ataskaitomis, ir

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

4. EIVT Saugumo institucija, taikydama pakopinės apsaugos koncepciją, nustato tinkamas įgyvendintinas fizinio saugumo priemones. Tai gali būti viena (ar daugiau) iš šių priemonių:

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

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

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

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

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

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

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

5. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas gali būti įgaliojamas apieškoti įeinančius ir išeinančius asmenis siekiant atgrasyti nuo neleistino medžiagos įnešimo arba neleistino ESĮI išnešimo iš patalpų ar pastatų.

6. Iškilus rizikai, kad ESĮI bus pamatyta, netgi atsitiktinai, imamasi tinkamų priemonių siekiant išvengti šios rizikos.

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

III. ESĮI FIZINEI APSAUGAI SKIRTA ĮRANGA

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

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

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

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

IV. FIZIŠKAI APSAUGOTOS ZONOS

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

    a) administracinės zonos ir

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

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

14. Administracinių zonų atveju:

    a) nustatomas aiškiai apibrėžtas perimetras, kad būtų galima tikrinti asmenis ir, jei įmanoma, transporto priemones;

    b) įeiti nelydimiems leidžiama tik tinkamą leidimą turintiems asmenims: į būstinę įeiti leidžiama tik turint už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktorato išduotą leidimą, o į Sąjungos delegacijų patalpas – delegacijos vadovo išduotą leidimą; ir

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

15. Saugumo zonų atveju:

    a) nustatomas aiškiai apibrėžtas ir saugomas perimetras, per kurį kiekvienas įėjimas ir išėjimas yra kontroliuojamas naudojantis leidimų arba asmens atpažinimo sistema;

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

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

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

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

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

    c) į zoną draudžiama įnešti bet kokius elektroninius prietaisus.

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

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

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

    c) tokios zonos reguliariai fiziškai ir (arba) techniškai tikrinamos, kaip reikalauja už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas. Tokie patikrinimai atliekami, kai į zoną buvo įeita be leidimo ar įtariama apie tokį patekimą, ir

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

18. Nepaisant 17 punkto d papunkčio, prieš naudojantis ryšių prietaisais ir elektros ar elektronine įranga zonose, kuriose rengiami posėdžiai ar atliekamas darbas, susijęs su SECRET UE/EU SECRET arba aukštesnio laipsnio slaptumo žyma pažymėta informacija, taip pat, kai grėsmė ESĮI vertinama kaip didelė, tokius prietaisus ir įrangą visų pirma ištiria už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktorato Techninių atsakomųjų priemonių saugumo srityje grupė (TSCM), siekdama užtikrinti, kad naudojantis šia įranga nebūtų galima perduoti jokios suprantamos informacijos per neapdairumą ar neteisėtai už saugumo zonos perimetro.

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

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

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

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

    b) įdiegtinos stebėjimo ir apsaugos priemonės;

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

    d) kai tinkama, palydos tvarka arba ESĮI apsaugos tvarka, kai patekti į zoną leidžiama kitiems asmenims,

    e) bet kurios kitos atitinkamos priemonės ir procedūros.

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

V. V. FIZINĖS APSAUGOS PRIEMONĖS TVARKANT IR SAUGANT ESĮI

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

a) saugumo zonose;

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

c) ne saugumo zonose ar administracinėse zonose, jeigu turėtojas gabena ESĮI pagal A III priedo 30–42 punktus ir yra įsipareigojęs taikyti kompensacines priemones, nustatytas EIVT Saugumo institucijos parengtose saugumo instrukcijose, kad būtų užtikrinta, jog ESĮI yra apsaugota taip, kad su ja negalėtų susipažinti leidimo neturintys asmenys.

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

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

a) saugumo zonose;

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

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

i) gabena ESĮI pagal A III priedo 30–42 punktus;

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

iii) visą laiką asmeniškai kontroliuoja šią ESĮI; ir

iv) jei dokumentai yra popierinio pavidalo, apie tai pranešė atitinkamam registrui.

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

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

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

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

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

ii) patvirtinta ĮAS kartu veikiant apsaugos reagavimo personalui

arba

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

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

VI. ESĮI APSAUGAI UŽTIKRINTI NAUDOJAMŲ RAKTŲ IR KODŲ KONTROLĖ

30. EIVT Saugumo institucija nustato visose EIVT patalpose esančių kabinetų, patalpų, saugyklų ir apsauginių talpyklų raktų bei kodų valdymo procedūras. Tokios procedūros apsaugo nuo neleistino susipažinimo su informacija.

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

    a) gavus naują talpyklą;

    b) pasikeitus kodus žinančiam personalui;

    c) neteisėto atskleidimo ar įtarimo apie jį atveju;

    d) po spynos techninio patikrinimo ar taisymo ir

    e) bent kas 12 mėnesių.

A III PRIEDAS

ĮSLAPTINTOS INFORMACIJOS ADMINISTRAVIMAS

I. ĮVADAS

1. Šiame priede pateiktos A priedo 7 straipsnio įgyvendinimo nuostatos. Jame išdėstytos administracinės ESĮI kontrolės visą jos gyvavimo ciklą priemonės siekiant atgrasyti nuo tokios informacijos sąmoningo ar atsitiktinio neteisėto atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius.

II. ĮSLAPTINIMO ADMINISTRAVIMAS

Slaptumo žymos ir kitos žymos

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

3. ESĮI rengėjas yra atsakingas už slaptumo žymos laipsnio nustatymą, pažymėjimą tinkama slaptumo žyma, informacijos platinimo numatytiems gavėjams nustatymą, pažymėjimą tinkama leidimo suteikti informaciją žyma pagal atitinkamas EIVT ESĮI rengimo ir tvarkymo gaires.

4. ESĮI slaptumo žymos laipsnis nustatomas vadovaujantis A priedo 2 straipsnio 2 dalimi ir remiantis saugumo gairėmis, kurios [...] tvirtinamos pagal A priedo 3 straipsnio 3 dalį.

5. Valstybių narių įslaptintai informacijai, kuria jos keičiasi su EIVT, suteikiamas toks pat apsaugos lygis, koks suteikiamas atitinkamo slaptumo laipsnio ESĮI. Atitikmenų lentelė pateikiama šio sprendimo B priedėlyje.

6. Slaptumo žyma ir, kai taikytina, data ar konkretus įvykis, po kurio informacijos slaptumo žymos laipsnis gali būti sumažintas arba ji gali būti išslaptinta, nurodoma aiškiai ir teisingai, neatsižvelgiant į tai, ar ESĮI yra pateikiama popieriuje, žodžiu, elektronine ar bet kuria kita forma.

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

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

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

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

CONFIDENTIEL UE/EU CONFIDENTIAL Be priedo(-ų) RESTREINT UE/EU RESTRICTED

Žymos

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

a) identifikatoriumi, kuriuo nurodomas įslaptintos informacijos rengėjas;

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

c) leidimo suteikti informaciją žymomis.

12. Priėmus sprendimą suteikti ESĮI trečiajai valstybei ar tarptautinei organizacijai, už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas perduoda atitinkamą įslaptintą informaciją, pažymėtą leidimo suteikti informaciją žyma, nurodančia trečiąją valstybę ar tarptautinę organizaciją, kuriai ji suteikiama.

13. Patvirtintų žymų sąrašą tvirtina EIVT Saugumo institucija.

Slaptumo žymų santrumpos

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

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

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

ESĮI rengimas

16. Rengiant ES įslaptintą dokumentą:

    a) kiekvienas puslapis aiškiai pažymimas atitinkamo laipsnio slaptumo žyma;

    b) kiekvienas puslapis numeruojamas;

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

    d) dokumente nurodoma data;

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

17. Kai rengiant ESĮI neįmanoma taikyti 16 punkte išdėstytų reikalavimų, taikomos kitos tinkamos priemonės vadovaujantis saugumo gairėmis, [...] parengtomis pagal šį sprendimą.

ESĮI slaptumo žymos laipsnio sumažinimas ir ESĮI išslaptinimas

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

19. EIVT reguliariai peržiūri jos turimą ESĮI, siekdama įsitikinti, ar slaptumo žymos laipsnis vis dar taikomas. EIVT sukuria sistemą, skirtą ne rečiau kaip kas penkerius metus peržiūrėti registruotos ESĮI, kurią ji parengė, slaptumo žymos laipsnį. Tokia peržiūra nėra reikalinga, jeigu įslaptintos informacijos rengėjas iš pat pradžių nurodo konkretų laiką, kada informacijos slaptumo žymos laipsnis bus sumažintas arba informacija bus išslaptinta automatiškai; informacija yra atitinkamai pažymėta.

III. ESĮI REGISTRAVIMAS SAUGUMO TIKSLAIS

20. Būstinėje įsteigiamas centrinis registras. Kiekviename EIVT organizaciniame vienete, kuriame tvarkoma ESĮI, steigiami atsakingi registrai, pavaldūs centriniam registrui, siekiant užtikrinti, kad ESĮI būtų tvarkoma pagal šį sprendimą. Registrai steigiami kaip A priede apibrėžtos saugumo zonos.

Kiekviena Sąjungos delegacija įsteigia savo ESĮI registrą.

Šiems registrams administruoti EIVT Saugumo institucija paskiria vyriausiąjį registro pareigūną.

21. Šiame sprendime registravimas saugumo tikslais (toliau – registravimas) – procedūrų, kuriomis užregistruojamas informacijos gyvavimo ciklas, įskaitant jos platinimą ir sunaikinimą, taikymas. RIS atveju registravimo procedūros gali būti atliekamos vykdant procesus pačioje RIS.

22. Kai organizacinis vienetas, įskaitant Sąjungos delegacijas, gauna CONFIDENTIEL UE/EU CONFIDENTIAL ir aukštesnio laipsnio slaptumo žyma pažymėtą medžiagą ir kai ją išsiunčia, visa ši medžiaga registruojama. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija registruojama tam skirtuose registruose.

23. EIVT būstinėje centrinis registras yra pagrindinis įslaptintos informacijos, kuria keičiamasi su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis, gavimo ir išsiuntimo punktas. Jis registruoja visus šiuos keitimosi informacija atvejus.

24. EIVT Saugumo institucija saugumo tikslais patvirtina ESĮI registravimo saugumo gaires pagal šio sprendimo 14 straipsnį.

TRES SECRET UE/EU TOP SECRET registrai

25. EIVT būstinėje paskiriamas centrinis registras, kuris veikia kaip centrinė slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtą informaciją gaunanti ir siunčianti institucija. Prireikus gali būti paskirti antriniai registrai, kurie tvarko tokią informaciją jos registravimo tikslais.

26. Tokie antriniai registrai negali perduoti slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtų dokumentų tiesiogiai kitiems to paties centrinio TRES SECRET UE/EU TOP SECRET registro antriniams registrams arba į išorę be aiškaus rašytinio to registro leidimo.

IV. ES ĮSLAPTINTŲ DOKUMENTŲ KOPIJAVIMAS IR VERTIMAS

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

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

29. Dokumento kopijoms ir vertimams taikomos tos pačios saugumo priemonės, kaip ir dokumento originalui. Dokumentų, pažymėtų CONFIDENTIEL UE/EU CONFIDENTIAL ar aukštesnio laipsnio slaptumo žyma, kopijas daro tik atitinkamas (sub)registras, naudodamas apsaugotą kopijavimo aparatą. Kopijos turi būti registruojamos.

V. ESĮI GABENIMAS

30. Gabenant ESĮI taikomos 32–42 punktuose išdėstytos apsaugos priemonės. Kai ESĮI gabenama elektroninėje laikmenoje ir nepaisant A priedo 7 straipsnio 4 dalies, toliau išvardytas apsaugos priemones gali papildyti EIVT Saugumo institucijos nurodytos atitinkamos techninės atsakomosios priemonės, kad būtų sumažinta rizika, jog informacija bus prarasta ar neteisėtai atskleista.

31. EIVT Saugumo institucija parengia ESĮI gabenimo instrukcijas pagal šį sprendimą.

Pastate arba uždaroje pastatų grupėje

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

33. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėta informacija pastate arba uždaroje pastatų grupėje turi būti gabenama apsaugotame voke, ant kurio nurodytas tik gavėjo vardas ir pavardė; ją gabena asmenys, kurių patikimumas tinkamai patikrintas.

Europos Sąjungoje

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

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

a) atitinkamai karinis, vyriausybinis ar diplomatinis kurjeris;

b) kurjeris su sąlyga, kad:

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

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

iii) asmenų patikimumas patikrintas atitinkamu lygiu ir jie informuoti apie jų pareigas saugumo srityje;

iv) prireikus asmenims suteikiamas kurjerio pažymėjimas;

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

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

ii) jos taiko tinkamas apsaugos priemones laikydamosi būtiniausių reikalavimų, kurie turi būti nustatyti saugumo gairėse pagal šio sprendimo 21 straipsnio 1 dalį.

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

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

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

Iš ES į trečiosios valstybės teritoriją arba tarp ES subjektų trečiosiose valstybėse

38. ESĮI, gabenama iš ES į trečiosios valstybės teritoriją arba tarp ES subjektų trečiosiose valstybėse, turi būti supakuota taip, kad ji būtų apsaugota nuo atskleidimo be leidimo.

39. Slaptumo žymomis CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET pažymėtą informaciją iš ES į trečiosios valstybės teritoriją ir slaptumo žyma SECRET UE/EU SECRET pažymėtą ir žemesnio laipsnio slaptumo žyma pažymėtą informaciją tarp ES subjektų trečiosiose valstybėse gabena:

a) karinis ar diplomatinis kurjeris;

b) kurjeris su sąlyga, kad:

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

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

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

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

v) asmenų patikimumas patikrintas tinkamu lygiu ir jie informuoti apie jų pareigas saugumo srityje.

40. Gabenant trečiajai valstybei ar tarptautinei organizacijai ES teikiamą slaptumo žymomis CONFIDENTIEL UE/EU CONFIDENTIAL ir SECRET UE/EU SECRET pažymėtą informaciją laikomasi atitinkamų nuostatų, numatytų susitarime dėl informacijos saugumo arba administraciniame susitarime pagal A priedo 10 straipsnio 2 dalį.

41. Slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėtą informaciją iš ES į trečiosios valstybės teritoriją taip pat gali gabenti pašto tarnybos ar komercinės kurjerių pašto tarnybos.

42. Slaptumo žyma TRES SECRET UE/EU TOP SECRET pažymėtą informaciją iš ES į trečiosios valstybės teritoriją arba tarp ES subjektų trečiosiose valstybėse gabena karinis ar diplomatinis kurjeris.

VI. ESĮI NAIKINIMAS

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

44. Dokumentus, kurie turi būti registruojami pagal A priedo 7 straipsnio 2 dalį, turėtojo arba kompetentingos institucijos nurodymu sunaikina atsakingas registras. Registracijos knygos ir kita registravimo informacija atitinkamai atnaujinama.

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

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

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

48. Kompiuterinių duomenų saugojimo laikmenos, naudotos ESĮI, sunaikinamos taikant EIVT Saugumo institucijos patvirtintas procedūras.

VII. SAUGUMO PATIKRINIMAI

EIVT saugumo patikrinimai

49. Pagal šio sprendimo 16 straipsnį EIVT saugumo patikrinimai yra:

a) bendrieji saugumo patikrinimai, kurių tikslas – nustatyti EIVT būstinės, Sąjungos delegacijų ir visų EIVT priklausančių ir su EIVT susijusių patalpų bendrą saugumo lygį, visų pirma siekiant įvertinti saugumo priemonių, įgyvendinamų siekiant apsaugoti EIVT saugumo interesus, efektyvumą;

b) ESĮI saugumo patikrinimai, kurių tikslas – akreditacijos požiūriu bendrai įvertinti EIVT būstinėje ir Sąjungos delegacijose įgyvendintų ESĮI apsaugos priemonių efektyvumą.

Visų pirma tokie patikrinimai atliekami, *inter alia*, siekiant:

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

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

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

iv) sustiprinti saugumo institucijų vykdomas švietimo ir informuotumo saugumo klausimais programas.

EIVT saugumo patikrinimų vykdymas ir jų ataskaitų teikimas

50. EIVT saugumo patikrinimus vykdo už būstinės saugumą ir EIVT informacijos saugumą atsakingo EIVT direktorato patikrinimo grupė, jei reikia, padedant kitų ES institucijų ar valstybių narių saugumo ekspertams.

Patikrinimo grupei leidžiama patekti į visas vietas, kuriose tvarkoma ESĮI, visų pirma į registrus ir RIS įrengimo vietas.

51. EIVT saugumo patikrinimai Sąjungos delegacijose vykdomi koordinuojant veiksmus su už Reagavimo į krizes centrą atsakingu direktoratu, o prireikus juos vykdyti gali padėti trečiosiose šalyse esančių valstybių narių ambasadų saugumo pareigūnai.

52. Iki kiekvienų kalendorinių metų pabaigos EIVT Saugumo institucija patvirtina kitų metų EIVT tikrinimo programą.

53. Prireikus EIVT Saugumo institucija gali surengti pirmiau nurodytoje programoje nenumatytus saugumo patikrinimus.

54. Pabaigus saugumo patikrinimą, tikrinamam subjektui pateikiamos pagrindinės išvados ir rekomendacijos. Po to patikrinimo grupė parengia patikrinimo ataskaitą. Jei buvo pasiūlyti taisomieji veiksmai ir pateiktos rekomendacijos, ataskaitoje padarytos išvados turėtų būti pakankamai išsamiai pagrįstos. Ataskaita dėl saugumo patikrinimų Sąjungos delegacijose perduodama EIVT Saugumo institucijai, Reagavimo į krizes centro direktoriui ir tikrinamo subjekto vadovui.

Už būstinės saugumą ir EIVT informacijos saugumą atsakingo direktorato atsakomybe rengiama reguliari ataskaita, skirta nurodytu laikotarpiu atliktų patikrinimų metu įgytai patirčiai pabrėžti; ją išnagrinėja EIVT Saugumo komitetas.

Saugumo patikrinimų vykdymas pagal ES sutarties V antraštinės dalies 2 skyrių įsteigtose ES agentūrose ir įstaigose ir šių patikrinimų ataskaitų teikimas

55. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas EIVT direktoratas gali, kai tinkama, paskirti papildomus ekspertus, kurie dalyvautų jungtinėse ES patikrinimo grupėse, vykdančiose patikrinimus ES agentūrose ir įstaigose, įsteigtose pagal ES sutarties V antraštinės dalies 2 skyrių.

EIVT saugumo patikrinimų kontrolinis sąrašas

56. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas EIVT direktoratas parengia ir atnaujina aspektų, kurie tikrintini vykdant EIVT saugumo patikrinimus, kontrolinį sąrašą. Šis kontrolinis sąrašas pateikiamas EIVT Saugumo komitetui.

57. Kontroliniam sąrašui užpildyti būtina informacija gaunama visų pirma patikrinimo metu iš tikrinamo subjekto saugumo valdymo tarnybų. Išsamiai atsakius į kontrolinio sąrašo klausimus, sąrašas įslaptinamas pagal susitarimą su tikrinamu subjektu. Jis negali būti įtrauktas į patikrinimo ataskaitą.

A IV PRIEDAS

RIS TVARKOMOS ESĮI APSAUGA

I. ĮVADAS

1. Šiame priede pateiktos A priedo 8 straipsnio įgyvendinimo nuostatos.

2. Toliau išdėstytos informacijos saugumo užtikrinimo (ISU) savybės ir sąvokos yra būtinos saugumui ir tinkamam ryšių ir informacinių sistemų (RIS) operacijų vykdymui užtikrinti:

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

II. INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI

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

Saugumo rizikos valdymas

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

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

6. Saugumo rizikos valdymo tikslas – taikyti saugumo priemonių rinkinį, kuris užtikrina tinkamą vartotojų reikalavimų ir likutinės rizikos, susijusios su saugumu, pusiausvyrą.

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

Saugumas viso RIS gyvavimo ciklo metu

8. Saugumas užtikrinamas viso RIS gyvavimo ciklo metu – nuo pradžios iki naudojimo pabaigos.

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

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

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

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

Geriausia praktika

13. EIVT bendradarbiauja su TGS, Komisija ir valstybėmis narėmis, kad nustatytų geriausią praktiką RIS tvarkomos ESĮI apsaugos srityje. Geriausios praktikos gairėse išdėstomos RIS skirtos techninės, fizinės, organizacinės ir procedūrinės saugumo priemonės, kurių veiksmingumas apsisaugant nuo konkrečių grėsmių ir pažeidžiamumo buvo įrodytas.

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

15. Geriausios praktikos platinimu ir įgyvendinimu turi būti prisidedama prie siekio užtikrinti lygiavertį įvairių EIVT naudojamų RIS, kuriose tvarkoma ESĮI, saugumo užtikrinimo lygį.

Pakopinė apsauga

16. Siekiant sušvelninti pavojų RIS, įgyvendinama daug techninių ir netechninių saugumo priemonių, kurios grupuojamos į kelis apsaugos lygius. Šie lygiai, be kita ko, yra:

    a) *atgrasymas*: saugumo priemonės, skirtos atgrasyti nuo priešiškų planų pulti RIS;

    b) *prevencija*: saugumo priemonės, skirtos RIS puolimui apsunkinti arba jam sutrukdyti;

    c) *aptikimas*: saugumo priemonės, skirtos RIS puolimo atvejui išaiškinti;

    d) *atsparumas*: saugumo priemonės, skirtos puolimo poveikiui apriboti iki mažiausio informacijos rinkinio ar RIS dalių grupės ir užkirsti kelią tolesnei žalai, ir

    e) *atkūrimas*: saugumo priemonės, skirtos RIS saugiai padėčiai atkurti.

    Tokių saugumo priemonių griežtumo ir taikymo lygis nustatomas atsižvelgiant į rizikos vertinimą.

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

Minimalumo ir mažiausių privilegijų principas

18. Siekiant išvengti nereikalingos rizikos, įdiegiamos tik tos funkcijos, prietaisai ir paslaugos, kurie atitinka operacinius reikalavimus.

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

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

Informuotumas informacijos saugumo užtikrinimo srityje

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

    a) kad saugumo spragos gali labai pakenkti RIS ir visai organizacijai;

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

    c) savo asmeninę atsakomybę ir atskaitomybę už RIS saugumą pagal savo vaidmenį naudojant sistemas ir procesus.

22. Siekiant užtikrinti, kad būtų suvokiama atsakomybė už saugumą, visiems dalyvaujantiems darbuotojams, įskaitant aukštesniąją vadovybę ir RIS naudotojus, yra privalomi ISU švietimo ir informuotumo mokymai.

IT saugumo priemonių vertinimas ir patvirtinimas

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

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

25. ESĮI apsaugai skirtas šifravimo priemones įvertina ir patvirtina valstybės narės nacionalinė kriptografijos patvirtinimo institucija (KPI).

26. Prieš rekomenduojant, kad pagal šio sprendimo 8 straipsnio 5 dalį jas patvirtintų EIVT KPI, tokias šifravimo priemones turi būti teigiamai įvertinusi antra šalis, t. y. valstybės narės kvalifikuota įvertinimo institucija (AQUA), kuri nesusijusi su įrangos projektavimu arba gamyba. Reikalaujamas antros šalies įvertinimo išsamumo lygis priklauso nuo numatomo didžiausio ESĮI, kuri bus apsaugoma šiomis priemonėmis, slaptumo žymos laipsnio.

27. EIVT KPI, remdamasi Tarybos saugumo komiteto rekomendacija, gali netaikyti 25 arba 26 dalyse nustatytų reikalavimų ir tam tikram laikotarpiui suteikti laikiną patvirtinimą pagal šio sprendimo 8 straipsnio 5 dalyje nustatytą tvarką, kai tai pateisinama dėl konkrečių su veikla susijusių priežasčių.

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

29. Vyriausiasis įgaliotinis patvirtina saugumo politiką dėl ne šifravimo IT saugumo priemonių atitikties reikalavimams ir patvirtinimo.

Perdavimas saugumo zonose

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

Saugus RIS sujungimas

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

32. RIS kiekviena sujungta IT sistema traktuojama kaip nepatikima ir joje įdiegiamos apsaugos priemonės keitimuisi įslaptinta informacija kontroliuoti.

33. Visais RIS sujungimo su kita IT sistema atvejais laikomasi toliau išdėstytų pagrindinių reikalavimų:

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

b) sujungimui taikomas rizikos valdymo ir akreditavimo procesas, taip pat yra reikalingas kompetentingų SAI patvirtinimas, ir

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

34. Akredituota RIS negali būti sujungta su neapsaugotu arba viešuoju tinklu, išskyrus atvejus, kai RIS yra patvirtintos RAP, tuo tikslu įdiegtos tarp RIS ir neapsaugoto arba viešojo tinklo. Tokiems sujungimams skirtas saugumo priemones peržiūri kompetentinga informacijos saugumo užtikrinimo institucija (ISUI) ir patvirtina kompetentinga SAI.

Kai neapsaugotas arba viešasis tinklas naudojamas tik perdavimo tikslais ir duomenys yra užšifruojami pagal šio sprendimo 8 straipsnio 5 dalį patvirtinta šifravimo priemone, tokia jungtis nelaikoma sujungimu.

35. Draudžiamas tiesioginis arba pakopinis RIS, akredituotos tvarkyti slaptumo žyma TRES SECFRET UE/EU TOP SECRET pažymėtą informaciją, sujungimas su neapsaugotu arba viešuoju tinklu.

Kompiuterinių duomenų saugojimo laikmenos

36. Kompiuterinių duomenų saugojimo laikmenos sunaikinamos laikantis EIVT Saugumo institucijos patvirtintų procedūrų.

37. Kompiuterinių duomenų saugojimo laikmenos pakartotinai naudojamos, jų slaptumo žymos laipsnis sumažinamas arba jos išslaptinamos laikantis EIVT gairių dėl ESĮI slaptumo žymos laipsnio sumažinimo ir išslaptinimo, nustatytų pagal šio sprendimo 8 straipsnio 2 dalį.

Ekstremaliosios situacijos sąlygos

38. Nepaisant šio sprendimo nuostatų, toliau apibūdintos konkrečios procedūros gali būti ribotą laiką taikomos esant ekstremaliajai situacijai, pavyzdžiui, gresiant ar kilus krizei, konfliktui, karo padėties atveju arba išskirtinėmis veiklos sąlygomis.

39. ESĮI gali būti perduodama naudojant šifravimo priemones, kurios buvo patvirtintos žemesnio slaptumo žymos laipsnio informacijai, arba nešifruota kompetentingai institucijai sutikus, jei dėl vėlavimo būtų padaryta aiškiai didesnė žala, negu įslaptintos medžiagos atskleidimas, ir jei:

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

b) įslaptinta medžiaga negali būti laiku perduota kitomis priemonėmis.

40. 39 punkte išdėstytomis aplinkybėmis perduodama įslaptinta informacija negali būti pažymėta jokiomis žymomis arba nuorodomis, kurios leistų ją atskirti nuo informacijos, kuri yra neįslaptinta arba kurią galima apsaugoti naudojant turimas šifravimo priemones. Gavėjams kitomis priemonėmis nedelsiant pranešama apie informacijos slaptumo laipsnį.

41. Jeigu taikoma 39 dalis, pateikiama ataskaita už būstinės saugumą ir EIVT informacijos saugumą atsakingam direktoratui, o per jį – EIVT Saugumo komitetui. Šioje ataskaitoje nurodomas bent kiekvieno ESĮI vieneto siuntėjas, gavėjas ir rengėjas.

III. INFORMACIJOS SAUGUMO UŽTIKRINIMO FUNKCIJOS IR INSTITUCIJOS

42. EIVT nustatomos toliau nurodytos informacijos saugumo užtikrinimo funkcijos. Šioms funkcijoms vykdyti nebūtini bendri organizaciniai subjektai. Joms vykdyti suteikiami atskiri įgaliojimai. Tačiau šios funkcijos ir su jomis susijusi atsakomybė gali būti sujungtos arba integruotos viename organizaciniame vienete arba padalytos skirtingiems organizaciniams vienetams, jei išvengiama vidaus interesų arba užduočių konfliktų.

Informacijos saugumo užtikrinimo institucija (ISUI)

43. ISUI atsako už:

a) ISU saugumo gairių rengimą ir jų veiksmingumo bei aktualumo stebėjimą;

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

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

d) užtikrinimą, kad šifravimo priemonės būtų parenkamos laikantis jų tinkamumo nustatymo ir atrankos gairių;

e) mokymo ir informuotumo ISU srityje koordinavimą;

f) konsultavimąsi su sistemos tiekėju, saugumo srities subjektais ir naudotojų atstovais ISU saugumo gairių klausimais ir

g) užtikrinimą, kad EIVT Saugumo komiteto ISU klausimų ekspertų pogrupis turėtų atitinkamų ekspertinių žinių.

TEMPEST institucija

44. TEMPEST institucija (TEI) yra atsakinga už užtikrinimą, kad RIS atitiktų TEMPEST politiką ir gaires. Ji patvirtina TEMPEST atsakomąsias priemones, skirtas įrenginiams ir priemonėms, siekiant apsaugoti ESĮI iki nustatyto slaptumo žymos laipsnio jos operacinėje aplinkoje.

Kriptografijos patvirtinimo institucija (KPI)

45. KPI yra atsakinga už užtikrinimą, kad šifravimo priemonės atitiktų atitinkamas šifravimo gaires. Ji patvirtina šifravimo priemonę siekiant apsaugoti ESĮI iki nustatyto slaptumo žymos laipsnio jos operacinėje aplinkoje.

Kriptografijos platinimo institucija (KPLI)

46. KPLI atsako už:

a) ES kriptografinės medžiagos valdymą ir apskaitą;

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

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

Saugumo akreditavimo institucija (SAI)

47. Kiekvienai sistemai skirta SAI atsako už:

a) užtikrinimą, kad RIS atitiktų atitinkamas saugumo gaires, pareiškimo dėl RIS patvirtinimo, leidžiant ją naudoti tvarkant ESĮI iki nustatyto slaptumo žymos laipsnio operacinėje aplinkoje, pateikimą, akreditavimo reikalavimų bei sąlygų ir kriterijų, pagal kuriuos sprendžiama, ar RIS reikia iš naujo patvirtinti, nustatymą;

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

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

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

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

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

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

h) RIS sujungimo su kitomis RIS patvirtinimą arba, kai aktualu, dalyvavimą bendrame patvirtinime ir

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

48. EIVT SAI atsako už visų į EIVT įgaliojimų sritį patenkančių RIS akreditavimą.

Saugumo akreditavimo valdyba (SAV)

49. Jungtinė SAV yra atsakinga už RIS, patenkančių tiek į EIVT SAI įgaliojimų, tiek į valstybių narių SAI įgaliojimų sritį, akreditavimą. Ją sudaro po vieną kiekvienos valstybės narės SAI atstovą, o jos posėdžiuose dalyvauja TGS ir Komisijos SAI atstovai. Kiti subjektai, turintys prijungimo prie RIS mazgus, kviečiami dalyvauti posėdžiuose, kai svarstomi su ta sistema susiję klausimai.

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

Informacijos saugumo užtikrinimo operacinė institucija

50. Kiekvienai sistemai skirta ISU operacinė institucija atsako už:

a) saugumo dokumentų, atitinkančių saugumo gaires, rengimą, visų pirma sistemos saugumo reikalavimų aktų (**SSRA**), įskaitant pareiškimą dėl likutinės rizikos, saugios eksploatacijos taisykles (**SecOPs**) ir šifravimo planą vykdant RIS akreditavimo procesą, rengimą;

b) dalyvavimą atrenkant ir testuojant konkrečioms sistemoms skirtas technines saugumo priemones, prietaisus ir programinę įrangą siekiant vykdyti jų įgyvendinimo priežiūrą ir užtikrinti, kad jie būtų saugiai įdiegti, sukonfigūruoti ir eksploatuojami pagal atitinkamus saugumo dokumentus;

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

d) SecOps įgyvendinimo ir taikymo stebėseną, kai tinkama, eksploatavimo saugumo pareigas deleguojant sistemos savininkui;

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

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

g) konkrečioms RIS skirto mokymo ISU klausimais teikimą;

h) konkrečioms RIS skirtų saugumo priemonių įgyvendinimą ir vykdymą.

A V PRIEDAS

PRAMONINIS SAUGUMAS

I. ĮVADAS

1. Šiame priede pateiktos A priedo 9 straipsnio įgyvendinimo nuostatos. Jame išdėstytos bendros saugumo nuostatos, taikomos pramonės ar kitiems subjektams derybų dėl sutarčių sudarymo metu arba visą EIVT sudarytų įslaptintų sutarčių gyvavimo ciklą.

2. EIVT Saugumo institucija patvirtina pramoninio saugumo gaires, kuriose apibrėžiami visų pirma išsamūs reikalavimai, susiję su Įmonės patikimumą patvirtinančiais pažymėjimais (ĮPPP), saugumo aspektų paaiškinimais (SAP), vizitais, ESĮI perdavimu ir gabenimu.

II. SAUGUMO ASPEKTAI ĮSLAPTINTOJE SUTARTYJE

Slaptumo žymų vadovas (SŽV)

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

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

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

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

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

Saugumo aspektų paaiškinimas (SAP)

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

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

Programos / projekto saugumo instrukcijos (PRSI)

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

III. ĮMONĖS PATIKIMUMĄ PATVIRTINANTIS PAŽYMĖJIMAS (ĮPPP)

8. Už būstinės saugumą ir EIVT informacijos saugumą atsakingas EIVT direktoratas prašo atitinkamos valstybės narės NSI, PSI ar kitos kompetentingos saugumo institucijos pagal nacionalinius įstatymus ir kitus teisės aktus suteikti ĮPPP, pažymintį, kad pramonės arba kitas subjektas savo patalpose gali apsaugoti atitinkamo slaptumo žymos laipsnio (CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET) ESĮI. Rangovui, subrangovui arba potencialiam rangovui ar subrangovui ESĮI arba galimybė susipažinti su ESĮI suteikiama tik tada, kai EIVT pateikiamas ĮPPP turėjimo įrodymas.

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

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

11. EIVT, kaip perkančioji organizacija, prašo NSI/PSI ar kitos ĮPPP išdavusios kompetentingos saugumo institucijos pranešti visą neigiamą informaciją, galinčią turėti įtakos ĮPPP. Subrangos sutarties atveju atitinkamai informuojama NSI/PSI arba kita kompetentinga saugumo institucija.

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

IV. Rangovo darbuotojams išduodami asmens patikimumo pažymėjimai (APP)

13. Visų rangovo darbuotojų, kuriems reikia susipažinti su CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma pažymėta ESĮI, patikimumas tinkamai patikrinamas ir jie turi galimybę susipažinti su informacija vadovaujantis principu „būtina žinoti“. Norint susipažinti su informacija, pažymėta slaptumo žyma RESTREINT UE/EU RESTRICTED, APP nereikia, tačiau vis tiek reikia atitikti principą „būtina žinoti“.

14. Prašymai rangovo darbuotojams išduoti APP teikiami už atitinkamą subjektą atsakingai NSI/PSI.

15. Rangovams, norintiems įdarbinti trečiosios valstybės pilietį į pareigas, kurias einant reikia susipažinti su ESĮI, EIVT nurodo, kad valstybės narės, kurioje samdantysis subjektas yra įsikūręs ir įregistruotas, NSI/PSI atsakomybė yra nustatyti, ar asmeniui galima suteikti galimybę susipažinti su tokia informacija, pagal šį sprendimą, ir patvirtinti, kad prieš suteikiant tokią teisę gautas informacijos rengėjo sutikimas.

V. ĮSLAPTINTOS SUTARTYS IR SUBRANGOS SUTARTYS

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

17. Sudarius įslaptintą sutartį ar subrangos sutartį, EIVT, kaip perkančioji organizacija, praneša rangovo ar subrangovo NSI/PSI ar kitai kompetentingai saugumo institucijai apie tos įslaptintos sutarties saugumo nuostatas.

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

19. Paprastai reikalaujama, kad nutraukus įslaptintą sutartį ar subrangos sutartį arba jai pasibaigus rangovas arba subrangovas perkančiajai organizacijai grąžintų visą turimą ESĮI.

20. Konkrečios nuostatos dėl ESĮI sunaikinimo vykdant sutartį, ją nutraukus arba jai pasibaigus nustatomos SAP.

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

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

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

24. 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 organizacijos sutikimo.

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

VI. SU ĮSLAPTINTOMIS SUTARTIMIS SUSIJĘ VIZITAI

26. Jei EIVT, rangovams ar subrangovams vykdant įslaptintą sutartį jiems reikia susipažinti su slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET pažymėta informacija vieni kitų patalpose, dėl jų vizitų susitariama palaikant ryšius su NSI/PSI arba kita susijusia kompetentinga saugumo institucija. Tai nepažeidžia NSI/PSI prerogatyvos konkrečių projektų atveju susitarti dėl tvarkos, pagal kurią dėl tokių vizitų gali būti susitariama tiesiogiai.

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

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

VII. ESĮI PERDAVIMAS IR GABENIMAS

29. Perduodant ESĮI elektroninėmis priemonėmis taikomos atitinkamos A priedo 8 straipsnio ir A IV priedo nuostatos.

30. Kiek tai susiję su ESĮI gabenimu, taikomos atitinkamos A III priedo nuostatos, laikantis nacionalinių įstatymų ir teisės aktų.

31. Nustatant įslaptintos medžiagos kaip krovinio gabenimui taikomą saugumo tvarką vadovaujamasi šiais principais:

a) saugumas užtikrinamas visais gabenimo etapais: nuo kilmės vietos iki galutinės paskirties vietos;

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

c) gabenimą užtikrinančios bendrovės turi gauti atitinkamo laipsnio slaptumo žymos ĮPPP, jei gabenant įslaptinta informacija saugoma taip pat ir rangovo patalpose. Bet kuriuo atveju siuntą gabenančio personalo patikimumas turi būti patikrintas pagal A I priedą;

d) prieš gabenant per valstybių sienas medžiagą, pažymėtą slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba SECRET UE/EU SECRET, siuntėjas parengia, o EIVT, jei tinkama, bendradarbiaudama su siuntėjo ir gavėjo valstybių NSI/DSI ar kitomis atitinkamomis kompetentingomis saugumo institucijomis, patvirtina gabenimo planą;

e) kelionės turi vykti, kiek tik įmanoma, be sustojimo ir būti užbaigtos kuo greičiau, atsižvelgiant į aplinkybes;

f) kai tik įmanoma, turėtų būti pasirenkami maršrutai tik per valstybių narių teritorijas. Maršrutais per valstybes, kurios nėra valstybės narės, turėtų būti gabenama tik gavus EIVT arba siuntėjo ir gavėjo valstybių kitų kompetentingų saugumo institucijų leidimą.

VIII. ESĮI PERDAVIMAS TREČIOSIOSE VALSTYBĖSE ĮSIKŪRUSIEMS RANGOVAMS

32. ESĮI trečiosiose valstybėse, kurios su ES yra sudariusios galiojantį saugumo susitarimą, įsikūrusiems rangovams ir subrangovams perduodama laikantis saugumo priemonių, dėl kurių susitarė EIVT, kaip perkančioji organizacija, ir atitinkamos trečiosios valstybės, kurioje registruotas rangovas, NSI/PSI.

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

33. Palaikydama ryšius su atitinkamai valstybės narės NSI/PSI EIVT, kaip perkančioji organizacija, turi teisę remiantis sutarties nuostatomis rengti vizitus į rangovo / subrangovo patalpas, kad patikrintų, ar įgyvendintos pagal sutartį reikalaujamos tinkamos saugumo priemonės, skirtos slaptumo žyma RESTREINT UE/EU RESTRICTED pažymėtai ESĮI apsaugoti.

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

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

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

37. Sąlygos, kuriomis rangovas gali sudaryti subrangos sutartis, turi atitikti 22–24 punktų reikalavimus.

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

A VI PRIEDAS

KEITIMASIS ĮSLAPTINTA INFORMACIJA SU TREČIOSIOMIS VALSTYBĖMIS IR TARPTAUTINĖMIS ORGANIZACIJOMIS

I. ĮVADAS

1. Šiame priede pateiktos A priedo 10 straipsnio įgyvendinimo nuostatos.

II. TVARKA, REGLAMENTUOJANTI KEITIMĄSI ĮSLAPTINTA INFORMACIJA

2. EIVT gali keistis ESĮI su trečiosiomis valstybėmis ar tarptautinėmis organizacijomis pagal A priedo 10 straipsnio 1 dalį.

Siekiant padėti vyriausiajam įgaliotiniui vykdyti SESV 218 straipsnyje nurodytas pareigas:

a) atitinkamas EIVT geografinis ar teminis padalinys, konsultuodamasis su už būstinės saugumą ir EIVT informacijos saugumą atsakingu direktoratu, kai tinkama, nustato ilgalaikio keitimosi ESĮI su atitinkama trečiąja valstybe ar tarptautine organizacija poreikį;

b) už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas, konsultuodamasis su atitinkamu EIVT geografiniu padaliniu, kai tinkama, vyriausiajam įgaliotiniui teikia projektų tekstus, kuriuos ketinama pasiūlyti Tarybai pagal SESV 218 straipsnio 3, 5 ir 6 dalis;

c) už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas padeda vyriausiajam įgaliotiniui vedant derybas;

d) susitarimų ar administracinių susitarimų su trečiosiomis valstybėmis dėl jų dalyvavimo BSGP krizių valdymo operacijose pagal A priedo 10 straipsnio 1 dalies c punktą atveju EIVT padeda vyriausiajam įgaliotiniui, kiek tai susiję su pasiūlymais, kurie turi būti teikiami Tarybai pagal SESV 218 straipsnio 3, 5 ir 6 dalis, ir padeda jam vedant derybas.

3. Jei susitarimuose dėl informacijos saugumo numatytos techninio įgyvendinimo nuostatos, dėl kurių už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas turi susitarti su atitinkamos trečiosios valstybės ar tarptautinės organizacijos kompetentinga saugumo institucija, tokiose nuostatose atsižvelgiama į apsaugos lygį, užtikrinamą atitinkamoje trečiojoje valstybėje ar tarptautinėje organizacijoje nustatytais teisės aktais, struktūromis ir procedūromis. Kiek tai susiję su tokiomis nuostatomis, už būstinės saugumą ir EIVT informacijos saugumą atsakingas direktoratas koordinuoja veiksmus su Komisijos Žmogiškųjų išteklių ir saugumo generalinio direktorato Saugumo direktoratu ir Tarybos generalinio sekretoriato Saugumo tarnyba.

4. Esant ilgalaikiam poreikiui su trečiąja valstybe ar tarptautine organizacija keistis įslaptinta informacija, kurios slaptumo žymos laipsnis nėra aukštesnis nei RESTREINT UE/EU RESTRICTED, ir nustačius, kad atitinkama šalis neturi pakankamai išplėtotos tokiai informacijai skirtos saugumo sistemos, kad galėtų sudaryti susitarimą dėl informacijos saugumo, vyriausiasis įgaliotinis gali, vieningai pritarus EIVT Saugumo komitetui pagal šio sprendimo 15 straipsnio 5 dalį, sudaryti administracinį susitarimą su atitinkamos trečiosios valstybės ar tarptautinės organizacijos kompetentingomis saugumo institucijomis.

5. Keistis ESĮI su trečiąja valstybe ar tarptautine organizacija elektroninėmis priemonėmis neleidžiama, nebent tai aiškiai numatyta susitarime dėl informacijos saugumo arba administraciniame susitarime.

6. Pagal administracinį susitarimą dėl keitimosi įslaptinta informacija EIVT ir trečioji valstybė ar tarptautinė organizacija paskiria savo registrus, kurie yra pagrindiniai įslaptintos informacijos, kuria keičiamasi, gavimo ir išsiuntimo punktai. EIVT atveju tai – EIVT centrinis registras.

7. Administraciniai susitarimai paprastai sudaromi pasikeičiant laiškais.

III. ĮVERTINIMO VIZITAI

8. Šio sprendimo 17 straipsnyje nurodyti įvertinimo vizitai vykdomi sudarius dvišalį susitarimą su atitinkama trečiąja valstybe ar tarptautine organizacija; jų metu vertinami šie aspektai:

   a) įslaptintai informacijai apsaugoti taikoma reglamentavimo sistema;

   b) bet kokie trečiosios valstybės ar tarptautinės organizacijos saugumo įstatymų, teisės aktų, politikos ar procedūrų ypatumai, kurie galėtų daryti poveikį įslaptintos informacijos, kuria gali būti keičiamasi, aukščiausiam slaptumo žymos laipsniui;

   c) esamos saugumo priemonės ir procedūros, skirtos įslaptintai informacijai apsaugoti, ir

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

9. Kol neįvykdytas įvertinimo vizitas ir nenustatytas slaptumo laipsnis, kurio žyma pažymėta įslaptinta informacija šalys gali keistis (remiantis apsaugos lygio, kuris bus jai suteiktas, lygiavertiškumo principu), ESĮI nesikeičiama.

   Jei prieš tokį įvertinimo vizitą vyriausiajam įgaliotiniui pranešama apie kokias nors išskirtines ar su skuba susijusias priežastis keistis įslaptinta informacija, EIVT Saugumo institucija vykdo šiuos veiksmus:

   a) visų pirma siekia gauti informacijos rengėjo rašytinį sutikimą, kad įsitikintų, jog nėra jokių prieštaravimų suteikti šią informaciją;

   b) gali nuspręsti suteikti informaciją, jei tam vieningai pritaria valstybės narės, atstovaujamos EIVT Saugumo komitete.

   Jei EIVT negali nustatyti atitinkamos informacijos rengėjo, EIVT Saugumo institucija, gavusi vieningą EIVT Saugumo komiteto narių pritarimą, perima rengėjo atsakomybę.

IV. LEIDIMAS SUTEIKTI ESĮI TREČIOSIOMS VALSTYBĖMS ARBA TARPTAUTINĖMS ORGANIZACIJOMS

10. Jei nustatyta keitimosi įslaptinta informacija su trečiąja valstybe ar tarptautine organizacija sistema pagal A priedo 10 straipsnio 1 dalį, sprendimą, kuriuo EIVT trečiajai valstybei ar tarptautinei organizacijai suteikia ESĮI, priima EIVT Saugumo institucija.

11. Jei EIVT nėra įslaptintos informacijos, kurią ketinama suteikti, rengėja, įskaitant pradinės medžiagos, kuri gali būti įtraukta į tą informaciją, rengėjus, EIVT Saugumo institucija pirmiausia prašo šios informacijos rengėjo pateikti rašytinį sutikimą, kad įsitikintų, jog nėra jokių prieštaravimų suteikti šią informaciją. Jei EIVT negali nustatyti atitinkamos informacijos rengėjo, EIVT Saugumo institucija, gavusi vieningą valstybių narių, atstovaujamų EIVT Saugumo komitete, pritarimą, perima rengėjo atsakomybę.

V. ESĮI *AD HOC* SUTEIKIMAS IŠIMTINE TVARKA

12. Jei nėra vienos iš A priedo 10 straipsnio 1 dalyje nurodytų sistemų ir jei ES arba viena ar daugiau jos valstybių narių dėl politinių, operacinių ar labai svarbių priežasčių yra suinteresuotos suteikti ESĮI, ESĮI gali būti išimties tvarka suteikta trečiajai valstybei ar tarptautinei organizacijai, jei imtasi toliau nurodytų veiksmų.

   EIVT Saugumo institucija, įsitikinusi, kad pirmiau pateiktoje 11 dalyje nurodytos sąlygos įvykdytos:

   a) kiek įmanoma, pasitikrina per atitinkamos trečiosios valstybės ar tarptautinės organizacijos saugumo institucijas, ar jos saugumo teisės aktai, struktūros bei procedūros yra pakankami, kad joms suteikta ESĮI būtų apsaugota pagal standartus, kurie yra ne mažiau griežti nei nustatyti šiame sprendime;

b) prašo EIVT Saugumo komiteto remiantis turima informacija pateikti nuomonę dėl to, kokiu mastu galima pasitikėti atitinkamos trečiosios valstybės ar tarptautinės organizacijos, kuriai bus suteikta ESĮI, saugumo teisės aktais, struktūromis ir procedūromis;

c) gali nuspręsti suteikti ESĮI, jei tam vieningai pritaria valstybės narės, atstovaujamos EIVT Saugumo komitete.

13. Jei nėra vienos iš A priedo 10 straipsnio 1 dalyje nurodytų sistemų, atitinkama trečioji šalis raštu įsipareigoja tinkamai apsaugoti ESĮI.

A priedėlis

Apibrėžtys

Šiame sprendime vartojamų terminų apibrėžtys:

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

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

c) leidimas susipažinti su ESĮI – EIVT Saugumo institucijos leidimas, kuris suteikiamas pagal šį sprendimą, po to, kai valstybės narės kompetentingos institucijos suteikia APP, ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jis atitinka principą „būtina žinoti“, suteikiamas leidimas iki nurodytos datos susipažinti su iki nurodyto laipsnio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma) pažymėta ESĮI pagal A I priedo 2 straipsnį;

d) pažeidimas – šiame sprendime nustatytoms saugumo taisyklėms ir (arba) saugumo politikai ar gairėms, kuriomis nustatytos šiam sprendimui įgyvendinti būtinos priemonės, priešingas asmens veiksmas arba neveikimas;

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

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

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

h) 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;

i) neteisėtas ESĮI atskleidimas – visiškas ar dalinis ESĮI atskleidimas leidimo neturintiems asmenims ar subjektams (žr. 9 straipsnio 2 dalį);

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

k) šifravimo priemonės – kriptografiniai algoritmai, kriptografiniai techninės ir programinės įrangos moduliai, priemonės, įskaitant vykdymo informaciją bei susijusius dokumentus ir raktų duomenis;

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

m) išslaptinimas – bet kokios slaptumo žymos panaikinimas;

n) pakopinė apsauga – saugumo priemonių, kurios grupuojamos į kelis apsaugos lygius, taikymas;

o) paskirtoji saugumo institucija (PSI) – valstybės narės nacionalinei saugumo institucijai (NSI) atskaitinga institucija, kuri atsako už pramonės ir kitų subjektų informavimą apie nacionalinę politiką visais pramoninio saugumo klausimais ir už gairių ir pagalbos teikimą ją įgyvendinant. PSI funkciją gali vykdyti NSI arba kita kompetentinga institucija;

p) dokumentas – registruota informacija, neatsižvelgiant į jos fizinę formą ar charakteristikas;

q) slaptumo žymos laipsnio sumažinimas – atvejis, kai sumažinamas slaptumo žymos laipsnis;

r) ES įslaptinta informacija (ESĮI) – bet kuri informacija arba medžiaga, kurią atskleidus be leidimo galėtų būti padaryta įvairaus dydžio žala Europos Sąjungos arba vienos ar kelių valstybių narių interesams ir kuriai suteikta ES slaptumo žyma (žr. 2 straipsnio f punktą);

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

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

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

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

w) pramoninis saugumas – priemonių, kurias rangovai arba subrangovai taiko derybų prieš sudarant sutartis metu ir visą įslaptintų sutarčių gyvavimo ciklą siekdami užtikrinti ESĮI apsaugą, taikymas (žr. A priedo 9 straipsnio 1 dalį);

x) informacijos saugumo užtikrinimas ryšių ir informacinių sistemų srityje – užtikrinimas, kad tokiose sistemose tvarkoma informacija bus apsaugota ir kad, valdant teisėtiems naudotojams, jos veiks taip, kaip turi veikti, ir tada, kada turi veikti. Veiksmingas ISU užtikrina tinkamą konfidencialumo, vientisumo, prieinamumo, atsakomybės už veiksmus prisiėmimo ir autentiškumo lygį. ISU grindžiamas rizikos valdymo procesu (žr. A priedo 8 straipsnio 1 dalį);

y) šiame sprendime sujungimas – tiesioginis dviejų ar daugiau IT sistemų sujungimas siekiant dalytis duomenimis ir kitais informacijos šaltiniais (pavyzdžiui, ryšiais) vienakrypčiu arba daugiakrypčiu būdu (žr. A IV priedo 31 dalį);

z) įslaptintos informacijos administravimas – administracinių ESĮI kontrolės priemonių taikymas visą jos gyvavimo ciklą siekiant papildyti 5, 6 ir 8 straipsniuose numatytas priemones ir tokiu būdu atgrasyti nuo tokios informacijos sąmoningo ar tikslingo neteisėto atskleidimo arba praradimo, nustatyti tokius atvejus ir pašalinti jų padarinius. Tokios priemonės visų pirma yra susijusios su ESĮI rengimu, registravimu, kopijavimu, vertimu, gabenimu, tvarkymu, saugojimu ir naikinimu (žr. A priedo 7 straipsnio 1 dalį);

aa) medžiaga – dokumentas arba pagaminti ar gaminami įrenginiai ar įranga;

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

cc) personalo patikimumas – priemonių taikymas, siekiant užtikrinti, kad galimybė susipažinti su ESĮI būtų suteikta tik asmenims:

— kuriems „būtina žinoti“,

— kurių patikimumas patikrintas atitinkamu lygiu ir kuriems suteikta teisė susipažinti su informacija, pažymėta slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma, arba kiti tinkami leidimai pagal nacionalinius įstatymus ir teisės aktus, ir

— kurie yra informuoti apie savo pareigas

pagal A priedo 5 straipsnio 1 dalį;

dd) asmens patikimumo pažymėjimas (APP), kuriuo suteikiama teisė susipažinti su ESĮI – valstybės narės kompetentingos institucijos patvirtinimas, kuris pateikiamas valstybės narės kompetentingoms institucijoms baigus patikimumo tyrimą ir kuriuo pažymima, kad atitinkamam asmeniui, nustačius, kad jis atitinka principą „būtina žinoti“, suteikiamas leidimas iki nurodytos datos susipažinti su iki nurodyto laipsnio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma) pažymėta ESĮI. Laikoma, kad asmens, kuris atitinka šią apibrėžtį, patikimumas yra patikrintas;

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

ff) fizinis saugumas – fizinių ir techninių apsaugos priemonių taikymas siekiant atgrasyti nuo neteisėtos prieigos prie ESĮI (žr. A priedo 6 straipsnį);

gg) programos / projekto saugumo instrukcija (PRSI) – saugumo procedūrų, kurios yra taikomos konkrečiai programai / projektui siekiant standartizuoti saugumo procedūras, sąrašas. Ji gali būti tikslinama įgyvendinant programą / projektą;

hh) registravimas – procedūrų, kuriomis užregistruojamas informacijos gyvavimo ciklas, įskaitant jo platinimą ir sunaikinimą, taikymas (žr. A III priedo 21 dalį);

ii) 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 elementai gali būti pašalinti;

jj) rizika – galimybė, kad tam tikros grėsmės atveju bus pasinaudota organizacijos ar sistemų vidiniu ir išoriniu pažeidžiamumu ir taip padaryta žala organizacijai ir jos materialiajam ar nematerialiajam turtui. Ji vertinama kaip kylančių grėsmių tikimybės ir į jų poveikio derinys;

kk) rizikos pripažinimas – sprendimas atlikus rizikos tvarkymą pripažinti, kad vis dar yra likutinė rizika;

ll) rizikos vertinimas – grėsmių bei pažeidžiamų sričių nustatymas ir susijusios rizikos analizės, t. y. galimumo ir poveikio analizės, atlikimas;

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

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

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

pp) saugumo aspektų paaiškinimas (SAP) – specialių sutartinių sąlygų rinkinys, kurį parengia perkančioji organizacija ir kuris yra įslaptintos sutarties, pagal kurią gali būti suteikiama galimybė susipažinti su ESĮI arba tokia informacija gali būti rengiama, sudėtinė dalis; jame nurodomi saugumo reikalavimai arba tos sutarties dalys, kurias reikia apsaugoti (žr. A V priedo II skirsnį);

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

rr) patikimumo tyrimas – tyrimo procedūros, kurias atlieka valstybės narės kompetentinga institucija, vadovaudamasi toje valstybėje narėje galiojančiais įstatymais ir teisės aktais, siekdama gauti užtikrinimą, kad nėra žinoma nieko, kas neleistų asmeniui išduoti nacionalinio arba ES APP, suteikiančio galimybę susipažinti su iki nurodyto laipsnio slaptumo žyma (CONFIDENTIEL UE/EU CONFIDENTIAL arba aukštesnio laipsnio slaptumo žyma) pažymėta ESĮI;

ss) saugios eksploatacijos taisyklės (SecOPs) – saugumo politikos įgyvendinimo, kurį ketinama patvirtinti, eksploatacijos taisyklių, kurių reikia laikytis, ir personalo pareigų aprašas;

tt) neskelbtina neįslaptinta informacija – informacija arba medžiaga, kurią EIVT privalo apsaugoti dėl Sutartyse ir ją įgyvendinant priimtuose aktuose nustatytų teisinių pareigų ir (arba) dėl jos neskelbtinumo. Neskelbtina neįslaptinta informacija apima (bet tuo neapsiriboja) informaciją ar medžiagą, kuriai taikoma pareiga saugoti tarnybinę paslaptį, kaip nurodyta SESV 339 straipsnyje, informaciją, kuri susijusi su interesais, saugomais Reglamento (EB) Nr. 1049/2001 ([1]) 4 straipsniu kartu su atitinkama Europos Sąjungos Teisingumo Teismo praktika, arba asmens duomenis, patenkančius į Reglamento (ES) 2018/1725 taikymo sritį;

uu) sistemos saugumo reikalavimų aktas (SSRA) – saugumo principų, kurių reikia laikytis, ir išsamių saugumo reikalavimų, kuriuos reikia įgyvendinti, rinkinys, kuris yra RIS sertifikavimo ir akreditavimo pagrindas;

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

ww) grėsmė – galimas nepageidaujamas atvejis, dėl kurio gali būti padaryta žala organizacijai ar jos naudojamoms sistemoms; tokios grėsmės gali kilti atsitiktinai arba būti sukeltos specialiai (siekiant pakenkti); jas apibūdina pavojingi elementai, galimi taikiniai ir puolimo būdai;

xx) pažeidžiamumas – bet kokio pobūdžio trūkumas, kuriuo gali būti naudojamasi vienos ar daugiau grėsmių atveju. Pažeidžiamumas gali atsirasti dėl neveikimo arba gali būti susijęs su kontrolės griežtumo, išsamumo ar nuoseklumo trūkumu ir gali būti techninio, procedūrinio, fizinio, organizacinio ar operacinio pobūdžio.

([1]) 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).

B priedėlis

Slaptumo žymų atitikmenys

ES	TRES SECRET UE/EU TOP SECRET	SECRET UE/ES SECRET	CONFIDENTIEL UE/ES CONFIDENTIAL	RESTREINT UE/EU RESTRICTED
EURATOM	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)	Pastaba ([1])
Bulgarija	Строго секретно	Секретно	Поверително	За служебно ползване
Čekija	Přísně tajné	Tajné	Důvěrné	Vyhrazené
Danija	YDERST HEMMELIGT	HEMMELIGT	FORTROLIGT	TIL TJENESTEBRUG
Vokietija	STRENG GEHEIM	GEHEIM	VS ([2]) — VERTRAULICH	VS — NUR FÜR DEN DIENSTGEBRAUCH
Estija	Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
Airija	Top Secret	Secret	Confidential	Restricted
Graikija	Άκρως Απόρρητο Santrumpa: ΑΑΠ	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Ispanija	SECRETO	RESERVADO	CONFIDENCIAL	DIFUSIÓN LIMITADA
Prancūzija	TRÈS SECRET TRÈS SECRET DÉFENSE ([3])	SECRET SECRET DÉFENSE ([3])	CONFIDENTIEL DÉFENSE ([3]), ([4])	Pastaba ([5])
Kroatija	VRLO TAJNO	TAJNO	POVJERLJIVO	OGRANIČENO
Italija	Segretissimo	Segreto	Riservatissimo	Riservato
Kipras	Άκρως Απόρρητο Santrumpa: (ΑΑΠ)	Απόρρητο Santrumpa: (ΑΠ)	Εμπιστευτικό Santrumpa: (ΕΜ)	Περιορισμένης Χρήσης Santrumpa: (ΠΧ)
Latvija	Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
Lietuva	Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
Liuksemburgas	Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
Vengrija	„Szigorúan titkos!“	„Titkos!“	„Bizalmas!“	„Korlátozott terjesztésű!“

Malta	L-Ogħla Segretezza Top Secret	Sigriet Secret	Kunfidenzjali Confidential	Ristrett Restricted ([6])
Nyderlandai	Stg. ZEER GEHEIM	Stg. GEHEIM	Stg. CONFIDENTIEEL	Dep. VERTROUWELIJK
Austrija	Streng Geheim	Geheim	Vertraulich	Eingeschränkt
Lenkija	Ściśle Tajne	Tajne	Poufne	Zastrzeżone
Portugalija	Muito Secreto	Secreto	Confidencial	Reservado
Rumunija	Strict secret de importanță deosebită	Strict secret	Secret	Secret de serviciu
Slovėnija	STROGO TAJNO	TAJNO	ZAUPNO	INTERNO
Slovakija	Prísne tajné	Tajné	Dôverné	Vyhradené
Suomija	ERITTÄIN SALAINEN YTTERST HEMLIG	SALAINEN HEMLIG	LUOTTAMUKSELLINEN KONFIDENTIELL	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG
Švedija	Kvaliciferat hemlig	Hemlig	Konfidentiell	Begränsat hemlig

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

([2]) Vokietija: VS = Verschlusssache.

([3]) Anksčiau nei 2021 m. liepos 1 d. Prancūzijos surinkta informacija ir slaptumo žyma TRÈS SECRET DÉFENSE, SECRET DÉFENSE ir CONFIDENTIEL DÉFENSE pažymėta informacija toliau tvarkoma ir saugoma atitinkamai TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET ir CONFIDENTIEL UE/EU CONFIDENTIAL lygiu;

([4]) Slaptumo žyma CONFIDENTIEL UE/EU CONFIDENTIAL pažymėtą informaciją Prancūzija tvarko ir saugo laikydamasi slaptumo žyma SECRET pažymėtai informacijai apsaugoti taikomų Prancūzijos saugumo priemonių.

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

([6]) Maltoje gali būti naudojamos slaptumo žymos tiek maltiečių, tiek anglų kalba.