2014 4 1 LT Europos Sąjungos oficialusis leidinys C 96/1

II

(Komunikatai)

EUROPOS SĄJUNGOS INSTITUCIJŲ, ĮSTAIGŲ IR ORGANŲ PRIIMTI KOMUNIKATAI

EUROPOS PARLAMENTAS

EUROPOS PARLAMENTO BIURO SPRENDIMAS

2013 m. balandžio 15 d.

dėl konfidencialios informacijos tvarkymo Europos Parlamente taisyklių

(2014/C 96/01)

EUROPOS PARLAMENTO BIURAS,

atsižvelgdamas į Europos Parlamento darbo tvarkos taisyklių 23 straipsnio 12 dalį,

kadangi:

(1) atsižvelgiant į 2010 m. spalio 20 d. pasirašytą Pagrindų susitarimą dėl Europos Parlamento ir Europos Komisijos santykių ([1]) (Pagrindų susitarimas) ir į 2014 m. kovo 12 d. pasirašytą Europos Parlamento ir Tarybos tarpinstitucinį susitarimą dėl Tarybos turimos įslaptintos informacijos klausimais, nesusijusiais su bendra užsienio ir saugumo politika, perdavimo Europos Parlamentui ir tvarkymo Europos Parlamente ([2]) (Tarpinstitucinis susitarimas), būtina nustatyti konkrečias konfidencialios informacijos tvarkymo Europos Parlamente taisykles;

(2) pagal Lisabonos sutartį Europos Parlamentui pavedamos naujos užduotys ir siekiant plėtoti Parlamento veiklą tose srityse, kuriose reikalingas tam tikras konfidencialumas, būtina nustatyti konfidencialios informacijos, įskaitant įslaptintą informaciją, tvarkymo Europos Parlamente pagrindinius principus, būtiniausius saugumo standartus ir tinkamas procedūras;

(3) šiame sprendime nustatytų taisyklių tikslas – užtikrinti atitinkamus apsaugos standartus ir suderinamumą su kitų institucijų, įstaigų, tarnybų ir agentūrų, įsteigtų pagal Sutartis arba remiantis jomis, arba valstybių narių priimtomis taisyklėmis, siekiant užtikrinti sklandų Europos Sąjungos sprendimų priėmimo procesą;

(4) šio sprendimo nuostatos nedaro poveikio esamoms ir būsimoms taisyklėms dėl galimybės susipažinti su dokumentais, priimtoms pagal Sutarties dėl Europos Sąjungos veikimo (SESV) 15 straipsnį;

([1]) OL L 304, 2010 11 20, p. 47.
([2]) OL C 95, 2014 4 1, p. 1.

(5) šio sprendimo nuostatos nedaro poveikio esamoms ir būsimoms taisyklėms dėl asmens duomenų apsaugos, priimtoms pagal SESV 16 straipsnį,

PRIĖMĖ ŠĮ SPRENDIMĄ:

1 straipsnis

Tikslas

Šiame sprendime reglamentuojamas Europos Parlamento vykdomas konfidencialios informacijos valdymas ir tvarkymas, įskaitant tokios informacijos rengimą, gavimą, perdavimą ir laikymą siekiant tinkamai apsaugoti jos konfidencialų pobūdį. Šiuo sprendimu įgyvendinamas Tarpinstitucinis susitarimas ir Pagrindų susitarimas, visų pirma jo II priedas.

2 straipsnis

Apibrėžtys

Šiame sprendime:

a) informacija – rašytinė ar žodinė informacija, kokia bebūtų jos laikmena ar autorius;

b) konfidenciali informacija – įslaptinta informacija ir neįslaptinta kita konfidenciali informacija;

c) įslaptinta informacija – ES įslaptinta informacija ir lygiavertė įslaptinta informacija;

d) ES įslaptinta informacija (ESĮI) – bet kokia informacija ir medžiaga, pažymėta slaptumo žymomis „TRÈS SECRET UE/EU TOP SECRET“, „SECRET UE/EU SECRET“, „CONFIDENTIEL UE/EU CONFIDENTIAL“ arba „RESTREINT UE/EU RESTRICTED“, kurią atskleidus be leidimo gali būti padaryta įvairaus laipsnio žalos Sąjungos interesams arba vienos ar daugiau valstybių narių interesams, neatsižvelgiant į tai, ar ta informacija buvo parengta institucijose, įstaigose, tarnybose ar agentūrose, įsteigtose pagal Sutartis arba jomis remiantis, ar yra gauta iš valstybių narių, trečiųjų šalių ar tarptautinių organizacijų. Šiuo atveju informacija ir medžiaga žymima slaptumo žymos laipsniu:

— „TRÈS SECRET UE/EU TOP SECRET“ – tai informacija ir medžiaga, kurią atskleidus be leidimo gali būti padaryta ypatingai didelė žala esminiams Sąjungos arba vienos ar daugiau valstybių narių interesams;

— „SECRET UE/EU SECRET“ – tai informacija ir medžiaga, kurią atskleidus be leidimo gali būti rimtai pakenkta esminiams Sąjungos arba vienos ar daugiau valstybių narių interesams;

— „CONFIDENTIEL UE/EU CONFIDENTIAL“ – tai informacija ir medžiaga, kurią atskleidus be leidimo gali būti pakenkta esminiams Sąjungos arba vienos ar daugiau valstybių narių interesams;

— „RESTREINT UE/EU RESTRICTED“ – tai informacija ir medžiaga, kurių atskleidimas be leidimo gali būti nenaudingas Sąjungos arba vienos ar daugiau valstybių narių interesams;

e) lygiavertė įslaptinta informacija – įslaptinta informacija, kurią parengė valstybės narės, trečiosios valstybės arba tarptautinės organizacijos, kuri pažymėta slaptumo žyma, lygiaverte vienai iš slaptumo žymų, naudojamų ESĮI, ir kurią Europos Parlamentui perdavė Taryba arba Komisija;

f) kita konfidenciali informacija – bet kokia kita neįslaptinta konfidenciali informacija, įskaitant informaciją, kuriai taikomos duomenų apsaugos taisyklės arba kuriai taikoma tarnybinės paslapties prievolė, ir kuri parengta Europos Parlamente ar Europos Parlamentui perduota kitų institucijų, įstaigų, tarnybų ir agentūrų, įsteigtų pagal Sutartis arba jomis remiantis, ar valstybių narių;

g) dokumentas – bet kokia fiksuota informacija, neatsižvelgiant į jos fizinę formą ar charakteristikas;

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

i) principas „būtina žinoti“ – asmens būtinybė susipažinti su konfidencialia informacija, kad jis galėtų atlikti oficialias pareigas ar užduotį;

j) leidimas – sprendimas suteikti asmeninę prieigą prie konkretaus laipsnio įslaptintos informacijos, kurį priima Parlamento pirmininkas, jei sprendimas susijęs su Europos Parlamento nariais, arba generalinis sekretorius, jei sprendimas susijęs su Europos Parlamento pareigūnais ir kitais Europos Parlamento darbuotojais, kurie dirba frakcijose, remdamasis teigiamais nacionalinės institucijos pagal nacionalinę teisę ir pagal I priedo 2 dalies nuostatas atlikto asmens patikimumo patikrinimo rezultatais;

k) laipsnio sumažinimas – įslaptinimo laipsnio sumažinimas;

l) išslaptinimas – bet kokios slaptumo žymos panaikinimas;

m) kita žyma – kitai konfidencialiai informacijai suteikiama žyma, pagal kurią atpažįstami iš anksto nustatyti konkretūs dokumento naudojimo nurodymai arba jame aptariama sritis. Šia žyma taip pat gali būti pažymėta įslaptinta informacija siekiant nustatyti papildomus jos naudojimo reikalavimus;

n) kitos žymos panaikinimas – bet kokios kitos žymos panaikinimas;

o) rengėjas – konfidencialios informacijos tinkamai įgaliotas autorius;

p) saugumo pranešimai – techninės įgyvendinimo priemonės, nustatytos II priede;

q) naudojimo nurodymai – techniniai nurodymai Europos Parlamento tarnyboms dėl konfidencialios informacijos valdymo.

3 straipsnis

Pagrindiniai principai ir būtiniausi standartai

1. Tvarkydamas konfidencialią informaciją Europos Parlamentas laikosi I priedo 1 dalyje nustatytų pagrindinių principų ir būtiniausių standartų.

2. Europos Parlamentas pagal pagrindinius principus ir būtiniausius standartus parengia Informacijos saugumo valdymo sistemą (ISVS). ISVS sudaro saugumo pranešimai, naudojimo nurodymai ir atitinkami Darbo tvarkos taisyklių straipsniai. Jos tikslas – palengvinti parlamentinę ir administracinę veiklą bei užtikrinti visos Parlamento tvarkomos konfidencialios informacijos apsaugą visapusiškai laikantis tokios informacijos rengėjo nustatytų taisyklių, pateikiamų saugumo pranešimuose.

Konfidencialios informacijos tvarkymas naudojant Europos Parlamento automatines ryšių ir informacijos sistemas (RIS), įgyvendinamas laikantis informacijos saugumo užtikrinimo (ISU) koncepcijos, kaip numatyta saugumo III pranešime.

3. Europos Parlamento nariai, neturėdami asmens patikimumo patvirtinimo, gali susipažinti su įslaptinta informacija iki slaptumo žymos laipsnio „RESTREINT UE/EU RESTRICTED“ ir įskaitant šį laipsnį.

4. Kai susijusi informacija pažymėta slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ arba jam lygiaverčiu, su ja leidžiama susipažinti tiems Europos Parlamento nariams, kuriems Parlamento pirmininkas suteikė leidimą pagal 5 dalį arba kurie pasirašė oficialų pareiškimą, kad neatskleis tos informacijos turinio tretiesiems asmenims, kad laikysis įsipareigojimo saugoti slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ pažymėtą informaciją ir kad yra susipažinę su šio įsipareigojimo nesilaikymo pasekmėmis.

5. Kai susijusi informacija pažymėta slaptumo žymos laipsniu „SECRET UE/EU SECRET“, „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu, su ja leidžiama susipažinti tiems Europos Parlamento nariams, kurie gavo Pirmininko leidimą po to, kai:

a) jų patikimumas buvo patikrintas pagal šio sprendimo I priedo 2 dalį arba

b) kompetentinga nacionalinė institucija pranešė, kad atitinkamiems nariams buvo išduotas tinkamas leidimas atsižvelgiant į jų atliekamas funkcijas pagal nacionalinius įstatymus ir kitus teisės aktus.

6. Prieš Europos Parlamento nariams suteikiant teisę susipažinti su įslaptinta informacija, jie informuojami apie pareigą saugoti tokią informaciją ir pripažįsta tokią pareigą pagal I priedą. Jie taip pat informuojami apie tokios apsaugos užtikrinimo priemones.

7. Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, dirbantys frakcijose, gali susipažinti su konfidencialia informacija, jeigu jie laikosi principo „būtina žinoti“, ir su įslaptinta aukštesnio laipsnio, kaip slaptumo žyma „RESTREINT UE/EU RESTRICTED“, pažymėta informacija – jeigu jie turi atitinkamo lygmens asmens patikimumo patvirtinimą. Jiems leidžiama susipažinti su įslaptinta informacija, jei jie buvo informuoti apie pareigą saugoti tokią informaciją ir apie tokios apsaugos užtikrinimo priemones bei gavo raštiškus nurodymus šiuo klausimu ir pasirašė pareiškimą, kuriuo patvirtino tokių nurodymų gavimą ir įsipareigojo jų laikytis pagal esamas taisykles.

4 straipsnis

Konfidencialios informacijos rengimas ir administracinis tvarkymas Europos Parlamente

1. Europos Parlamento pirmininkas, susijusio Parlamento komiteto pirmininkai ir generalinis sekretorius, ir (arba) asmuo, kuriam jis tinkamai suteikė leidimą raštu, gali parengti konfidencialią informaciją ir (arba) įslaptinti informaciją, kaip numatyta saugumo pranešimuose.

2. Rengdamas įslaptintą informaciją, rengėjas taiko atitinkamą slaptumo žymos laipsnį pagal tarptautinius standartus ir I priede nustatytas apibrėžtis. Rengėjas taip pat paprastai nustato gavėjus, kuriems turi būti suteiktas leidimas susipažinti su informacija, atitinkančia slaptumo žymos laipsnį. Ši informacija suteikiama Įslaptintos informacijos skyriui (ĮIS), kai jam pateikiamas dokumentas.

3. Kita konfidenciali informacija, kuriai taikoma tarnybinės paslapties saugojimo prievolė, tvarkoma laikantis I ir II priedų ir naudojimo nurodymų.

5 straipsnis

Konfidencialios informacijos gavimas Europos Parlamente

1. Apie Europos Parlamento gautą konfidencialią informaciją pranešama:

a) prašymą pateikusio Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatui arba tiesiogiai ĮIS – apie informaciją, pažymėtą slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu ir apie kitą konfidencialią informaciją;

b) ĮIS – apie informaciją, pažymėtą slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu.

2. Konfidencialios informacijos registravimu, laikymu ir atsekamumu, atsižvelgiant į konkretų atvejį, užsiima informaciją gavęs Parlamento organo sekretoriatas ar atitinkamas pareigas einantis asmuo arba ĮIS.

3. Komisijai pagal Pagrindų susitarimo II priedo 3.2 punktą perduodamos konfidencialios informacijos atveju arba Tarybai pagal Tarpinstitucinio susitarimo 5 straipsnio 4 dalį perduodamos įslaptintos informacijos atveju suderintos nuostatos, kurios turi būti nustatytos bendru sutarimu ir kuriomis siekiama išsaugoti informacijos konfidencialumą, pateikiamos atitinkamai Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatui arba ĮIS.

4. 3 dalyje minimos nuostatos taip pat gali būti taikomos mutatis mutandis, kai konfidencialią informaciją perduoda kitos institucijos, įstaigos, tarnybos ir agentūros, įsteigtos pagal Sutartis ar jomis remiantis, arba valstybės narės.

5. Siekiant užtikrinti apsaugos lygį, atitinkantį slaptumo žymos laipsnį „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiavertį, Pirmininkų sueiga įsteigia priežiūros komitetą. Informacija, pažymėta slaptumo žymos laipsniu „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu, perduodama Europos Parlamentui pagal papildomas nuostatas, dėl kurių susitaria Europos Parlamentas ir informaciją teikianti Sąjungos institucija.

6 straipsnis

Europos Parlamento vykdomas įslaptintos informacijos perdavimas trečiosioms šalims

Europos Parlamentas, gavęs išankstinį raštišką įslaptintos informacijos rengėjo arba Europos Parlamentui ją perdavusios Sąjungos institucijos sutikimą, gali persiųsti tokią įslaptintą informaciją trečiosioms šalims, jeigu jos užtikrina, kad tokia informacija jų tarnybose ir pastatuose tvarkoma laikantis šiame sprendime nurodytoms taisyklėms lygiaverčių taisyklių.

7 straipsnis

Saugios patalpos

1. Konfidencialios informacijos tvarkymo Europos Parlamente tikslais Europos Parlamentas įrengia saugią zoną ir saugias skaityklas.

2. Saugioje zonoje numatomos patalpos įslaptintai informacijai registruoti, skaityti, archyvuoti, perduoti ir tvarkyti. Jose turi būti įrengta, inter alia, skaitykla ir posėdžių salė, kuriose būtų galima susipažinti su įslaptinta informacija ir kurias prižiūrėtų ĮIS.

3. Už saugios zonos ribų gali būti įrengtos saugios skaityklos, kuriose būtų galima susipažinti su ne aukštesniu kaip slaptumo žymos „RESTREINT UE/EU RESTRICTED“ laipsniu arba jam lygiaverčiu pažymėta informacija ir kita konfidencialia informacija. Už tas saugias skaityklas atsakingos Parlamento organo ar atitinkamas pareigas užimančio asmens sekretoriato kompetentingos tarnybos arba ĮIS. Jose užtikrinamas saugus laikymas ir nėra kopijavimo aparatų, telefonų, faksų, skaitytuvų ar kitų dokumentų dauginimo ar perdavimo priemonių.

8 straipsnis

Konfidencialios informacijos registravimas, tvarkymas ir saugojimas

1. Informaciją, pažymėtą slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu, ir kitą konfidencialią informaciją gali registruoti ir saugoti Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato kompetentingos tarnybos arba ĮIS, priklausomai nuo to, kas gavo informaciją.

2. Taikomos šios slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu pažymėtos informacijos ir kitos konfidencialios informacijos tvarkymo sąlygos:

a) dokumentai asmeniškai perduodami sekretoriato vadovui, jis šiuos dokumentus įregistruoja ir išduoda gavimo patvirtinimą;

b) faktiškai nenaudojami dokumentai laikomi užrakintoje vietoje ir už juos atsako sekretoriatas;

c) jokiu atveju informacija negali būti išsaugota kitoje laikmenoje arba perduota kitam asmeniui. Tokius dokumentus galima dauginti tik tinkamai akredituota įranga, kaip apibrėžta saugumo pranešimuose;

d) prieiga prie tokios informacijos suteikiama tik rengėjo arba Sąjungos institucijos, kuri perdavė informaciją Europos Parlamentui, nurodytiems asmenims pagal 4 straipsnio 2 dalyje arba 5 straipsnio 3, 4 ir 5 dalyse numatytą tvarką;

e) Parlamento organo ar atitinkamas pareigas užimančio asmens sekretoriatas pildo asmenų, kurie susipažino su informacija, ir datų bei laiko, kai su jais susipažinta, registrą, ir perduoda šį registrą ĮIS tuo metu, kai ĮIS pateikiama informacija.

3. Informaciją, pažymėtą slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu, saugioje zonoje registruoja ir saugo ĮIS pagal atitinkamą slaptumo žymos laipsnį ir kaip apibrėžta saugumo pranešimuose.

4. Jei pažeidžiamos 1-3 dalyse nustatytos taisyklės, Parlamento organo ar atitinkamas pareigas užimančio asmens sekretoriato, arba ĮIS atsakingas pareigūnas apie tai praneša generaliniam sekretoriui ir šis perduoda šį klausimą Pirmininkui, jei su tuo susijęs Europos Parlamento narys.

9 straipsnis

Teisė patekti į saugias patalpas

1. Į saugią zoną gali patekti tik šie asmenys:

a) asmenys, kurie pagal 3 straipsnio 4–7 dalis turi leidimą susipažinti su joje laikoma informacija ir kurie pateikė prašymą pagal 10 straipsnio 1 dalį;

b) asmenys, kurie pagal 4 straipsnio 1 dalį turi leidimą rengti įslaptintą informaciją ir kurie pateikė prašymą pagal 10 straipsnio 1 dalį;

c) Europos Parlamento pareigūnai, dirbantys ĮIS;

d) už ĮIS valdymą atsakingi Europos Parlamento pareigūnai;

e) kai būtina, už saugumą ir priešgaisrinę saugą atsakingi Europos Parlamento pareigūnai;

f) valytojai – bet tik esant ir atidžiai prižiūrint ĮIS pareigūnui.

2. ĮIS gali atsisakyti į saugią zoną įleisti asmenis, neturinčius leidimo. Prašymą patekti į patalpas pateikę Europos Parlamento nariai, norėdami užginčyti atsisakymą įleisti, kreipiasi į Pirmininką, kiti asmenys – į generalinį sekretorių.

3. Generalinis sekretorius gali leisti surengti nedidelio skaičiaus asmenų posėdį posėdžių salėje, esančioje saugioje zonoje.

4. Į saugią skaityklą gali patekti tik šie asmenys:

a) Europos Parlamento nariai, Europos Parlamento pareigūnai ir kiti Europos Parlamento darbuotojai, dirbantys frakcijose, kurių tapatybė tinkamai nustatyta susipažinimo su konfidencialia informacija arba jos rengimo tikslais;

b) Europos Parlamento pareigūnai, atsakingi už ĮIS valdymą, informaciją gavusio Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato pareigūnai ir ĮIS pareigūnai;

c) kai reikia, už saugumą ir priešgaisrinę saugą atsakingi Europos Parlamento pareigūnai;

d) valytojai – bet tik esant ir atidžiai prižiūrint atitinkamai Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato arba ĮIS pareigūnui.

5. Atsakingas Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatas arba ĮIS, priklausomai nuo atvejo, gali atsisakyti į saugią skaityklą įleisti asmenis, neturinčius leidimo. Prašymą patekti į patalpas pateikę Europos Parlamento nariai, norėdami užginčyti atsisakymą įleisti, kreipiasi į Pirmininką, kiti asmenys – į generalinį sekretorių.

10 straipsnis

Susipažinimas su konfidencialia informacija ir jos rengimas saugiose patalpose

1. Asmuo, norintis susipažinti su konfidencialia informacija arba ją rengti saugioje zonoje, iš anksto praneša savo vardą ir pavardę ĮIS. ĮIS patikrina to pateikusio asmens tapatybę ir patikrina, ar tam asmeniui pagal 3 straipsnio 3–7 dalis, 4 straipsnio 1 dalį arba 5 straipsnio 3, 4 ir 5 dalis leidžiama susipažinti su konfidencialia informacija arba ją rengti.

2. Asmuo, norintis pagal 3 straipsnio 3 ir 7 dalis susipažinti su konfidencialia informacija, pažymėta slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu, ir su kita konfidencialia informacija saugioje skaityklose, iš anksto praneša savo vardą ir pavardę Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato kompetentingoms tarnyboms arba ĮIS.

3. Išskyrus ypatingus atvejus (pvz., per trumpą laikotarpį gaunama daug prašymų leisti susipažinti su konfidencialia informacija), su konfidencialia informacija susipažinti saugioje patalpoje vienu metu leidžiama tik vienam asmeniui, esant Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato arba ĮIS pareigūnui.

4. Susipažįstant su dokumentais draudžiama bendrauti su išorine aplinka (įskaitant draudimą naudotis telefonu ar kitomis technologijų priemonėmis), užsirašinėti ir dauginti ar fotografuoti konfidencialią informaciją, su kuria susipažįstama;

5. Prieš leisdamas asmeniui išeiti iš saugios patalpos, Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato arba ĮIS pareigūnas patikrina, ar konfidenciali informacija, su kuria asmuo susipažino, vis dar yra vietoje, nesugadinta ir tebėra išsami.

6. Jei pažeidžiamos pirmiau nustatytos taisyklės, Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriato arba ĮIS pareigūnas apie tai praneša generaliniam sekretoriui ir šis informuoja Pirmininką, jei pažeidimas susijęs su Europos Parlamento nariu.

11 straipsnis

Susipažinimo su konfidencialia informacija uždarame posėdyje, vykstančiame ne saugiose patalpose, būtiniausi standartai

1. Parlamento komitetų arba kitų Europos Parlamento politinių ar administracinių organų nariai gali susipažinti su informacija, pažymėta slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu, ir kita konfidencialia informacija uždarame posėdyje ne saugiose patalpose.

2. 1 dalyje nurodytomis aplinkybėmis už posėdį atsakingas Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatas užtikrina, kad būtų laikomasi šių sąlygų:

a) į posėdžio salę įleidžiami tik kompetentingo komiteto ar organo pirmininko nurodyti asmenys, kurie turi dalyvauti posėdyje;

b) visi dokumentai sunumeruojami, išdalijami posėdžio pradžioje ir surenkami posėdžio pabaigoje, nedaromi šių dokumentų nuorašai ir šie dokumentai nedauginami ir nefotografuojami;

c) posėdžio protokole nenurodomas aptariamos informacijos turinys. Gali būti užrašomas tik atitinkamas sprendimas, jei jis priimamas;

d) konfidencialiai informacijai, kuri pateikiama žodžiu Europos Parlamento gavėjams, taikomas toks pat konfidencialios informacijos apsaugos lygis, koks taikomas raštu pateikiamai informacijai;

e) posėdžių salėje nelaikomi jokie papildomi dokumentai;

f) dalyviams ir vertėjams žodžiu posėdžio pradžioje išdalijama tik tiek dokumentų kopijų, kiek būtina;

g) posėdžio pradžioje posėdžio pirmininkas aiškiai informuoja apie dokumentų įslaptinimo (kitos žymos) laipsnį;

h) dalyviai negali išsinešti dokumentų iš posėdžių salės;

i) Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatas posėdžio pabaigoje surenka visas dokumentų kopijas ir už jas atsiskaito; ir

j) į posėdžių salę, kurioje susipažįstama su konfidencialia informacija arba kurioje ji aptariama, negalima įsinešti jokių elektroninės komunikacijos priemonių ar kitų elektroninių įtaisų.

3. Kai, laikantis Pagrindų susitarimo II priedo 3.2.2 punkte ir Tarpinstitucinio susitarimo 6 straipsnio 5 dalyje nurodytų išimčių, informacija, pažymėta slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ arba jam lygiaverčiu, aptariama uždarame posėdyje, už posėdį atsakingas Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatas užtikrina ne tik 2 dalyje numatytas nuostatas, bet ir tai, kad, kad posėdyje turintys dalyvauti nurodyti asmenys atitiktų 3 straipsnio 4 ir 7 dalyje išdėstytus reikalavimus.

4. 3 dalyje numatytu atveju ĮIS už uždarą posėdį atsakingam Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatui pateikia reikiamą dokumentų, kurie bus aptariami, kopijų skaičių. Po posėdžio jos grąžinamos ĮIS.

12 straipsnis

Konfidencialios informacijos saugojimas archyve

1. Saugioje zonoje teikiamos saugaus archyvo paslaugos. ĮIS yra atsakinga už saugaus archyvo tvarkymą laikantis standartinių archyvavimo kriterijų.

2. Įslaptinta informacija, galutinai pateikta ĮIS ir informacija, pažymėta slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu, pateikta Parlamento organo atitinkamas pareigas einančio asmens sekretoriatui, perkeliama į saugioje zonoje esantį saugų archyvą praėjus šešiems mėnesiams po to, kai su ja buvo paskutinį kartą susipažinta, ir vėliausiai per metus nuo tos dienos, kai ji buvo pateikta. Už kitos konfidencialios informacijos, jei ji nebuvo pateikta ĮIS, archyvavimą yra atsakingas atitinkamo Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatas pagal bendrąsias dokumentų tvarkymo taisykles.

3. Su saugiame archyve saugoma konfidencialia informacija gali būti susipažįstama laikantis šių sąlygų:

a) į archyvą susipažinti su konfidencialia informacija įleidžiami tik tie asmenys, kurių vardas, pavardė, funkcijos arba pareigos nurodyti lydraštyje, pildomame perduodant saugoti tą informaciją;

b) prašymas susipažinti su konfidencialia informacija turi būti teikiamas ĮIS, o ši perkelia reikiamą dokumentą iš archyvo į saugią skaityklą; ir

c) taikoma 10 straipsnyje nustatyta susipažinimo su konfidencialia informacija tvarka ir sąlygos.

13 straipsnis

Konfidencialios informacijos žymos laipsnio sumažinimas, išslaptinimas ir kitos žymos panaikinimas

1. Konfidencialios informacijos slaptumo žymos laipsnis gali būti sumažintas, ji gali būti visiškai išslaptinta ar jos kita žyma gali būti panaikinta tik gavus rengėjo išankstinį sutikimą, ir, jei reikia, pasitarus su kitomis suinteresuotomis šalimis.

2. Dokumentų slaptumo žymos laipsnio sumažinimas arba jų išslaptinimas patvirtinamas raštu. Rengėjas atsako už to dokumento gavėjų informavimą apie slaptumo žymos pakeitimą, o šie atitinkamai atsako už kitų gavėjų, kuriems yra nusiuntę dokumentą arba jo kopiją, informavimą apie slaptumo žymos pakeitimą. Jei įmanoma, ant įslaptintų dokumentų jų rengėjai nurodo datą, laikotarpį arba įvykį, nuo kurio turinio slaptumo žymos laipsnis gali būti sumažintas arba dokumentas išslaptintas. Priešingu atveju rengėjai peržiūri dokumentus ne rečiau kaip kas penkerius metus, kad garantuotų, jog reikalingas pirminis įslaptinimas.

3. Saugiame archyve saugoma konfidenciali informacija atitinkamu laiku, bet ne vėliau kaip 25-aisias metais nuo jos parengimo, patikrinama, siekiant nuspręsti, ar ji turėtų būti išslaptinta, ar turėtų būti sumažintas jos slaptumo žymos laipsnis, ar kita žyma turėtų būti panaikinta. Tokia informacija tikrinama ir skelbiama laikantis 1983 m. vasario 1 d. Tarybos reglamento (EEB, Euratomas) Nr. 354/83 dėl Europos ekonominės bendrijos ir Europos atominės energijos bendrijos istorinių archyvų atvėrimo visuomenei ([1]) nuostatų. Išslaptinimą atliks įslaptintos informacijos rengėjas arba tuo metu atsakinga tarnyba pagal I priedo 1 dalies 10 skirsnį.

4. Atlikus išslaptinimą, anksčiau saugiame archyve laikyta įslaptinta informacija perkeliama į Europos Parlamento istorinį archyvą, kuriame ji nuolat saugoma ir toliau tvarkoma pagal taikytinas nuostatas.

5. Panaikinus žymą, anksčiau kita konfidencialia informacija laikytai informacijai taikomos Europos Parlamento dokumentų tvarkymo taisyklės.

14 straipsnis

Konfidencialios informacijos saugumo pažeidimai, praradimas arba neteisėtas atskleidimas

1. Pažeidus konfidencialumą apskritai ir, visų pirma, pažeidus šios sprendimo nuostatas Europos Parlamento narių atžvilgiu taikomos atitinkamos Europos Parlamento darbo tvarkos taisyklių nuostatos dėl sankcijų.

2. Jei pažeidimą padaro Europos Parlamento darbuotojas, taikomos atitinkamai Pareigūnų tarnybos nuostatuose ir kitų Europos Sąjungos tarnautojų įdarbinimo sąlygose, nustatytose Reglamente (EEB, Euratomas, EAPB) Nr. 259/68 ([2]) („Tarnybos nuostatai“), numatytos procedūros ir sankcijos.

([1]) OL L 43, 1983 2 15, p. 1.
([2]) OL L 56, 1968 3 4, p. 1.

3. Parlamento Pirmininkas ir (arba) generalinis sekretorius organizuoja visus būtinus pažeidimo tyrimus, kaip apibrėžta VI saugumo pranešime.

4. Jei konfidencialią informaciją Europos Parlamentui perdavė kita Sąjungos institucija arba valstybė narė, Pirmininkas ir (arba) generalinis sekretorius atitinkamai Sąjungos institucijai arba valstybei narei praneša apie įrodytą ar įtariamą įslaptintos informacijos praradimą arba neteisėtą atskleidimą, tyrimo rezultatus bei priemones, kurių imtasi siekiant, kad tai nepasikartotų.

15 straipsnis

Šio sprendimo ir jo įgyvendinimo taisyklių keitimas ir metinė šio sprendimo įgyvendinimo ataskaita

1. Generalinis sekretorius siūlo visus šio sprendimo ir jo įgyvendinimo priedų pakeitimus ir teikia šiuos pasiūlymus Biurui, kad šis priimtų sprendimą.

2. Generalinis sekretorius yra atsakingas už tai, kaip Europos Parlamento tarnybos įgyvendina šį sprendimą, ir pagal šiame sprendime išdėstytus principus parengia naudojimo nurodymus dėl klausimų, kurie numatyti ISVS.

3. Generalinis sekretorius pateikia Biurui metinę šio sprendimo įgyvendinimo ataskaitą.

16 straipsnis

Pereinamojo laikotarpio ir baigiamosios nuostatos

1. ĮIS ar bet kuriame kitame Europos Parlamento archyve laikoma neįslaptinta informacija, kuri laikoma konfidencialia ir kuri pateikta prieš 2014 m. balandžio 1 d., šiame sprendime laikoma kita konfidencialia informacija. Jos rengėjas gali bet kuriuo metu pakeisti konfidencialumo laipsnį.

2. Nukrypstant nuo šio sprendimo 5 straipsnio 1 dalies a punkto ir 8 straipsnio 1 dalies, Tarybos pagal Tarpinstitucinį susitarimą pateikta informacija, pažymėta slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ ar jam lygiaverčiu, dvylikos mėnesių laikotarpiui nuo 2014 m. balandžio 1 d. pateikiama, registruojama ir laikoma ĮIS. Su tokia informacija galima susipažinti pagal Tarpinstitucinio susitarimo 4 straipsnio 2 dalies a ir c punktus ir 5 straipsnio 4 dalį.

3. 2011 m. birželio 6 d. Biuro sprendimas dėl konfidencialios informacijos tvarkymo Europos Parlamente taisyklių panaikinamas.

17 straipsnis

Įsigaliojimas

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

I PRIEDAS

1 dalis.

KONFIDENCIALIOS INFORMACIJOS APSAUGOS PAGRINDINIAI SAUGUMO PRINCIPAI IR BŪTINIAUSI STANDARTAI

1. **ĮVADAS**

Šiose nuostatose nustatomi pagrindiniai konfidencialios informacijos apsaugos principai ir būtiniausi standartai, kurių turi laikytis Europos Parlamentas visose savo darbo vietose, taip pat visi įslaptintos informacijos ir kitos konfidencialios informacijos gavėjai, kad būtų užtikrinamas saugumas ir visiems susijusiems asmenims būtų galima garantuoti, jog taikomi bendri apsaugos standartai. Šiuos principus ir standartus papildo saugumo pranešimai, esantys II priede, ir kitos Parlamento komitetų ir kitų Parlamento organų ar atitinkamas pareigas einančių asmenų elgesio su konfidencialia informacija taisyklės.

2. **PAGRINDINIAI PRINCIPAI**

Europos Parlamento saugumo politika yra sudėtinė jo bendros vidaus valdymo politikos dalis ir todėl yra grindžiama tai bendrai politikai taikomais principais. Tie principai yra: teisėtumas, skaidrumas, atskaitomybė ir subsidiarumas bei proporcingumas.

Teisėtumo principas atspindi būtinybę griežtai laikytis teisinės sistemos vykdant saugumo funkcijas ir būtinybę laikytis taikytinų teisinių reikalavimų. Tai taip pat reiškia, kad atsakomybė saugumo srityje privalo būti pagrįsta tinkamomis teisinėmis nuostatomis. Visa apimtimi taikomos Tarnybos nuostatų taisyklės, ypač jų 17 straipsnis dėl darbuotojų įpareigojimo neteisėtai neatskleisti informacijos, gautos einant pareigas, ir jų VI dalis dėl drausminių priemonių. Be to, saugumo pažeidimai Europos Parlamento atsakomybės ribose nagrinėjami vadovaujantis Europos Parlamento darbo tvarkos taisyklėmis ir jo drausminių priemonių politika.

Skaidrumo principas atspindi būtinybę užtikrinti visų saugumo taisyklių ir nuostatų aiškumą, įvairių tarnybų ir sričių pusiausvyrą (fizinis saugumas palyginti su informacijos apsauga ir pan.), taip pat nuoseklią bei konstruktyvią informavimo saugumo klausimais politiką. Be to, dėl skaidrumo taip pat reikalingos aiškios rašytinės saugumo priemonių įgyvendinimo gairės.

Atskaitingumo principas reiškia, kad turi būti aiškiai apibrėžtos pareigos saugumo srityje. Be to, atskaitingumas žymi poreikį reguliariai tikrinti, ar tos pareigos tinkamai vykdomos.

Subsidiarumo principas reiškia, kad saugumu turi būti pasirūpinama pačiu žemiausiu lygmeniu ir kuo arčiau arčiau Europos Parlamento generalinių direktoratų bei tarnybų. Proporcingumo principas reiškia, kad saugumo veikla turi griežtai apsiriboti tomis sritimis, kurioms saugumas tikrai reikalingas, o saugumo priemonės turi būti proporcingos ginamiems interesams bei tikrai arba galimai grėsmei tiems interesams, siekiant, kad jie būtų ginami taip, kad būtų sukeliama mažiausiai nepatogumų.

3. **INFORMACIJOS SAUGUMO PAGRINDAI**

Patikimas informacijos saugumas grindžiamas:

a) tinkamomis ryšių ir informacijos sistemomis (RIS). Už jas yras atsakinga Europos Parlamento saugumo institucija (kaip apibrėžta I saugumo pranešime);

b) Europos Parlamente – Informacijos saugumo užtikrinimo institucija (kaip apibrėžta I saugumo pranešime), atsakinga už bendradarbiavimą su atitinkama saugumo institucija, ir už informacijos ir konsultacijų apie technines grėsmes RIS ir apsaugos nuo tų grėsmių priemonių teikimą;

c) glaudžiu atsakingų Europos Parlamento tarnybų ir kitų Sąjungos institucijų saugumo tarnybų bendradarbiavimu.

4. **INFORMACIJOS APSAUGOS PRINCIPAI**

4.1. ***Tikslai***

Svarbiausi informacijos apsaugos tikslai yra:

a) apsaugoti konfidencialią informaciją nuo šnipinėjimo, neteisėto atskleidimo arba neleistino platinimo;

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

c) apsaugoti Europos Parlamento pastatus, kuriuose saugoma įslaptinta informacija, nuo sabotažo ir tyčinės žalos;

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

4.2. ***Įslaptinimas***

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

4.2.2. Įslaptinimo sistema – šioje dalyje nustatytų principų įgyvendinimo priemonė. Numatant ir organizuojant kovos su šnipinėjimu, sabotažu, terorizmu ir kitokiomis grėsmėmis veiksmus reikia laikytis panašios įslaptinimo sistemos, kad labiausiai būtų apsaugoti svarbiausi pastatai, kuriuose laikoma įslaptinta informacija, ir lengviausiai pažeidžiamos vietos tuose pastatuose.

4.2.3. Atsakomybė už informacijos įslaptinimą tenka tik susijusios informacijos rengėjui.

4.2.4. Slaptumo žymos laipsnis gali būti grindžiamas tik susijusios informacijos turiniu.

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

4.2.6. Slaptumo žymos dedamos tik tuomet, kai būtina, ir tik tokiam laikotarpiui, kokiam reikia.

4.3. ***Saugumo priemonių paskirtis***

Saugumo priemonės:

a) taikomos visiems įslaptinta informacija, elektroninėmis laikmenomis, kuriose saugoma įslaptinta informacija, ir kita konfidencialia informacija galintiems naudotis asmenims, taip pat visiems pastatams, kuriuose yra tokios informacijos ir svarbių įrengimų;

b) sukuriamos taip, kad būtų galima nustatyti asmenis, kurių padėtis (prieigos teisės, ryšiai ar kt.) gali kelti grėsmę tokios informacijos ir svarbių įrengimų, kuriuose laikoma tokia informacija, saugumui, ir neprileisti tokių asmenų prie minėtos informacijos arba nušalinti nuo jos;

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

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

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

5. **BENDRI BŪTINIAUSI STANDARTAI**

Europos Parlamentas užtikrina, jog visi įslaptintos informacijos gavėjai pačioje institucijoje ir jos kompetencijai priklausančiose institucijose, t. y. visos tarnybos ir sutarčių partneriai, laikytųsi bendrų būtiniausių saugumo standartų, kad tokia informacija būtų perduodama įsitikinus, jog ji bus taip pat atsakingai tvarkoma. Prie tokių būtiniausių standartų priskiriami asmens patikimumo patvirtinimo Europos Parlamento pareigūnams ir kitiems Parlamento darbuotojams, frakcijose dirbantiems, suteikimo kriterijai ir konfidencialios informacijos apsaugos procedūros.

Europos Parlamentas suteikia teisę trečiosioms šalims naudotis tokia informacija tik jei šios užtikrina, kad tvarkydamos ją griežtai laikysis bent šiuos būtiniausius standartus tiksliai atitinkančių nuostatų.

Tokie bendri būtiniausi standartai taip pat taikomi, kai Europos Parlamentas pagal sutartį ar susitarimą dėl leidimo pramonės ar kitokiems subjektams paveda atlikti užduotis, susijusias su konfidencialia informacija.

6. **EUROPOS PARLAMENTO PAREIGŪNŲ IR KITŲ FRAKCIJOSE DIRBANČIŲ PARLAMENTO DARBUOTOJŲ SAUGUMAS**

6.1. ***Europos Parlamento pareigūnų ir kitų Parlamento darbuotojų, kurie dirba frakcijose, instruktavimas saugumo klausimais***

Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, kurie dirba frakcijose, einantys pareigas, sudarančias galimybes naudotis įslaptinta informacija, pradėdami eiti pareigas ir vėliau reguliariai nuodugniai instruktuojami apie saugumo svarbą ir jo užtikrinimo procedūras. Tokie asmenys privalo raštu patvirtinti, kad susipažino su taikytinais saugumo reikalavimais ir kad juos visiškai supranta.

6.2. ***Vadovų atsakomybė***

Žinoti, kurie vadovų darbuotojai dirba su įslaptinta informacija arba gali naudotis saugiomis ryšių ar informacijos sistemomis, bei registruoti ir pranešti apie visus galinčius turėti įtakos saugumui incidentus arba pažeidimus, turi būti tų vadovų atsakomybės dalis.

6.3. ***Europos Parlamento pareigūnų ir kitų Parlamento darbuotojų, dirbančių frakcijose, saugumo statusas***

Nustatoma tvarka, užtikrinanti, kad, gavus nepalankios informacijos apie Europos Parlamento pareigūną ar apie kitą Parlamento darbuotoją, dirbantį frakcijose, imamasi veiksmų siekiant nustatyti, ar tas asmuo darbo metu gali susipažinti su įslaptinta informacija arba ar gali naudotis saugiomis ryšių arba informacijos sistemomis, ir informuojama atsakinga Europos Parlamento tarnyba. Jei kompetentinga nacionalinė saugumo institucija nurodo, kad toks asmuo kelia grėsmę saugumui, jam neleidžiama atlikti pareigų arba jis nušalinamas nuo pareigų, kurias eidamas gali kelti grėsmę saugumui.

7. **FIZINIS SAUGUMAS**

Fizinis saugumas – fizinių ir techninių apsaugos priemonių taikymas siekiant užkirsti kelią leidimo neturintiems asmenims susipažinti su įslaptinta informacija.

7.1. ***Apsaugos poreikis***

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

7.2. ***Tikrinimas***

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

7.3. ***Pastatų saugumas***

Pastatai, kuriuose kaupiama įslaptinta informacija arba laikomos saugios ryšių ir informacijos sistemos, saugomi, kad į juos nepatektų leidimo neturintys asmenys.

Įslaptintos informacijos apsaugos pobūdis, pvz., langų grotos, durų užraktai, apsauga prie įėjimų, automatizuotos prieigos kontrolės sistemos, apsaugos tikrinimai ir patruliai, signalizacijos sistemos, į įsibrovimą reaguojančios sistemos ir sarginiai šunys, priklauso nuo:

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

b) atitinkamos informacijos ir medžiagos apsauginių talpyklų kokybės ir

c) pastato fizinių savybių ir vietos.

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

7.4. ***Nenumatytų atvejų planai***

Iš anksto parengiami išsamūs įslaptintos informacijos apsaugos ištikus nenumatytam atvejui planai.

8. **SLAPTUMO ŽYMOS GALIOJIMO ŽYMOS, KITOS ŽYMOS, ŽYMŲ NURODYMAS IR ĮSLAPTINIMO ADMINISTRAVIMAS**

8.1. ***Slaptumo žymos galiojimo žymos***

Nėra leidžiamos jokios kitos slaptumo žymos, kaip tik tos, kurios nurodytos šio sprendimo 2 straipsnio d punkte.

Slaptumo žymos galiojimo terminams nustatyti (įslaptintai informacijai, kuriai taikomas automatinis slaptumo laipsnio sumažinimas arba išslaptinimas) gali būti naudojama sutarta slaptumo žymos galiojimo žyma.

Slaptumo žymos galiojimo žymos naudojamos tik kartu su slaptumo žymomis.

Slaptumo žymos galiojimo žymos išsamiau reglamentuotos II saugumo pranešime ir nustatytos naudojimo nurodymuose.

8.2. ***Kitos žymos***

Kita žyma naudojama, kai reikia tiksliai apibrėžti iš anksto numatytus konkrečius nurodymus dėl konfidencialios informacijos tvarkymo. Kitos žymos taip pat gali nurodyti tam tikro dokumento taikymo sritį, pažymėti specialų jo platinimą vadovaujantis principu "būtina žinoti" ar nurodyti, kada baigiasi draudimas platinti (neįslaptintos informacijos atveju).

Kita žyma nėra slaptumo žyma, todėl vietoje jos nenaudojama.

Kitos žymos išsamiau reglamentuotos II saugumo pranešime ir nustatytos naudojimo nurodymuose.

8.3. ***Slaptumo žymų ir slaptumo žymų galiojimo žymų nurodymas***

Slaptumo žymos, slaptumo žymų galiojimo žymos ir kitos žymos nurodomos pagal II saugumo pranešimo E dalį ir naudojimo nurodymus.

8.4. ***Įslaptinimo administravimas***

8.4.1 *Bendra padėtis*

Informacija įslaptinama tik tuomet, kai tai būtina. Slaptumo žyma aiškiai ir teisingai nurodoma ir taikoma tik tol, kol informaciją reikia saugoti.

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

Europos Parlamento pareigūnai informaciją įslaptina, sumažina jos slaptumo laipsnį arba informaciją išslaptina tik gavę generalinio sekretoriaus nurodymą arba remdamiesi jo suteiktais įgaliojimais.

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

Asmenų, turinčių leidimą rengti slaptumo žymos laipsniu „TRÈS SECRET UE/EU TOP SECRET" žymimą informaciją, turi būti kuo mažiau, o jų vardai ir pavardės įtraukiamos į ĮIS sudarytą sąrašą.

8.4.2 *Slaptumo žymų naudojimas*

Dokumento slaptumo žymos laipsnis nustatomas pagal 2 straipsnio d punkte apibrėžtą jo turinio slaptumo laipsnį. Svarbu, kad slaptumo žymos būtų taikomos teisingai ir nuosaikiai.

Pridedamų dokumentų lydraščių arba pranešimų slaptumo žymos laipsnis atitinka priedų aukščiausio laipsnio slaptumo žymos laipsnį. Jei lydraščiai ar pranešimai pateikiami atskirai nuo priedų, rengėjas turi aiškiai nurodyti, koks slaptumo žymos laipsnis jiems suteikiamas.

Įslaptinamo dokumento rengėjas turi laikytis minėtų taisyklių ir vengti suteikti pernelyg aukštą ar pernelyg žemą slaptumo žymos laipsnį.

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

9. **PATIKRINIMAI**

Europos Parlamento Saugos ir rizikos vertinimo direktoratas, kuris gali prašyti pagalbos Komisijos arba Tarybos saugumo tarnybų, reguliariai atlieka vidinius įslaptintos informacijos apsaugai skirtų saugumo priemonių patikrinimus.

Sąjungos institucijų saugumo tarnybos ir kompetentingos tarnybos, vykdydamos vieno iš subjektų inicijuotą ir kitiems subjektams sutinkant pradėtą procedūrą, gali atlikti apsaugos priemonių, kuriomis siekiama apsaugoti įslaptintą informaciją, kuria apsikeista pagal atitinkamus tarpinstitucinius susitarimus, tarpusavio vertinimą.

10. **IŠSLAPTINIMO IR KITŲ ŽYMŲ PANAIKINIMO PROCEDŪROS**

10.1. ĮIS išnagrinėja savo registre laikomą konfidencialią informaciją ir prašo dokumento rengėjo leisti išslaptinti arba panaikinti kitas dokumento žymas ne vėliau kaip 25-aisias metais nuo jo parengimo. Po pirmo patikrinimo neišslaptinti dokumentai arba dokumentai, kurių žymos nepanaikintos, dar kartą tikrinami periodiškai ir ne rečiau nei kas penkeri metai. Kitų žymų panaikinimo procedūra gali būti taikoma ne tik dokumentams, kurie šiuo metu jau saugomi saugioje zonoje esančiuose saugiuose archyvuose ir yra tinkamai įslaptinti, bet ir kitai konfidencialiai informacijai, laikomai Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriate arba už Parlamento istorinius archyvus atsakingoje tarnyboje.

10.2 Sprendimą dėl dokumento išslaptinimo arba kitų žymų panaikinimo paprastai priima tik rengėjas arba, išimtiniais atvejais, prieš dokumento informaciją persiunčiant už Parlamento istorinius archyvus atsakingai tarnybai, toks sprendimas priimamas bendradarbiaujant su tokią informaciją turinčia Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatu. Išslaptinti įslaptintą informaciją ar panaikinti jos žymą galima tik gavus išankstinį raštišką rengėjo sutikimą. Kitos konfidencialios informacijos atveju tokią informaciją turinčios Parlamento organo ar atitinkamas pareigas einančio asmens sekretoriatas, bendradarbiaudamas su informacijos rengėju, priima sprendimą dėl tokio dokumento žymos panaikinimo.

10.3. Rengėjo vardu ĮIS atsako už to dokumento gavėjų informavimą apie slaptumo žymos arba kitos žymos pakeitimą, o šie atitinkamai atsako už kitų gavėjų, kuriems jie yra nusiuntę dokumentą arba jo kopiją, informavimą.

10.4. Išslaptinimas neturi jokio poveikio kitoms slaptumo žymų galiojimo žymoms arba kitoms žymoms, galinčioms atsirasti ant dokumento.

10.5. Išslaptinimo atveju pradinė slaptumo žyma kiekvieno puslapio viršuje ir apačioje išbraukiama. Ant pirmo dokumento puslapio dedamas antspaudas ir pateikiama ĮIS nuoroda. Kitos žymos panaikinimo atveju pradinė žyma kiekvieno (antraštinio) pirmo puslapio viršuje išbraukiama.

10.6. Išslaptinto dokumento arba dokumento, kurio žyma panaikinta, tekstas pridedamas prie elektroninės formos ar atitinkamos sistemos, kurioje jis buvo registruotas.

10.7. Kai dokumentams taikoma išimtis, susijusi su privatumu ir asmens neliečiamumu ar fizinio arba juridinio asmens prekybiniais interesais ir kai dokumentai yra slapto pobūdžio, taikomas Reglamento (EEB, Euratomas) Nr. 354/83 2 straipsnis.

10.8. Be 10.1–10.7 punktų nuostatų taip pat taikomos šios taisyklės:

a) kalbant apie trečiųjų šalių dokumentus ĮIS, prieš vykdydamas išslaptinimą arba panaikindamas kitą žymą, konsultuojasi su susijusia trečiąja šalimi;

b) kalbant apie taikomas išimtis, susijusias su privatumu ir asmens neliečiamumu, vykdant išslaptinimo arba kitos žymos panaikinimo procedūrą yra ypatingai atsižvelgiama į susijusio asmens sutikimą arba, jei reikia, į tai, kad neįmanoma nustatyti susijusio asmens tapatybės;

c) kalbant apie taikomas išimtis, susijusias su fizinio ar juridinio asmens prekybiniais interesais, susijusiam asmeniui gali būti pranešama paskelbus informaciją *Europos Sąjungos oficialiajame leidinyje*, ir jam gali būti suteiktas keturių savaičių terminas nuo informacijos paskelbimo dienos pastaboms pateikti.

2 dalis.

ASMENS PATIKIMUMO TIKRINIMO TVARKA

11. **ASMENS PATIKIMUMO TIKRINIMO TVARKA, TAIKOMA EUROPOS PARLAMENTO NARIAMS**

11.1. Kad galėtų susipažinti su slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ arba jam lygiaverčiu pažymėta informacija, Europos Parlamento nariai turi turėti leidimą, suteiktą šio priedo 11.3 ir 11.4 punktuose nustatyta tvarka arba būti pasirašę šio sprendimo 3 straipsnio 4 dalyje nurodytą oficialų pareiškimą neatskleisti informacijos.

11.2 Kad galėtų susipažinti su slaptumo žymos laipsniu „SECRET UE/EU SECRET“ arba „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu pažymėta informacija, Europos Parlamento nariai turi turėti leidimą, suteiktą 11.14 ir 11.4 punktuose nustatyta tvarka.

11.3. Leidimas suteikiamas tik tiems Europos Parlamento nariams, kurių patikimumą 11.9–11.14 punktuose nurodyta tvarka yra patikrinusios valstybių narių kompetentingos nacionalinės institucijos. Pirmininkas atsakingas už leidimų suteikimą nariams.

11.4 Pirmininkas gali išduoti raštišką leidimą gavęs valstybės narės kompetentingos nacionalinės institucijos nuomonę, pagrįstą 11.8–11.13 punktuose nurodyta tvarka atlikto asmens patikimumo patikrinimo rezultatais.

11.5. Europos Parlamento Saugos ir rizikos vertinimo direktoratas veda nuolat atnaujinamą visų Europos Parlamento narių, kuriems buvo suteiktas leidimas, sąrašą, įskaitant laikinus leidimus, kaip nurodyta 11.15 punkte.

11.6. Leidimas galioja penkerius metus arba laikotarpiu, kurio reikia užduotims, kurioms jis buvo išduotas, atlikti, atsižvelgiant į tai, kuris laikotarpis trumpesnis. Leidimą galima atnaujinti 11.4 punkte nurodyta tvarka.

11.7. Pirmininkas panaikina leidimą, jei mano esant pagrįstų priežasčių tokiam panaikinimui. Apie bet kokį sprendimą panaikinti leidimą turi būti pranešta atitinkamam Europos Parlamento nariui, kuris, prieš sprendimui įsigaliojant, gali prašyti, kad Pirmininkas jį išklausytų, taip pat apie tai pranešama kompetentingai nacionalinei institucijai.

11.8. Asmens patikimumo patikrinimas atliekamas padedant atitinkamam Europos Parlamento nariui ir Pirmininko prašymu. Patikrinimą turi atlikti tik tos valstybės narės, kurios pilietis yra leidimo prašantis Parlamento narys, kompetentinga nacionalinė institucija.

11.9. Pagal tikrinimo tvarką reikalaujama, kad atitinkamas Europos Parlamento narys užpildytų asmens informacijos anketą.

11.10. Savo prašyme kompetentingai nacionalinei institucijai Pirmininkas patikslina įslaptintos informacijos, su kuria susipažins atitinkamas Europos Parlamento narys, laipsnį, kad jos galėtų atlikti patikrinimą.

11.11 Visa asmens patikimumo patikrinimo procedūra, kurią vykdo kompetentinga nacionalinė institucija, ir gauti rezultatai turi atitikti atitinkamoje valstybėje narėje galiojančias normas ir taisykles, įskaitant su apeliacijomis susijusias normas ir taisykles.

11.12. Gavęs kompetentingos nacionalinės institucijos teigiamą nuomonę, Pirmininkas gali atitinkamam Europos Parlamento nariui suteikti leidimą.

11.13. Apie neigiamą kompetentingos nacionalinės institucijos nuomonę pranešama atitinkamam Europos Parlamento nariui, kuris gali prašyti, kad Pirmininkas jį išklausytų. Pirmininkas, jei mano esant reikalinga, gali paprašyti kompetentingos nacionalinės institucijos papildomo paaiškinimo. Jei neigiama nuomonė patvirtinama, leidimas nesuteikiamas.

11.14. Visi Europos Parlamento nariai, kuriems pagal 11.3 punktą suteiktas leidimas, leidimo suteikimo metu ir reguliariai po to gauna visus būtinus nurodymus, susijusius su įslaptintos informacijos apsauga ir šios apsaugos užtikrinimo priemonėmis. Tokie nariai pasirašo pareiškimą, kuriame patvirtina gavę tas instrukcijas.

11.15. Išskirtiniais atvejais Pirmininkas, pranešęs kompetentingai nacionalinei institucijai ir per vieną mėnesį negavęs tos institucijos atsakymo, kol laukiama 11.11 punkte nurodyto patikrinimo rezultatų, gali Europos Parlamento nariui ne ilgiau kaip šešiems mėnesiams suteikti laikinąjį leidimą. Laikinieji leidimai nesuteikia teisės susipažinti su slaptumo žymos laipsniu „TRÈS SECRET UE/EU TOP SECRET“ ar jam lygiaverčiu pažymėta informacija.

12. ASMENS PATIKIMUMO TIKRINIMO TVARKA, TAIKOMA EUROPOS PARLAMENTO PAREIGŪNAMS IR KITIEMS PARLAMENTO DARBUOTOJAMS, DIRBANTIEMS FRAKCIJOSE

12.1. Tik Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, dirbantys frakcijose, kurie dėl savo pareigų ir tarnybos reikalavimų turi būti susipažinę su įslaptinta informacija arba turi ją naudoti, gali susipažinti su tokia informacija.

12.2. Kad atitinkami Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, dirbantys frakcijose, galėtų susipažinti su slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ ar jam lygiaverčiu pažymėta informacija, jiems suteikiamas leidimas 12.3 ir 12.4 punktuose nustatyta tvarka.

12.3. Leidimas išduodamas tik 12.1 punkte nurodytiems asmenims, kurių patikimumą 12.9–12.14 punktuose nurodyta tvarka yra patikrinusios valstybių narių kompetentingos nacionalinės institucijos. Generalinis sekretorius atsakingas už leidimų suteikimą Europos Parlamento pareigūnams ir kitiems Parlamento darbuotojams, dirbantiems frakcijose.

12.4. Generalinis sekretorius gali išduoti raštišką leidimą gavęs valstybės narės kompetentingos nacionalinės institucijos nuomonę, pagrįstą 12.8–12.13 punktuose nurodyta tvarka atlikto asmens patikimumo patikrinimo rezultatais.

12.5. Europos Parlamento Saugos ir rizikos vertinimo direktoratas veda nuolat atnaujinamą visų pareigų, kurias einantys asmenys turi turėti asmens patikimumo patvirtinimą ir kurias nurodo atitinkamos Europos Parlamento tarnybos, ir visų asmenų, kuriems suteiktas leidimas, įskaitant laikinąjį leidimą pagal 12.15 punktą, sąrašą.

12.6. Leidimas galioja penkerius metus arba laikotarpiu, kurio reikia užduotims, kurioms jis buvo išduotas, atlikti, atsižvelgiant į tai, kuris laikotarpis trumpesnis. Leidimą galima atnaujinti 12.4 punkte nurodyta tvarka.

12.7. Generalinis sekretorius panaikina leidimą, jei mano esant pagrįstų priežasčių tam panaikinimui. Apie bet kokį sprendimą panaikinti leidimą turi būti pranešta atitinkamam Europos Parlamento pareigūnui ar kitam Parlamento darbuotojui, dirbančiam frakcijoje, kuris, prieš įsigaliojant sprendimui panaikinti leidimą, gali prašyti, kad generalinis sekretorius jį išklausytų, taip pat apie tai pranešama ir kompetentingai nacionalinei institucijai.

12.8. Asmens patikimumo patikrinimas generalinio sekretoriaus prašymu atliekamas padedant atitinkamam Europos Parlamento pareigūnui arba kitam Parlamento darbuotojui, dirbančiam frakcijose. Patikrinimą atlieka tos valstybės narės, kurios pilietis yra leidimo prašantis asmuo, kompetentinga nacionalinė institucija. Kai leidžiama pagal nacionalinius įstatymus ir teisės aktus, kompetentingos nacionalinės institucijos gali atlikti tyrimus, susijusius su užsienio piliečių reikalavimu susipažinti su slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“, pažymėta informacija.

12.9. Pagal tikrinimo tvarką reikalaujama, kad atitinkamas Europos Parlamento pareigūnas ar kitas Parlamento darbuotojas, dirbantis frakcijoje, užpildytų asmens informacijos anketą.

12.10. Generalinis sekretorius savo prašyme kompetentingai nacionalinei institucijai nurodo įslaptintos informacijos, su kuria atitinkamam Europos Parlamento pareigūnui arba kitam Parlamento darbuotojui, dirbančiam frakcijose, turėtų būti leista susipažinti, slaptumo žymos laipsnį, kad ji galėtų atlikti patikrinimą ir pateikti savo nuomonę dėl to, su kokio slaptumo žymos laipsnio informacija derėtų leisti susipažinti šiam asmeniui.

12.11. Visa kompetentingos nacionalinės institucijos atliekamo asmens patikimumo patikrinimo tvarka ir gauti rezultatai turi atitikti atitinkamoje valstybėje narėje galiojančias normas ir taisykles, įskaitant su apeliacijomis susijusias normas ir taisykles.

12.12. Gavęs kompetentingos nacionalinės institucijos teigiamą nuomonę, generalinis sekretorius gali atitinkamam Europos Parlamento pareigūnui arba kitam Parlamento darbuotojui, dirbančiam frakcijose, suteikti leidimą.

12.13. Apie neigiamą kompetentingos nacionalinės institucijos nuomonę pranešama atitinkamam Europos Parlamento pareigūnui ir kitam Parlamento darbuotojui, dirbančiam frakcijoje, o jis gali prašyti, kad generalinis sekretorius jį išklausytų. Jei generalinis sekretorius mano, kad tai tikslinga, jis gali paprašyti kompetentingos nacionalinės institucijos papildomo paaiškinimo. Jei neigiama nuomonė patvirtinama, leidimas nesuteikiamas.

12.14. Visi Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, dirbantys frakcijose, kuriems leidimai suteikti pagal 12.4 ir 12.5 punktus, leidimo suteikimo metu ir reguliariai po to gauna visus būtinus nurodymus, susijusius su įslaptintos informacijos apsauga ir šios apsaugos užtikrinimo priemonėmis. Tokie pareigūnai ir darbuotojai pasirašo deklaracijas, kuriose patvirtina gavę nurodymus ir įsipareigoja jų laikytis.

12.15. Išskirtiniais atvejais generalinis sekretorius, pranešęs kompetentingai nacionalinei institucijai ir per vieną mėnesį negavęs jos atsakymo, kol laukiama šios dalies 12.11 punkte nurodyto patikrinimo rezultatų, gali ne ilgiau kaip šešiems mėnesiams Europos Parlamento pareigūnui ar kitam Parlamento darbuotojui, dirbančiam frakcijoje, suteikti laikinąjį leidimą. Laikinieji leidimai nesuteikia teisės susipažinti su slaptumo žymos laipsniu „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu pažymėta informacija.

II PRIEDAS

ĮŽANGA

Šiomis nuostatomis apibrėžiami saugumo pranešimai, kuriais reglamentuojamas ir užtikrinamas Europos Parlamento atliekamas saugus konfidencialios informacijos tvarkymas ir valdymas. Tie saugumo pranešimai kartu su visais naudojimo nurodymais sudaro šio sprendimo 3 straipsnio 2 dalyje nurodytą Europos Parlamento informacijos saugumo valdymo sistemą (ISVS):

I SAUGUMO PRANEŠIMAS

Saugumo organizavimas Europos Parlamente siekiant apsaugoti konfidencialią informaciją

II SAUGUMO PRANEŠIMAS

Konfidencialios informacijos valdymas

III SAUGUMO PRANEŠIMAS

Konfidencialios informacijos tvarkymas naudojant automatines ryšių informacines sistemas (RIS)

IV SAUGUMO PRANEŠIMAS

Fizinis saugumas

V SAUGUMO PRANEŠIMAS

Pramoninis saugumas

VI SAUGUMO PRANEŠIMAS

Konfidencialios informacijos saugumo pažeidimai, praradimas arba neteisėtas atskleidimas

I SAUGUMO PRANEŠIMAS

SAUGUMO ORGANIZAVIMAS EUROPOS PARLAMENTE SIEKIANT APSAUGOTI KONFIDENCIALIĄ INFORMACIJĄ

1. Generalinis sekretorius atsakingas už visapusišką ir nuoseklų šio sprendimo įgyvendinimą.

Generalinis sekretorius imasi visų reikiamų priemonių, kad užtikrintų, jog konfidencialios informacijos tvarkymo ar saugojimo atveju Europos Parlamento nariai, Europos Parlamento pareigūnai, kiti Parlamento darbuotojai, dirbantys frakcijose, ir rangovai Parlamento patalpose taikytų šį sprendimą.

2. Generalinis sekretorius yra saugumo institucija (SĮ). Vykdydamas šias funkcijas generalinis sekretorius atsako už:

2.1. visų su Parlamento veikla susijusių saugumo klausimų koordinavimą konfidencialios informacijos apsaugos srityje;

2.2. leidimą įrengti saugią zoną, saugias skaityklas ir įdiegti saugią įrangą;

2.3. sprendimų, kuriais pagal šio sprendimo 6 straipsnį suteikiamas leidimas Parlamentui perduoti įslaptintą informaciją trečiosioms šalims, įgyvendinimą;

2.4. už tyrimą ir nurodymą atlikti tyrimą dėl neteisėto konfidencialios informacijos atskleidimo, kuri prima facie buvo atskleista Parlamente, o jei su tuo susijęs Europos Parlamento narys – pasitarus su Europos Parlamento pirmininku;

2.5. glaudų bendradarbiavimą su Sąjungos kitų institucijų saugumo tarnybomis ir valstybių narių nacionalinėmis saugumo institucijomis, siekiant užtikrinti geriausią su įslaptinta informacija susijusios saugumo politikos koordinavimą;

2.6. nuolatinį Parlamento saugumo politikos ir tvarkos tikrinimą ir atitinkamų deramų rekomendacijų teikimą;

2.7. nacionalinės saugumo institucijos (NSI), kuri pagal I priedo 2 dalies 11.3 punktą atliko asmens patikimumo patikrinimą, informavimą tais atvejais, kai bet kokia neigiama informacija gali turėti poveikį tai institucijai.

3. Atvejais, kurie susiję su Europos Parlamento nariais, generalinis sekretorius savo pareigas vykdo glaudžiai bendradarbiaudamas su Europos Parlamento pirmininku.

4. Generaliniam sekretoriui atliekant savo pareigas pagal 2 ir 3 dalis padeda generalinio sekretoriaus pavaduotojas, Saugos ir rizikos vertinimo direktoratas, Informacinių technologijų direktoratas (ITD) ir Įslaptintos informacijos skyrius (ĮIS).

4.1. Saugos ir rizikos vertinimo direktoratas atsakingas už asmenines apsaugos priemones ir ypač už asmens patikimumo tikrinimą, kaip nustatyta I priedo 2 dalyje. Saugos ir rizikos vertinimo direktoratas taip pat:

a) yra Sąjungos kitų institucijų saugumo tarnybų ir nacionalinių saugumo tarnybų kontaktinis centras klausimais, susijusiais su asmens patikimumo tikrinimu, atliekamu dėl Europos Parlamento narių, Europos Parlamento pareigūnų ir kitų Parlamento darbuotojų, dirbančių frakcijose;

b) rengia būtinus informavimo renginius bendro saugumo klausimais apie prievolę apsaugoti įslaptintą informaciją ir bet kokio šios prievolės pažeidimo pasekmes;

c) stebi, kaip naudojamasi saugia zona ir saugiomis skaityklomis Parlamento patalpose, jei reikia, bendradarbiaudamas su Sąjungos kitų institucijų ir valstybių narių saugumo tarnybomis;

d) kontroliuoja, bendradarbiaudamas su kitų Sąjungos institucijų ir valstybių narių saugumo tarnybomis, įslaptintos informacijos valdymą ir laikymą, saugią zoną ir saugias skaityklas Parlamento patalpose, kuriose tvarkoma įslaptinta informacija;

e) generaliniam sekretoriui teikia pasiūlymus dėl reikiamų naudojimo nurodymų.

4.2. ITD atsakingas už saugias IT sistemas, kurias Europos Parlamentas naudoja tvarkydamas konfidencialią informaciją.

4.3. ĮIS atsakingas už:

a) saugumo poreikių nustatymą siekiant veiksmingai apsaugoti konfidencialią informaciją, glaudžiai bendradarbiaujant su Saugos ir rizikos vertinimo direktoratu ir ITD ir kitų Sąjungos institucijų saugumo tarnybomis;

b) konfidencialios informacijos valdymo ir laikymo Parlamente visų aspektų nustatymą, kaip nustatyta naudojimo nurodymuose;

c) saugios zonos naudojimą;

d) konfidencialios informacijos valdymą ir susipažinimą su ja saugioje zonoje arba ĮIS saugioje skaitykloje pagal šio sprendimo 7 straipsnio 2 ir 3 dalis;

e) ĮIS registro valdymą;

f) SI informavimą apie bet kokius įrodytus ar tariamus konfidencialios informacijos, pateikiamos ĮIS ir laikomos saugioje zonoje arba ĮIS saugioje skaitykloje, saugumo pažeidimus, praradimą arba neteisėtą atskleidimą.

5. Be to, generalinis sekretorius, kaip SI, skiria šias institucijas:

a) Saugumo akreditavimo instituciją (SAI);

b) Informacijos saugumo užtikrinimo operacinę instituciją (ISUOI);

c) Kriptografijos platinimo instituciją (KPLI);

d) TEMPEST instituciją (TEI);

e) Informacijos saugumo užtikrinimo instituciją (ISUI).

Šioms funkcijoms atlikti nereikia atskirų organizacinių vienetų. Šioms institucijoms suteikiami atskiri įgaliojimai. Tačiau šios funkcijos ir su jomis susijusi atsakomybė gali būti susietos arba integruotos viename organizaciniame vienete arba padalytos skirtingiems organizaciniams vienetams, jei išvengiama interesų konfliktų ir užduočių kartojimosi.

6. SAI konsultuoja visais saugumo klausimais, susijusiais su visų informacinių technologijų sistemų ir tinklų akreditavimu Parlamente:

6.1. užtikrindama, kad RIS atitiktų atitinkamą saugumo politiką ir saugumo gaires, pateikdama pareiškimą dėl RIS patvirtinimo, leidžiant ją naudoti įslaptintos informacijos tvarkymui iki nustatyto slaptumo žymos laipsnio informacijos operacinėje aplinkoje, ir nurodydama akreditavimo reikalavimus ir sąlygas bei kriterijus, kuriais remiantis reikalaujama, kad reikia iš naujo patvirtinti RIS;

6.2. nustatydama saugumo akreditavimo tvarką pagal atitinkamą politiką, aiškiai nurodydama patvirtinimo sąlygas, nustatytas jos priežiūrai pavestoms RIS;

6.3. parengdama saugumo akreditavimo strategiją, kurioje nustatytas akreditavimo tvarkos išsamumo lygis, atitinkantis reikiamą saugumo užtikrinimo lygį;

6.4. tikrindama ir patvirtindama su saugumu susijusius dokumentus, įskaitant pareiškimus dėl rizikos valdymo ir likutinės rizikos, saugumo įgyvendinimo patikrinimo dokumentus ir saugios eksploatacijos taisykles, taip pat užtikrindama, kad šie dokumentai atitiktų Parlamento saugumo taisykles ir politiką;

6.5. tikrindama su RIS susijusių saugumo priemonių įgyvendinimą vykdant saugumo įvertinimus, patikrinimus ar peržiūras arba juos finansuojant;

6.6. nustatydama saugumo reikalavimus (pavyzdžiui, susijusius su personalo patikimumo laipsniais), taikomus su RIS saugumo atžvilgiu susijusioms pareigybėms;

6.7. patvirtindama arba, jei reikia, dalyvaudama bendrame patvirtinime apie atitinkamos RIS sujungimą su kita RIS;

6.8. patvirtindama techninės įrangos, naudojamos saugiam įslaptintos informacijos tvarkymui ir apsaugai, saugumo standartus;

6.9. užtikrindama, kad Parlamente naudojamos šifravimo priemonės būtų įtrauktos į ES patvirtintų priemonių sąrašą, ir

6.10. konsultuodama sistemos tiekėją, saugumo srities subjektus ir vartotojų atstovus saugumo rizikos valdymo, visų pirma likutinės rizikos, ir pareiškimo dėl patvirtinimo reikalavimų ir sąlygų klausimais.

7. ISUOI atsakinga už:

7.1. saugumo dokumentų, atitinkančių saugumo politiką ir saugumo gaires, rengimą, ypač įskaitant pareiškimą dėl likutinės rizikos, saugios eksploatacijos taisykles ir šifravimo planą vykdant RIS akreditavimo procesą;

7.2. dalyvavimą atrenkant ir bandant konkrečioms sistemoms skirtas techninio saugumo priemones, prietaisus ir programinę įrangą, siekiant prižiūrėti, kaip jie taikomi, ir užtikrinti, kad jie būtų saugiai įdiegti, sukonfigūruoti ir eksploatuojami pagal atitinkamus saugumo dokumentus;

7.3. saugios eksploatacijos taisyklių įgyvendinimo ir taikymo stebėseną ir prireikus – atsakomybės už eksploatavimo saugumą delegavimą sistemos savininkui, būtent, ĮIS;

7.4. šifravimo priemonių valdymą ir tvarkymą užtikrinant šifravimo ir kontroliuojamų objektų saugojimą ir prireikus užtikrinant šifravimo kintamųjų generavimą;

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

7.6. mokymo konkrečioms RIS skirto informacijos saugumo užtikrinimo (ISU) klausimais rengimą;

7.7. konkrečioms RIS skirtų apsaugos priemonių įgyvendinimą ir naudojimą.

8. KPLI atsako už:

8.1. ES šifravimo medžiagos valdymą ir apskaitą;

8.2. užtikrinimą, glaudžiai bendradarbiaujant su SAI, kad visos ES šifravimo medžiagos apskaitai, saugiam tvarkymui, laikymui ir platinimui būtų taikomos tinkamos procedūros ir nustatyti tinkami planai, ir

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

9. TEI atsako už RIS atitikties TEMPEST politikai ir naudojimo nurodymams užtikrinimą. Ši institucija patvirtina TEMPEST atsakomąsias priemones, skirtas įrenginiams ir priemonėms, siekiant apsaugoti įslaptintą informaciją iki nustatyto slaptumo žymos laipsnio informacijos operacinėje aplinkoje.

10. ISUI atsako už visus konfidencialios informacijos valdymo ir tvarkymo Parlamente aspektus ir ypač už:

10.1 informacijos saugumo užtikrinimo saugumo politikos formavimą ir saugumo gairių rengimą bei jų veiksmingumo ir tinkamumo stebėseną;

10.2. su šifravimo priemonėmis susijusios techninės informacijos apsaugą ir administravimą;

10.3. užtikrinimą, kad įslaptintos informacijos apsaugai parinktos ISU priemonės atitiktų atitinkamą jų tinkamumo nustatymo ir atrankos politiką;

10.4. užtikrinimą, kad šifravimo priemonės būtų pasirenkamos laikantis jų tinkamumo nustatymo ir atrankos politikos;

10.5. konsultavimąsi su sistemos tiekėju, saugumo srities subjektais ir vartotojų atstovais ISU saugumo politikos klausimais.

II SAUGUMO PRANEŠIMAS

KONFIDENCIALIOS INFORMACIJOS VALDYMAS

A. **ĮŽANGA**

1. Šiuo saugumo pranešimu nustatytos Parlamento vykdomo konfidencialios informacijos valdymo nuostatos.

2. Rengėjas, rengdamas konfidencialią informaciją, įvertina konfidencialumo laipsnį ir priima sprendimą remdamasis šiuo saugumo pranešimu nustatytais principais dėl tokios informacijos žymėjimo slaptumo žymomis arba kitomis žymomis.

B. **ESĮI ĮSLAPTINIMAS**

3. Sprendimas įslaptinti dokumentą priimamas prieš jį rengiant. Tuo tikslu informacija nurodoma kaip ESĮI informacijos rengėjui iš anksto įvertinus jos konfidencialumo laipsnį ir nusprendus, kad neteisėtas tokios informacijos atskleidimas galėtų tam tikru aspektu daryti poveikį Europos Sąjungos, vienos ar kelių valstybių narių arba asmenų interesams.

4. Priėmus sprendimą įslaptinti informaciją atliekamas antras išankstinis vertinimas, siekiant nustatyti tinkamą slaptumo žymos laipsnį. Dokumento įslaptinimo laipsnis nustatomas pagal dokumento turinio slaptumo laipsnį.

5. Atsakomybė už informacijos įslaptinimą tenka tik jos rengėjui. Parlamento pareigūnai informaciją įslaptina gavę generalinio sekretoriaus nurodymą arba remdamiesi jo suteiktais įgaliojimais.

6. Slaptumo žymos taikomos teisingai ir nuosaikiai. Įslaptinamo dokumento rengėjas vengia suteikti pernelyg aukštą ar pernelyg žemą slaptumo žymos laipsnį.

7. Informacijai paskirtas slaptumo žymos laipsnis nurodo apsaugos lygį, taikomą personalo patikimumo, fizinio saugumo, procedūrų saugumo ir informacijos saugumo užtikrinimo srityse.

8. Informacija, kurią reikia įslaptinti, žymima ir tvarkoma kaip įslaptinta informacija nepriklausomai nuo jos fizinės formos. Informacijos gavėjai aiškiai informuojami apie jos įslaptinimą nurodant slaptumo žymą (jei informacija pateikiama rašytine – popieriuje arba RIS – forma) arba pateikiant pranešimą (jei informacija pateikiama žodine forma, pvz., pokalbyje arba uždarame posėdyje). Įslaptinta informacija fiziškai žymima, kad būtų galima paprastai nustatyti jos slaptumo žymą.

9. ESĮI elektronine forma rengiama tik naudojant akredituotą RIS. Pati įslaptinta informacija, rinkmenos pavadinimas ir laikmena (jei išorinė laikmena, pvz., pastoviosios atminties kompaktinis diskas arba USB atmintinė) žymimi atitinkama slaptumo žyma.

10. Informacija įslaptinama, kai tik įgauna formą. Pavyzdžiui, asmeninius užrašus, projektus arba el. pašto pranešimus, kuriuose yra informacijos, kurią reikia įslaptinti, iš pat pradžių reikia pažymėti kaip ESĮI, tokia informacija rengiama ir tvarkoma pagal šį sprendimą ir jo nurodymus dėl fizinių ir techninių aspektų. Tokią informaciją galima naudoti oficialiame dokumente, kuris atitinkamai pažymimas ir tvarkomas. Rengiant oficialų dokumentą gali prireikti iš naujo jį įvertinti ir priskirti jam aukštesnį ar žemesnį už pradinį slaptumo žymos laipsnį.

11. Rengėjas gali nuspręsti skirti standartinį slaptumo žymos laipsnį tų kategorijų informacijai, kurią nuolat rengia. Tačiau rengėjas užtikrina, kad tokiu atveju atskiroms informacijos dalims jis sistemingai neskirs pernelyg aukšto arba pernelyg žemo slaptumo žymos laipsnio.

12. ESĮI visuomet žymima slaptumo žyma, atitinkančia jos slaptumo žymos laipsnį.

B.1. ***Slaptumo žymų laipsniai***

13. ESĮI skiriamas vienas iš šių slaptumo žymų laipsnių:

— „TRÈS SECRET UE/EU TOP SECRET“, kaip apibrėžta šio sprendimo 2 straipsnio d punkte, jei neteisėtas tokios informacijos atskleidimas gali:

a) kelti tiesioginę grėsmę Sąjungos, vienos ar kelių valstybių narių, trečiųjų valstybių arba tarptautinių organizacijų vidaus stabilumui;

b) daryti nepaprastai didelę žalą santykiams su trečiosiomis valstybėmis arba tarptautinėmis organizacijomis;

c) tiesiogiai lemti daugelio asmenų mirt;

d) nepaprastai smarkiai pakenkti valstybių narių arba kitų partnerių dislokuotų darbuotojų veiklos veiksmingumui arba saugumui, arba ypač svarbių saugumo ar žvalgybos operacijų nuolatiniam veiksmingumui; ar

e) daryti didelę ilgalaikę žalą Sąjungos arba valstybių narių ekonomikai;

— „SECRET UE/EU SECRET“, kaip apibrėžta šio sprendimo 2 straipsnio d punkte, jei neteisėtas tokios informacijos atskleidimas gali:

a) sukelti didelę tarptautinę įtampą,

b) padaryti didelę žalą santykiams su trečiosiomis valstybėmis ir tarptautinėmis organizacijomis;

c) sukelti tiesioginę arba didelę žalą viešajam arba asmenų saugumui, arba laisvei;

d) kenkti svarbioms prekybos arba politinėms deryboms, taip sukeliant didelių veiklos sunkumų Sąjungai arba valstybėms narėms;

e) stipriai kenkti valstybių narių veiklos saugumui arba ypač svarbių saugumo arba žvalgybos operacijų veiksmingumui;

f) daryti didelę materialinę žalą Sąjungos arba valstybių narių finansiniams, pinigų politikos, ekonominiams ir prekybos interesams;

g) iš esmės pakenkti pagrindinių organizacijų arba partnerių finansiniam gyvybingumui; ar

h) stipriai trukdyti kurti Sąjungos politiką arba ją vykdyti, taip sukeliant dideles ekonomines, prekybos arba finansines pasekmes;

— „CONFIDENTIEL UE/EU CONFIDENTIAL“, kaip apibrėžta šio sprendimo 2 straipsnio d punkte, jei neteisėtas tokios informacijos atskleidimas gali:

a) daryti didelę žalą diplomatiniams santykiams, jei tokie veiksmai sukeltų oficialų protestą arba kitas sankcijas;

b) kelti grėsmę asmens saugumui arba laisvei;

c) kelti didelę grėsmę prekybos arba politikos deryboms, taip sukeliant didelių veiklos sunkumų Sąjungai arba valstybėms narėms;

d) kenkti valstybių narių veiklos saugumui arba ypač svarbių saugumo arba žvalgybos operacijų veiksmingumui;

e) iš esmės pakenkti pagrindinių organizacijų arba partnerių finansiniam gyvybingumui;

f) trukdyti tirti nusikaltimą arba terorizmo veiklą, arba sudaryti palankesnes sąlygas įvykdyti nusikaltimą arba užsiimti tokia veikla;

g) atlikti esminius veiksmus, nukreiptus prieš Sąjungos ar valstybių narių finansinius, pinigų politikos, ekonominius ar prekybos interesus; ar

h) stipriai trukdyti kurti Sąjungos politiką arba ją vykdyti, taip sukeliant dideles ekonomines, prekybos arba finansines pasekmes;

— „RESTREINT UE/EU RESTRICTED“, kaip apibrėžta šio sprendimo 2 straipsnio d punkte, jei neteisėtas tokios informacijos atskleidimas gali:

a) būti nenaudingas bendriems Sąjungoms interesams,

b) daryti neigiamą įtaką diplomatiniams santykiams;

c) labai pakenkti asmenims arba įmonėms;

d) būti nenaudingas Sąjungai arba valstybėms narėms prekybos arba politikos derybose;

e) apsunkinti pastangas veiksmingai išlaikyti veiksmingą saugumą Sąjungoje arba valstybėse narėse;

f) trukdyti veiksmingai kurti Sąjungos politiką arba ją vykdyti;

g) trukdyti tinkamam Sąjungos ir jos politikos administravimui;

h) pažeisti Parlamento įsipareigojimus išlaikyti trečiųjų šalių suteiktos informacijos įslaptinimo statusą;

i) pažeisti teisės aktais nustatytus informacijos atskleidimo apribojimus;

j) asmenims arba įmonėms padaryti finansinių nuostolių arba sudaryti palankesnes sąlygas jiems neteisėtai pasipelnyti ar įgyti pranašumo; ar

k) pakenkti tyrimui arba sudaryti palankesnes sąlygas nusikaltimui padaryti.

B.2. ***Rinkinių, antraštinių puslapių ir ištraukų įslaptinimas***

14. Pridedamų dokumentų lydraščių arba pranešimų slaptumo žymos laipsnis atitinka priedų aukščiausio laipsnio slaptumo žymų laipsnį. Jei pranešimas arba lydraštis pateikiami atskirai nuo priedų, rengėjas aiškiai nurodo, koks slaptumo žymos laipsnis jiems suteikiamas. Jei nereikia įslaptinti pridedamo pranešimo (lydraščio), jame pateikiamas toks galutinis tekstas: „Šis pridedamas pranešimas (lydraštis) yra neįslaptintas, jei pateikiamas atskirai nuo priedų“.

15. Reikia sukurti tokią dokumentų arba rinkmenų, kurių dalys pažymėtos skirtingais slaptumo žymų laipsniais, struktūrą, kad būtų galima kuo paprasčiau nustatyti dalis, pažymėtas skirtingais slaptumo žymų laipsniais, ir prireikus jas atskirti. Dokumento ar dokumentų bylos bendras slaptumo žymos laipsnis atitinka aukščiausią slaptumo žymos laipsnį turinčią jo dalį.

16 Prireikus atitinkamo dokumento atskiriems lapams, dalims, skyriams, priedams, priedėliams ir pridedamiems dokumentams suteikti skirtingus slaptumo žymų laipsnius, jie yra atitinkamai įslaptinami. Dokumentuose, kuriuose yra ESĮI, galima naudoti standartines santrumpas, kuriomis nurodomas teksto skirsnių arba dalių, užimančių mažiau nei vieną puslapį, slaptumo žymos laipsnis.

17. Renkant informaciją 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 sudėtinėms dalims.

C. **KITA KONFIDENCIALI INFORMACIJA**

18. Kita konfidenciali informacija žymima pagal šio saugumo pranešimo E punktą ir naudojimo nurodymus.

D. **KONFIDENCIALIOS INFORMACIJOS RENGIMAS**

19. Konfidencialią informaciją gali rengti tik tie asmenys, kuriems šiuo sprendimu suteikiama teisė tai daryti arba kuriems tokį leidimą suteikė SI.

20. Konfidenciali informacija netalpinama interneto arba intraneto dokumentų valdymo sistemose.

D.1. ***ESĮI rengimas***

21. Siekiant rengti ESĮI, kuri žymima slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“, atitinkamam asmeniui suteikiama teisė rengti tokią informaciją remiantis šiuo sprendimu arba toks asmuo pirmiausia turi gauti leidimą pagal šio sprendimo 4 straipsnio 1 dalį.

22. Slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ žymima ESĮI rengiama tik saugioje zonoje.

23. ESĮI rengimui taikomos šios taisyklės:

a) kiekviename puslapyje aiškiai nurodomas atitinkamas slaptumo žymos laipsnis;

b) kiekvienas puslapis sunumeruojamas ir nurodomas bendras puslapių skaičius;

c) dokumento pirmame puslapyje nurodomas jo numeris ir dalykas, kurie nėra įslaptinta informacija, išskyrus tuos atvejus, kai jie pažymėti kaip įslaptinta informacija;

d) dokumento pirmame puslapyje nurodoma data;

e) bet kokio dokumento, pažymėto slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“, pirmame puslapyje nurodomas visų priedų ir pridedamų dokumentų sąrašas;

f) jei platinamos kelios dokumentų, pažymėtų slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“, kopijos, kiekvienos iš jų kiekviename puslapyje nurodomas kopijos numeris. Kiekvienos kopijos pirmame puslapyje taip pat nurodomas bendras kopijų ir puslapių skaičius ir

g) jei dokumente pateikiamos nuorodos į iš kitų Sąjungos institucijų gautus kitus dokumentus, kuriuose yra įslaptintos informacijos, arba jei dokumente yra šių dokumentų įslaptintos informacijos, dokumentas žymimas tokio paties laipsnio slaptumo žyma, kokia pažymėti šie dokumentai, ir be išankstinio raštiško jų rengėjo sutikimo negali būti platinami kitiems asmenims, kurių vardai ir pavardės nenurodytos originalaus dokumento arba dokumentų, kuriuose yra įslaptintos informacijos, platinimo sąraše.

24. Rengėjas vykdo ESĮI, kurią parengė, kontrolę. Prašoma suteikti išankstinį raštišką rengėjo sutikimą prieš:

a) sumažinant ESĮI slaptumo žymos laipsnį arba informaciją išslaptinant;

b) naudojant ESĮI kitiems, nei nustatė rengėjas, tikslams;

c) atskleidžiant ESĮI bet kokiai trečiajai valstybei arba tarptautinei organizacijai;

d) atskleidžiant ESĮI bet kokiam asmeniui, institucijai, šaliai arba tarptautinei organizacijai, kurie nenurodyti tarp gavėjų, kuriems rengėjas suteikė leidimą susipažinti su minima informacija;

e) atskleidžiant ESĮI rangovui arba numatomam rangovui, kuris yra trečiojoje valstybėje;

f) kopijuojant arba verčiant ESĮI, jeigu ji pažymėta slaptumo žymos laipsniu „TRES SECRET UE/EU TOP SECRET“;

g) sunaikinant ESĮI.

D.2. ***Kitos konfidencialios informacijos rengimas***

25. Generalinis sekretorius, kaip SI, gali nuspręsti, ar suteikti leidimą rengti kitą konfidencialią informaciją atitinkamai pareigybei, tarnybai ir (arba) asmeniui.

26. Kita konfidenciali informacija žymima viena iš naudojimo nurodymuose nurodytų žymų.

27. Kitos konfidencialios informacijos rengimui taikomos šios taisyklės:

a) jos žymos nurodomos dokumento pirmo puslapio viršuje;

b) kiekvienas puslapis sunumeruojamas ir nurodomas bendras puslapių skaičius;

c) dokumento pirmame puslapyje nurodomas jo numeris ir dalykas;

d) dokumento pirmame puslapyje nurodoma data ir

e) paskutiniame dokumento puslapyje pateikiamas visų priedų ir pridedamųjų dokumentų sąrašas.

28. Kitos konfidencialios informacijos rengimui taikomos naudojimo nurodymuose nustatytos specialios taisyklės ir tvarka.

E. **SLAPTUMO ŽYMOS GALIOJIMO ŽYMOS IR KITOS ŽYMOS**

29. Slaptumo žymų galiojimo žymos ir kitos žymos dokumentuose yra skirtos informacijos srautui kontroliuoti ir teisei susipažinti su konfidencialia informacija apriboti remiantis principu „būtina žinoti“.

30. Naudojant arba nurodant slaptumo žymų galiojimo žymas arba kitas žymas, būtina imtis veiksmų, kad jos nebūtų painiojamos su ESĮI žymėti naudojamomis slaptumo žymomis „RESTREINT UE/EU RESTRICTED“, „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“, „TRES SECRET UE/EU TOP SECRET“.

31. Naudojimo nurodymuose nustatomos specialios taisyklės dėl slaptumo žymų galiojimo žymų ir kitų žymų naudojimo, taip pat nustatomas patvirtintų Europos Parlamento slaptumo žymų sąrašas.

E.1. ***Slaptumo žymos galiojimo žymos***

32. Slaptumo žymos galiojimo žymos gali būti naudojamos tik kartu su slaptumo žyma ir netaikomos atskirai dokumentams. Slaptumo žymos galiojimo žyma gali būti taikoma ESĮI siekiant:

a) nustatyti slaptumo žymos galiojimo terminus (įslaptintos informacijos, kuriai taikomas automatinis slaptumo laipsnio sumažinimas arba išslaptinimas, atveju);

b) riboti ESĮI platinimą;

c) nustatyti konkrečias papildomas tvarkymo priemones, kurios atitinka slaptumo žymos laipsnį.

33. Dokumentų, kuriuose yra ESĮI, tvarkymui ir laikymui taikoma papildoma kontrolė lemia papildomą naštą visiems susijusiems subjektams. Siekiant sumažinti šiuo atveju reikalingą darbą, rengiant tokį dokumentą geroji patirtis yra nustatyti terminą arba įvykį, po kurio automatiškai nustoja galioti slaptumo žyma ir sumažinamas šiame dokumente pateiktos informacijos slaptumo žymos laipsnis arba informacija išslaptinama.

34. Jei dokumento sritis yra konkreti darbo sritis ir reikia apriboti dokumento platinimą ir (arba) taikyti jam konkrečias tvarkymo priemones, prie slaptumo žymos galima pridėti pareiškimą, kad būtų galima nustatyti dokumento tikslinę auditoriją.

E.2. ***Kitos žymos***

35. Kitos žymos nėra slaptumo žymos. Kitos žymos naudojamos tik siekiant suteikti konkrečius nurodymus dėl dokumento tvarkymo ir nenaudojamos tokio dokumento turiniui aprašyti.

36. Kitos žymos gali būti naudojamos atskirai nuo dokumentų arba naudojamos kartu su slaptumo žyma.

37. Kitos žymos paprastai naudojamos informacijai, kuriai taikoma profesinė paslaptis, nurodyta SESV 339 straipsnyje ir Tarnybos nuostatų 17 straipsnyje, žymėti arba kurią Parlamentas turi apsaugoti dėl teisinių priežasčių, tačiau kurios nereikia arba negalima įslaptinti.

E.3. ***Kitų žymų naudojimas RIS***

38. Kitų žymų naudojimo taisyklės taip pat taikomos akredituotoje RIS.

39. SAI nustato konkrečias kitų žymų akredituotoje RIS naudojimo taisykles.

F. **INFORMACIJOS PRIĖMIMAS**

40. Tik ĮIS turi teisę Parlamente iš trečiųjų šalių priimti slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu pažymėtą informaciją.

41. Jei informacija pažymėta slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu, arba jei tai yra kita konfidenciali informacija, tiek ĮIS, tiek kompetentingas Parlamento organas ir (arba) atitinkamas pareigas einantis asmuo gali priimti šią informaciją iš trečiųjų šalių ir yra atsakingas už šiuo saugumo pranešimu nustatytų principų taikymą.

G. **REGISTRAVIMAS**

42. Registravimas – procedūrų, kuriomis naudojantis registruojamas konfidencialios informacijos gyvavimo ciklas, įskaitant jos platinimą, sunaikinimą ir susipažinimą su ja, taikymas.

43. Šiame saugumo pranešime registracijos knyga yra registras, kuriame ypač registruojama data ir laikas, kai konfidenciali informacija:

a) patenka į atitinkamą Parlamento organo ir (arba) atitinkamas pareigas einančio asmens sekretoriatą arba ĮIS, arba išsiunčiama (išgabenama);

b) kai su ja susipažįsta asmuo, kurio patikimumas patikrintas, arba kuriam ji persiunčiama, ir

c) sunaikinama.

44. Įslaptintos informacijos rengėjas atsakingas už pradinio pareiškimo žymėjimą parengus dokumentą, kuriame yra tokios informacijos. Rengiant šį dokumentą ĮIS pranešama apie tą pareiškimą.

45. Slaptumo žyma „CONFIDENTIEL UE/EU CONFIDENTIAL“, aukštesnio laipsnio arba lygiaverte žyma pažymėtą informaciją dėl saugumo gali registruoti tik ĮIS. Iš trečiųjų šalių gautą slaptumo žyma „RESTREINT UE/EU RESTRICTED“ arba lygiaverte žyma pažymėtą informaciją, arba kitą konfidencialią informaciją administraciniais tikslais registruoja už oficialų dokumento priėmimą atsakinga tarnyba, kuri yra ĮIS, Parlamento organo arba atitinkamas pareigas einančio asmens sekretoriatas. Parlamente parengtą kitą konfidencialią informaciją administraciniais tikslais registruoja rengėjas.

46. Slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu žymima informacija visų pirma registruojama, kai:

a) informacija rengiama;

b) informacija patenka į ĮIS ar iš jo išsiunčiama (išgabenama), ir

c) informacija patenka į RIS ar iš jos išsiunčiama.

47. Slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ arba jam lygiaverčiu žymima informacija visų pirma registruojama, kai:

a) informacija rengiama;

b) informacija patenka atitinkamam Parlamento organo ir (arba) atitinkamas pareigas einančio asmens sekretoriatui arba ĮIS, arba iš jų išsiunčiama (išgabenama), ir

c) informacija patenka į RIS ar iš jos išsiunčiama.

48. Konfidenciali informacija gali būti registruojama popierinėse arba elektroninėse registracijos knygose, arba RIS.

49. Jei informacija žymima slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu, arba jei ji yra kita konfidenciali informacija, registruojami bent šie duomenys:

a) data ir laikas, kai informacija patenka atitinkamam Parlamento organo ir (arba) atitinkamas pareigas einančio asmens sekretoriatui arba ĮIS, ar iš jų išsiunčiama (išgabenama);

b) dokumento pavadinimas, įslaptinimo laipsnis arba kita žyma, įslaptinimo (arba kitos žymos) galiojimo pabaigos data ir dokumentui priskirti visi numeriai.

50. Jei informacija žymima slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu, registruojami bent šie duomenys:

a) data ir laikas, kai informacija patenka ĮIS arba yra iš jo išsiunčiama (išgabenama);

b) dokumento pavadinimas, įslaptinimo laipsnis arba kita žyma, dokumentui priskirti visi numeriai ir įslaptinimo (arba kitos žymos) galiojimo pabaigos data;

c) rengėjo rekvizitai;

d) įrašas apie asmens tapatybę, kuriam suteikta teisė susipažinti su dokumentu ir data, kada su tam asmeniui buvo leista susipažinta;

e) įrašas apie padarytas dokumento kopijas arba vertimus;

f) data ir laikas, kada ĮIS išsiunčia (išgabena) arba gauna dokumento kopijas arba vertimus, ir informacija apie tai, kam jie buvo siųsti ir kas juos grąžino;

g) data ir laikas, kai dokumentas sunaikintas, ir duomenys apie tai, kas jį sunaikino, laikantis sunaikinimą reglamentuojančių Parlamento saugumo taisyklių, ir

h) duomenys apie dokumento išslaptinimą arba slaptumo laipsnio sumažinimą.

51. Atitinkamai įslaptinamos arba žymimos registracijos knygos. Registruojamoms informacijai skirtoms registracijos knygoms, pažymėtoms slaptumo žymos laipsniu „TRES SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu, suteikiama tokio paties laipsnio žyma.

52. Įslaptinta informacija gali būti registruojama:

a) vienoje registracijos knygoje arba

b) atskirose registracijos knygose pagal informacijos slaptumo žymos laipsnį, pagal tai, ar informacija gaunama ar išsiunčiama, ir pagal tai, iš kur ji gauta ar kur išsiunčiama.

53. Jei informacija tvarkoma elektroniniu būdu RIS, registravimo procedūros gali būti atliekamos pasitelkiant tas RIS priemones, kurios atitinka minėtiems reikalavimams lygiaverčius reikalavimus. Kai ESĮI išsiunčiama iš RIS, taikoma nurodyta registravimo procedūra.

54. ĮIS registruoja visą įslaptintą informaciją, kurią Parlamentas suteikė trečiosioms šalims, ir iš trečiųjų šalių Parlamento gautą įslaptintą informaciją.

55. Užregistravus slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu žymimą informaciją, ĮIS patikrina, ar gavėjas turi galiojantį saugumo leidimą. Jei toks leidimas yra, ĮIS informuoja gavėją. Susipažinti su įslaptinta informacija galima tik tuomet, kai užregistruojamas dokumentas, kuriame yra tokios informacijos.

H. **PLATINIMAS**

56. Rengėjas sudaro pradinį ESĮS, kurią parengė, platinimo sąrašą.

57. Slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ žymima informacija arba kita konfidenciali informacija, kurią parengė Parlamentas, rengėjo platinama Parlamente, laikantis atitinkamų naudojimo nurodymų ir pagal principą „būtina žinoti“. Jei informacija, žymima slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“, yra parengta Parlamento saugioje zonoje, platinimo sąrašas (ir kiti nurodymai dėl platinimo) pateikiamas ĮIS, kuris yra atsakingas už šio sąrašo tvarkymą.

58. Parlamento parengtą ESĮI platinti trečiosioms šalims gali tik ĮIS pagal principą „būtina žinoti“.

59. Konfidenciali informacija, kurią gavo IĮS, bet koks Parlamento organas arba pareigas einantis asmuo, pateikęs atitinkamą prašymą, platinama laikantis informacijos rengėjo pateiktų nurodymų.

I. **TVARKYMAS, LAIKYMAS IR SUSIPAŽINIMAS**

60. Konfidenciali informacija tvarkoma, laikoma ir su ja susipažįstama laikantis IV saugumo pranešimo nuostatų ir naudojimo nurodymų.

J. **ĮSLAPTINTOS INFORMACIJOS KOPIJAVIMAS, VERTIMAS RAŠTU IR ŽODŽIU**

61. Dokumentai, kuriuose yra slaptumo žymos laipsniu „TRES SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu žymimos informacijos, kopijuojami arba verčiami tik gavus išankstinį raštišką informacijos rengėjo sutikimą. Dokumentai, kuriuose yra slaptumo žymos laipsniu „SECRET UE/EU SECRET“ arba jam lygiaverčiu, arba slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ arba jam lygiaverčiu žymimos informacijos, gali būti kopijuojami arba verčiami gavus turėtojo nurodymą, jeigu rengėjas neuždraudė to daryti.

62. Kiekviena dokumento, kuriame yra slaptumo žymos laipsniu „TRES SECRET UE/EU TOP SECRET“, „SECRET UE/EU SECRET EU“ arba „CONFIDENTIEL UE/EU CONFIDENTIAL“, arba jam lygiaverčiu žymimos informacijos, kopija dėl saugumo registruojama.

63. Dokumento kopijoms ir vertimams taikomos tos pačios saugumo priemonės, kaip ir dokumento, kuriame yra įslaptintos informacijos, originalui.

64. Iš Tarybos gaunami dokumentai turėtų būti parengti visomis oficialiomis kalbomis.

65. Rengėjas arba kopijos turėtojas gali paprašyti pateikti dokumento, kuriame yra įslaptintos informacijos, kopijas ir (arba) vertimus. Dokumentus, kuriuose yra slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu žymimos informacijos, galima kopijuoti tik saugioje zonoje naudojantis kopijavimo aparatais, kurie priklauso akredituotai RIS. Dokumentai, kuriuose yra slaptumo žyma „RESTREINT UE/EU RESTRICTED“ arba lygiaverte žyma žymimos informacijos, arba kitos konfidencialios informacijos, kopijuojami naudojantis akredituotais atgaminimo įrenginiais Parlamento patalpose.

66. Visos bet kokių dokumentų arba dokumentų dalių, kuriose yra įslaptintos informacijos, kopijos ir visi vertimai atitinkamai žymimi, sunumeruojami ir registruojami.

67. Nedaroma daugiau kopijų, nei būtinai reikia. Susipažinimo su informacija laikotarpio pabaigoje visos kopijos sunaikinamos laikantis naudojimo nurodymų.

68. Tik vertėjai žodžiu ir raštu, kurie yra Parlamento pareigūnai, gauna prieigą prie įslaptintos informacijos.

69. Prieigą prie dokumentų, kuriuose yra slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu žymimos informacijos, turintys vertėjai žodžiu ir raštu yra atitinkamai tikrinami dėl patikimumo.

70. Vertėjai žodžiu ir raštu, dirbdami su dokumentais, kuriuose yra slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu žymimos informacijos, dirba saugioje zonoje.

K. **KONFIDENCIALIOS INFORMACIJOS SLAPTUMO ŽYMOS ARBA KITOS ŽYMOS LAIPSNIO SUMAŽINIMAS IR KONFIDENCIALIOS INFORMACIJOS IŠSLAPTINIMAS**

K.1. ***Bendrieji principai***

71. Konfidenciali informacija išslaptinama, sumažinamas jos slaptumo žymos ar kitos žymos laipsnis, jei nebereikia ilgiau apsaugoti šios informacijos arba jei nebereikia šios informacijos saugoti pirminiu lygiu.

72. Sprendimus dėl informacijos, esančios Parlamente parengtuose dokumentuose, slaptumo žymos ar kitos žymos laipsnio sumažinimo, informacijos išslaptinimo gali prireikti priimti ir pagal principą ad hoc, pvz., nagrinėjant viešosios arba Sąjungos kitos institucijos prašymą leisti susipažinti su informacija, arba pareiškus iniciatyvą ĮIS, Parlamento organui ir (arba) atitinkamas pareigas einančiam asmeniui.

73. ESĮI rengėjas, rengdamas informacija, jei įmanoma, nurodo, ar tam tikrą dieną arba po tam tikro įvykio galima sumažinti atitinkamos ESĮI slaptumo žymos laipsnį arba išslaptinti šią informaciją. Jei to nurodyti neįmanoma, informaciją turintis rengėjas, ĮIS, Parlamento organas ir (arba) atitinkamas pareigas einantis asmuo peržiūri ESĮI slaptumo žymos laipsnį bent kas penkerius metus. Bet kokiu atveju galima sumažinti ESĮI slaptumo žymos laipsnį arba išslaptinti šią informaciją tik gavus išankstinį rašytinį informacijos rengėjo sutikimą.

74. Jei negalima nustatyti arba atsekti dokumentų, kurie parengti Parlamente, rengėjo SI peržiūri ESĮI slaptumo žymos laipsnį remdamasi informaciją turinčio Parlamento organo ir (arba) atitinkamas pareigas einančio asmens pasiūlymu, kuris šiuo klausimu gali pasikonsultuoti su ĮIS.

75. Informaciją turintis ĮIS, Parlamento organas ir (arba) atitinkamas pareigas einantis asmuo atsakingas už gavėjo (-ų) informavimą apie informacijos slaptumo žymos laipsnio sumažinimą arba informacijos išslaptinimą, o šis (-ie) gavėjas (-ai) atsako už kito (-ų) gavėjo (-ų), kuriam (-iems) nusiuntė arba kopijavo dokumentą, informavimą.

76. Registruojamas dokumente esančios informacijos išslaptinimas, slaptumo žymos arba kitos žymos laipsnio sumažinimas.

K.2. ***Išslaptinimas***

77. ESĮI galima išslaptinti visą arba tik jos dalį. Gali būti išslaptinama ESĮI dalis, jei manoma, kad nebereikia ilgiau apsaugoti tam tikros dokumento dalies, kurioje yra šios informacijos, tačiau manoma, kad pagrįsta toliau apsaugoti likusią dokumento dalį.

78. Jei peržiūrint ESĮI, kuri yra Parlamente parengtame dokumente, nusprendžiama išslaptinti šią informaciją, atsižvelgiama į tai, ar dokumentą galima skelbti viešai, ar reikia jį pažymėti platinimo žyma (t. y., dokumentas neviešinamas).

79. Išslaptinus ESĮI, tai turi būti užfiksuojama registracijos knygoje nurodant šiuos duomenis: išslaptinimo datą, prašymą išslaptinti pateikusio asmens ir leidimą davusio asmens vardus ir pavardes, išslaptinto dokumento numerį ir jo galutinį gavėją.

80. Senos slaptumo žymos išslaptintame dokumente ir visose jo kopijose turi būti perbraukiamos. Dokumentai ir visos jų kopijos atitinkamai laikomi.

81. Išslaptinus dalį įslaptintos informacijos, parengiamas ir atitinkamai laikomas išslaptintos dalies išrašas. Kompetentinga tarnyba registruoja:

a) dalinio išslaptinimo datą;

b) asmenų, kurie pateikė prašymą išslaptinti informaciją, ir kurie suteikė leidimą, vardus ir pavardes, ir

c) išslaptinto išrašo numerį.

K.3. ***Slaptumo žymos laipsnio sumažinimas***

82. Sumažinus įslaptintos informacijos slaptumo žymos laipsnį, dokumentas, kuriami ji yra, registruojamas registracijos knygose pagal seną ir naują slaptumo žymos laipsnį. Registruojama slaptumo žymos laipsnio sumažinimo data ir slaptumo žymos laipsnį sumažinti leidusio asmens vardas ir pavardė.

83. Dokumentui, kuriame yra informacijos, kurios slaptumo žymos laipsnis sumažintas, ir visoms jo kopijoms suteikiama kitas slaptumo žymos laipsnis, šis dokumentas ir visos jo kopijos atitinkamai laikom.

L. **KONFIDENCIALIOS INFORMACIJOS SUNAIKINIMAS**

84. Konfidenciali informacija (spausdintine arba elektronine forma), kurios nebereikia, sunaikinama arba ištrinama laikantis naudojimo nurodymų ir atitinkamų archyvavimo taisyklių.

85. Slaptumo žymos laipsniu „TRES SECRET UE/EU TOP SECRET“, lygiaverte žyma, slaptumo žyma „SECRET UE/EU SECRET“ arba lygiaverte žyma žymimą informaciją sunaikina ĮIS, dalyvaujant asmeniui, kurio patikimumas patikrintas, atitinkamai pagal žemiausią sunaikinamos informacijos slaptumo žymos laipsnį.

86. Slaptumo žymos laipsniu „TRES SECRET UE/EU TOP SECRET“ arba lygiaverte žyma pažymėti dokumentai sunaikinami tik gavus išankstinį rašytinį dokumento rengėjo sutikimą.

87. Slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu žymimą informaciją sunaikina ir šalina ĮIS, gavęs informacijos rengėjo arba kompetentingos institucijos nurodymą. Registracijos knygos ir kiti registrai atitinkamai atnaujinami. Slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu pažymėtą informaciją sunaikina ir šalina ĮIS, atitinkamas Parlamento organas arba pareigas einantis asmuo.

88. Už sunaikinimą atsakingas pareigūnas ir asmuo, esantis sunaikinimo liudininku, pasirašo sunaikinimo aktą, kuris registruojamas ir saugomas archyve ĮIS. ĮIS saugo slaptumo žymos laipsniu „TRES SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu pažymėtos informacijos sunaikinimo aktus kartu su platinimo formomis bent dešimt metų, o jei informacija pažymėta slaptumo žyma „SECRET UE/EU SECRET“, lygiaverte žyma, slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ arba jam lygiaverčiu – bent penkerius metus.

89. Dokumentas, kuriame yra įslaptintos informacijos, sunaikinamas naudojant atitinkamus Sąjungos standartus arba jiems lygiaverčius standartus atitinkančius metodus, kad nebūtų galima atkurti visos šios informacijos arba jos dalies.

90. Įslaptintai informacijai saugoti naudotos kompiuterinių duomenų saugojimo laikmenos sunaikinamos laikantis atitinkamų naudojimo nurodymų.

91. Informacija apie įslaptintos informacijos sunaikinimą registruojama atitinkamoje registracijos knygoje nurodant šiuos duomenis:

a) sunaikinimo datą ir laiką;

b) už sunaikinimą atsakingo pareigūno vardą ir pavardę;

c) sunaikinto dokumento arba kopijų identifikacinį numerį;

d) pirminę sunaikintos ESĮI fizinę formą;

e) sunaikinimo priemonę ir

f) sunaikinimo vietą.

M. **ARCHYVAVIMAS**

92. Įslaptinta informacija, įskaitant pridedamą pranešimą (lydraštį), priedus, pateikimo kvitą ir (ar) kitas rinkinio dalis, perduodama saugioje zonoje esančiam saugiam archyvui per šešis mėnesius nuo paskutinės susipažinimo su informacija datos, o vėliausiai – per vienerius metus nuo informacijos pateikimo. Išsamios įslaptintos informacijos archyvavimo taisyklės nustatomos naudojimo nurodymuose.

93. Kitos konfidencialios informacijos atveju bendrosios dokumento naudojimo taisyklės taikomos nedarant poveikio kitoms taisyklėms dėl dokumento tvarkymo.

III SAUGUMO PRANEŠIMAS

KONFIDENCIALIOS INFORMACIJOS TVARKYMAS NAUDOJANT AUTOMATINES RYŠIŲ INFORMACINES SISTEMAS (RIS)

A. **INFORMACINĖSE SISTEMOSE TVARKOMOS ĮSPAPTINTOS INFORMACIJOS SAUGUMO UŽTIKRINIMAS**

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

2. Ryšių informacinė sistema (RIS), skirta įslaptintos informacijos tvarkymui, – sistema, sudaranti sąlygas tvarkyti informaciją elektroniniu būdu. Tokia informacinė sistema apima visas sistemos dalis, kurių reikia jos veikimui, įskaitant infrastruktūrą, organizavimą, personalą ir informacijos šaltinius.

3. Įslaptinta informacija pagal RIS tvarkoma laikantis ISU principo.

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

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

a) Autentiškumas: užtikrinimas, kad informacija yra tikra ir kad ji gauta iš bona fide šaltinių;

b) Prieinamumas: galimybė leidimą turinčiam subjektui pateikus prašymą gauti informaciją ir ja naudotis;

c) Konfidencialumas: savybė, kuri reiškia, kad informacija nėra atskleidžiama neturintiems leidimo asmenims, subjektams ar procesams;

d) Vientisumas: savybė, kuri reiškia, kad apsaugomas informacijos tikslumas ir išsamumas bei turtas;

e) Atsakomybės už veiksmus prisiėmimas: galimybė įrodyti, kad veiksmas buvo atliktas ar įvykis įvyko, kad šio įvykio ar veiksmo po to negalima būtų išsižadėti.

B. **INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI**

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

B.1. ***Saugumo rizikos valdymas***

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

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

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

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

B.2. ***Saugumas viso RIS gyvavimo ciklo metu***

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

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

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

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

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

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

B.3. ***Geriausia patirtis***

17. ISUI parengia geriausios praktikos pavyzdžius, susijusius su RIS tvarkomos įslaptintos informacijos apsauga. Geriausios praktikos gairėse išdėstomos RIS skirtos techninės, fizinės, organizacinės ir procedūrinės saugumo priemonės, kurių veiksmingumas apsisaugant nuo konkrečių grėsmių ir pažeidžiamumo buvo įrodytas.

18. RIS tvarkomos įslaptintos informacijos apsauga užtikrinama, remiantis ISU dalyvaujančių subjektų įgyta patirtimi.

19. Geriausios praktikos pavyzdžių platinimu ir jų įgyvendinimu prisidedama prie siekio užtikrinti lygiavertį Parlamento sekretoriato naudojamų RIS, kuriose tvarkoma įslaptinta informacija, saugumo užtikrinimo lygį.

B.4. ***Nuodugni apsauga***

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

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

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

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

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

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

Tokių saugumo priemonių griežtumo lygis nustatomas atsižvelgiant į rizikos įvertinimą.

21. Kompetentingos institucijos, kaip tiksliai nurodyta I saugumo pranešime, užtikrina savo gebėjimus reaguoti į incidentus, kurie gali apimti kelias organizacijas, kad galėtų derinti reagavimo veiksmus ir dalytis informacija apie tuos incidentus bei susijusią riziką (kompiuterinių incidentų tyrimo gebėjimai).

B.5. ***Minimalumo ir mažiausių privilegijų principas***

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

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

B.6. ***Informuotumas informacijos saugumo užtikrinimo srityje***

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

a) kad naudojant įslaptintą informaciją saugumo spragos gali labai pakenkti RIS;

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

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

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

B.7. ***IT saugumo priemonių vertinimas ir patvirtinimas***

26. RIS, kurioje tvarkoma slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ ar jam lygiaverčiu,pažymėta informacija, apsaugoma tokiu būdu, kad informacija negalėtų būti neteisėtai atskleista dėl netyčinio elektromagnetinio spinduliavimo (TEMPEST apsaugos priemonės).

27. Kai įslaptinta informacija apsaugoma šifravimo priemonėmis, tas priemones patvirtina SAI kaip ES patvirtintas priemones.

28. Perduodant įslaptintą informaciją elektroninėmis priemonėmis naudojamos ES patvirtintos šifravimo priemonės. Nepaisant šio reikalavimo, esant nepaprastosios padėties sąlygoms arba specifinių techninių konfigūracijų atvejais, kaip nurodyta 41 ir 44 punktuose, gali būti taikomos specialios procedūros.

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

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

31. SAI patvirtina ne šifravimo IT saugumo priemonių reikalavimų atitikimo ir patvirtinimo saugumo gaires.

B.8. ***Perdavimas saugioje zonoje***

32. Kai įslaptintos informacijos perdavimas vykdomas saugioje zonoje, remiantis rizikos valdymo proceso rezultatais ir SAI pritarus, informacija gali būti platinama nešifruota arba šifruota žemesniu lygiu.

B.9. ***Saugus RIS tarpusavio sujungimas***

33. Sistemų tarpusavio sujungimas reiškia tiesioginį dviejų ar daugiau IT sistemų sujungimą siekiant dalytis duomenimis ir kitais informacijos šaltiniais vienakrypčiu arba daugiakrypčiu būdu.

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

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

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

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

c) apsaugos priemonės (AP) įdiegiamos RIS perimetre.

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

37. Kai duomenys, perduodami neapsaugotu arba viešu tinklu, yra užšifruojami pagal 27 straipsnį patvirtinta ES šifravimo priemone, toks sujungimas nelaikomas tarpusavio sujungimu.

38. Draudžiamas tiesioginis arba pakopinis RIS, akredituotos tvarkyti slaptumo žymos laipsniu „TRES SECFRET UE/EU TOP SECRET“ ar jam lygiaverčiu pažymėtą informaciją, ar slaptumo žymos laipsniu „SECRET UE/EU SECRET“ arba jam lygiaverčiu pažymėtą informaciją, ir neapsaugoto arba viešo tinklo tarpusavio sujungimas.

B.10. ***Kompiuterinių duomenų saugojimo laikmenos***

39. Šifravimo priemonės sunaikinamos laikantis kompetentingos saugumo institucijos patvirtintų procedūrų.

40. Kompiuterinių duomenų saugojimo laikmenos pakartotinai naudojamos, jų slaptumo žymos laipsnis gali būti sumažintas arba laikmenos išslaptintos laikantis naudojimo nurodymų.

B.11. ***Nepaprastosios padėties sąlygos***

41. Toliau aprašytos specialios procedūros gali būti taikomos esant nepaprastajai padėčiai, pavyzdžiui, gresiant ar esant krizei, konfliktui ar karinei padėčiai, arba susidarius išskirtinėms su eksploatavimu susijusioms sąlygoms.

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

a) siuntėjas ir gavėjas neturi reikiamos šifravimo įrangos arba jokios šifravimo įrangos, taip pat

b) įslaptinta medžiaga negali būti laiku perduota kitomis priemonėmis.

43. 41 dalyje išdėstytomis aplinkybėmis perduodama įslaptinta informacija nėra pažymėta jokiomis žymomis arba nuorodomis, kurios sudarytų sąlygas ją atskirti nuo neįslaptintos informacijos arba kurią galima apsaugoti naudojant turimas šifravimo priemones. Gavėjams kitomis priemonėmis nedelsiant pranešama apie informacijos slaptumo laipsnį.

44. Jeigu taikomos 41 ir 42 dalys, kompetentingai institucijai vėliau pateikiama ataskaita.

IV SAUGUMO PRANEŠIMAS

FIZINIS SAUGUMAS

A. **ĮVADAS**

Šiame saugumo pranešime nustatomi saugumo principai, kuriais siekiama sukurti saugią aplinką konfidencialios informacijos Europos Parlamente tvarkymui užtikrinti. Šiuos principus, įskaitant susijusius su techniniu saugumu, papildys naudojimo nurodymai.

B. **SAUGUMO RIZIKOS VALDYMAS**

1. Įslaptintai informacijai kylančios rizikos valdymas yra procesas. To proceso tikslas – nustatyti žinomą saugumo riziką, apibrėžti saugumo priemones tokiai rizikai sumažinti iki priimtino lygio pagal saugumo pranešime išdėstytus pagrindinius principus ir būtiniausius standartus ir taikyti tas priemones laikantis nuodugnios apsaugos sąvokos, kaip apibrėžta III saugumo pranešime. Reguliariai atliekamas tokių priemonių efektyvumo vertinimas.

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

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

4. Veiklos tęstinumo planuose numatomos prevencinės ir atstatymo priemonės siekiant sumažinti didelių klaidų ar incidentų poveikį įslaptintos informacijos naudojimui ir saugojimui.

C. **BENDRIEJI PRINCIPAI**

5. Informacijai suteiktas slaptumo žymos laipsnis ar kitos žymos nulemia tai, kokio lygio apsauga informacijai bus taikoma fizinio saugumo srityse.

6. Informacija, kurią reikia įslaptinti, žymima ir tvarkoma kaip įslaptinta informacija nepriklausomai nuo jos fizinės formos. Apie jos įslaptinimą aiškiai nurodoma jos gavėjams nurodant slaptumo žymą (jeigu ji pateikiama rašytine forma – popieriuje ar RIS) arba apie tai pranešant (jeigu ji pateikiama žodine forma, pavyzdžiui, pokalbio metu arba darant pranešimą). Įslaptinta informacija fiziškai žymima, kad būtų galima paprastai nustatyti jos slaptumo žymą.

7. Konfidenciali informacija jokiomis aplinkybėmis neturi būti skaitoma viešose vietose, kur ją gali pamatyti asmenys, kurie neturėtų su ja susipažinti, pvz., traukiniuose, lėktuvuose, kavinėse, baruose ir k. t. Jos negalima palikti viešbučių seifuose ir kambariuose ar be priežiūros palikti viešose vietose.

D. **ATSAKOMYBĖ**

8. ĮIS atsako už fizinio saugumo užtikrinimą valdant konfidencialią informaciją, laikomą ĮIS saugiose patalpose. ĮIS taip pat atsako už saugių patalpų administravimą.

9. Už slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ ar jam lygiaverčiu pažymėtos informacijos arba kitos konfidencialios informacijos fizinį saugumą ją tvarkant atsako atitinkamas Parlamento organas ir (arba) atitinkamas pareigas einantis asmuo.

10. Saugos ir rizikos vertinimo direktoratas užtikrina reikiamą asmens saugumą ir asmens patikimumo patikrinimą, kad būtų užtikrintas saugus konfidencialios informacijos naudojimas Europos Parlamente.

11. ITD konsultuoja ir užtikrina, kad visos sukurtos ir naudojamos RIS visiškai atitiktų III saugumo pranešimą ir atitinkamus naudojimo nurodymus.

E. **SAUGIOS PATALPOS**

12. Saugios patalpos gali būti įrengtos laikantis techninių saugumo standartų ir atsižvelgiant į konfidencialiai informacijai suteiktą slaptumo laipsnį, kaip nurodyta 7 straipsnyje.

13. Saugias patalpas turi sertifikuoti SAI ir patvirtinti SI.

F. **SUSIPAŽINIMAS SU KONFIDENCIA INFORMACIJA**

14. Kai slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ ar jam lygiaverčiu žymima informacija arba kita konfidenciali informacija pateikiama ĮIS ir su ja turi būti susipažįstama už saugios zonos ribų, ĮIS perduoda kopiją atitinkamai tarnybai, gavusiai leidimą užtikrinti, kad susipažinimas su šia informacija ir naudojimasis ja atitiktų šio sprendimo 8 straipsnio 2 dalį ir 10 straipsnį bei atitinkamus naudojimo nurodymus.

15. Kai slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ ar jam lygiaverčiu žymima informacija arba kita konfidenciali informacija pateikiama Parlamento organui ir (arba) pareigas einančiam asmeniui, o ne ĮIS, to Parlamento organo sekretoriatas ir (arba) tas pareigas einantis asmuo užtikrina, kad susipažinimas su susijusia informacija ir naudojimasis ja atitiktų 7 straipsnio 3 dalį, 8 straipsnio 1, 2 ir 4 dalis, 9 straipsnio 3, 4 ir 5 dalis, 10 straipsnio 2 ir 6 dalis ir 11 straipsnį bei atitinkamus naudojimo nurodymus.

16. Kai su slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ ar jam lygiaverčiu žymima informacija reikia susipažinti saugioje zonoje, ĮIS užtikrina, kad susipažinimas su šia informacija ir naudojimasis ja atitiktų šio sprendimo 9 ir 10 straipsnius bei atitinkamus naudojimo nurodymus.

G. **TECHNINIS SAUGUMAS**

17. Už techninio saugumo priemones atsako SAI, ji nustato konkrečias techninio saugumo priemones, kurias reikia taikyti atitinkamuose naudojimo nurodymuose.

18. Saugios skaityklos, skirtos susipažinti su slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ ar jam lygiaverčiu pažymėta informacija arba kita konfidenciali informacija atitinka specifinius techninio saugumo reikalavimus, kaip nurodyta naudojimo nurodymuose.

19. Saugi zona apima šias patalpas:

a) saugios prieigos patikrinimo patalpą, kuri turi būti įrengta pagal techninio saugumo reikalavimus, kaip nustatyta naudojimo nurodymuose. Patekimas į šią patalpą turi būti registruojamas. Ši patalpa turi atitikti aukštus turinčių teisę į ją patekti asmenų tapatybės nustatymo ir vaizdo stebėjimo kameromis standartus, joje turi būti įrengta saugi zona, skirta pasidėti asmeninius daiktus, kurių neleidžiama įsinešti į saugias patalpas (telefonai, rašikliai ir t. t.);

b) ryšių patalpą, skirtą įslaptintai informacijai perduoti ar gauti, įskaitant koduotą įslaptintą informaciją, laikantis III saugumo pranešimo ir atitinkamų naudojimo nurodymų;

c) saugų archyvą, kuriame slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“, „CONFIDENTIEL UE/EU CONFIDENTIAL“ ir „SECRET UE/EU SECRET“ arba ar jam lygiaverčiu pažymėtai informacijai atskirai naudojamos patvirtintos ir sertifikuotos talpyklos. Informacija, pažymėta slaptumo žymos laipsniu „TRES SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu laikoma skirtingose patalpose specialiose sertifikuotose talpyklose. Vienintelė papildoma įranga, kurią leidžiama laikyti šioje patalpoje, yra pagalbinis stalelis, skirtas ĮIS tvarkyti archyvą;

d) registravimo patalpą, kurioje turi būti reikalingos priemonės, kad būtų galima vykdyti registraciją popieriuje ar elektroniškai, ir todėl joje turi būti reikalingos saugios priemonės, skirtos atitinkamai RIS įdiegti. Tik registravimo patalpoje gali būti patvirtinti ir akredituoti dauginimo įrenginiai (popierinės ar elektroninės kopijos). Naudojimo nurodymuose nurodoma, kurie dauginimo įtaisai yra patvirtinti ir akredituoti. Registravimo patalpoje taip pat turi būti galimybė saugoti ir naudoti akredituotus įrenginius, reikalingus fiziniam įslaptintos informacijos žymėjimui, kopijavimui ir skirstymui pagal slaptumo žymos laipsnį. Visus akredituotus įrenginius apibrėžia ĮIS ir akredituoja SAI, vadovaudamasi Informacijos saugumo užtikrinimo operacinės institucijos patarimu. Registravimo patalpoje taip pat turi būti akredituotas dokumentų naikinimo prietaisas, patvirtintas aukščiausio laipsnio slaptumo žymai, kaip aprašyta naudojimo nurodymuose. Slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ ar jam lygiaverčiu pažymėta informacija verčiama registravimo patalpoje, naudojantis patvirtinta ir akredituota sistema. Registravimo patalpoje turi būti dvi darbo vietos, kad du vertėjai vienu metu galėtų versti tą patį dokumentą. Verčiant turi dalyvauti ĮIS darbuotojas;

e) skaityklą, kurioje tinkamai leidimą gavę asmenys gali individualiai susipažinti su įslaptinta informacija. Skaitykloje turi būti pakankamai vietos dviem asmenims, įskaitant ĮIS darbuotoją, kuris visąlaik turi būti kiekvieno susipažinimo su informacija metu. Šiai patalpai numatytas saugumo laipsnis yra „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ ar jam lygiavertis. Skaitykloje gali būti įdiegta TEMPEST įranga, skirta, kai reikia, susipažinti su informacija elektroniniu būdu, atsižvelgiant į slaptumo žymos laipsnį;

f) posėdžių salė, kurioje turi tilpti iki 25 asmenų ir kurioje aptariama informacija, pažymėta slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ arba jam lygiaverčiu. Posėdžių salėje turi būti techniškai saugi ir sertifikuota įranga, būtina vertimui žodžiu mažiausiai į dvi kalbas užtikrinti. Kai nenaudojama posėdžiams, ši posėdžių salė gali būti naudojama kaip papildoma skaitykla individualiai su informacija susipažįstantiems asmenims. Išimtiniais atvejais ĮIS gali leisti daugiau nei vienam leidimą turinčiam asmeniui susipažinti su įslaptinta informacija, jeigu visų salėje esančių asmenų patikimumo patikrinimo lygmuo yra vienodas ir visi asmenys atitinka principą „būtina žinoti“. Su įslaptinta informacija vienu metu gali susipažinti ne daugiau kaip keturi asmenys. Numatomas didesnis ĮIS darbuotojų skaičius;

g) saugias technines patalpas, kuriose yra visa techninė įranga, susijusi su visos saugios zonos saugumu, ir apsaugoti IT serveriai;

20. Saugi zonos turi atitikti tarptautinius saugumo standartus ir turi būti sertifikuota Saugos ir rizikos vertinimo direktorato. Saugi zona turi atitikti šiuos minimalius saugumo techninius reikalavimus:

a) įrengtos signalizacijos ir saugumo stebėsenos sistemos;

b) saugos įrangos ir avarinės sistemos (dvipusio įspėjimo sistema);

c) apsauginė vaizdo stebėjimo sistema (AVSS);

d) įsibrovimo aptikimo sistema;

e) patekimo kontrolė (įskaitant biometrinio saugumo sistemą);

f) talpyklos;

g) užrakinamos spintelės;

h) apsauga nuo elektromagnetinio lauko.

21. Glaudžiai bendradarbiaudama su ĮIS ir laikydamasi SI nurodymų, SAI gali pridėti papildomų reikalingų techninio saugumo priemonių.

22. Infrastruktūros įranga gali būti prijungta prie pastato, kuriame yra saugi zona, bendrųjų valdymo sistemų. Tačiau saugos įranga, skirta prieigos kontrolei ir RIS, turi būti nepriklausoma nuo visų kitų Europos Parlamente esamų sistemų.

H. **SAUGIOS ZONOS TIKRINIMAI**

23. SAI saugios zonos tikrinimus vykdo reguliariai ir paprašius ĮIS.

24. SAI sudaro ir atnaujina saugumo patikrinimo sąrašus, kuriuose nurodo, ką tikrinimų metų reikia patikrinti laikantis naudojimo nurodymų.

I. **KONFIDENCIALIOS INFORMACIJOS TRANSPORTAVIMAS**

25. Konfidenciali informacija gabenama taip, kad nebūtų matoma, ir nepateikiant jokios nuorodos į tai, kad jos turinys konfidencialaus pobūdžio, laikantis naudojimo nurodymų.

26. Tik pasiuntiniai ir darbuotojai, turintys leidimą dirbti su atitinkamo slaptumo žymos laipsnio informacija, gali gabenti informaciją su slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu.

27. Konfidenciali informacija gali būti siunčiama išorės paštu ar nešama per pasiuntinį už pastato ribų tik laikantis sąlygų, nustatytų naudojimo nurodymuose.

28. Informacija su slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu niekada nesiunčiama elektroniniu paštu ar faksu, net jei yra įrengta saugaus elektroninio pašto sistema ar koduojantis faksas. Slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu pažymėta informacija arba kita konfidenciali informacija gali būti siunčiama elektroniniu paštu, naudojant akredituotą kodavimo sistemą.

J. **KONFIDENCIALIOS INFORMACIJOS LAIKYMAS**

29. Konfidencialiai informacijai suteiktas slaptumo ar kitos žymos nulemia tai, kokio lygio apsauga jai bus taikoma numatant jos laikymą. Ji laikoma naudojant tam tikslui sertifikuotą įrangą pagal naudojimo nurodymus.

30. Slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu žymima informacija ir kita konfidenciali informacija:

a) laikoma standartinėje metalinėje užrakintoje spintoje kabinete ar darbo zonoje, kai ja nesinaudojama;

b) nepaliekama be priežiūros, nebent yra saugiai padėta ir užrakinta;

c) nepaliekama ant stalo ar darbo stalo ir pan. taip, kad bet koks neįgaliotas asmuo, pvz., lankytojai, valytojai, priežiūros darbuotojai ir t. t., galėtų ją perskaityti ar išsinešti;

d) nerodoma neįgaliotiems asmenims arba su jais neaptariama.

31. Informacija, pažymėta slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ arba jam lygiaverčiu ir kita konfidenciali informacija laikoma tik Parlamento organo ir (arba) atitinkamas pareigas einančių asmenų sekretoriatuose arba ĮIS, laikantis naudojimosi nurodymų.

32. Slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“, „SECRET UE/EU SECRET“ ar „TRÈS SECRET UE/EU TOP SECRET“ arba jam lygiaverčiu žymima informacija:

a) laikoma saugioje zonoje, apsauginėje talpykloje arba saugykloje. Išimtiniais atvejais, pavyzdžiui, jei ĮIS uždarytas, ji gali būti laikoma saugumo tarnybų patvirtintame ir sertifikuotame seife;

b) niekada negali būti palikta be priežiūros saugioje zonoje prieš tai jos neužrakinus patvirtintame seife (net ir trumpiausiam laikui);

c) nepaliekama ant stalo ar darbo stalo ir pan. taip, kad bet koks neįgaliotas asmuo galėtų ją perskaityti ar išsinešti, net jei atsakingas ĮIS darbuotojas yra patalpoje.

Kai dokumentas, kuriame yra įslaptintos informacijos, kuriamas elektronine forma saugioje zonoje, kompiuteris užrakinamas, o ekranas turi būti neprieinamas, jei autorius arba atsakingas ĮIS darbuotojas išeina iš patalpos (net ir trumpiausiam laikui). Automatinis apsauginis užraktas suveikiantis po kelių minučių negali būti laikomas pakankama priemone.

V SAUGUMO PRANEŠIMAS

PRAMONINIS SAUGUMAS

A. **ĮVADAS**

1. Šis saugumo pranešimas taikomas tik įslaptintai informacijai.

2. Jame išdėstomos šio sprendimo I priedo 1 dalyje nurodytų bendrųjų būtiniausių standartų įgyvendinimo nuostatos.

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

4. Europos Parlamentas, kaip perkančioji institucija, užtikrina, kad skiriant įslaptintas sutartis su pramonės ar kitais subjektais būtų laikomasi šiame sprendime išdėstytų ir sutartyje nurodytų būtiniausių pramoninio saugumo standartų.

B. **SAUGUMO ASPEKTAI ĮSLAPTINTOSE SUTARTYSE**

B.1. ***Slaptumo žymų vadovas (SŽV)***

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

6. Siekiant nustatyti skirtingų įslaptintos sutarties dalių slaptumo žymos laipsnį, taikomi toliau nurodyti principai:

a) rengdamas SŽV, Europos Parlamentas atsižvelgia į visus svarbius saugumo aspektus, įskaitant slaptumo žymą, priskirtą informacijai, kurią jos rengėjas pateikė ir patvirtino kaip naudotiną tai sutarčiai;

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

B.2. ***Saugumo aspektų paaiškinimas (SAP)***

7. Konkrečioms sutartims skirti saugumo reikalavimai aprašomi saugumo aspektų paaiškinime (SAP). Prireikus į SAP įtraukiamas SŽV; SAP yra neatsiejama įslaptintos sutarties ar subrangos sutarties dalis.

8. Į SAP įtraukiamos nuostatos, pagal kurias reikalaujama, kad rangovas ir (arba) subrangovas laikytųsi būtiniausių šiame sprendime nustatytų standartų. Tų būtiniausių standartų nesilaikymas gali būti pakankamas pagrindas sutarčiai nutraukti.

B.3. ***Programos (projekto) saugumo instrukcijos (PSI)***

9. Atsižvelgiant į programų ar projektų, kuriuos vykdant reikia susipažinti su ESĮI arba ją tvarkyti ar saugoti, apimtį, programą ar projektą valdyti paskirta perkančioji institucija gali parengti konkrečios programos ar projekto saugumo instrukcijas (PSI).

C. **ĮMONĖS PATIKIMUMĄ PATVIRTINANTIS PAŽYMĖJIMAS (ĮPPP)**

10. ĮPPP išduoda valstybės narės NSI arba PSI ar kita kompetentinga saugumo institucija ir jame pagal nacionalinius įstatymus ir kitus teisės aktus nurodoma, kad pramonės arba kitas subjektas savo patalpose gali apsaugoti ESĮI slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ arba „SECRET UE/EU SECRET“ arba jam lygiaverčiu. Prieš rangovui ar subrangovui arba potencialiam rangovui ar subrangovui suteikiant ESĮI arba galimybę susipažinti su ESĮI, Europos Parlamentui, kaip perkančiajai institucijai, pateikiamas kaip įrodymas ĮPPP.

11. ĮPPP:

a) įvertina pramonės ar kitų subjektų patikimumą;

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

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

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

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

12. Atitinkamais atvejais Europos Parlamentas, kaip perkančioji institucija, praneša atitinkamai NSI ar kitai kompetentingai saugumo institucijai, kad prieš sudarant sutartį arba sutarties vykdymui reikalingas ĮPPP. ĮPPP arba APP reikalaujama pateikti prieš sudarant sutartį tais atvejais, kai slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ arba „SECRET UE/EU SECRET“ pažymėta informacija turi būti suteikta paraiškų teikimo proceso metu.

13. Perkančioji institucija neskiria įslaptintos sutarties pasirinktam dalyviui prieš tai negavusi valstybės narės, kurioje yra registruotas atitinkamas rangovas ar subrangovas, NSI ar kitos kompetentingos saugumo institucijos patvirtinimo, kad reikiamais atvejais yra išduotas tinkamas ĮPPP.

14. ĮPPP išdavusi kompetentinga saugumo institucija praneša Europos Parlamentui, kaip perkančiajai institucijai, apie pasikeitimus, turinčius įtakos ĮPPP. Subrangos sutarties atveju atitinkamai informuojama kompetentinga saugumo institucija.

15. Jeigu atitinkama NSI ar kita kompetentinga saugumo institucija panaikina ĮPPP, tai yra pakankamas pagrindas Europos Parlamentui, kaip perkančiajai institucijai, nutraukti įslaptintą sutartį arba pašalinti dalyvį iš konkurso.

D. **ĮSLAPTINTOS SUTARTYS IR SUBRANGOS SUTARTYS**

16. Tais atvejais, kai įslaptinta informacija suteikiama dalyviui prieš sudarant sutartį, kvietime teikti paraiškas numatoma nuostata, pagal kurią paraiškos nepateikęs arba neatrinktas dalyvis įpareigojamas per nurodytą laiką grąžinti visus įslaptintus dokumentus.

17. Sudarius įslaptintą sutartį ar subrangos sutartį, Europos Parlamentas, kaip perkančioji institucija, praneša rangovo ir (arba) subrangovo NSI ar kitai kompetentingai saugumo institucijai tos įslaptintos sutarties saugumo nuostatas.

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

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

20. Konkrečios nuostatos dėl įslaptintos informacijos sunaikinimo vykdant sutartį arba ją nutraukus išdėstomos saugumo aspektų paaiškinime.

21. Tais atvejais, kai rangovui arba subrangovui duotas leidimas nutraukus sutartį pasilikti įslaptintą informaciją, šiame sprendime nustatyti būtiniausi standartai toliau galioja, o rangovas ir subrangovas 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 Europos Parlamento, kaip perkančiosios institucijos, leidimą. Su pramonės arba kitais subjektais, registruotais trečioje šalyje. kuri nėra sudariusi susitarimo dėl informacijos saugumo su Sąjunga, 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 institucijos sutikimo.

25. Įslaptintos informacijos, kurią parengė ar tvarko rangovas arba subrangovas, atžvilgiu perkančioji institucija naudojasi rengėjui priklausančiomis teisėmis.

E. **VIZITAI, SUSIJĘ SU ĮSLAPTINTOMIS SUTARTIMIS**

26. Jei Europos Parlamentui, rangovams ar subrangovams reikia susipažinti su slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ arba „SECRET UE/EU SECRET“ pažymėta informacija vieniems kitų patalpose, kad galėtų įvykdyti sutartį, dėl jų vizitų susitariama palaikant ryšius su nacionalinėmis saugumo institucijomis arba bet kokia kita atitinkama kompetentinga saugumo institucija. Tačiau tam tikrų projektų atveju nacionalinės saugumo institucijos gali taip pat susitarti dėl tvarkos, pagal kurią dėl tokių vizitų gali būti susitariama tiesiogiai.

27. Kad galėtų susipažinti su įslaptinta informacija, susijusia su Europos Parlamento sutartimi, visi lankytojai turi turėti atitinkamą APP ir turi būti vadovaujamasi principu ”būtina žinoti”.

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

F. **ĮSLAPTINTOS INFORMACIJOS PERDAVIMAS IR GABENIMAS**

29. Perduodant įslaptintą informaciją elektroninėmis priemonėmis, taikomos atitinkamos III saugumo pranešimo nuostatos.

30. Įslaptintos informacijos pervežimui taikomos atitinkamos IV saugumo pranešimo nuostatos ir atitinkami naudojimo nurodymai.

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

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

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

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

d) prieš gabenant per valstybių sienas medžiagą, pažymėtą slaptumo žymos laipsniu „CONFIDENTIEL UE/EU CONFIDENTIAL“ arba „SECRET UE/EU SECRET“ ar jam lygiaverčiu, siuntėjas parengia, o generalinis sekretorius patvirtina gabenimo planą;

e) stengiamasi, kad kelionės vyktų be sustojimo ir būtų užbaigtos taip greitai, kaip leidžia aplinkybės;

f) kai tik įmanoma, pasirenkami maršrutai per valstybių narių teritoriją.

G. **ĮSLAPTINTOS INFORMACIJOS PERDAVIMAS TREČIOSIOSE VALSTYBĖSE ĮSISTEIGUSIEMS RANGOVAMS**

32. ESĮI Įslaptinta informacija perduodama trečiosiose valstybėse įsisteigusiems rangovams ir subrangovams laikantis saugumo priemonių, dėl kurių susitarė Europos Parlamentas, kaip perkančioji institucija, ir atitinkama trečioji valstybė, kurioje registruotas rangovas.

H. **SLAPTUMO ŽYMOS LAIPSNIU „RESTREINT UE/EU RESTRICTED“ PAŽYMĖTOS INFORMACIJOS TVARKYMAS IR LAIKYMAS**

33. Palaikydamas ryšius su valstybės narės NSI, Europos Parlamentas, kaip perkančioji institucija, prireikus turi teisę remdamasis sutarties nuostatomis rengti vizitus į rangovo (subrangovo) patalpas, kad patikrintų, ar įgyvendintos pagal sutartį reikalaujamos tinkamos saugumo priemonės, skirtos apsaugoti slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ pažymėtą ESĮI.

34. Kiek būtina pagal nacionalinius įstatymus ir kitus teisės aktus, nacionalinėms saugumo institucijoms (NSI) ar bet kokioms kitoms kompetentingoms saugumo institucijoms Europos Parlamentas, kaip perkančioji institucija, praneša apie sutartis arba subrangos sutartis, kuriose yra slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ pažymėtos informacijos.

35. Europos Parlamento sudarytų sutarčių, kuriose yra slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ pažymėtos informacijos, atveju rangovai ar subrangovai ir jų personalas neprivalo turėti ĮPPP ar APP.

36. Europos Parlamentas, kaip perkančioji institucija, išnagrinėja atsakymus į kvietimus dalyvauti konkurse dėl sutarčių, pagal kurias turi būti suteikta galimybė susipažinti su slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“ pažymėta informacija, neatsižvelgdamas į reikalavimus, susijusius su ĮPPP ar APP, kurie gali būti numatyti nacionaliniuose įstatymuose ir kituose teisės aktuose.

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

38. Kai pagal sutartį numatytas informacijos, pažymėtos slaptumo žymos laipsniu „RESTREINT UE/EU RESTRICTED“, tvarkymas rangovo naudojamoje ryšių ir informacijos sistemoje, Europos Parlamentas, kaip perkančioji institucija, užtikrina, kad sutartyje arba subrangos sutartyje būtų nustatyti su ryšio ir informacijos sistemos akreditavimu susiję būtini techniniai ir administraciniai reikalavimai, kurie atitiktų įvertintą riziką, atsižvelgiant į visus svarbius veiksnius. Perkančioji institucija ir atitinkama NSI susitaria dėl tokio ryšių ir informacijos sistemų akreditavimo masto.

VI SAUGUMO PRANEŠIMAS

KONFINDENCIALIOS INFORMACIJOS SAUGUMO PAŽEIDIMAI, PRARADIMAS ARBA NETEISĖTAS ATSKLEIDIMAS

1. Saugumas pažeidžiamas dėl veiksmo ar neveikimo, prieštaraujančio šiam sprendimui, dėl ko gali kilti pavojus ar būti neteisėtai atskleista konfidenciali informacija.

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

3. Konfidenciali informacija gali būti neteisėtai atskleista dėl nerūpestingumo, neapdairumo ar neatsargumo, taip pat dėl tarnybų veiklos, nukreiptos apie ES, arba ardomąja veikla užsiimančių organizacijų veiklos.

4. Kai generalinis sekretorius sužino ar yra informuojamas apie įrodytus ar tariamus konfidencialios informacijos saugumo pažeidimus, praradimą arba neteisėtą atskleidimą, jis:

a) nustato faktus;

b) įvertina ir kuo labiau sumažina padarytą žalą;

c) imasi atitinkamų priemonių, kad pažeidimas nepasikartotų;

d) praneša trečiosios šalies kompetentingai institucijai ar valstybei narei, kuri sukūrė arba perdavė konfidencialią informaciją.

Jeigu su tokiu įvykiu yra susijęs Europos Parlamento narys, generalinis sekretorius veikia kartu su Europos Parlamento pirmininku.

Jei informacija gauta iš kitos Sąjungos institucijos, generalinis sekretorius veikia vadovaudamasis atitinkamomis saugumo priemonėmis, nustatytomis įslaptintai informacijai, ir įsipareigojimais, nustatytais pagal Pagrindų susitarimą su Komisija ar Tarpinstitucinį susitarimą su Taryba.

5. Visi su konfidencialia informacija turintys dirbti asmenys tinkamai informuojami apie saugumo procedūras, neatsargių pokalbių ir ryšių su žiniasklaida keliamus pavojus, ir, kai tikslinga, pasirašo pareiškimą, kad neatskleis konfidencialaus turinio informacijos tretiesiems asmenims, kad laikysis įsipareigojimo saugoti įslaptintą informaciją ir kad pripažįsta suvokią padarinius, jei nesilaikys reikalavimų. Jei asmuo, kuris nebuvo informuotas ir nepasirašė atitinkamo pranešimo, turi prieigą prie įslaptintos informacijos ar ja naudojasi, tai laikoma saugumo pažeidimu.

6. Europos Parlamento nariai, Europos Parlamento pareigūnai ir kiti Parlamento darbuotojai, kurie dirba frakcijose arba yra laikinai samdomi, tučtuojau paneša generaliniam sekretoriui apie jų pastebėtus bet kokius saugumo pažeidimus, konfidencialios informacijos praradimą ar neteisėtą atskleidimą.

7. Asmuo, dėl kurio kaltės buvo neteisėtai atskleista konfidenciali informacija, baudžiamas drausmine nuobauda pagal atitinkamas teisės normas ir nuostatas. Toks veiksmas nedaro poveikio teisinėms priemonėms, kurių gali būti imamasi pagal atitinkamus taikomus teisės aktus.

8. Nedarant poveikio kitoms teisinėms priemonėms, jei pažeidimą padaro Parlamento pareigūnai ir kiti Parlamento darbuotojai, kurie dirba frakcijose, taikomos Tarnybos nuostatų VI Antraštinėje dalyje numatytos procedūros ir sankcijos.

9. Nedarant poveikio kitoms teisinėms priemonėms, jei pažeidimą padaro Europos Parlamento nariai, atitinkamai taikoma Parlamento Darbo tvarkos taisyklių 9 straipsnio 2 dalis ir 152, 153 ir 154 straipsniai.