1.4.2014. LV Eiropas Savienības Oficiālais Vēstnesis C 96/1

II

(Informācija)

EIROPAS SAVIENĪBAS IESTĀŽU UN STRUKTŪRU SNIEGTI PAZIŅOJUMI

EIROPAS PARLAMENTS

EIROPAS PARLAMENTA PREZIDIJA LĒMUMS

(2013. gada 15. aprīlis)

par noteikumiem attiecībā uz rīcību ar konfidenciālu informāciju Eiropas Parlamentā

(2014/C 96/01)

EIROPAS PARLAMENTA PREZIDIJS,

ņemot vērā Eiropas Parlamenta Reglamenta 23. panta 12. punktu,

tā kā:

1) Sakarā ar 2010. gada 20. oktobrī parakstīto pamatnolīgumu par Eiropas Parlamenta un Eiropas Komisijas attiecībām [1] ("Pamatnolīgums") un Iestāžu nolīgumu starp Eiropas Parlamentu un Padomi par to, kā Eiropas Parlamentam nosūta un kā tas apstrādā Padomes rīcībā esošu klasificētu informāciju par jautājumiem, kas nav kopējās ārpolitikas un drošības politikas darbības jomā [2], kas parakstīts 2014. gada 12. martā ("Iestāžu nolīgums"), ir nepieciešams paredzēt īpašus noteikumus par rīcību ar konfidenciālu informāciju Eiropas Parlamentā.

2) Lisabonas līgumā Eiropas Parlamentam noteikti jauni uzdevumi, un, lai aktīvāk veiktu Eiropas Parlamenta darbības jomās, kurās nepieciešama konfidencialitāte, ir jānosaka pamatprincipi, obligātie drošības standarti un atbilstīgas procedūras rīcībai ar konfidenciālu, tostarp klasificētu, informāciju Eiropas Parlamentā.

3) Šā lēmuma noteikumu mērķis ir nodrošināt līdzvērtīgus aizsardzības standartus un atbilstību noteikumiem, ko pieņēmušas citas iestādes, organizācijas, struktūras un aģentūras, kas izveidotas ar Līgumiem vai uz to pamata, vai arī izveidotas dalībvalstīs, lai veicinātu raitu lēmumu pieņemšanas procesu Eiropas Savienībā.

4) Šā lēmuma noteikumi neskar noteikumus par piekļuvi dokumentiem, kas ir spēkā pašlaik un ko pieņems turpmāk saskaņā ar Līguma par Eiropas Savienības darbību (LESD) 15. pantu.

[1] OV L 304, 20.11.2010., 47. lpp.
[2] OV C 95, 1.4.2014., 1. lpp.

5) Šā lēmuma noteikumi neskar noteikumus par personas datu aizsardzību, kas ir spēkā pašlaik un ko pieņems turpmāk saskaņā ar LESD 16. pantu,

IR PIEŅĒMIS ŠĀDU LĒMUMU:

1. pants

Mērķis

Šis lēmums nosaka konfidenciālas informācijas pārvaldību un apstrādi Eiropas Parlamentā, tostarp kārtību, kādā veic šādas informācijas sagatavošanu, saņemšanu, pārsūtīšanu un glabāšanu Eiropas Parlamentā, lai nodrošinātu tās konfidenciālā rakstura atbilstīgu aizsardzību. Ar to īsteno Iestāžu nolīgumu un Pamatnolīgumu, jo īpaši tā II pielikumu.

2. pants

Definīcijas

Šajā lēmumā:

a) "informācija" ir jebkura rakstiska vai mutiska informācija neatkarīgi no tās pasniegšanas veida vai sagatavotāja;

b) "konfidenciāla informācija" ir "klasificēta informācija" un neklasificēta "cita konfidenciāla informācija";

c) "klasificēta informācija" ir "ES klasificēta informācija" un "līdzvērtīga klasificēta informācija";

d) "ES klasificēta informācija" (ESKI) ir visu veidu informācija un materiāli, kas ir klasificēti kā ES SEVIŠĶI SLEPENI (TRÈS SECRET UE/EU TOP SECRET), ES SLEPENI (SECRET UE/EU SECRET), ES KONFIDENCIĀLI (CONFIDENTIEL UE/EU CONFIDENTIAL) vai ES DIENESTA VAJADZĪBĀM (RESTREINT UE/EU RESTRICTED), un kuru neatļauta izpaušana varētu radīt dažādas pakāpes kaitējumu Savienības vai vienas vai vairāku tās dalībvalstu interesēm neatkarīgi no tā, vai šāda informācija ir sagatavota kādā no iestādēm, struktūrām, birojiem un aģentūrām, kas izveidotas saskaņā ar Līgumiem vai uz to pamata. Šajā sakarā informācija un materiāli, kas klasificēti līmenī:

— TRÈS SECRET UE/EU TOP SECRET ir informācija un materiāli, kuru neatļauta izpaušana var nodarīt ārkārtīgi smagu kaitējumu Savienības vai vienas vai vairāku dalībvalstu būtiskām interesēm;

— SECRET UE/EU SECRET ir informācija un materiāli, kuru neatļauta izpaušana var nodarīt nopietnu kaitējumu Savienības vai vienas vai vairāku dalībvalstu būtiskām interesēm;

— CONFIDENTIEL UE/EU CONFIDENTIAL ir informācija un materiāli, kuru neatļauta izpaušana var nodarīt kaitējumu Savienības vai vienas vai vairāku dalībvalstu būtiskām interesēm;

— RESTREINT UE/EU RESTRICTED ir informācija un materiāli, kuru neatļauta izpaušana var būt nevēlama Savienības vai vienas vai vairāku dalībvalstu interesēm;

e) "līdzvērtīga klasificēta informācija" ir klasificēta informācija, kas sagatavota dalībvalstīs, trešās valstīs vai starptautiskās organizācijās, kas marķēta ar drošības klasifikācijas marķējumu, kurš ir līdzvērtīgs kādam ESKI drošības klasifikācijas marķējumam, un ko Padome vai Komisija nosūtījusi Eiropas Parlamentam;

f) "cita konfidenciāla informācija" ir jebkura cita neklasificēta konfidenciāla informācija, tostarp informācija, uz ko attiecas datu aizsardzības noteikumi vai pienākums glabāt dienesta noslēpumu, un kura sagatavota Eiropas Parlamentā vai nosūtīta Eiropas Parlamentam no citām iestādēm, struktūrām, birojiem un aģentūrām, kas izveidotas ar Līgumiem vai uz to pamata, vai arī no dalībvalstīm;

g) "dokuments" ir jebkāda veida fiksēta informācija neatkarīgi no tās fiziskā veidola vai īpašībām;

h) "materiāls" ir jebkāda veida dokuments vai iekārtas vai ierīces daļa, kas jau ir izstrādāta vai vēl tiek izstrādāta;

i) "vajadzība pēc informācijas" ir vajadzība kādai personai piekļūt konfidenciālai informācijai, lai varētu veikt oficiālus amata pienākumus vai uzdevumu;

j) "atļaujas piešķiršana" ir lēmums, ko pieņem priekšsēdētājs, ja tas attiecas uz Eiropas Parlamenta deputātiem, vai ģenerālsekretārs, ja tas attiecas uz Parlamenta ierēdņiem un citiem Eiropas Parlamenta darbiniekiem, kuri strādā politiskajās grupās, lai piešķirtu individuālu pieeju klasificētai informācijai līdz noteiktam līmenim, balstoties uz drošības pārbaužu pozitīvu rezultātu, ko veikusi valsts iestāde saskaņā ar valsts tiesību aktiem un noteikumiem, kas paredzēti I pielikuma 2. daļā;

k) "klasifikācijas samazināšana" ir klasifikācijas līmeņa samazināšana;

l) "deklasificēšana" ir jebkāda klasifikācijas līmeņa atcelšana;

m) "marķēšana" ir tādas zīmes piestiprināšana "citai konfidenciālai informācijai", ar ko paredz specifisku iepriekš noteiktu norādījumu ievērošanu attiecībā uz šīs informācijas apstrādi vai jomu, uz kuru konkrētais dokuments attiecas. To var piestiprināt arī klasificētai informācijai, lai noteiktu papildu prasības tās apstrādei;

n) "marķējuma noņemšana" ir jebkāda veida marķējuma noņemšana;

o) "sagatavotājs" ir pienācīgu atļauju saņēmis konfidenciālas informācijas autors;

p) "drošības paziņojumi" ir tehniski īstenošanas pasākumi, kā noteikts II pielikumā;

q) "apstrādes instrukcijas" ir tehniskas instrukcijas, kas izdotas Eiropas Parlamenta dienestiem par konfidenciālas informācijas pārvaldību.

3. pants

Pamatprincipi un obligātie standarti

1. Rīcība ar konfidenciālu informāciju Eiropas Parlamentā notiek saskaņā ar pamatprincipiem un obligātajiem standartiem, kas noteikti I pielikuma 1. daļā.

2. Eiropas Parlaments izveido informācijas drošības pārvaldības sistēmu (IDPS) saskaņā ar šiem pamatprincipiem un obligātajiem standartiem. IDPS veido drošības paziņojumi, apstrādes instrukcijas un attiecīgie Reglamenta noteikumi. Tās mērķis ir veicināt parlamentāro un administratīvo darbu, vienlaikus nodrošinot jebkuras Parlamentā apstrādātās konfidenciālās informācijas aizsardzību, pilnībā ievērojot šīs informācijas sagatavotāja drošības paziņojumos paredzētos noteikumus.

Konfidenciālas informācijas apstrāde ar Eiropas Parlamenta automatizētām komunikāciju un informācijas sistēmām (KIS) notiek saskaņā ar koncepciju par informācijas aizsardzību (IA) kā noteikts drošības paziņojumā Nr. 3.

3. Eiropas Parlamenta deputāti bez drošības pielaides var iepazīties ar klasificēto informāciju līdz līmenim RESTREINT UE/EU RESTRICTED un ieskaitot to.

4. Informācijai, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, vai līdzvērtīgai informācijai pielaidi piešķir tiem Eiropas Parlamenta deputātiem, kuriem atļauju piešķīris priekšsēdētājs saskaņā ar 5. punktu, vai kuri parakstījuši oficiālu deklarāciju par šīs informācijas satura neizpaušanu trešām personām un par pienākumu aizsargāt CONFIDENTIEL UE/EU CONFIDENTIAL līmenī klasificētu informāciju, kā arī apliecinājuši, ka apzinās sekas gadījumā, ja šīs prasības tiks pārkāptas.

5. Informācijai, kas klasificēta līmenī SECRET UE/EU SECRET, TRÈS SECRET/EU TOP SECRET, vai līdzvērtīgai informācijai pielaidi piešķir tiem Eiropas Parlamenta deputātiem, kuriem atļauju piešķīris priekšsēdētājs un:

a) kuriem ir drošības pielaide saskaņā ar šā lēmuma I pielikuma 2. daļu vai

b) par kuriem no kompetenta valsts iestādes ir saņemts paziņojums, ka viņi drošības pielaidi ir saņēmuši amata pienākumu dēļ saskaņā ar valsts tiesību aktiem.

6. Pirms Eiropas Parlamenta deputātiem sniedz piekļuvi klasificētai informācijai, viņus informē par pienākumu aizsargāt šo informāciju, un viņi atzīst savu pienākumu attiecībā uz šādas informācijas aizsardzību saskaņā ar I pielikumu. Viņus arī informē par šādas aizsardzības nodrošināšanas līdzekļiem.

7. Eiropas Parlamenta ierēdņi un citi Parlamenta darbinieki, kuri strādā politiskajās grupās, var iepazīties ar konfidenciālu informāciju, ja ir apliecināta viņu vajadzība pēc informācijas, ka arī ar informāciju, kas klasificēta augstāk par līmeni RESTREINT UE/EU RESTRICTED, ja viņiem ir atbilstīgs drošības pielaides līmenis. Piekļuvi klasificētai informācijai sniedz tikai tad, ja minētās personas ir informētas un saņēmušas rakstiskas instrukcijas par saviem pienākumiem attiecībā uz šādas informācijas aizsardzību, kā arī par šādas aizsardzības nodrošināšanas līdzekļiem, un ir parakstījuši deklarāciju par šo instrukciju saņemšanu un apņemšanos tās ievērot saskaņā ar spēkā esošajiem noteikumiem.

4. pants

Konfidenciālas informācijas sagatavošana un administratīvā apstrāde Eiropas Parlamentā

1. Eiropas Parlamenta priekšsēdētājs, attiecīgo Parlamenta komiteju priekšsēdētāji un ģenerālsekretārs, un/vai jebkura cita persona, kurai viņš ir izsniedzis atbilstošu rakstisku atļauju, var sagatavot konfidenciālu informāciju un/vai klasificētu informāciju, kā noteikts drošības paziņojumos.

2. Sagatavojot klasificētu informāciju, sagatavotājs piemēro atbilstoša līmeņa klasifikāciju saskaņā ar starptautiskiem standartiem un definīcijām, kas izklāstītas I pielikumā. Sagatavotājs parasti nosaka arī adresātus, kuriem ir atļauts iepazīties ar šo informāciju atbilstoši tās klasifikācijas līmenim. Šo informāciju paziņo Klasificētās informācijas nodaļai (KIN), kad dokuments tai tiek nodots.

3. Ar citu konfidenciālu informāciju, uz kuru attiecas dienesta noslēpums, rīkojas saskaņā ar I un II pielikumu un apstrādes instrukcijām.

5. pants

Konfidenciālas informācijas saņemšana Eiropas Parlamentā

1. Par Eiropas Parlamentā saņemtu konfidenciālu informāciju paziņo:

a) par informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED vai tai līdzvērtīgu informāciju, un citu konfidenciālu informāciju – tās Parlamenta struktūras/pilnvarotās personas sekretariātam, kura iesniegusi pieprasījumu vai tieši KIN;

b) par informāciju, kas klasificēta kā CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai līdzvērtīgai informāciju – KIN.

2. Konfidenciālas informācijas reģistrāciju, glabāšanu un izsekojamību attiecīgā gadījumā nodrošina vai nu Parlamenta struktūras/pilnvarotās personas sekretariāts, kura saņēmusi informāciju, vai KIN.

3. Ja konfidenciālu informāciju nosūtījusi Komisija saskaņā ar Pamatnolīguma II pielikuma 3.2. punktu vai ja klasificētu informāciju ir nosūtījusi Padome saskaņā ar Iestāžu nolīguma 5. panta 4. punktu, kopīgi pieņemtos noteikumus, par kuriem savstarpēji vienojas un kuru mērķis ir saglabāt informācijas konfidencialitāti uzglabā kopā ar konfidenciālo informāciju attiecīgā gadījumā Parlamenta struktūras/pilnvarotās personas sekretariātā vai KIN.

4. Šā panta 3. punktā minēto kārtību konfidenciālas informācijas nosūtīšanai mutatis mutandis var piemērot arī citās iestādēs, organizācijās, birojos un aģentūrās, kas izveidotas saskaņā ar Līgumiem vai arī izveidotas dalībvalstīs.

5. Lai nodrošinātu aizsardzības līmeni, kas atbilst klasifikācijas līmenim TRÈS SECRET UE/EU TOP SECRET vai līdzvērtīgam līmenim, Priekšsēdētāju konference izveido uzraudzības komiteju. Informāciju, kas klasificēta līmenī TRÈS SECRET UE/EU TOP SECRET, vai tai līdzvērtīgu informāciju nosūta Eiropas Parlamentam saskaņā ar turpmāku kārtību, par kuru vienojas Eiropas Parlaments un tā Savienības iestāde, no kuras šī informācija saņemta.

6. pants

Eiropas Parlamenta veikta klasificētas informācijas nosūtīšana trešām personām

Ja attiecīgā gadījumā sagatavotājs vai tā Savienības iestāde, kas klasificētu informāciju nosūtījusi Eiropas Parlamentam, iepriekš rakstiski piekrīt, Eiropas Parlaments var nosūtīt šādu klasificētu informāciju trešajām personām, ar nosacījumu, ka, rīkojoties ar klasificētu informāciju, tās attiecībā uz savām darbībām un telpām nodrošina tādu noteikumu ievērošanu, kas ir līdzvērtīgi šajā lēmumā minētajiem.

7. pants

Drošās telpas

1. Konfidenciālas informācijas pārvaldības nolūkā Eiropas Parlaments izveido drošības zonu un drošās lasītavas.

2. Drošības zonā ietilpst telpas klasificētas informācijas reģistrācijai, arhivēšanai, pārsūtīšanai un apstrādei, kā arī telpas, kur ar šo informāciju var iepazīties. Tajā ietilpst *inter alia* lasītava un sanāksmju zāle, kur var iepazīties ar klasificētu informāciju, un ko pārvalda KIN.

3. Ārpus drošības zonas var ierīkot drošās lasītavas, lai tajās varētu iepazīties ar informāciju, kura klasificēta līmenī RESTREINT UE/EU RESTRICTED vai tai līdzvērtīgu informāciju un ar citu konfidenciālu informāciju. Minētās drošās lasītavas attiecīgā gadījumā pārvalda Parlamenta struktūru/pilnvaroto personu sekretariātu kompetentie dienesti vai KIN. Tajās nav kopēšanas iekārtu, telefonu, faksa aparātu, skeneru vai citu tehnisku iekārtu dokumentu kopēšanai un pārraidīšanai.

8. pants

Konfidenciālas informācijas reģistrācija, apstrāde un glabāšana

1. Informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai tai līdzvērtīgu informāciju un "citu konfidenciālu informāciju" var reģistrēt un glabāt Parlamenta struktūru/pilnvaroto personu sekretariātu kompetentie dienesti vai KIN atkarībā no tā, kurš šo informāciju saņēmis.

2. Uz tās informācijas apstrādi, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai tai līdzvērtīgas informācijas un "citas konfidenciālas informācijas" apstrādi attiecas šādi nosacījumi:

a) dokumentus personīgi nodod sekretariāta vadītājam, kurš tos reģistrē un sniedz apstiprinājumu par saņemšanu;

b) šādus dokumentus glabā slēgtā vietā un par tiem atbild sekretariāts, izņemot laiku, kad tos faktiski izmanto;

c) informāciju nekādā gadījumā nedrīkst saglabāt citā datu nesējā vai nosūtīt citai personai. Šādus dokumentus var pavairot vienīgi ar atbilstoši akreditētām iekārtām, kas noteiktas drošības paziņojumos;

d) piekļūt šādai informācijai drīkst tikai tās personas, kuras norādījis sagatavotājs vai tā Savienības iestāde, kas šo informāciju nosūtījusi Eiropas Parlamentam, turklāt saskaņā ar 4. panta 2. punktā vai 5. panta 3., 4. un 5. punktā minēto kārtību;

e) Parlamenta struktūras/pilnvarotās personas sekretariāts reģistrē tās personas, kuras ir iepazinušās ar dokumentiem, un reģistrē arī laiku un datumu, kad šāda iepazīšanās notikusi., un nodod reģistrētos datus KIN laika tad, kad KIN tiek nodota attiecīgā informācija.

3. Informāciju, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai tai līdzvērtīgu informāciju KIN reģistrē, apstrādā un uzglabā drošības zonā, turklāt atbilstoši attiecīgam klasifikācijas līmenim un tā, kā noteikts drošības paziņojumos.

4. Ja 1. līdz 3. punkta minētie noteikumi tiek pārkāpti, attiecīgā gadījumā Parlamenta struktūras/pilnvarotās personas sekretariāta vai KIN atbildīgā amatpersona informē ģenerālsekretāru, kurš gadījumā, ja pārkāpumus ir veicis Eiropas Parlamenta deputāts, šo informāciju nodod Parlamenta priekšsēdētājam.

9. pants

Piekļuve drošajām telpām

1. Drošības zonā var iekļūt tikai šādas personas:

a) personas, kurām saskaņā ar 3. panta 4. līdz 7. punktu ir atļauja iepazīties ar tajās uzglabāto informāciju, un kuras ir iesniegušas pieteikumu saskaņā ar 10. panta 1. punktu;

b) personas, kurām saskaņā ar 4. panta 1. punktu ir atļauja sagatavot klasificētu informāciju, un kuras ir iesniegušas pieteikumu saskaņā ar 10. panta 1. punktu;

c) KIN sastāvā iekļauti Eiropas Parlamenta ierēdņi;

d) Eiropas Parlamenta ierēdņi, kuri atbildīgi par KIN pārvaldību;

e) nepieciešamības gadījumā – Eiropas Parlamenta ierēdņi, kuri atbildīgi par drošību un ugunsdrošību;

f) uzkopšanas darbinieki, bet tikai KIN darbinieka klātbūtnē un stingrā uzraudzībā.

2. KIN var liegt piekļuvi drošības zonai jebkurai personai, kam nav vajadzīgās atļaujas. Jebkurus iebildumus par KIN lēmumu par piekļuves liegšanu iesniedz Eiropas Parlamenta priekšsēdētājam Eiropas Parlamenta deputātu pieprasījuma gadījumā un ģenerālsekretāram citos gadījumos.

3. Ģenerālsekretārs var atļaut ierobežotam skaitam personu tikties drošības zonas sanāksmju zālē.

4. Drošajā lasītavā var iekļūt tikai šādas personas:

a) Eiropas Parlamenta deputāti, Eiropas Parlamenta ierēdņi un citi politiskajās grupās strādājoši Eiropas Parlamenta darbinieki, kuri pienācīgi identificēti, lai iepazītos ar konfidenciālu informāciju vai to sagatavotu;

b) Eiropas Parlamenta ierēdņi, kuri atbildīgi par KIN pārvaldību, tās Parlamenta struktūras/pilnvarotās personas sekretariāta amatpersonas, kura saņēmusi informāciju, un KIN strādājoši ierēdņi;

c) ja nepieciešams – Eiropas Parlamenta ierēdņi, kuri atbildīgi par drošību un ugunsdrošību;

d) uzkopšanas darbinieki, bet tikai attiecīgā gadījumā Parlamenta struktūras/pilnvarotās personas sekretariāta amatpersonas vai KIN darbinieka klātbūtnē un stingrā uzraudzībā.

5. Attiecīgā gadījumā Parlamenta struktūras/pilnvarotās personas atbildīgais sekretariāts vai KIN var liegt piekļuvi drošajai lasītavai jebkurai personai, kurai nav vajadzīgās atļaujas. Eiropas Parlamenta deputātu iebildumi par Parlamenta struktūras/pilnvarotās personas atbildīgā sekretariāta vai KIN lēmumu par šādu piekļuves liegšanu iesniedzami Eiropas Parlamenta priekšsēdētājam, savukārt ierēdņu un citu darbinieku iebildumi – ģenerālsekretāram.

10. pants

Iepazīšanās ar konfidenciālu informāciju vai tās sagatavošana drošajās telpās

1. Jebkurai personai, kura vēlas iepazīties ar konfidenciālu informāciju vai sagatavot to drošības zonā, ir pienākums iepriekš paziņot savu vārdu un uzvārdu KIN. KIN pārbauda m,inētās personas identitāti, kura iesniedz pieteikumu, un pārliecinās, vai šai personai ir atļauts iepazīties ar konfidenciālu informāciju vai sagatavot konfidenciālu informāciju saskaņā ar noteikumiem, kas minēti 3. panta 3. līdz 7. punktā, 4. panta 1. punktā vai 5. panta 3., 4. un 5. punktā;

2. Jebkura persona, kura saskaņā ar 3. panta 3. un 7. punktu drošajā lasītavā vēlas iepazīties ar konfidenciālu informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED vai tai līdzvērtīgu informāciju un citu konfidenciālu informāciju, iepriekš paziņo savu vārdu un uzvārdu Parlamenta struktūru/pilnvaroto personu sekretariātu atbildīgajiem dienestiem vai KIN.

3. Izņemot ārkārtas apstākļus (piemēram, saņemti daudzi lūgumi iepazīties ar informāciju īsā laikā), atrasties drošajās telpās un iepazīties ar konfidenciālo informāciju drīkst tikai viena persona, turklāt Parlamenta struktūras/pilnvarotās personas sekretariāta amatpersonas vai KIN amatpersonas klātbūtnē.

4. Kamēr notiek iepazīšanās ar konfidenciālo informāciju, nedrīkst ne sazināties ar ārpasauli (aizliegta telefona vai citu saziņas tehnoloģijas ierīču lietošana), ne arī norakstīt, kopēt vai fotografēt minēto informāciju.

5. Pirms dot atļauju pamest drošo lasītavu, Parlamenta struktūras/pilnvarotās personas sekretariāta amatpersona vai KIN amatpersona pārliecinās, vai tā konfidenciālā informācija, ar kuru notika iepazīšanās, atrodas savā vietā, ir neskarta un pilnīga.

6. Ja minētie noteikumi tiek pārkāpti, attiecīgā gadījumā Parlamenta struktūras/pilnvarotās personas sekretariāta amatpersona vai KIN amatpersona informē ģenerālsekretāru, kurš gadījumā, ja pārkāpumus ir veicis Eiropas Parlamenta deputāts, šo informāciju nodod Parlamenta priekšsēdētājam.

11. pants

Obligātie standarti attiecībā uz iepazīšanos ar konfidenciālu informāciju sanāksmē aiz slēgtām durvīm, kas notiek ārpus drošajām telpām

1. Ar informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai tai līdzvērtīgu informāciju un citu konfidenciālu informāciju Parlamenta komitejas vai citas Eiropas Parlamenta politiskās un administratīvās struktūras var iepazīties arī sanāksmē aiz slēgtām durvīm, kas notiek ārpus drošajām telpām.

2. Šā panta 1. punktā minētajos apstākļos Parlamenta struktūras sekretariāts/pilnvarotā persona, kas atbild par sanāksmi, nodrošina, ka tiek ievēroti šādi nosacījumi:

a) sanāksmes telpā drīkst ienākt tikai personas, kuras kompetentās komitejas vai struktūras vadītājs izraudzījies dalībai sanāksmē;

b) visi dokumenti ir numurēti, tie tiek izdalīti sanāksmes sākumā un savākti tās beigās, par tiem netiek izdarītas nekādas piezīmes un tie netiek ne kopēti, ne fotografēti;

c) sanāksmes protokolā nekādā veidā netiek pieminēts diskusiju saturs par attiecīgo informāciju; protokolā var reģistrēt vienīgi attiecīgo lēmumu, ja tāds ir pieņemts;

d) uz konfidenciālu informāciju, kas saņēmējiem Eiropas Parlamentā sniegta mutiski, attiecas rakstiskā veidā sniegtai konfidenciālai informācijai līdzvērtīgs aizsardzības līmenis;

e) sanāksmju telpās netiek glabāti nekādi papildu dokumentu krājumi;

f) sanāksmes sākumā tās dalībniekiem un tulkiem izsniedz tikai nepieciešamo dokumentu kopiju skaitu;

g) sanāksmes vadītājs sanāksmes sākumā skaidri norāda dokumentu klasifikācijas/marķējuma statusu;

h) dalībnieki neiznes dokumentus no sanāksmes telpas;

i) Parlamenta struktūras/pilnvarotās personas sekretariāta pārstāvis pēc sanāksmes savāc un saskaita visas izsniegtās dokumentu kopijas; un

j) sanāksmes telpā, kurā iepazīstas ar konfidenciālu informāciju vai apspriež to, netiek ienestes nekādas elektronisko sakaru ierīces vai citas elektroniskas ierīces.

3. Ja saskaņā ar Pamatnolīguma 2. pielikuma 3.2.2. punktā un Iestāžu nolīguma 6. panta 5. punktā paredzētajiem izņēmumiem informāciju, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, vai tai līdzvērtīgu informāciju apspriež sanāksmē aiz slēgtām durvīm, Parlamenta struktūras/pilnvarotās personas, kas atbild par sanāksmi, sekretariāts papildus tam, ka tiek nodrošināta atbilstība 2. punkta noteikumiem, nodrošina arī to, ka personas, kuras izraudzītas piedalīties sanāksmē, atbilst 3. panta 4. un 7. punkta prasībām.

4. Šā panta 3. punktā paredzētajā gadījumā KIN Parlamenta struktūras/pilnvarotās personas, kas atbild par sanāksmi aiz slēgtām durvīm, sekretariāts izsniedz apspriešanai nepieciešamo dokumentu kopiju skaitu, kuras pēc sanāksmes nodod atpakaļ KIN.

12. pants

Konfidenciālas informācijas arhivēšana

1. Drošības zonā nodrošina telpas drošai informācijas arhivēšanai. Par drošo arhīvu pārvaldību ir atbildīgs KIN, rīkojoties saskaņā ar arhivēšanas standarta kritērijiem.

2. Klasificētu informāciju, ko galīgi deponē KIN, un informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai tai līdzvērtīgu informāciju, ko deponē Parlamenta struktūras sekretariātā/pie pilnvarotās personas, nodod drošā arhīvā drošības zonā sešu mēnešu laikā pēc tam, kad ar to pēdējo reizi notikusi iepazīšanās, un, vēlākais, vienu gadu pēc tam, kad tā tikusi deponēta. Citu konfidenciālu informāciju, kas netiek deponēta KIN, arhivē attiecīgie Parlamenta struktūras/pilnvarotās personas sekretariāti saskaņā ar vispārējiem noteikumiem par dokumentu pārvaldību.

3. Ar drošā arhīvā glabātu konfidenciālu informāciju var iepazīties, ievērojot šādus nosacījumus:

a) ar informāciju var iepazīties tikai tās personas, kuru vārds un uzvārds, veicamais pienākums vai amats minēts dokumentā, kas sastādīts konfidenciālas informācijas deponēšanas brīdī;

b) pieteikumu par iepazīšanos ar konfidenciālu informāciju iesniedz KIN, kas nodrošina attiecīgā dokumenta pārvietošanu uz drošo lasītavu; un

c) piemēro visas 10. pantā noteiktās procedūras un nosacījumus attiecībā uz iepazīšanos ar konfidenciālu informāciju.

13. pants

Konfidenciālas informācijas klasifikācijas līmeņa samazināšana, deklasificēšana un marķējuma noņemšana

1. Konfidenciālas informācijas klasifikācijas līmeni var samazināt, šo informāciju deklasificēt vai marķējumu noņem tikai ar sagatavotāja piekrišanu un – vajadzības gadījumā – pēc apspriešanās ar citām ieinteresētajām pusēm.

2. Klasifikācijas līmeņa samazināšanu vai deklasificēšanu apstiprina rakstiski. Sagatavotājs atbild par izmaiņu paziņošanu adresātiem un tie, savukārt, atbild par izmaiņu paziņošanu citiem tālākajiem adresātiem, kuriem tie ir nosūtījuši vai nokopējuši dokumentu. Ja iespējams, sagatavotāji uz klasificētiem dokumentiem norāda datumu, laika posmu vai notikumu, pēc kuriem to klasifikācijas līmeni var samazināt vai informāciju deklasificēt. Pretējā gadījumā tie dokumentus pārskata, vēlākais, ik pēc pieciem gadiem, lai pārliecinātos, ka sākotnējā klasifikācija vēl arvien ir nepieciešama.

3. Drošos arhīvos glabātu konfidenciālu informāciju savlaicīgi pārbauda, taču ne vēlāk kā 25 gadus pēc sagatavošanas dienas, lai noteiktu, vai tās klasifikācijas līmenis būtu jāsamazina, šī informācija deklasificējama vai tās marķējums noņemams. Šādas informācijas pārbaude un publicēšana notiek saskaņā ar noteikumiem 1983. gada 1. februāra Padomes Regulā (EEK, Euratom) Nr. 354/83 par Eiropas Ekonomikas kopienas un Eiropas Atomenerģijas kopienas vēsturisko arhīva materiālu nodošanu atklātībai ([1]). Deklasificēšanu veic klasificētās informācijas sagatavotājs vai dienests, kurš par to atbildīgs saskaņā ar I pielikuma 1. daļas 10. pantu.

4. Iepriekš drošā arhīvā turētu klasificētu informāciju pēc deklasificēšanas nodod Eiropas Parlamenta vēstures arhīvam pastāvīgai glabāšanai un turpmākai rīcībai saskaņā ar piemērojamajiem noteikumiem.

5. Pēc marķējuma noņemšanas uz informāciju, kas iepriekš bija klasificēta kā cita konfidenciāla informācija, attiecas Eiropas Parlamenta noteikumi par dokumentu pārvaldību.

14. pants

Drošības pārkāpumi attiecībā uz konfidenciālu informāciju, tās zudums vai apdraudēšana

1. Ja pieļauti konfidencialitātes pārkāpumi kopumā un jo īpaši šā lēmuma pārkāpumi, attiecībā uz Eiropas Parlamenta deputātiem piemēro attiecīgos noteikumus par sodiem, kas paredzēti Eiropas Parlamenta Reglamentā.

2. Ja pārkāpumus izdarījis kāds no Eiropas Parlamenta darbiniekiem, piemēro procedūras un sodus, kuri paredzēti attiecīgi Civildienesta noteikumos un Eiropas Kopienu pārējo darbinieku nodarbināšanas kārtībā, kas noteikta ar Regulu (EEK, Euratom, EOTK) Nr. 259/68 ([2]) ("Civildienesta noteikumi").

([1]) OV L 43, 15.2.1983., 1. lpp.
([2]) OV L 56, 4.3.1968., 1. lpp.

3. Priekšsēdētājs un/vai ģenerālsekretārs attiecīgā situācijā organizē jebkādu nepieciešamo izmeklēšanu gadījumos, ja noticis pārkāpums, kā minēts drošības paziņojumā Nr. 6.

4. Ja konfidenciālu informāciju Eiropas Parlamentam nosūtījusi Savienības iestāde vai dalībvalsts, attiecīgā gadījumā priekšsēdētājs un/vai ģenerālsekretārs informē šo Savienības iestādi vai attiecīgo dalībvalsti par jebkuru notikušu vai iespējamu klasificētas informācijas zaudēšanas vai apdraudējuma gadījumu, izmeklēšanas rezultātiem un veiktajiem pasākumiem, lai nepieļautu šādu gadījumu atkārtošanos.

15. pants

Šā lēmuma un īstenošanas noteikumu pielāgošana un gada pārskats par šā lēmuma piemērošanu

1. Ģenerālsekretārs ierosina vajadzīgos pielāgojumus šajā lēmumā un pielikumos, ar kuriem to īsteno, un nosūta šos priekšlikumus Prezidijam lēmuma pieņemšanai.

2. Ģenerālsekretārs ir atbildīgs par to, kā Eiropas Parlamenta dienesti īsteno šo lēmumu un saskaņā ar šajā lēmumā noteiktajiem principiem viņš sniedz apstrādes norādījumus par jautājumiem, uz kuriem attiecas IDPS.

3. Ģenerālsekretārs iesniedz Prezidijam gada ziņojumu par šā lēmuma piemērošanu.

16. pants

Pārejas un nobeiguma noteikumi

1. Neklasificēta informācija, kas jau atrodas KIN vai jebkurā citā Eiropas Parlamenta arhīvā, un kas ir atzīta par konfidenciālu un ir datēta ar laiku pirms 2014. gada 1. aprīlis, šā lēmuma nolūkiem tiek uzskatīta par "citu konfidenciālu informāciju". Tās sagatavotājs jebkurā laikā var pārskatīt tās konfidencialitātes līmeni.

2. Atkāpjoties no šā lēmuma 5. panta 1. punkta a) apakšpunkta un no 8. panta 1. punkta uz divpadsmit mēnešu laika posmu no 2014. gada 1. aprīlis informāciju, ko sniegusi Padome saskaņā ar Iestāžu nolīgumu, un kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai tai līdzvērtīgu informāciju deponē, reģistrē un uzglabā KIN. Ar šādu informāciju var iepazīties saskaņā ar Iestāžu nolīguma 4. panta 2. punkta a) un c) apakšpunktu un 5. panta 4. punktu.

3. Prezidija 2011. gada 6. jūnija Lēmums par noteikumiem par rīcību ar konfidenciālu informāciju Eiropas Parlamentā tiek atcelts.

17. pants

Stāšanās spēkā

Šis lēmums stājas spēkā dienā, kad to publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

I PIELIKUMS

1. daļa

DROŠĪBAS PAMATPRINCIPI UN OBLIGĀTIE STANDARTI KONFIDENCIĀLAS INFORMĀCIJAS AIZSARDZĪBAI

1. **IEVADS**

Ar šiem noteikumiem nosaka drošības pamatprincipus un minimālos drošības standartus konfidenciālas informācijas aizsardzībai, kuri jāievēro Eiropas Parlamentam visās tā darba vietās, tostarp visiem klasificētas informācijas un "citas konfidenciālas informācijas" saņēmējiem, lai aizsargātu drošību un visas attiecīgās personas būtu pārliecinātas, ka ir izstrādāts vienots aizsardzības standarts. Šos noteikumus papildina ar drošības paziņojumiem, kas ietverti II pielikumā, un citiem noteikumiem, kas reglamentē to, kā konfidenciālu informāciju apstrādā Parlamenta komitejas un citas Parlamenta struktūras / pilnvarotās personas.

2. **PAMATPRINCIPI**

Eiropas Parlamenta drošības politika ir tā vispārējās iekšējās pārvaldības politikas neatņemama sastāvdaļa un tādējādi balstās uz principiem, kas reglamentē tā vispārējo politiku. Šie principi ir likumība, pārredzamība, atbildība un subsidiaritāte un samērīgums.

Likumība nozīmē nepieciešamību stingri ievērot tiesisko regulējumu drošības funkciju veikšanā un nepieciešamību ievērot piemērojamās tiesiskās prasības. Turklāt arī atbildībai drošības jomā jāpamatojas uz atbilstīgām tiesību normām. Civildienesta noteikumus piemēro pilnībā, jo īpaši to 17. pantu par prasību darbiniekiem atturēties no neatļautas amata pienākumu veikšanai saņemtās informācijas izpaušanas un VI sadaļu par disciplinārsodiem. Visbeidzot, tas nozīmē arī to, ka attiecībā uz Eiropas Parlamentā pieļautiem drošības pārkāpumiem rīkojas veidā, kas atbilst Reglamentam un tā politikai disciplināro pasākumu jomā.

Pārredzamība paredz skaidrību attiecībā uz visiem drošības noteikumiem un nosacījumiem, lai tādējādi nodrošinātu līdzsvaru starp dažādiem dienestiem un dažādām jomām (fiziskā drošība salīdzinājumā ar informācijas aizsardzību u. c.), gan arī konsekventa un strukturēta drošības izpratnes politika. Turklāt nepieciešamas precīzas rakstiskas pamatnostādnes drošības pasākumu īstenošanai.

Atbildība nozīmē to, ka skaidri jānosaka pienākumi drošības jomā. Turklāt tā nozīmē arī to, ka ir nepieciešams regulāri pārbaudīt šo pienākumu pareizu izpildi.

Subsidiaritāte nozīmē to, ka drošība jāorganizē iespējami zemākā līmenī un pēc iespējas ciešākā saiknē ar Eiropas Parlamenta ģenerāldirektorātiem un dienestiem. Samērīgums nozīmē to, ka drošības darbībās jāiekļauj tikai tas, kas patiešām ir nepieciešams un ka drošības pasākumiem jābūt samērīgiem ar aizsargājamām interesēm un faktiskiem vai iespējamiem draudiem šīm interesēm, lai aizsargātu tās veidā, kas izraisa vismazāko iespējamo traucējumu.

3. **INFORMĀCIJAS DROŠĪBAS PAMATI**

Efektīvas informācijas drošības pamati ir:

a) pienācīgas komunikāciju un informācijas sistēmas (KIS), par kurām atbild drošības iestāde.

b) Eiropas Parlamentā – Informācijas aizsardzības iestāde (kā noteikts drošības paziņojumā Nr. 1), kas atbild par sadarbību ar attiecīgo drošības iestādi. lai sniegtu informāciju un konsultācijas par tehnisku apdraudējumu komunikāciju un informācijas sistēmām (KIS) un veidiem, kā pret šo apdraudējumu aizsargāties;

c) cieša sadarbība starp Eiropas Parlamenta atbildīgajiem dienestiem un citu Savienības iestāžu drošības dienestiem;

4. **INFORMĀCIJAS DROŠĪBAS PRINCIPI**

4.1. ***Mērķi***

Galvenie informācijas drošības mērķi ir šādi:

a) aizsargāt klasificētu informāciju un citu konfidenciālu informāciju no spiegošanas, apdraudējuma vai neatļautas atklāšanas;

b) aizsargāt klasificētu informāciju, ko apstrādā komunikāciju un informācijas sistēmās un tīklos, no draudiem tās konfidencialitātei, integritātei un pieejamībai;

c) aizsargāt Eiropas Parlamenta telpas, kurās glabā klasificētu informāciju, no sabotāžas un ar nodomu nodarīta kaitējuma;

d) drošības kļūdas gadījumā izvērtēt nodarīto kaitējumu, ierobežot tās sekas un veikt izmeklēšanu par drošības jautājumiem un pieņemt visus nepieciešamos pasākumus stāvokļa uzlabošanai.

4.2. ***Klasificēšana***

4.2.1. Attiecībā uz konfidencialitāti nepieciešama rūpība un pieredze, izvēloties informāciju un materiālu, kas ir jāaizsargā, kā arī izvērtējot tiem piemērojamo aizsardzības pakāpi. Ir būtiski, lai aizsardzības pakāpe atbilstu konkrētās aizsargājamās informācijas vai materiāla jutībai drošības aspektā. Lai nodrošinātu raitu informācijas plūsmu, izvairās no pārlieku augstas vai pārlieku zemas klasifikācijas pakāpes piešķiršanas.

4.2.2. Klasifikācijas sistēma ir instruments, ar ko īstenot šajā nodaļā minētos principus. Līdzīgu klasifikācijas sistēmu ievēro, plānojot un organizējot veidus, lai apkarotu spiegošanu, sabotāžu, terorismu un citus apdraudējumus un lai nodrošinātu maksimālu aizsardzību vissvarīgākajām telpām, kurās atrodas klasificēta informācija, un visjutīgākajām t vietām minētajās telpās;

4.2.3. Par attiecīgās informācijas klasificēšanu ir atbildīgs vienīgi tās sagatavotājs.

4.2.4. Klasifikācijas līmeni var pamatot tikai ar attiecīgās informācijas saturu.

4.2.5. Ja vairākas informācijas vienības tiek grupētas kopā, to klasifikācijas līmenis ir vismaz tikpat augsts kā visaugstākais vienam no tās atsevišķām daļām individuāli piešķirtais klasifikācijas līmenis. Tomēr grupētai informācijai var piešķirt augstāku klasifikāciju kā tās sastāvdaļām.

4.2.6. Klasifikāciju piešķir tikai tad, kad tas ir nepieciešams, un tikai uz nepieciešamo laiku.

4.3. ***Drošības pasākumu mērķi***

Drošības pasākumi:

a) attiecas uz visām personām, kurām ir piekļuve klasificētai informācijai, klasificētas informācijas nesējiem un "citai konfidenciālai informācijai", kā arī visām telpām, kurās atrodas šāda informācija, un svarīgām iekārtām;

b) ir izveidoti tā, lai identificētu personas, kuru stāvoklis (attiecībā uz pieeju, saistību vai citādi) var apdraudēt šādas informācijas drošību un svarīgas iekārtas, kas satur šādu informāciju un kas paredzētas to izslēgšanai vai iznīcināšanai;

c) liedz jebkurai personai, kurai nav vajadzīgās atļaujas, piekļūt šādai informācijai vai iekārtām, kas to satur;

d) nodrošina to, ka šādu informāciju izplata, vienīgi pamatojoties uz principu "vajadzība pēc informācijas", kas ir visu drošības aspektu pamatā;

e) nodrošina visas klasificētas vai neklasificētas konfidenciālas informācijas integritāti (piemēram, nepieļaujot bojāšanu, neatļautu izmaiņu veikšanu vai neatļautu izdzēšanu) un pieejamību (tiem, kam tā ir nepieciešama un atļauta), jo īpaši attiecībā uz tādu informāciju, ko uzglabā, apstrādā vai pārsūta elektromagnētiskā formā.

5. KOPĒJIE OBLIGĀTIE STANDARTI

Eiropas Parlaments nodrošina to, ka kopējos obligātos drošības standartus ievēro visi klasificētas informācijas saņēmēji iestādē un tās kompetencēs esošās struktūrvienībās, piemēram, visi dienesti un līgumdarbinieki, lai šo informāciju var nodot ar pārliecību, ka to apstrādās ar pienācīgu rūpību. Šādi obligātie standarti paredz kritērijus drošības pielaides izsniegšanai Eiropas Parlamenta ierēdņiem un citiem Parlamenta darbiniekiem, kuri strādā politiskajās grupās, un procedūras konfidenciālas informācijas aizsardzībai.

Eiropas Parlaments ļauj piekļūt šai informācijai trešajām personām tikai tad, ja tās nodrošina, ka šīs informācijas apstrādes laikā tiek ievēroti tādi noteikumi, kas ir vismaz tikpat stingri kā šie kopējie obligātie standarti.

Šādus kopējos obligātos standartus piemēro arī tad, kad Parlaments ar līgumu vai dotāciju nolīgumu rūpniecības vai citām struktūrām uztic uzdevumus, kuru veikšanai nepieciešama konfidenciāla informācija.

6. DROŠĪBA ATTIECĪBĀ UZ EIROPAS PARLAMENTA IERĒDŅIEM UN CITIEM PARLAMENTA DARBINIEKIEM, KURI STRĀDĀ POLITISKAJĀS GRUPĀS

6.1. *Drošības instrukcijas attiecībā uz Eiropas Parlamenta ierēdņiem un citiem Parlamenta darbiniekiem, kuri strādā politiskajās grupās*

Eiropas Parlamenta ierēdņus un citus Parlamenta darbiniekus, kuri strādā politiskajās grupās un ieņem amatus, kur tiem var būt piekļuve klasificētai informācijai, stājoties amatā un pēc regulāriem starplaikiem, rūpīgi instruē par nepieciešamību ievērot drošību un tās nodrošināšanas procedūrām. Šādām personām prasa rakstiski apstiprināt, ka tās ir izlasījušas un pilnīgi saprot piemērojamos drošības noteikumus.

6.2. *Vadītāju atbildība*

Vadītāju pienākumos jāietilpst apzināt tos sev pakļautos darbiniekus, kuri ir iesaistīti darbā ar klasificētu informāciju vai kuriem ir piekļuve drošām komunikāciju vai informācijas sistēmām, kā arī reģistrēt un paziņot jebkurus starpgadījumus vai acīmredzamus trūkumus, kas varētu ietekmēt drošību.

6.3. *Eiropas Parlamenta ierēdņu un citu Parlamenta darbinieku, kuri strādā politiskajās grupās, drošības statuss*

Izveido procedūras, lai nodrošinātu to, ka, uzzinot negatīvu informāciju par Eiropas Parlamenta ierēdni vai citu Parlamenta darbinieku, kas strādā kādā politiskajā grupā, nosaka, vai šī indivīda darbs ir saistīts ar klasificētu informāciju un vai viņam ir piekļuve drošām komunikāciju vai informācijas sistēmām, par ko informē Eiropas Parlamenta attiecīgo dienestu. Ja kompetenta valsts drošības iestāde norāda, ka šāds indivīds apdraud drošību, to atceļ no tādiem darbiem vai liedz pildīt uzdevumus, kuros tas var apdraudēt drošību.

7. FIZISKĀ DROŠĪBA

Fiziskā drošība ir fiziski un tehniski aizsardzības pasākumi, lai novērstu neatļautu piekļuvi klasificētai informācijai.

7.1. ***Vajadzība pēc aizsardzības***

Klasificētas informācijas aizsardzības nodrošināšanai piemēroto fiziskās drošības pasākumu pakāpe ir samērīga ar uzglabātās informācijas un materiāla klasifikāciju, apjomu un apdraudējumu. Visi klasificētas informācijas turētāji ievēro vienotu praksi attiecībā uz šīs informācijas klasifikāciju, kā arī kopējus aizsardzības standartus attiecībā uz informācijas un materiāla, kam nepieciešama aizsardzība, glabāšanu, nosūtīšanu un iznīcināšanu.

7.2. ***Pārbaudes***

Pirms atstāt bez uzraudzības zonas, kurās atrodas klasificēta informācija, atbildīgās personas nodrošina, ka tā tiek droši uzglabāta un darbojas visas drošības ierīces (slēdzenes, apsardzes sistēmas u. c.). Papildu neatkarīgu pārbaudi veic pēc darba dienas beigām.

7.3. ***Ēku drošība***

Ēkas, kurās atrodas klasificēta informācija vai drošas komunikāciju un informācijas sistēmas, aizsargā pret neatļautu piekļuvi.

Klasificētas informācijas aizsardzības pasākumi, piemēram, logu aizrestošana, durvju slēdzenes, durvju apsardze, automatizētas piekļūšanas kontroles sistēmas, drošības pārbaudes un patruļas, signalizācijas sistēmas, iekļūšanas noteikšanas sistēmas un sargsuņi, ir atkarīgi no:

a) aizsargājamās informācijas un materiāla klasifikācijas, apjoma un izvietojuma ēkā;

b) minētās informācijas un attiecīgā materiāla drošības konteineru kvalitātes un

c) ēkas fiziskajām īpašībām un novietojuma.

Komunikāciju un informācijas sistēmu aizsardzības pasākumi ir atkarīgi no to vērtības un iespējamā kaitējuma, kāds varētu rasties drošības neievērošanas dēļ, no ēkas, kurā atrodas šī sistēma, fiziskajām īpašībām un novietojuma, kā arī no sistēmas novietojuma pašā ēkā.

7.4. ***Ārkārtas pasākumu plāni***

Iepriekš sagatavo sīki izstrādātus plānus klasificētas informācijas aizsardzībai ārkārtas situācijas gadījumā.

8. **DROŠĪBAS APZĪMĒJUMI, MARĶĒJUMS, PIEŠĶIRŠANA UN KLASIFIKĀCIJAS PĀRVALDĪBA**

8.1. ***Drošības apzīmējumi***

Atļauti ir tikai šā lēmuma 2. panta d) punktā minētie klasifikācijas veidi.

Lai ierobežotu klasifikācijas derīgumu (klasificētai informācijai, paredzot automātisku klasifikācijas līmeņa samazināšanu vai deklasificēšanu), var izmantot norunātus drošības apzīmējumus, par kuriem panākta vienošanās.

Drošības apzīmējumus izmanto tikai kopā ar klasifikāciju.

Drošības apzīmējumus papildus regulē drošības paziņojumā Nr. 2 un nosaka apstrādes instrukcijās.

8.2. ***Marķējums***

Marķējumu izmanto, lai norādītu uz iepriekš noteiktiem specifiskiem norādījumiem par konfidenciālas informācijas apstrādi. Ar marķējumu var arī norādīt jomu, uz ko attiecas dokumenti, īpašu izplatīšanas veidu, pamatojoties uz vajadzību pēc informācijas, vai (neklasificētai informācijai) – ierobežojuma beigas.

Marķēšana nav klasificēšana, un to nelieto klasifikācijas aizstāšanai.

Marķējumu papildus regulē drošības paziņojumā Nr. 2 un nosaka apstrādes instrukcijās.

8.3. ***Klasifikācijas piešķiršana un drošības apzīmējumi***

Klasifikāciju, drošības apzīmējumus un marķējumus piešķir saskaņā ar drošības paziņojuma Nr. 2 E nodaļu un apstrādes instrukcijām.

8.4. ***Klasificēšanas pārvaldība***

8.4.1. *Vispārējs pārskats*

Informāciju klasificē tikai tad, kad tas ir nepieciešams. Klasifikācija ir skaidra un pareizi norādīta, un to piemēro tikai tik ilgi, kamēr informācijai nepieciešama aizsardzība.

Par informācijas klasificēšanu un tās tālāku klasifikācijas līmeņa samazināšanu vai deklasificēšanu ir atbildīgs vienīgi tās sagatavotājs.

Eiropas Parlamenta ierēdņi klasificē, samazina klasifikācijas līmeni vai deklasificē informāciju pēc ģenerālsekretāra norādījuma vai ja tiem deleģēts šāds uzdevums.

Sīki izstrādātas procedūras rīcībai ar klasificētiem dokumentiem veido tā, lai nodrošinātu, ka šiem dokumentiem piemēro aizsardzību, kas atbilst tajos ietvertajai informācijai.

Personu skaitu, kurām ir atļauts izstrādāt informāciju, kas klasificēta līmenī TRÈS SECRET UE/EU TOP SECRET, pēc iespējas ierobežo un viņu vārdus ieraksta KIN sagatavotā sarakstā.

8.4.2. *Klasifikācijas piemērošana*

Dokumenta klasifikāciju nosaka pēc dokumenta satura jutības pakāpes saskaņā ar 2. panta d) punktā doto definīciju. Svarīgi, lai klasifikāciju piešķirtu pareizi un iespējami maz.

Vēstules vai piezīmes klasifikācija ar pielikumu ir tikpat augsta, kā tai pievienoto dokumentu visaugstākā klasifikācija. Sagatavotājs skaidri norāda, kāds klasifikācijas līmenis vēstulei vai piezīmei būtu piešķirams, kad tās atdala no pievienotajiem dokumentiem,

Tāda dokumenta sagatavotājs, kuram tiks piešķirta klasifikācija, ievēro iepriekš izklāstītos noteikumus un ierobežo jebkuru tendenci piešķirt augstāku vai zemāku klasifikāciju.

Atsevišķām konkrēta dokumenta lappusēm, daļām, iedaļām, pielikumiem un papildinājumiem var būt nepieciešama atšķirīga klasifikācija, un tos atbilstoši klasificē. Visa dokumenta klasifikācija atbilst tai, kāda piešķirta tā visaugstāk klasificētajai daļai.

9. **PĀRBAUDES**

Eiropas Parlamenta Drošības un riska novērtēšanas direktorāts periodiski pārbauda klasificētas informācijas aizsardzībai paredzētos drošības pasākumus, un šā uzdevuma veikšanai tas var lūgt Komisijas vai Padomes drošības iestāžu palīdzību.

Kā daļu no visu pušu ierosināta un apstiprināta procesa Savienības iestāžu drošības iestādes un kompetentie dienesti var veikt salīdzinošu novērtēšanu par drošības pasākumiem tās klasificētās informācijas aizsardzībai, kuras apmaiņa notiek saskaņā ar attiecīgajiem iestāžu nolīgumiem.

10. **DEKLASIFICĒŠANAS UN MARĶĒJUMA NOŅEMŠANAS PROCEDŪRAS**

10.1. KIN izvērtē tā reģistrā esošo konfidenciālo informāciju un lūdz dokumenta sagatavotāja piekrišanu deklasificēšanai vai marķējuma noņemšanai ne vēlāk kā 25. gadā pēc dokumenta sagatavošanas. Dokumentus, kuru klasifikācijas pakāpe nav atcelta vai marķējums nav noņemts jau pirmajā pārbaudē, pārbauda regulāri un vismaz reizi piecos gados. Marķējuma noņemšanas process var attiekties ne tikai uz dokumentiem, kuri jau atrodas drošos arhīvos drošības zonā un ir attiecīgi klasificēti, bet arī uz citu konfidenciālu informāciju, kas atrodas vai nu Parlamenta struktūras / pilnvarotās personas, vai dienestā, kas atbild par Parlamenta vēstures arhīvu.

10.2. Lēmumu par dokumenta deklasificēšanu vai marķējuma noņemšanu parasti pieņem tā sagatavotājs vai, izņēmuma kārtā, sadarbībā ar Parlamenta struktūru / pilnvaroto personu, kas ir šādas informācijas turētājs, un to veic, pirms informāciju, ko dokuments satur, nodod Parlamenta vēstures arhīvu attiecīgajam dienestam. Klasificētu informāciju var deklasificēt vai tai var noņemt marķējumu tikai ar tās sagatavotāja iepriekšēju rakstisku piekrišanu. "Citas konfidenciālas informācijas" gadījumā par marķējuma noņemšanu lemj tās Parlamenta struktūras / pilnvarotās personas sekretariāts, kas ir šādas informācijas turētājs, turklāt sadarbībā ar dokumenta sagatavotāju.

10.3. Sagatavotāja vārdā KIN atbild par dokumentam izdarīto klasifikācijas vai marķējuma izmaiņu paziņošanu adresātiem; savukārt tie atbild par izmaiņu paziņošanu citiem tālākajiem adresātiem, kuriem tie ir nosūtījuši vai nokopējuši dokumentu.

10.4. Deklasificēšana neskar drošības apzīmējumus vai marķējumus, kas var būt norādīti uz dokumenta.

10.5. Deklasificēšanas gadījumā svītro sākotnējo klasifikāciju, kas ir norādīta katras lappuses augšā un apakšā. Uz dokumenta pirmās lapas (titullapas) uzliek zīmogu un papildina ar KIN norādi. Demarķēšanas gadījumā svītro sākotnējo marķējumu, kas ir norādīts katras lappuses augšā un apakšā.

10.6. Deklasificēta vai demarķēta dokumenta tekstu pievieno elektroniskajai tematiskajai nodaļai vai atbilstīgajai sistēmai, kurā šis dokuments ir reģistrēts.

10.7. Attiecībā uz dokumentiem, kuriem saistībā ar personas privātumu vai privātas vai juridiskas personas komerciālām interesēm paredzēts izņēmums, un attiecībā uz jutīgiem dokumentiem piemēro Regulas (EEK, Euratom) Nr. 354/83 2. panta noteikumus.

10.8. Papildus 10.1. līdz 10.7. apakšpunkta noteikumiem:

a) pirms uzsākt trešo pušu dokumentu deklasificēšanu vai demarķēšanu, KIN apspriežas ar attiecīgo trešo pusi;

b) attiecībā uz izņēmumiem, kas saistās ar privātumu un indivīda neaizskaramību, deklasificēšanā vai demarķēšanā jo īpaši ņem vērā attiecīgās personas piekrišanu, vai, attiecīgā gadījumā, nespēju noteikt attiecīgo personu;

c) attiecībā uz izņēmumu, kas saistās ar kādas fiziskas vai juridiskas personas komerciālām interesēm, informāciju par attiecīgo personu var darīt zināmu, publicējot to *Eiropas Savienības Oficiālajā Vēstnesī*, un termiņš iespējamiem apsvērumiem būtu četras nedēļas pēc publicēšanas dienas.

2. daļa

DROŠĪBAS PIELAIDES IZSNIEGŠANAS PROCEDŪRA

11. **DROŠĪBAS PIELAIDES IZSNIEGŠANAS PROCEDŪRA EIROPAS PARLAMENTA DEPUTĀTIEM**

11.1. Lai varētu piekļūt informācijai, kas klasificēta līmenī CONFIDENTIEL UE / EU CONFIDENTIAL, vai tai līdzvērtīgai informācijai Eiropas Parlamenta deputātiem ir jābūt piešķirtai atļaujai vai nu saskaņā ar procedūru, kas minēta šī pielikuma 11. 3. un 11.4. punktā, vai pamatojoties uz oficiālu deklarāciju par informācijas neizpaušanu saskaņā ar šā lēmuma 3. panta 4. punktu.

11.2. Lai piekļūtu informācijai, kas klasificēta līmenī TRÈS SECRET UE/EU TOP SECRET vai SECRET UE/EU SECRET, vai tai līdzvērtīgai informācijai, Eiropas Parlamenta deputātiem jābūt piešķirtai atļaujai saskaņā ar procedūru, kas minēta 11.3. un 11.14. punktā.

11.3. Atļauju piešķir tikai tiem Eiropas Parlamenta deputātiem, kuri izturējuši dalībvalstu kompetento iestāžu veiktu drošības pārbaudi saskaņā ar procedūru, kas minēta 11.9. līdz 11.14. punktā. Par atļaujas piešķiršanu deputātiem atbild priekšsēdētājs.

11.4. Priekšsēdētājs var piešķirt rakstisku atļauju pēc dalībvalstu kompetento iestāžu atzinuma saņemšanas, pamatojoties uz drošības pārbaudi, kura ir veikta saskaņā ar 11.8. līdz 11.13. punktu.

11.5. Eiropas Parlamenta Drošības un riska novērtēšanas direktorāts uzglabā aktualizētu visu to Eiropas Parlamenta deputātu sarakstu, kuriem ir piešķirta atļauja, tostarp pagaidu atļauja saskaņā ar 11.15. punktu.

11.6. Atļauja ir derīga piecus gadus vai ne ilgāk par to pienākumu termiņu, uz kuru pamata to piešķīra (piemēro īsāko termiņu). To var pagarināt saskaņā ar 11.4. punktā noteikto procedūru.

11.7. Priekšsēdētājs atsauc atļauju, ja viņš uzskata, ka šādai atsaukšanai ir pamatoti iemesli. Ikviens lēmums atsaukt atļauju tiek darīts zināms attiecīgajam Eiropas Parlamenta deputātam, kurš pirms šā lēmuma stāšanās spēkā var lūgt, lai viņu uzklausa priekšsēdētājs un dalībvalsts kompetentā iestāde.

11.8. Drošības pārbaudi veic ar attiecīgā Eiropas Parlamenta deputāta palīdzību un pēc priekšsēdētāja pieprasījuma. Par pārbaudi ir atbildīga tās dalībvalsts kompetentā iestāde, kuras valstspiederīgais ir attiecīgais deputāts.

11.9. Veicot pārbaudes procedūru, attiecīgajam Eiropas Parlamenta deputātam pieprasa aizpildīt personas informācijas veidlapu.

11.10. Pieprasījumā dalībvalsts kompetentajām iestādēm priekšsēdētājs norāda konkrētu klasificētas informācijas līmeni, ko darīs pieejamu attiecīgajam Eiropas Parlamenta deputātam, lai tās varētu veikt pārbaudes procedūru.

11.11. Uz visu drošības pārbaudes procedūru, ko veic dalībvalstu kompetentās iestādes, kā arī uz iegūtajiem rezultātiem attiecas atbilstīgās tiesību normas, kas ir spēkā attiecīgajā dalībvalstī, tostarp tiesību normas par pārsūdzēšanu.

11.12. Ja dalībvalsts kompetentās iestādes sniedz pozitīvu atzinumu, priekšsēdētājs var piešķirt attiecīgajam Eiropas Parlamenta deputātam atļauju.

11.13. Dalībvalsts kompetento iestāžu negatīvu atzinumu dara zināmu attiecīgajam Eiropas Parlamenta deputātam, kurš var lūgt, lai viņu uzklausa priekšsēdētājs. Ja priekšsēdētājs uzskata par nepieciešamu, viņš var lūgt dalībvalsts kompetentajām iestādēm veikt papildu pārbaudi. Ja negatīvu atzinumu apstiprina, atļauju nepiešķir.

11.14. Visi Eiropas Parlamenta deputāti, kuriem ir piešķirta atļauja saskaņā ar 11.3. punktu, atļaujas piešķiršanas laikā un turpmāk regulāri saņem visu nepieciešamās norādes par klasificētas informācijas aizsargāšanu un šādas aizsardzības nodrošināšanas līdzekļiem. Deputāti paraksta deklarāciju par minēto norāžu saņemšanu.

11.15. Izņēmuma gadījumā priekšsēdētājs pēc paziņojuma nosūtīšanas dalībvalsts kompetentajai iestādei un ar noteikumu, ka minētās kompetentās iestādes mēneša laikā nav saņemta reakcija, var piešķirt Eiropas Parlamenta deputātam pagaidu atļauju uz laiku, kas nepārsniedz sešus mēnešus, līdz būs zināmi 11.11. punktā minētās pārbaudes rezultāti. Šādi piešķirtas pagaidu atļaujas nedod piekļuvi informācijai, kas klasificēta līmenī TRÈS SECRET UE/EU TOP SECRET, vai tai līdzvērtīgai informācijai.

12. DROŠĪBAS PIELAIDES IZSNIEGŠANAS PROCEDŪRA EIROPAS PARLAMENTA IERĒDŅIEM UN CITIEM PARLAMENTA DARBINIEKIEM, KURI STRĀDĀ POLITISKAJĀS GRUPĀS

12.1. Klasificētai informācijai drīkst piekļūt tikai tie Eiropas Parlamenta ierēdņi un citi politiskajās grupās strādājoši Eiropas Parlamenta darbinieki, kuriem saistībā ar to pienākumiem vai darba prasībām ir nepieciešams zināt vai izmantot šādu informāciju.

12.2. Lai piekļūtu informācijai, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL vai TRÈS SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET vai līdzvērtīgai informācijai, Eiropas Parlamenta ierēdņiem un citiem politiskajās grupās strādājošiem Eiropas Parlamenta darbiniekiem jāsaņem atļauja atbilstoši 12.3. un 12.4. punktā minētajai procedūrai.

12.3. Atļauju piešķir tikai tām 12.1. punktā minētajām personām, kuras ir pārbaudījusi dalībvalsts kompetentā iestāde saskaņā ar 12.9. līdz 12.14. punktā minēto procedūru. Par atļaujas piešķiršanu Eiropas Parlamenta ierēdņiem un citiem Eiropas Parlamenta darbiniekiem, kuri strādā politiskajās grupās, atbild ģenerālsekretārs.

12.4. Ģenerālsekretārs var piešķirt rakstisku atļauju pēc tam, kad ir saņemts dalībvalstu kompetento iestāžu atzinums, pamatojoties uz drošības pārbaudi, kura ir veikta saskaņā ar 12.8. līdz 12.13. punktu.

12.5. Eiropas Parlamenta Drošības un riska novērtēšanas direktorāts uzglabā aktualizētu visu to amatu sarakstu, kuriem ir nepieciešama drošības pielaide, ko sniedz attiecīgie Eiropas Parlamenta dienesti, un visu to personu sarakstu, kurām ir piešķirta atļauja, tostarp pagaidu atļauja saskaņā ar 12.15. punktu.

12.6. Atļauja ir derīga piecus gadus vai ne ilgāk par to pienākumu termiņu, uz kuru pamata to piešķīra (piemēro īsāko termiņu). To var pagarināt saskaņā ar šīs daļas 12.4. punktā noteikto procedūru.

12.7. Ģenerālsekretārs atsauc atļauju, ja viņš uzskata, ka šādai atsauksanai ir pamatoti iemesli. Ikviens lēmums atsaukt atļauju tiek darīts zināms attiecīgajam Parlamenta ierēdnim vai citam Parlamenta darbiniekam, kurš strādā politiskajā grupā, un šis ierēdnis vai darbinieks pirms atsaukšanas stāšanās spēkā var lūgt, lai viņu uzklausa ģenerālsekretārs un dalībvalsts kompetentā iestāde.

12.8. Drošības pārbaudi veic ar attiecīgā Parlamenta ierēdņa vai cita Parlamenta darbinieka, kurš strādā politiskajā grupā, palīdzību un pēc priekšsēdētāja pieprasījuma. Par pārbaudi ir atbildīga tās dalībvalsts kompetentā iestāde, kuras valstspiederīgais ir attiecīgā persona. Ja to paredz valsts normatīvie akti, dalībvalsts kompetentās iestādes var veikt izmeklēšanu par ārvalstniekiem, kuri pieprasa piekļūšanu informācijai, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET.

12.9. Veicot pārbaudes procedūru, attiecīgajam Eiropas Parlamenta ierēdnim vai citam Parlamenta darbiniekam, kurš strādā politiskajā grupā, pieprasa aizpildīt personas informācijas veidlapu.

12.10. Pieprasījumā dalībvalsts kompetentajām iestādēm ģenerālsekretārs norāda konkrētu klasificētas informācijas līmeni, ko darīs pieejamu attiecīgajam Eiropas Parlamenta ierēdnim vai citam Parlamenta darbiniekam, kurš strādā politiskajā grupā, lai tās varētu veikt pārbaudes procedūru un sniegt atzinumu par to, kāda līmeņa atļauju šai personai var piešķirt.

12.11. Uz visu drošības pārbaudes procedūru, ko veic dalībvalstu kompetentās iestādes, kā arī uz iegūtajiem rezultātiem attiecas atbilstīgās tiesību normas, kas ir spēkā attiecīgajā dalībvalstī, tostarp tiesību normas par pārsūdzēšanu.

12.12. Ja dalībvalsts kompetentās iestādes sniedz pozitīvu atzinumu, priekšsēdētājs var piešķirt atļauju attiecīgajam Eiropas Parlamenta ierēdnim vai citam Parlamenta darbiniekam, kurš strādā politiskajā grupā.

12.13. Dalībvalsts kompetento iestāžu negatīvu atzinumu dara zināmu attiecīgajam Eiropas Parlamenta ierēdnim vai Parlamenta darbiniekam, kurš strādā politiskajā grupā, un šis ierēdnis vai darbinieks var lūgt, lai viņu uzklausa ģenerālsekretārs. Ja ģenerālsekretārs uzskata par nepieciešamu, viņš var lūgt dalībvalsts kompetentajām iestādēm veikt papildu pārbaudi. Ja negatīvu atzinumu apstiprina, atļauju nepiešķir.

12.14. Visi Eiropas Parlamenta ierēdņi un citi Parlamenta darbinieki, kuri strādā politiskajās grupās un kuriem ir piešķirta atļauja saskaņā ar 12.4. un 12.5. punktu, atļaujas piešķiršanas laikā un turpmāk regulāri saņem visas nepieciešamās instrukcijas par klasificētas informācijas aizsargāšanu un šādas aizsardzības nodrošināšanas līdzekļiem. Šādi ierēdņi un darbinieki paraksta deklarāciju par minēto instrukciju saņemšanu un uzņemas saistības tās ievērot.

12.15. Izņēmuma gadījumā ģenerālsekretārs pēc paziņojuma nosūtīšanas dalībvalsts kompetentajai iestādei un ar noteikumu, ka no minētās kompetentās iestādes mēneša laikā nav saņemta reakcija, var piešķirt Eiropas Parlamenta ierēdnim vai citam Parlamenta darbiniekam, kurš strādā poliskajā grupā, pagaidu atļauju uz laiku, kas nepārsniedz sešus mēnešus, līdz būs zināmi 12.11. punktā minētās pārbaudes rezultāti. Šādi piešķirtās pagaidu atļaujas nedod piekļuvi informācijai, kas klasificēta līmenī TRÈS SECRET UE/EU TOP SECRET, vai tai līdzvērtīgai informācijai.

II PIELIKUMS

IEVADS

Šajos noteikumos ir paredzēti drošības paziņojumi, ar kuriem nosaka un nodrošina drošu konfidenciālas informācijas apstrādi un pārvaldību Eiropas Parlamentā. Minētie drošības paziņojumi kopā ar apstrādes instrukcijām veido šā lēmuma 3. panta 2. punktā minēto Eiropas Parlamenta informācijas drošības pārvaldības sistēmu (IDPS):

DROŠĪBAS PAZIŅOJUMS Nr. 1

Drošības organizēšana Eiropas Parlamentā konfidenciālas informācijas aizsardzībai

DROŠĪBAS PAZIŅOJUMS Nr. 2

Konfidenciālas informācijas pārvaldība

DROŠĪBAS PAZIŅOJUMS Nr. 3

Konfidenciālas informācijas apstrāde, izmantojot automatizētas komunikāciju informācijas sistēmas (KIS)

DROŠĪBAS PAZIŅOJUMS Nr. 4

Fiziskā drošība

DROŠĪBAS PAZIŅOJUMS Nr. 5

Industriālā drošība

DROŠĪBAS PAZIŅOJUMS Nr. 6

Drošības pārkāpumi attiecībā uz konfidenciālu informāciju, tās zudums vai apdraudēšana

DROŠĪBAS PAZIŅOJUMS Nr. 1

DROŠĪBAS ORGANIZĒŠANA EIROPAS PARLAMENTĀ KONFIDENCIĀLAS INFORMĀCIJAS AIZSARDZĪBAI

1. Ģenerālsekretārs ir atbildīgs par šā lēmuma vispārēju un konsekventu īstenošanu.

Ģenerālsekretārs veic visus pasākumus, kas vajadzīgi, lai nodrošinātu, ka, strādājot ar konfidenciālu informāciju vai glabājot to, Eiropas Parlamenta deputāti, tā ierēdņi, citi Parlamenta darbinieki, kas strādā politiskajās grupās, un līgumdarbinieki piemēro šo lēmumu Parlamenta telpās.

2. Ģenerālsekretārs veic drošības iestādes (DI) funkcijas. Šajā statusā ģenerālsekretārs ir atbildīgs par:

2.1. visu tādu drošības jautājumu koordinēšanu, kas saistīti ar Parlamenta darbību konfidenciālas informācijas aizsardzības jomā;

2.2. drošības zonas un drošu lasītavu ierīkošanas un droša aprīkojuma uzstādīšanas apstiprināšanu;

2.3. tādu lēmumu īstenošanu, ar kuriem saskaņā ar šā lēmuma 6. pantu Eiropas Parlamentam ir atļauts klasificētu informāciju nosūtīt trešām pusēm;

2.4. visu konfidenciālas informācijas noplūžu, kas saskaņā ar sākotnējiem pierādījumiem ir notikušas Parlamentā, izmeklēšanu vai izmeklēšanas pasūtīšanu – sadarbībā ar Eiropas Parlamenta priekšsēdētāju, ja ir skarts Eiropas Parlamenta deputāts;

2.5. ciešas saziņas nodrošināšanu ar citu Savienības iestāžu un aģentūru drošības iestādēm un dalībvalstu drošības iestādēm, lai nodrošinātu ar klasificētu informāciju saistītās drošības politikas optimālu koordināciju;

2.6. Parlamenta drošības politikas un procedūru pastāvīgu pārskatīšanu un no tās izrietošo attiecīgo ieteikumu sniegšanu;

2.7. tās attiecīgās valsts drošības iestādes (VDI) informēšanu, kura veikusi drošības pārbaudi saskaņā ar I pielikuma 2. daļas 11.3. punktu gadījumos, kad ir zināma jebkāda negatīva informācija, kas varētu skart attiecīgo iestādi.

3. Ja ir skarts Eiropas Parlamenta deputāts, ģenerālsekretārs veic savus uzdevumus, cieši sadarbojoties ar Eiropas Parlamenta priekšsēdētāju.

4. Ģenerālsekretāram 2. un 3. punktā minētos pasākumus palīdz veikt ģenerālsekretāra vietnieks, Drošības un riska novērtēšanas direktorāts, Informācijas tehnoloģiju direktorāts (ITD) un Klasificētās informācijas nodaļa (KIN).

4.1. Drošības un riska novērtēšanas direktorāts ir atbildīgs par individuālajiem aizsardzības pasākumiem un jo īpaši par I pielikuma 2. daļā paredzēto drošības pielaides izsniegšanas procedūru. Drošības un riska novērtēšanas direktorāts arī:

a) kalpo par kontaktpunktu citu Savienības iestāžu un aģentūru drošības iestādēm un dalībvalstu drošības iestādēm attiecībā uz jautājumiem, kas saistīti ar procedūru drošības pielaides izsniegšanai Eiropas Parlamenta deputātiem, tā ierēdņiem un citiem Parlamenta darbiniekiem, kas strādā politiskajās grupās;

b) sniedz vajadzīgo ar vispārējo drošību saistītu informāciju par pienākumiem aizsargāt klasificētu informāciju un par to, kādas būs sekas, ja tas netiks veikts;

c) uzrauga Parlamenta telpās esošās drošības zonas un drošu lasītavu darbību, attiecīgā gadījumā sadarbojoties ar citu Savienības iestāžu un dalībvalstu drošības dienestiem;

d) sadarbībā ar citu Savienības iestāžu un dalībvalstu drošības dienestiem veic klasificētas informācijas pārvaldības un glabāšanas procedūru revīzijas un pārbauda Parlamenta telpās esošo drošības zonu un drošās lasītavas, kurās notiek klasificētas informācijas apstrāde;

e) ierosina ģenerālsekretāram nepieciešamās apstrādes instrukcijas.

4.2. ITD ir atbildīgs par konfidenciālas informācijas apstrādi Eiropas Parlamentā, izmantojot drošas IT sistēmas.

4.3. KIN ir atbildīga par:

a) drošības vajadzību noteikšanu efektīvai konfidenciālas informācijas aizsardzībai, cieši sadarbojoties ar Drošības un riska novērtējuma ģenerāldirektorātu un ITD un citu Savienības iestāžu drošības dienestiem;

b) visu aspektu noteikšanu attiecībā uz konfidenciālas informācijas pārvaldību un glabāšanu Parlamentā, kā paredzēts apstrādes instrukcijās;

c) drošības zonas darbību;

d) konfidenciālas informācijas pārvaldību vai iepazīšanos ar to drošības zonā vai KIN drošajā lasītavā saskaņā ar šā lēmuma 7. panta 2. un 3. punktu;

e) KIN reģistra pārvaldību;

f) ziņošanu DI par jebkuriem pierādītiem vai iespējamiem drošības pārkāpumiem, zudumu vai apdraudējumu saistībā ar konfidenciālu informāciju, kas nodota KIN un tiek glabāta drošības zonā vai KIN drošajā lasītavā;

5. Turklāt ģenerālsekretārs, veicot drošības iestādes funkcijas, ieceļ šādas iestādes:

a) drošības akreditācijas iestādi (DAI);

b) informācijas aizsardzības operatīvo iestādi (IAOI);

c) kriptogrāfijas izplatīšanas iestādi (KII);

d) TEMPEST iestādi (TI);

e) informācijas aizsardzības iestādi (IAI);

Minēto funkciju īstenošanai nav vajadzīgas vienotas organizatoriskas vienības. Tām ir atsevišķas pilnvaras. Tomēr šīs funkcijas un ar tām saistītos pienākumus var apvienot vai integrēt vienā organizatoriskajā vienībā vai sadalīt dažādās organizatoriskās vienībās ar noteikumu, ka nerodas interešu konflikti un uzdevumu dublēšanās.

6. Drošības akreditācijas iestāde konsultē par visiem drošības jautājumiem saistībā ar katras Parlamenta informācijas tehnoloģiju sistēmas un tīkla akreditāciju:

6.1. nodrošinot, ka KIS atbilst attiecīgajai drošības politikai un drošības pamatnostādnēm, sniedzot paziņojumus par to, ka KIS ir apstiprinātas savā ekspluatācijas vidē apstrādāt klasificētu informāciju līdz konkrētam klasifikācijas līmenim un norādot akreditācijas noteikumus un kritērijus, pēc kuriem nosaka vajadzību veikt atkārotu apstiprināšanu;

6.2. izstrādājot drošības akreditācijas procesu atbilstīgi attiecīgajai politikai, skaidri nosakot apstiprināšanas noteikumus KIS, par ko tā ir atbildīga;

6.3. izstrādājot drošības akreditācijas stratēģiju, kurā izklāsta akreditācijas procesa sarežģītības pakāpi, kas ir samērīga ar vajadzīgo aizsardzības līmeni;

6.4. izvērtējot un apstiprinot ar drošību saistītu dokumentāciju, tostarp riska pārvaldību un paziņojumus par neapzinātu apdraudējumu, drošības īstenošanas pārbaudes dokumentus un drošības darba procedūras, un nodrošinot, ka tas atbilst Parlamenta drošības noteikumiem un politikai;

6.5. pārbaudot, kā tiek īstenoti ar KIS saistīti drošības pasākumi, šajā nolūkā veicot vai atbalstot drošības novērtējumus, pārbaudes vai pārskatus;

6.6. nosakot ar KIS saistītas drošības prasības (piemēram, personāla pielaides līmeņus) palielināta riska amatos;

6.7. apstiprinot konkrētas KIS savstarpēju savienošanu ar citām KIS vai attiecīgā gadījumā piedaloties to kopīgā apstiprināšanā;

6.8. apstiprinot tāda tehniskā aprīkojuma drošības standartus, kas paredzēts drošai klasificētas informācijas apstrādei un aizsardzībai;

6.9. nodrošinot, ka Eiropas Parlamentā izmantotie kriptogrāfijas produkti ir iekļauti ES apstiprināto produktu sarakstā, un

6.10. sniedzot konsultācijas sistēmas nodrošinātājam, drošības sistēmas dalībniekiem un lietotāju pārstāvjiem attiecībā uz drošības riska pārvaldību, jo īpaši par neapzinātu apdraudējumu, un apstiprināšanas paziņojuma noteikumiem.

7. IAOI ir atbildīga par:

7.1. drošības dokumentācijas izstrāde saskaņā ar drošības politiku un drošības pamatnostādnēm, jo īpaši iekļaujot paziņojumu par neapzinātu apdraudējumu, drošības darba procedūras un kriptogrāfijas plānu saistībā ar KIS akreditācijas procesu;

7.2. dalība katrai sistēmai īpašu tehnisku drošības pasākumu, iekārtu un programmatūras izvēlē un pārbaudē, to īstenošanas uzraudzība un to drošas instalēšanas, konfigurēšanas un uzturēšanas nodrošināšana atbilstīgi attiecīgajiem drošības dokumentiem;

7.3. drošības darba procedūru īstenošanas un piemērošanas uzraudzība un – attiecīgā gadījumā – atbildības par operatīvo drošību deleģēšana sistēmas īpašniekam, proti, KIN;

7.4. kriptogrāfijas produktu pārvaldība un darbības ar tiem, nodrošinot šifrētu un kontrolētu materiālu uzraudzību, un vajadzības gadījumā kriptogrāfisku mainīgo veidošanas nodrošināšana;

7.5. drošības analīzes pārskatīšanas un pārbaužu veikšana, jo īpaši nolūkā sagatavot vajadzīgos apdraudējuma ziņojumus, kādus pieprasa DAI;

7.6. apmācības nodrošināšana saistībā ar elektroniskas klasificētas informācijas aizsardzību attiecībā uz katru KIS;

7.7. drošības pasākumu īstenošana un izpilde attiecībā uz katru KIS.

8. Kriptogrāfijas izplatīšanas iestāde (KII) ir atbildīga par šādiem jautājumiem:

8.1. ES kriptogrāfiskā materiāla pārvaldība un uzskaite;

8.2. ciešā sadarbībā ar DAI nodrošināt atbilstīgu procedūru izpildi un to, ka ir izveidoti plāni ES kriptogrāfiskā materiāla uzskaitei, drošai apstrādei, glabāšanai un izplatīšanai, un

8.3. ES kriptogrāfiskā materiāla nosūtīšana atsevišķām personām vai dienestiem, kas tos izmanto, vai minēto materiālu saņemšana no tiem.

9. TI atbild par to, lai nodrošinātu KIS atbilstību TEMPEST politikai un apstrādes instrukcijām. Tā apstiprina TEMPEST pretpasākumus iekārtām un produktiem, lai aizsargātu klasificētu informāciju līdz noteiktam klasifikācijas līmenim tās ekspluatācijas vidē.

10. IAI atbild par visiem aspektiem saistībā ar konfidenciālas informācijas pārvaldību un apstrādi Parlamentā un jo īpaši par šādiem uzdevumiem:

10.1 izstrādāt informācijas aizsardzības nodrošināšanas politiku un tās drošības pamatnostādnes un uzraudzīt to efektivitāti un piemērotību;

10.2. nodrošināt un administrēt ar kriptogrāfijas produktiem saistīto tehnisko informāciju;

10.3. nodrošināt, ka informācijas aizsardzības pasākumi, kas izraudzīti klasificētas informācijas aizsardzībai, atbilst attiecīgajai politikai, kas nosaka to atbilstību un atlasi;

10.4. nodrošināt, ka kriptogrāfijas produktus izraugās saskaņā ar politiku, kas nosaka to atbilstību un atlasi;

10.5. konsultēties ar sistēmas nodrošinātāju, drošības dalībniekiem un lietotāju pārstāvjiem par informācijas aizsardzības drošību;

DROŠĪBAS PAZIŅOJUMS Nr. 2

KONFIDENCIĀLAS INFORMĀCIJAS PĀRVALDĪBA

A. **IEVADS**

1. Šajā drošības paziņojumā ir izklāstīti noteikumi par to, kā Parlamentā pārvaldīt konfidenciālo informāciju.

2. Izstrādājot konfidenciālu informāciju, sagatavotājs izvērtē konfidencialitātes līmeni un, pamatojoties uz šajā drošības paziņojumā izklāstītajiem principiem, pieņem lēmumu par minētās informācijas klasificēšanu vai marķēšanu.

B. **ESKI KLASIFIKĀCIJA**

3. Lēmumu par dokumenta klasifikāciju pieņem pirms tā izstrādes. Tādēļ informācijas klasificēšana kā ESKI ietver iepriekšēju novērtējumu par šādas informācijas konfidencialitātes līmeni un sagatavotāja lēmumu par to, ka šādas informācijas neatļauta izpaušana varētu radīt dažādas pakāpes kaitējumu Eiropas Savienības, vienas vai vairāku dalībvalstu vai privātpersonu interesēm.

4. Tiklīdz tiek pieņemts lēmums par informācijas klasificēšanu, tiek veikts otrs iepriekšējs novērtējums, lai noteiktu atbilstīgo klasifikācijas līmeni. Dokumenta klasifikāciju nosaka pēc tā satura jutības pakāpes.

5. Par informācijas klasificēšanu ir atbildīgs vienīgi tās sagatavotājs. Parlamenta ierēdņi klasificē informāciju pēc ģenerālsekretāra norādījuma vai saskaņā ar viņa deleģējumu.

6. Klasificēšanu izmanto pareizi un ierobežoti. Tāda dokumenta sagatavotājs, kuram tiks piešķirta klasifikācija, ierobežo jebkuru tendenci piešķirt augstāku vai zemāku klasifikāciju.

7. No informācijai piešķirtā klasifikācijas līmeņa ir atkarīgs šai informācijai piešķirtais drošības līmenis personāla drošības, fiziskās drošības, procedūras drošības un informācijas aizsardzības jomā.

8. Informāciju, kurai ir vajadzīga klasifikācija, marķē un ar to attiecīgi rīkojas kā ar klasificētu informāciju neatkarīgi no informācijas fiziskās formas. Informācijas klasifikāciju skaidri dara zināmu tās saņēmējiem, vai nu izmantojot klasifikācijas marķējumu (ja tā sniegta rakstiski – uz papīra vai ar KIS starpniecību), vai paziņojumu (ja tā sniegta mutiski, piemēram sarunā vai sanāksmē aiz slēgtām durvīm). Klasificētus materiālus fiziski marķē, lai varētu viegli identificēt to drošības klasifikācijas līmeni.

9. ESKI elektroniskā formā var izstrādāt, tikai izmantojot akreditētu KIS. Gan klasificētajai informācijai, gan datnes nosaukumam un datu nesējam (ja tas ir ārējs, kā, piemēram, CD-ROM vai USB atmiņas karte) ir jābūt marķētam ar attiecīgo drošības klasifikācijas marķējumu.

10. Informāciju klasificē jau tās formulēšanas stadijā. Piemēram, personīgas piezīmes, dokumentu projektus vai e-pasta sūtījumus, kas satur informāciju, kuru nepieciešams klasificēt, marķē kā ESKI jau no sākuma, un tos izstrādā un ar tiem rīkojas saskaņā ar šo lēmumu un tās apstrādes instrukcijām fiziskās un tehniskās aizsardzības ziņā. Šāda informācija var vēlāk pārtapt par oficiālu dokumentu, kas savukārt tiks pienācīgi marķēts un apstrādāts. Izstrādes procesa laikā oficiāls dokuments, iespējams, ir vēlreiz jāizvērtē un, mainoties tā saturam, tam ir jāpiešķir augstāka vai zemāka klasifikācijas pakāpe.

11. Sagatavotājs var pieņemt lēmumu piešķirt standarta klasifikācijas līmeni tādas informācijas kategorijām, ko tas regulāri izstrādā. Tomēr sagatavotājam ir jānodrošina, lai, to darot, atsevišķām informācijas vienībām sistemātiski nepiešķirtu pārāk augstu vai pārāk zemu klasifikācijas līmeni.

12. ESKI ir vienmēr jābūt apzīmētai ar drošības klasifikācijas marķējumu, kas atbilst tās drošības klasifikācijas līmenim.

B.1. ***Klasifikācijas līmeņi***

13. ESKI piešķir kādu no šiem klasifikācijas līmeņiem:

— TRÈS SECRET UE/EU TOP SECRET, kā definēts šā lēmuma 2. panta d) punktā, ja šādas informācijas apdraudējums varētu:

a) tieši apdraudēt Savienības, vienas vai vairāku tās dalībvalstu, trešo valstu vai starptautisku organizāciju iekšējo stabilitāti;

b) ārkārtīgi smagi kaitēt attiecībām ar trešām valstīm vai starptautiskām organizācijām;

c) tieši izraisīt daudzu cilvēku bojāeju;

d) ārkārtīgi smagi kaitēt dalībvalstu vai citu dalībnieku norīkotā personāla darbību efektivitātei vai drošībai, vai ārkārtīgi vērtīgu drošības vai izlūkošanas darbību nepārtrauktai efektivitātei;

e) izraisīt nopietnu ilglaicīgu kaitējumu Savienības vai dalībvalstu ekonomikai;

— SECRET UE/EU SECRET, kā definēts šā lēmuma 2. panta d) punktā, ja šādas informācijas apdraudējums varētu:

a) radīt ievērojamu starptautisku saspīlējumu;

b) nopietni kaitēt attiecībām ar trešām valstīm un starptautiskām organizācijām;

c) tieši apdraudēt cilvēku dzīvību vai nopietni ietekmēt sabiedrisko kārtību vai personas drošību un brīvību;

d) kaitēt būtiskām tirdzniecības vai politiskajām sarunām, tādējādi radot Savienībai vai tās dalībvalstīm ievērojamas darbības problēmas;

e) izraisīt nopietnu kaitējumu dalībvalstu operatīvajai drošībai, vai ārkārtīgi vērtīgu drošības vai izlūkošanas darbību efektivitātei;

f) izraisīt būtisku materiālu kaitējumu Savienības vai dalībvalsts finansiālajām, monetārajām, ekonomiskajām un komerciālajām interesēm;

g) būtiski apdraudēt nozīmīgu organizāciju vai uzņēmumu finansiālo stabilitāti; vai

h) būtiski kavēt tādu Savienības politikas jomu izstrādi un īstenošanu, kas būtiski ietekmē ekonomiku, tirdzniecību vai finanses;

— CONFIDENTIEL UE/EU CONFIDENTIAL, kā definēts šā lēmuma 2. panta d) punktā, ja šādas informācijas apdraudējums varētu:

a) būtiski kaitēt diplomātiskajām attiecībām, t.i., ja tas izraisītu oficiālus protestus vai citas sankcijas;

b) apdraudēt personas drošību vai brīvību;

c) būtiski apdraudēt tirdzniecības vai politisko sarunu rezultātus un radīt Savienībai vai dalībvalstīm darbības problēmas;

d) kaitēt dalībvalstu operatīvajai drošībai vai drošības vai izlūkošanas darbību efektivitātei;

e) būtiski apdraudēt nozīmīgu organizāciju vai uzņēmumu finansiālo stabilitāti;

f) kavēt izmeklēšanu vai atvieglot noziegumu izdarīšanu vai terora aktu īstenošanu;

g) būtiski kaitēt Savienības vai dalībvalstu finansiālajām, monetārajām, ekonomiskajām un komerciālajām interesēm; vai

h) būtiski kavēt tādu Savienības politikas jomu izstrādi un īstenošanu, kas būtiski ietekmē ekonomiku, tirdzniecību vai finanses;

— RESTREINT UE/EU RESTRICTED, kā definēts šā lēmuma 2. panta d) punktā, ja šādas informācijas apdraudējums varētu:

a) būt nevēlama Savienības vispārējām interesēm;

b) negatīvi ietekmēt diplomātiskās attiecības;

c) ievērojami apdraudēt personas vai uzņēmumus;

d) radīt neizdevīgus apstākļus Savienībai vai dalībvalstīm tirdzniecības vai politikas sarunās;

e) sarežģīt efektīva drošības līmeņa saglabāšanu Savienībā vai dalībvalstīs;

f) kavēt ES politikas efektīvu izstrādi vai īstenošanu;

g) apdraudēt pienācīgu Savienības un tās darbību pārvaldību;

h) pārkāpt saistības, ko Parlaments uzņēmies, lai nodrošinātu klasificētas informācijas statusu trešo personu sniegtai informācijai;

i) pārkāpt likumiskus informācijas izpaušanas ierobežojumus;

j) radīt finansiālus zaudējumus vai veicināt nelikumīgus ieguvumus vai priekšrocības personām vai uzņēmumiem; vai

k) kavēt izmeklēšanu vai atvieglot noziegumu izdarīšanu.

B.2. ***Kompilāciju, titullapu un fragmentu klasifikācija***

14. Vēstules vai piezīmes klasifikācijas līmenis ir tikpat augsts, cik tai pievienoto dokumentu visaugstākais klasifikācijas līmenis. Sagatavotājs skaidri norāda, kāds klasifikācijas līmenis jāpiešķir vēstulei vai piezīmei, kad to atdala no tai pievienotajiem dokumentiem. Ja pavadvēstule vai piezīme nav jāklasificē, tajā iekļauj šādu noslēguma frāzi: "Ja šī pavadvēstule vai piezīme ir atdalīta no tai pievienotajiem dokumentiem, to neklasificē".

15. Dokumentus vai lietas, kas ietver daļas ar dažādiem klasifikācijas līmeņiem, pēc iespējas jāveido tā, lai daļas ar dažādiem klasifikācijas līmeņiem varētu viegli identificēt un vajadzības gadījumā atdalīt. Vispārējais dokumenta vai lietas klasifikācijas līmenis ir vismaz tikpat augsts, cik tā daļai ar visaugstāko klasifikācijas līmeni.

16. Atsevišķām konkrēta dokumenta lappusēm, daļām, iedaļām, pielikumiem un papildinājumiem var būt nepieciešams atšķirīgs klasifikācijas līmenis, un tos atbilstoši klasificē. Dokumentos, kuros ir ESKI, var izmantot standarta saīsinājumus, lai norādītu tāda teksta iedaļu vai nodaļu klasifikācijas līmeni, kas ir mazāks par vienu lapu.

17. Apkopojot informāciju no dažādiem avotiem, galaproduktu pārskata, lai noteiktu tā vispārējo drošības klasifikācijas līmeni, jo tam, iespējams, ir jāpiešķir augstāks klasifikācijas līmenis nekā tā atsevišķām sastāvdaļām.

C. **CITA KONFIDENCIĀLA INFORMĀCIJA**

18. Citu konfidenciālu informāciju marķē atbilstīgi šā drošības paziņojuma E punktam un apstrādes instrukcijām.

D. **KONFIDENCIĀLAS INFORMĀCIJAS IZSTRĀDE**

19. Konfidenciālu informāciju drīkst izstrādāt tikai personas, kuras ir atbilstīgi pilnvarotas ar šo lēmumu vai kurām to atļāvusi drošības iestāde.

20. Konfidenciālu informāciju neievieto internetā vai iekštīkla dokumentu pārvaldības sistēmās.

D.1. ***ESKI izstrāde***

21. Lai izstrādātu ESKI, kas klasificēta līmeni CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET, attiecīgā persona ir pilnvarota saskaņā ar šo lēmumu vai arī tai jau ir atļauja, kas piešķirta saskaņā ar šā lēmuma 4. panta 1. punktu.

22. ESKI, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET, izstrādā tikai drošības zonā.

23. ESKI izstrādei piemēro šādus noteikumus:

a) katru lappusi skaidri marķē atbilstīgi piemērotajam klasifikācijas līmenim;

b) katru lappusi numurē, norādot kopējo lappušu skaitu;

c) dokumenta pirmajā lappusē norāda atsauces numuru un tematu, kurš pats par sevi nav klasificēta informācija, ja vien tas nav marķēts kā klasificēta informācija;

d) dokumenta pirmajā lappusē norāda datumu;

e) jebkura tāda dokumenta pirmajā lappusē, kas klasificēts līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET, norāda visu pielikumu un papildinājumu sarakstu;

f) dokumentiem, kas klasificēti līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET, katrā lappusē norāda kopijas numuru, ja tos izplata vairākos eksemplāros. Katras kopijas pirmajā lappusē norāda arī kopējo kopiju un lappušu skaitu un

g) ja dokumentā ir atsauce uz citiem dokumentiem, kas ietver klasificētu informāciju, kura saņemta no citām Savienības iestādēm, vai ja tas ietver klasificētu informāciju, kas iegūta no šiem dokumentiem, – tajā norāda to pašu klasifikācijas līmeni, kāds ir minētajiem dokumentiem, un šo dokumentu bez tā sagatavotāja iepriekšējas rakstiskas atļaujas drīkst izplatīt tikai tām personām, kuras ir minētas izplatīšanas sarakstā attiecībā uz oriģināldokumentu(-iem), kas satur klasificētu informāciju.

24. Sagatavotājs saglabā kontroli attiecībā uz paša izstrādāto ESKI. Sagatavotāja iepriekšēja rakstiska atļauja ir vajadzīga, pirms ESKI:

a) klasificē zemākā līmenī vai deklasificē;

b) izmanto mērķiem, kurus sagatavotājs nav noteicis;

c) atklāj kādai trešai valstij vai starptautiskai organizācijai;

d) atklāj jebkurai personai, iestādei, valstij vai starptautiskai organizācijai, kas nav adresāti, kuriem sagatavotājs sākotnēji ir atļāvis iepazīties ar attiecīgo informāciju;

e) atklāj līgumslēdzējam vai iespējamam līgumslēdzējam, kas atrodas trešā valstī;

f) kopē vai tulko – ja informācija ir klasificēta līmenī TRES SECRET UE/EU TOP SECRET;

g) iznīcina.

D.2. ***Citas konfidenciālas informācijas izstrāde***

25. Ģenerālsekretārs kā drošības iestāde var lemt par to, vai atļaut konkrētajai amatpersonai, dienestam un/vai personai izstrādāt citu konfidenciālu informāciju.

26. Citai konfidenciālai informācijai piemēro vienu no apstrādes instrukcijās minētajiem marķējumiem.

27. Citas konfidenciālas informācijas izstrādei piemēro šādus noteikumus:

a) tās marķējumu norāda dokumenta pirmās lappuses augšā;

b) katru lappusi numurē, norādot kopējo lappušu skaitu;

c) dokumenta pirmajā lappusē norāda atsauces numuru un tematu;

d) dokumenta pirmajā lappusē norāda datumu, un

e) dokumenta pēdējā lappusē norāda visu pielikumu un papildinājumu sarakstu.

28. "Citas konfidenciālas informācijas izstrādi" nosaka īpaši noteikumi un procedūras, kas paredzēti apstrādes instrukcijās.

E. **DROŠĪBAS APZĪMĒJUMI UN MARĶĒJUMI**

29. Drošības apzīmējumi un marķējumi uz dokumentiem ir paredzēti, lai kontrolētu informācijas plūsmu un ierobežotu piekļuvi konfidenciālai informācijai, pamatojoties uz principu "vajadzība pēc informācijas".

30. Izmantojot vai piestiprinot drošības apzīmējumus un/vai marķējumus, cenšas novērst pārpratumus attiecībā uz ESKI drošības klasifikāciju: RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRES SECRET UE/EU TOP SECRET .

31. Apstrādes instrukcijās nosaka konkrētus noteikumus par drošības apzīmējumu un marķējumu izmantošanu, kā arī Eiropas Parlamenta apstiprinātos drošības marķējumus.

E.1. ***Drošības apzīmējumi***

32. Drošības apzīmējumus var izmantot tikai kopā ar drošības klasifikāciju, un dokumentiem tos atsevišķi nepiemēro. Drošības apzīmējumu var piemērot ESKI, lai:

a) ierobežotu klasifikācijas derīgumu (klasificētai informācijai, kas paredz automātisku klasifikācijas līmeņa pazemināšanu vai deklasificēšanu);

b) ierobežotu attiecīgās ESKI izplatīšanu;

c) noteiktu īpašu apstrādes kārtību papildus tai, kas atbilst attiecīgajam drošības klasifikācijas līmenim.

33. Papildu kontrole, ko piemēro ESKI saturošu dokumentu apstrādei un glabāšanai, rada papildu slogu visām iesaistītajām pusēm. Lai šajā sakarībā samazinātu nepieciešamā darba apjomu, izstrādājot šādu dokumentu, laba prakse ir noteikt termiņu vai notikumu, pēc kura klasificēšanai automātiski jābeidzas un dokumentā ietvertā informācijā jāklasificē zemākā līmenī vai jādeklasificē.

34. Ja dokuments ietver informāciju par konkrētu darba jomu un tā izplatīšana ir jāierobežo, un/vai tai ir jāpiemēro īpaši apstrādes noteikumi, paziņojumu par to var pievienot dokumenta klasifikācijai, lai palīdzētu noteikt mērķauditoriju.

E.2. ***Marķējums***

35. Marķējumi nav drošības klasifikācija. Marķējumi ir paredzēti, tikai lai sniegtu konkrētas instrukcijas par dokumenta apstrādi, un tos neizmanto šāda dokumenta satura aprakstam.

36. Marķējumu var piemērot dokumentiem atsevišķi vai kopā ar drošības klasifikāciju.

37. Parasti marķējumus piemēro informācijai, uz kuru attiecas dienesta noslēpums kā minēts LESD 339. pantā un Civildienesta noteikumu 17. pantā, vai informācijai, kas jāaizsargā Parlamenta juridisku apsvērumu dēļ, bet kuru nav nepieciešams vai kuru nevar klasificēt.

E.3. ***Marķējumu izmantošana KIS***

38. Noteikumus par marķējumu izmantošanu piemēro arī akreditētās KIS.

39. DAI izveido īpašus noteikumus par marķējumu izmantošanu akreditētās KIS.

F. **INFORMĀCIJAS SAŅEMŠANA**

40. Parlamentā tikai KIN ir tiesīga no trešām pusēm pieņemt informāciju, kas klasificēta kā CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai tai līdzvērtīga līmeņa informācija.

41. Attiecībā uz informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED vai tai līdzvērtīga informācija, un citu konfidenciālu informāciju gan KIN, gan kompetentā Parlamenta struktūra/pilnvarotā persona var būt atbildīga par tās pieņemšanu no trešām pusēm un šajā drošības paziņojumā paredzēto principu piemērošanu.

G. **REĢISTRĀCIJA**

42. Reģistrācija ir tādu procedūru piemērošana, kas reģistrē konfidenciālas informācijas aprites ciklu, tostarp tās izplatīšanu, iepazīšanos ar to un iznīcināšanu.

43. Šajā drošības paziņojumā "reģistrācijas žurnāls" ir reģistrs, kurā jo īpaši iegrāmato datumu un laiku, kad:

a) konfidenciālu informāciju saņem vai nosūta attiecīgās Parlamenta struktūras / pilnvarotās personas sekretariāts vai attiecīgā gadījumā KIN;

b) konfidenciālai informācijai piekļūst vai to saņem persona, kurai ir drošības pielaide, un

c) konfidenciālu informāciju iznīcina.

44. Klasificētas informācijas sagatavotājs ir atbildīgs par to, lai šādu informāciju saturoša dokumenta izstrādē tiktu marķēta sākotnējā deklarācija. Pēc dokumenta izstrādes minēto deklarāciju nodod KIN.

45. Drošības nolūkā informāciju, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai tai līdzvērtīgu informāciju var reģistrēt tikai KIN. Administratīviem mērķiem informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED vai līdzvērtīgu informāciju, un no trešām pusēm saņemtu "citu konfidenciālu informāciju" reģistrē dienests, kas ir oficiāli saņēmis attiecīgo dokumentu, proti, vai nu KIN, vai attiecīgās Parlamenta struktūras / pilnvarotās personas sekretariāts. Administratīviem mērķiem citu konfidenciālu informāciju, kas izstrādāta Parlamentā, reģistrē tā sagatavotājs.

46. Informāciju, kas klasificēta kā CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai tai līdzvērtīgu informāciju jo īpaši reģistrē šādos gadījumos:

a) kad to izstrādā;

b) kad to saņem vai nosūta KIN un

c) kad to saņem vai nosūta KIS.

47. Informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED vai tai līdzvērtīgu informāciju jo īpaši reģistrē šādos gadījumos:

a) kad to izstrādā;

b) kad to saņem vai nosūta attiecīgais Parlamenta struktūras / pilnvarotās personas sekretariāts vai KIN un

c) kad to saņem vai nosūta KIS.

48. Konfidenciālas informācijas reģistrāciju veic uz papīra vai elektroniskos reģistrācijas žurnālos / KIS.

49. Attiecībā uz informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai līdzvērtīgu informāciju un citu konfidenciālu informāciju reģistrē vismaz šādus datus:

a) datumu un laiku, kad to saņem vai nosūta attiecīgais Parlamenta struktūras / pilnvarotās personas sekretariāts vai attiecīgā gadījumā KIN;

b) dokumenta virsrakstu, klasifikācijas līmeni vai marķējumu, klasifikācijas / marķējuma derīguma termiņu un dokumentam piešķirto atsauces numuru.

50. Attiecībā uz informāciju, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai tai līdzvērtīgu informāciju reģistrē vismaz šādus datus:

a) datumu un laiku, kad to saņem vai nosūta KIN;

b) dokumenta virsrakstu, klasifikācijas līmeni vai marķējumu, dokumentam piešķirto atsauces numuru, kā arī klasifikācijas / marķējuma derīguma termiņu;

c) ziņas par sagatavotāju;

d) pārskatu par to personu identitāti, kam ir dota piekļuve dokumentam, un laikiem, kad minētā persona tam piekļuvusi;

e) pārskatu par dokumenta kopijām vai tulkojumiem;

f) datumu un laiku, kad dokumenta kopijas vai tulkojumus izsūtīja KIN vai tie tika atgādāti atpakaļ šajā nodaļā, un ziņas par to, uz kurieni šie dokumenti tika nosūtīti un kas tos atgādāja atpakaļ;

g) datumu un laiku, kad dokuments tika iznīcināts, un kas to izdarīja, saskaņā ar Parlamenta drošības noteikumiem attiecībā uz dokumentu iznīcināšanu un

h) dokumenta deklasifikācija vai slepenības pakāpes pazemināšana.

51. Reģistrācijas žurnālus attiecīgi klasificē vai marķē. Žurnālus, kuros iegrāmato informāciju, kas ir klasificēta līmenī TRES SECRET UE/EU TOP SECRET, vai tai līdzvērtīgu informāciju, reģistrē tādā pašā klasifikācijas līmenī.

52. Klasificētu informāciju var reģistrēt:

a) vienā reģistrācijas žurnālā vai

b) dažādos reģistrācijas žurnālos atkarībā no tās klasifikācijas līmeņa, ienākošā vai izejošā dokumenta statusa, izcelsmes vai galamērķa.

53. Ja elektronisku dokumenta apstrādi veic KIS, reģistrācijas procedūras var veikt, izmantojot to pašu KIS un ievērojot iepriekš minētās prasības. Ja Eiropas Savienības konfidenciālā informācija nonāk ārpus KIS perimetra, piemēro iepriekš minēto procedūru.

54. KIN reģistrē visu klasificēto informāciju, ko Parlaments ir nosūtījis trešām personām vai saņēmis no tām.

55. Kad pabeigta informācijas, kas ir klasificēta kā CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai tai līdzvērtīgas informācijas reģistrācija, KIN pārbauda, vai saņēmējam ir derīga drošības dienestu atļauja. Ja tas apstiprinās, KIN saņēmējam paziņo par klasificēto informāciju. Iepazīties ar klasificēto informāciju var tikai tad, kad ir reģistrēts šo informāciju saturošais dokuments.

H. **IZPLATĪŠANA**

56. Sagatavotājs izveido savas izstrādātās ESKI sākotnējo izplatīšanas sarakstu.

57. Informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, un citu Parlamenta izstrādātu konfidenciālu informāciju Parlamentā izplata tā sagatavotājs saskaņā ar attiecīgajām apstrādes instrukcijām un pamatojoties uz principu "vajadzība pēc informācijas". Tādas informācijas, kas klasificēta kā CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET, ko Parlaments izstrādājis drošības zonā, izplatīšanas sarakstu (un citus norādījumus par tās izplatīšanu) nodod KIN, kas ir atbildīga par tā pārvaldību.

58. Vienīgi KIN var trešām personām izplatīt Parlamenta izstrādātu ESKI, pamatojoties uz principu "vajadzība pēc informācijas".

59. Konfidenciālo informāciju, kuru ir saņēmusi vai nu KIN, vai cita Parlamenta struktūra / pilnvarotā persona, kas ir iesniegusi pieprasījumu, izplata saskaņā ar sagatavotāja sniegtajiem norādījumiem.

I. **KONFIDENCIĀLAS INFORMĀCIJAS APSTRĀDE, GLABĀŠANA UN IEPAZĪŠANĀS AR TO**

60. Konfidenciālas informācijas apstrādi, glabāšanu un iepazīšanos ar to veic saskaņā ar drošības paziņojumu Nr. 4 un apstrādes instrukcijām.

J. **KLASIFICĒTAS INFORMĀCIJAS KOPĒŠANA/TULKOŠANA/MUTISKĀ TULKOŠANA**

61. Kopēt vai tulkot dokumentus, kas satur informāciju, kura klasificēta līmenī TRES SECRET UE/EU TOP SECRET, vai līdzvērtīgu informāciju, drīkst tikai ar sagatavotāja iepriekšēju rakstisku piekrišanu. Dokumentus, kas satur informāciju, kas klasificēta līmenī SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL, vai tai līdzvērtīgu informāciju var kopēt vai tulkot pēc turētāja norādījumiem, ja to nav aizliedzis sagatavotājs.

62. Drošības nolūkā reģistrē katru tāda dokumenta kopiju, kas satur informāciju, kura klasificēta līmenī TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECRET vai CONFIDENTIEL UE/EU CONFIDENTIAL, vai tai līdzvērtīgu informāciju.

63. Drošības pasākumus, ko piemēro klasificētu informāciju saturošajam oriģināldokumentam, piemēro arī tā kopijām un tulkojumiem.

64. Padomes sūtītajiem dokumentiem ir jābūt visās oficiālajās valodās.

65. Kopijas un/vai tulkojumus dokumentiem, kas satur klasificētu informāciju, var pieprasīt dokumenta sagatavotājs vai kopijas turētājs. Dokumentus, kas satur informāciju, kura klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai tai līdzvērtīgu informāciju, var kopēt vienīgi drošības zonā un izmantojot kopētājus, kas ir daļa no akreditētas KIS. Dokumentus, kas satur informāciju, kura klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai tai līdzvērtīgu informāciju un citu konfidenciālu informāciju, kopē Parlamenta telpās, izmantojot akreditētu pavairošanas iekārtu.

66. Visas klasificētu informāciju saturoša dokumenta vai tā daļas kopijas un tulkojumus pienācīgi marķē, numurē un reģistrē.

67. Dokumentu kopē tikai tik eksemplāros, cik tas ir patiesi nepieciešams. Visas kopijas iznīcina saskaņā ar apstrādes instrukcijām pēc tam, kad ir beidzies periods, kurā ar tām varēja iepazīties.

68. Piekļuvi klasificētai informācijai sniedz tikai tiem tulkiem un tulkotājiem, kuri ir Parlamenta ierēdņi.

69. Tulkiem un tulkotājiem, kuriem ir piekļuve dokumentiem, kas satur informāciju, kura klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai tai līdzvērtīgu informāciju, ir pienācīga drošības pielaide.

70. Ar dokumentiem, kas satur informāciju, kura ir klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai tai līdzvērtīgu informāciju, tulki un tulkotāji strādā drošības zonā.

K. KONFIDENCIĀLAS INFORMĀCIJAS KLASIFIKĀCIJAS LĪMEŅA PAZEMINĀŠANA, DEKLASIFIKĀCIJA UN MARĶĒJUMA NOŅEMŠANA

K.1. *Vispārējie principi*

71. Ja vairs nav vajadzīga klasificētas informācijas aizsardzība vai aizsardzība sākotnējā līmenī, to deklasificē, pazemina tās klasifikācijas līmeni vai noņem marķējumu.

72. Lēmumi par Parlamentā izstrādātu dokumentu klasifikācijas līmeņa pazemināšanu, klasificēšanu vai marķējuma noņemšanu var būt pieņemami arī ad hoc kārtā, piemēram, atbildot uz sabiedrības vai citas Savienības iestādes piekļuves pieprasījumu vai pēc KIN vai Parlamenta struktūras / pilnvarotās personas ierosmes.

73. Izstrādājot ESKI, tās sagatavotājs, ja iespējams, norāda, vai var pazemināt attiecīgās ESKI klasifikācijas līmeni vai to deklasificēt konkrētā dienā vai pēc konkrēta notikuma. Ja šādu informāciju nav iespējams nodrošināt, sagatavotājs, KIN vai Parlamenta struktūra / pilnvarotā persona, kas ir informācijas turētāja, ESKI klasifikācijas līmeni pārskata vismaz reizi piecos gados. Visos gadījumos ESKI klasifikācijas līmeni var pazemināt vai to deklasificēt vienīgi ar iepriekšēju informācijas sagatavotāja rakstisku piekrišanu.

74. Ja nav iespējams noteikt vai atrast Parlamentā izstrādātu dokumentu sagatavotāju, drošības iestāde pārskata attiecīgā ESKI klasifikācijas līmeni, pamatojoties uz tādas Parlamenta struktūras / pilnvarotā personas priekšlikumu, kas ir informācijas turētāja, un vajadzības gadījumā par to apspriežoties ar KIN.

75. KIN vai Parlamenta struktūra / pilnvarotā persona, kas ir informācijas turētāja, atbild par paziņošanu adresātam par to, ka informācija ir deklasificēta vai ka ir pazemināts tās klasifikācijas līmenis, un šie adresāti savukārt atbild par paziņošanu tām personām, kam viņi ir sūtījuši vai kopējuši attiecīgo dokumentu.

76. Tiek reģistrēta dokumentā esošās informācijas deklasifikācija, klasifikācijas līmeņa pazemināšana vai marķējuma noņemšana.

K.2. *Deklasificēšana*

77. ESKI var deklasificēt pilnībā vai daļēji. To var deklasificēt daļēji, ja aizsardzība vairs netiek uzskatīta par vajadzīgu konkrētai dokumenta daļai, kas satur šo informāciju, tomēr tā ir pamatota pārējam dokumentam.

78. Ja, pārskatot Parlamentā izstrādātā dokumentā esošo ESKI, tiek pieņemts lēmums par tā deklasifikāciju, ir jāapsver tas, vai attiecīgo var dokumentu publisko, vai arī tam jāpiešķir izplatīšanas marķējums (t.i. nepubliskot).

79. ESKI deklasifikāciju reģistrē reģistrācijas žurnālā, norādot: deklasifikācijas dienu, deklasifikācijas pieprasītāju un deklasifikācijas atļaujas sniedzēju vārdus, deklasificētā dokumenta atsauces numuru un tā galamērķi.

80. Deklasificētajā dokumentā un visās tā kopijās svītro novecojušo klasifikācijas marķējumu. Attiecīgo dokumentu un tā kopijas pienācīgi glabā.

81. Daļēji deklasificējot klasificētu informāciju, deklasificēto daļu sagatavo kā izvilkumu un pienācīgi glabā. Kompetentais dienests reģistrē:

a) daļējās deklasifikācijas dienu;

b) deklasifikācijas pieprasītāju un deklasifikācijas atļaujas sniedzēju vārdus un

c) deklasificētās daļas atsauces numuru.

K.3. ***Klasifikācijas līmeņa pazemināšana***

82. Pēc klasificētās informācijas klasifikācijas līmeņa pazemināšanas attiecīgo dokumentu, kas to satur, ieraksta abos – gan vecā, gan jaunā klasifikācijas līmeņa – reģistrācijas žurnālos. Reģistrē gan klasifikācijas līmeņa pazemināšanas dienu, gan attiecīgās atļaujas sniedzēja vārdu.

83. Dokumentu, kas satur pazemināta klasifikācijas līmeņa informāciju, un visas tā kopijas klasificē pēc jaunā klasifikācijas līmeņa un pienācīgi glabā.

L. **KONFIDENCIĀLAS INFORMĀCIJAS IZNĪCINĀŠANA**

84. Nevajadzīgu konfidenciālu informāciju (papīra vai elektroniskā formātā) iznīcina vai izdzēš atbilstīgi apstrādes instrukcijām un attiecīgajiem arhivēšanas noteikumiem.

85. Informāciju, kas klasificēta līmenī TRES SECRET UE/EU TOP SECRET, SECRET UE/EU SECET, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai līdzvērtīgu informāciju iznīcina KIN. Tās iznīcināšanu veic tāda liecinieka klātbūtnē, kuram ir vismaz tāda līmeņa drošības pielaide, kas atbilst iznīcināmā dokumenta klasifikācijas līmenim.

86. Informācija, kas klasificēta līmenī TRES SECRET UE/EU TOP SECRET, vai tai līdzvērtīgu informāciju iznīcina tikai ar sagatavotāja iepriekšēju rakstisku piekrišanu.

87. Pēc sagatavotāja vai kompetentās iestādes norādījuma KIN iznīcina un galīgi apstrādā informāciju, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai līdzvērtīgu informāciju. Reģistrācijas žurnālus un pārējos reģistrus atbilstīgi atjaunina. Informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai tai līdzvērtīgu informāciju iznīcina un galīgi apstrādā vai nu KIN, vai attiecīgā Parlamenta struktūra / pilnvarotā persona.

88. Par iznīcināšanu oficiāli atbildīgā persona un persona, kas ir iznīcināšanas liecinieks, paraksta iznīcināšanas sertifikātu, kuru iesniedz un arhivē konfidenciālo dokumentu nodaļā (KIN). Informācijas, kas klasificēta līmenī TRES SECRET UE/EU TOP SECRET, vai līdzvērtīgas informācijas iznīcināšanas sertifikātus un izplatīšanas veidlapas KIN glabā vismaz 10 gadus, savukārt attiecībā uz informāciju, kas klasificēta līmenī SECRET UE/EU SECRET, CONFIDENTIEL UE/EU CONFIDENTIAL, vai tai līdzvērtīgu informāciju šis glabāšanas laiks ir vismaz pieci gadi.

89. Klasificētu informāciju saturošus dokumentus iznīcina ar tādām metodēm, kas atbilst attiecīgajiem Savienības vai līdzvērtīgiem standartiem, lai novērstu iespēju, ka dokumentu varētu pilnīgi vai daļēji atjaunot.

90. Klasificētās informācijas ierakstīšanai izmantotu elektronisko informācijas nesēju iznīcināšana notiek saskaņā ar attiecīgajām apstrādes instrukcijām.

91. Klasificētās informācijas iznīcināšanu ieraksta attiecīgajā reģistrācijas žurnālā, norādot:

a) iznīcināšanas dienu un laiku;

b) par iznīcināšanu oficiāli atbildīgās personas vārdu;

c) iznīcinātā dokumentu vai kopiju identifikācijas datus;

d) iznīcinātās ESKI fizisko formu;

e) iznīcināšanas metodi un

f) iznīcināšanas vietu.

M. **ARHIVĒŠANA**

92. Klasificēto informāciju, tostarp jebkādu pavadvēstuli/piezīmi, pielikumus, sūtījuma nodošanas kvīti un/vai citu dokumentāciju, nodod drošības zonā esošajā drošajā arhīvā sešu mēnešu laikā pēc tam, kad pēdējoreiz notikusi iepazīšanās ar to un, vēlākais, vienu gadu pēc tam, kad tā tikusi deponēta. Sīkākus noteikumus par klasificētas informācijas arhivēšanu paredz apstrādes instrukcijās.

93. Attiecībā uz citu konfidenciālu informāciju piemēro vispārējos noteikumus par dokumentu pārvaldību, neskarot citus konkrētus noteikumu par tās apstrādi.

DROŠĪBAS PAZIŅOJUMS Nr. 3

KONFIDENCIĀLAS INFORMĀCIJAS APSTRĀDE AR AUTOMATIZĒTĀM KOMUNIKĀCIJU UN INFORMĀCIJAS SISTĒMĀM (KIS)

A. **KLASIFICĒTĀS INFORMĀCIJAS AIZSARDZĪBA, APSTRĀDĀJOT TO KOMUNIKĀCIJU UN INFORMĀCIJAS SISTĒMĀS**

1. "Informācijas aizsardzība" (IA) informācijas sistēmu jomā ir pārliecība, ka šīs sistēmas aizsargās klasificētu informāciju, darbosies atbilstīgi, paredzētajā laikā un likumīgu lietotāju kontrolē. Ar efektīvu IA nodrošina atbilstīga līmeņa konfidencialitāti, integritāti, pieejamību, nenoliedzamību un autentiskumu. IA pamatā ir riska pārvaldības process.

2. Klasificētas informācijas apstrādei paredzēta "komunikāciju un informācijas sistēma" (KIS) ir sistēma, ar kuru informāciju var apstrādāt elektroniski. Šāda informācijas sistēma ietver visus sistēmas darbībai vajadzīgos resursus, tostarp attiecībā uz infrastruktūru, organizāciju, personālu un informāciju.

3. KIS apstrādā klasificētu informāciju atbilstīgi IA koncepcijai.

4. Visām KIS ir jāiziet akreditācija. Akreditācijas mērķis ir saņemt garantiju, ka ir īstenotas visas attiecīgās drošības procedūras un ka ir sasniegts pietiekams klasificētās informācijas un KIS aizsardzības līmenis, kas atbilst šim drošības paziņojumam. Akreditācijas paziņojumā nosaka augstāko informācijas klasifikācijas līmeni, ar kādu atļauts strādāt KIS, kā arī šādas atļaujas nosacījumus.

5. Lai KIS darbības notiktu droši un pareizi, būtiskas ir šādas IA īpašības un koncepcijas:

a) autentiskums – garantija, ka informācija ir īsta un ka tā ir iegūta no bona fide avotiem;

b) pieejamība – tai var piekļūt un to var izmantot pēc pilnvarotas iestādes pieprasījuma;

c) konfidencialitāte – informāciju neatklāj tādām personām, iestādēm vai procedūrām, kas nav saņēmušas attiecīgu atļauju;

d) integritāte – spēja nosargāt informācijas un materiālu precizitāti un pilnīgumu;

e) nenoliedzamība – spēja pierādīt, ka darbība vai notikums ir noticis, lai būtu izslēgta iespēja, ka minēto notikumu vai darbību vēlāk varētu noliegt.

B. **INFORMĀCIJAS AIZSARDZĪBAS PRINCIPI**

6. Turpmāk izklāstītie noteikumi veido jebkuras tādas KIS drošības pamatus, kura apstrādā klasificētu informāciju. IA drošības politikā un drošības pamatnostādnēs nosaka sīki izstrādātas minēto noteikumu īstenošanas prasības.

B.1. ***Drošības riska pārvaldība***

7. Drošības riska pārvaldība ir neatņemama daļa KIS definēšanā, izstrādē, darbībā un uzturēšanā. Riska pārvaldību (izvērtējums, risinājums, pieņemšana, paziņošana) veic kā iteratīvu procesu kopīgi ar sistēmu īpašnieku pārstāvjiem, projekta iestādēm, darbības iestādēm un drošības paziņojumā Nr. 1 noteiktajām drošības apstiprināšanas iestādēm, izmantojot apliecinātu, pārskatāmu un pilnīgi izprotamu riska izvērtējuma procesu. KIS darbības jomu un tās materiālus skaidri definē riska pārvaldības procesa sākumā.

8. Drošības paziņojumā Nr. 1 noteiktās kompetentās iestādes pārskata iespējamos komunikāciju un informācijas sistēmas apdraudējumus un uztur aktuālus un precīzus apdraudējumu izvērtējumus, kas atspoguļo pašreizējo darbības vidi. Tās pastāvīgi atjaunina informāciju par ietekmējamību un periodiski pārskata ietekmējamības izvērtējumu, lai atbilstu mainīgajai informāciju tehnoloģiju (IT) videi.

9. Drošības riska risinājuma mērķis ir piemērot drošības pasākumu kopumu, kuru rezultātā panāk apmierinošu līdzsvaru starp lietotāja vajadzībām, izmaksām un neapzinātu drošības risku.

10. KIS sistēmas akreditācijā ietver oficiālu paziņojumu par neapzināto apdraudējumu un to, ka atbildīgā iestāde pieņem neapzināto apdraudējumu. Atbilstīgās drošības akreditācijas iestādes noteiktās īpašās prasības, darbības mērogs un sarežģītības pakāpe atbilst novērtētajam riskam, ņemot vērā visus atbilstīgos faktorus, tostarp KIS apstrādātās klasificētās informācijas klasifikācijas līmeni.

B.2. ***Drošība visā KIS aprites cikla laikā***

11. Drošība ir būtiska prasība, kas ir aktuāla visā KIS aprites ciklā no sākuma līdz izņemšanai no aprites.

12. Katrā aprites cikla posmā nosaka katra ar KIS saistītā dalībnieka lomu un sadarbības veidu drošības jautājumos.

13. Akreditācijas laikā KIS, tostarp tās tehniskajiem un netehniskajiem drošības pasākumiem, veic drošības pārbaudes, lai pārliecinātos, ka panākts piemērots aizsardzības līmenis, un pārbaudītu, ka KIS, tostarp tās tehniskie un netehniskie drošības pasākumi, tiek pareizi īstenoti, integrēti un konfigurēti.

14. KIS darbības un uzturēšanas laikā periodiski, kā arī ārkārtas apstākļu gadījumā veic drošības izvērtējumus, inspekcijas un pārskatīšanu.

15. Drošības informācija KIS vajadzībām tās aprites ciklā mainās, tā ir neatņemama daļa no pārmaiņu procesa pārvaldības.

16. KIS veiktās reģistrācijas procedūras vajadzības gadījumā pārbauda akreditācijas procesa laikā.

B.3. ***Paraugprakse***

17. IAI izstrādā KIS paraugpraksi, kā aizsargājama KIS apstrādātā klasificētā informācija. Paraugprakses pamatnostādnēs iekļauj KIS tehniskus, fiziskus, organizatoriskus un procedūras drošības pasākumus, kuru iedarbība cīņā pret konkrētiem apdraudējumiem un ietekmējamību ir pierādīta.

18. KIS apstrādātas klasificētas informācijas aizsardzībā izmanto pieredzi, ko guvušas IA iesaistītās vienības.

19. Paraugprakses izplatīšana un attiecīga īstenošana palīdz panākt līdzvērtīgu aizsardzības līmeni dažādās Parlamenta sekretariāta vadītās KIS, kurās apstrādā klasificētu informāciju.

B.4. ***Padziļināta aizsardzība***

20. Lai mazinātu apdraudējumu komunikāciju un informācijas sistēmai, īsteno plaša spektra tehniskus drošības pasākumus un pasākumus, kas nav tehniski drošības pasākumi, izveidojot daudzslāņainu aizsardzību. Minētie slāņi ir:

a) atturēšana – drošības pasākumi, lai atturētu no jebkādiem kaitnieciskiem plāniem, kas vērsti pret KIS;

b) novēršana – drošības pasākumi, kuru mērķis ir traucēt vai novērst pret KIS vērstu uzbrukumu;

c) atklāšana – drošības pasākumi, kuru mērķis ir atklāt pret KIS vērstu uzbrukumu;

d) izturība – drošības pasākumi, kuru mērķis ir maksimāli ierobežot uzbrukuma ietekmi uz informācijas kopumu vai KIS materiāliem un pasargāt tos no turpmākiem bojājumiem, un

e) atjaunošana – drošības pasākumi, kuru mērķis ir atjaunot drošu KIS stāvokli.

Minēto pasākumu stingrību nosaka pēc apdraudējuma izvērtējuma.

21. Kompetentās iestādes, kas precizētas drošības paziņojumā Nr. 1, nodrošina, ka tās spēj reaģēt uz gadījumiem, kuri var sniegties pāri organizācijas un valsts robežām, tādā veidā, lai koordinētu reakciju un sniegtu informāciju par šiem gadījumiem un saistīto risku (ārkārtas reaģēšanas spējas datordrošības jomā).

B.5. ***Ierobežojumu un mazākās konfidencialitātes pielaides princips***

22. Lai izvairītos no nevajadzīga apdraudējuma, ievieš tikai būtiskās darbībai vajadzīgās funkcijas, iekārtas un dienestus.

23. KIS lietotājiem un automatizētiem procesiem nodrošina tikai tādu piekļuvi, privilēģijas vai pilnvaras, kas vajadzīgas to pienākumu veikšanai, lai tādējādi ierobežotu negadījumu, kļūdu vai bojājumu, vai neatļautas KIS resursu izmantošanas rezultātā radušos bojājumus.

B.6. ***Informētība par informācijas aizsardzību***

24. KIS aizsardzības pirmais priekšnoteikums ir informētība par risku un pieejamiem drošības pasākumiem. Visas personas, kas iesaistītas KIS aprites ciklā, tostarp tās lietotāji, saprot:

a) ka trūkumi drošības sistēmā var būtiski kaitēt KIS, kas apstrādā klasificētu informāciju;

b) ka savstarpējās savienojamības un atkarības dēļ kaitējums var tikt nodarīts arī citiem un

c) ka tās personiski atbild un atskaitās par KIS drošību saskaņā ar saviem pienākumiem sistēmās un procesos.

25. Lai nodrošinātu, ka viss iesaistītais personāls, tostarp augstākā līmeņa vadība, Eiropas Parlamenta deputāti un KIS lietotāji, ir sapratuši atbildību par drošības garantēšanu, tiem ir obligāti jāsaņem izglītība un apmācība par informācijas aizsardzību.

B.7. ***IT drošības produktu izvērtēšana un apstiprināšana***

26. KIS, kurās apstrādā informāciju, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET un tai līdzvērtīgu informāciju, ir aizsargātas pret informācijas apdraudējumu, ko izraisa netīšas elektromagnētiskas emisijas ("TEMPEST drošības pasākumi").

27. Ja klasificētu informāciju aizsargā ar kriptogrāfijas produktiem, tos sertificē drošības akreditācijas iestāde kā ES apstiprinātus kriptogrāfijas produktus.

28. Klasificētu informāciju sūtot elektroniski, izmanto ES apstiprinātus kriptogrāfijas produktus. Neskarot šo prasību, ārkārtas apstākļos vai īpašās tehniskās konfigurācijās var piemērot īpašas procedūras, kā noteikts 41.–44. punktā.

29. Vajadzīgo uzticamības līmeni drošības pasākumos, ko definē kā aizsardzības līmeni, nosaka atbilstīgi riska pārvaldības procesā gūtajiem rezultātiem un saskaņā ar attiecīgo drošības politiku un pamatnostādnēm.

30. Aizsardzības līmeni pārbauda, lietojot starptautiski plaši izmantotus vai valstī apstiprinātus procesus un metodikas. Tas ietver sākotnējo izvērtēšanu, kontroli un revīziju.

31. DAI apstiprina drošības pamatnostādnes attiecībā uz tādu IT produktu kvalificēšanu un apstiprināšanu, kas nav saistīti ar kriptogrāfiju.

B.8. ***Nosūtīšana drošības zonās***

32. Ja klasificētu informāciju nosūta tikai drošības zonā, nešifrētu izplatīšanu vai zemāka līmeņa šifrēšanu var izmantot, pamatojoties uz riska pārvaldības procesa rezultātiem un ar DAI apstiprinājumu.

B.9. ***Drošs KIS savstarpējs savienojums***

33. Savstarpējs savienojums ir tieši savienotas divas vai vairākas IT sistēmas, lai apmainītos ar datiem un citiem informācijas resursiem vienā vai vairākos virzienos.

34. KIS jebkuru pieslēgtu IT sistēmu uzskata par neuzticamu un ievieš aizsargpasākumus, lai kontrolētu klasificētas informācijas apmaiņu ar citu KIS.

35. Visi KIS un citas IT sistēmas savstarpēji savienojumi atbilst šādām pamatprasībām:

a) kompetentās iestādes nosaka un apstiprina šādu savienojumu darbības vai operatīvās prasības;

b) attiecīgajam savstarpējam savienojumam piemēro riska pārvaldības un akreditācijas procesu, un to apstiprina kompetentā DAI;

c) KIS perimetrā izvieto aizsardzības dienestus (AD).

36. Nedrīkst savstarpēji saslēgt akreditētu KIS un neaizsargātu vai publiski pieejamu tīklu, izņemot gadījumus, ja KIS apstiprinājusi šādiem mērķiem ieviesto AD starp KIS un neaizsargāto vai publiski pieejamo tīklu. Šādu savstarpēju savienojumu drošības pasākumus pārskata kompetentā IAI un apstiprina kompetentā DAI.

37. Ja neaizsargāto vai publiski pieejamo tīklu izmanto vienīgi tādas informācijas transportēšanai, kura ir šifrēta ar ES kriptogrāfijas produktu, kas apstiprināts saskaņā ar 27. punktu, šādu savienojumu neuzskata par savstarpēju savienojumu.

38. Ir aizliegts tādas KIS, kas ir akreditēta informācijas, kura klasificēta līmenī TRES SECRET UE/EU TOP SECRET vai līdzvērtīgas informācijas, vai SECRET UE/EU SECRET vai līdzvērtīgas informācijas apstrādei, tiešs vai pakāpenisks savstarpējs savienojums ar neaizsargātu vai publiski pieejamu tīklu.

B.10. ***Elektroniskie informācijas nesēji***

39. Elektroniskos informācijas nesējus iznīcina saskaņā ar kompetentās drošības iestādes apstiprinātām procedūrām.

40. Elektroniskos informācijas nesējus atkārtoti izmanto, pazemina to klasifikācijas līmeni vai deklasificē saskaņā ar apstrādes instrukcijām.

B.11. ***Ārkārtas apstākļi***

41. Ārkārtas gadījumā, piemēram, gaidāmas vai notiekošas krīzes situācijā, konflikta vai kara situācijā vai ārkārtas operatīvajā situācijā var piemērot turpmāk aprakstītās īpašās procedūras.

42. Ar kompetentās iestādes piekrišanu klasificēto informāciju var nosūtīt, izmantojot kriptogrāfijas produktus, kas apstiprināti lietošanai zemākam klasifikācijas līmenim, vai nešifrētā veidā, ja kavējumi varētu radīt kaitējumu, kas nepārprotami būtu lielāks par kaitējumu, ko rada klasificēta materiāla izpaušana, un ja:

a) sūtītājam un saņēmējam nav vajadzīgo kriptogrāfijas iekārtu vai nekādu kriptogrāfijas iekārtu un

b) klasificēto materiālu nevar nodot pietiekami savlaicīgi, izmantojot citus līdzekļus.

43. Klasificētā informācijā, kas nosūtīta 41. punktā izklāstītajos apstākļos, nav atzīmju vai norāžu, kas to ļautu atšķirt no neklasificētas informācijas vai informācijas, ko var aizsargāt ar pieejamu kriptogrāfijas iekārtu. Informācijas saņēmējus par tās klasifikācijas līmeni nekavējoties informē ar citiem līdzekļiem.

44. Ja tiek izmantota 41. vai 42. punktā minētā procedūra, par to sniedz ziņojumu kompetentajai iestādei.

DROŠĪBAS PAZIŅOJUMS Nr. 4

FIZISKĀ DROŠĪBA

A. **IEVADS**

Šajā drošības paziņojumā noteikti drošas vides izveides drošības principi pareizai rīcībai ar konfidenciālu informāciju Eiropas Parlamentā. Šos principus, tostarp principus, kas attiecas uz tehnisko drošību, papildinās apstrādes instrukcijas.

B. **DROŠĪBAS RISKA PĀRVALDĪBA**

1. Klasificētas informācijas apdraudējumu pārvalda kā procesu. Šā procesa mērķis ir konstatēt zināmos drošības apdraudējumus, definēt drošības pasākumus, lai mazinātu šādus apdraudējumus līdz pieņemamam līmenim atbilstīgi šajā drošības paziņojumā izklāstītajiem pamatprincipiem un obligātajiem standartiem un piemērot šos pasākumus saskaņā ar pastiprinātas aizsardzības koncepciju, kā definēts drošības paziņojumā Nr. 3. Minēto pasākumu efektivitāti nepārtraukti izvērtē.

2. Drošības pasākumi klasificētas informācijas aizsardzībai visā tās aprites laikā jo īpaši atbilst tās drošības klasifikācijai, attiecīgās informācijas vai materiāla fiziskajai formai un apjomam, to iekārtu atrašanās vietai un uzbūvei, kurās klasificētā informācija atrodas, un vietēji izvērtētam vardarbīga un/vai noziedzīgu nodarījuma apdraudējumam, tostarp spiegošanai, ļaunprātībai vai terorismam.

3. Ārkārtas rīcības plānos ņem vērā vajadzību aizsargāt klasificētu informāciju ārkārtas situācijās, lai novērstu neatļautu piekļuvi, izpaušanu, integritātes vai piekļuves zaudējumu.

4. Darbības nepārtrauktības plānos iekļauj preventīvus un atgūšanas pasākumus, lai mazinātu ietekmi, ko rada būtiski trūkumi vai starpgadījumi saistībā ar klasificētas informācijas apstrādi un glabāšanu.

C. **VISPĀRĒJIE PRINCIPI**

5. Informācijai piešķirtais klasifikācijas vai marķējuma līmenis nosaka aizsardzības līmeni, ko attiecīgajai informācijai piemēro fiziskās drošības jomā.

6. Informāciju, kurai ir vajadzīga klasifikācija, marķē un to attiecīgi apstrādā kā klasificētu informāciju – neatkarīgi no informācijas fiziskās formas. Informācijas klasifikāciju skaidri dara zināmu tās saņēmējiem, vai nu izmantojot klasifikācijas marķējumu (ja tā sniegta rakstiski – uz papīra vai ar KIS starpniecību), vai paziņojumu (ja tā sniegta mutiski, piemēram, sarunā vai izklāstā). Klasificētus materiālus fiziski marķē, lai varētu viegli noteikt to klasifikācijas līmeni.

7. Konfidenciālu informāciju nekādos apstākļos nelasa publiskās vietās, kur to varētu redzēt persona, kurai nav pamatotas vajadzības pēc informācijas, proti, vilcienos vai lidmašīnās, kafejnīcās, bāros u. tml. Toneatstāj viesnīcu seifos vai istabās vai bez uzraudzības publiskās vietās.

D. **ATBILDĪBA**

8. Klasificētās informācijas nodaļa (KIN) ir atbildīga par fiziskās drošības nodrošināšanu attiecībā uz tās konfidenciālās informācijas pārvaldību, kas glabājas tās drošajās telpās. KIN ir arī atbildīga par tās drošo telpu pārvaldību.

9. Atbildība par fizisku drošību tās informācijas pārvaldībā, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai tai līdzvērtīgu informāciju un citu konfidenciālu informāciju, ir attiecīgajai Parlamenta struktūrai / pilnvarotajai personai.

10. Drošības un riska novērtēšanas direktorāts nodrošina personāla drošību un drošības pielaidi, kas nepieciešama drošai konfidenciālas informācijas apstrādei Eiropas Parlamentā.

11. Informācijas tehnoloģiju direktorāts konsultē un nodrošina, ka jebkura izveidotā vai izmantotā komunikāciju un informācijas sistēma (KIS) pilnībā atbilst drošības paziņojuma Nr. 3 noteikumiem un attiecīgajām apstrādes instrukcijām.

E. **DROŠĀS TELPAS**

12. Saskaņā ar tehniskās drošības standartiem un atbilstīgi konfidenciālajai informācijai piešķirtajam līmenim, kā noteikts 7. pantā, var tikt aprīkotas drošās telpas.

13. Drošības akreditācijas iestāde (DAI) sertificē drošās telpas, savukārt Drošības iestāde (DI) tās apstiprina.

F. **IEPAZĪŠANĀS AR KONFIDENCIĀLU INFORMĀCIJU**

14. Ja informācija, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai tai līdzvērtīga informācija un cita konfidenciāla informācija atrodas KIN un ar to jāiepazīstas ārpus drošības zonas, KIN pārsūta kopiju atbilstīgajam pilnvarotajam dienestam, kurš nodrošina, ka iepazīšanās ar attiecīgo informāciju un tās apstrāde atbilst šā lēmuma 8. panta 2. punktam un 10. pantam, kā arī atbilstīgajām apstrādes instrukcijām.

15. Ja informācija, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai līdzvērtīga informācija un cita konfidenciāla informācija ir nodota Parlamenta struktūrai / pilnvarotajai personai, kuras nav KIN, minētās Parlamenta struktūras/pilnvarotas personas sekretariāts nodrošina, ka iepazīšanās ar attiecīgo informāciju un tās apstrāde atbilst šā lēmuma 7. panta 3. punktam, 8. panta 1., 2., un 4. punktam, 9. panta 3., 4. un 5. punktam, 10. panta 2. līdz 6. punktam un 11. pantam, kā arī attiecīgajām apstrādes instrukcijām.

16. Ja ar informāciju, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET, vai tai līdzvērtīgu informāciju ir jāiepazīstas drošības zonā, KIN nodrošina, ka iepazīšanās ar attiecīgo informāciju un tās apstrāde atbilst šā lēmuma 9. un 10. pantam un atbilstīgajām apstrādes instrukcijām.

G. **TEHNISKĀ DROŠĪBA**

17. Par tehniskās drošības pasākumiem ir atbildīga DAI, kas attiecīgajās apstrādes instrukcijās nosaka īpašus piemērojamos tehniskās drošības pasākumus.

18. Drošās lasītavas, kurās iepazīstas ar informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai līdzvērtīgu informāciju un citu konfidenciālu informāciju atbilst īpašiem drošības noteikumiem saskaņā ar šā lēmuma 7. panta 3. punktu, kā noteikts apstrādes instrukcijās.

19. Saskaņā ar šā lēmuma 7. panta 2. punktu drošības zona sastāv no šādām telpām:

a) piekļuves drošības pārbaudes telpa, kuru aprīko saskaņā ar tehniskajiem drošības pasākumiem, kā noteikts apstrādes instrukcijās. Piekļuvi šai telpai reģistrē. Piekļuves drošības pārbaudes telpa atbilst augstiem standartiem saistībā ar personu identifikāciju, kurām ir piekļuve, kā arī videoierakstiem, un drošām vietām to personisko lietu glabāšanai (piemēram, tālruņi, rakstāmlīdzekļi u. c.), kuras nav atļauts ienest drošajās telpās;

b) komunikāciju telpa klasificētas informācijas, tostarp šifrētas klasificētas informācijas, pārsūtīšanai un saņemšanai atbilstīgi drošības paziņojumam Nr. 3 un attiecīgajām apstrādes instrukcijām;

c) droša arhīva telpa, kurā tiek izmantoti apstiprināti un sertificēti konteineri atsevišķi informācijai, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, kā CONFIDENTIEL UE/EU CONFIDENTIAL un/vai kā SECRET EU/EU SECRET, vai līdzvērtīgai informācijai. Informāciju, kas klasificēta līmenī TRES SECRETUE/EU TOP SECRET, vai līdzvērtīgu informāciju izvieto atsevišķā telpā īpašā sertificētā konteinerā. Šajā telpā vienīgo pieejamo papildu materiālu sniedz atbalsta punkts KIN arhīva apstrādei;

d) reģistrācijas telpa, kurā tiek nodrošināti rīki, kas nepieciešami reģistrācijai papīra formātā vai elektroniski, un tāpēc tā ir iekārtota ar vajadzīgajām drošajām iekārtām, lai uzstādītu attiecīgo KIS. Vienīgi reģistrācijas telpā var atrasties apstiprinātas un akreditētas pavairošanas ierīces (papīra kopiju vai elektronisku kopiju iegūšanai). Apstrādes instrukcijās ir precizēts, kuras pavairošanas ierīces ir apstiprinātas un akreditētas. Reģistrācijas telpā tiek nodrošināta vajadzīgā glabāšana, lai akreditēta materiālu varētu glabāt un apstrādāt tā, lai to varētu marķēt, kopēt un nosūtīt fiziskā formā atkarībā no klasifikācijas līmeņa. Visu akreditēto materiālu nosaka KIN, un to akreditē DAI, ņemot vērā no Informācijas aizsardzības operatīvās iestādes (IAOI) saņemto ieteikumu. Reģistrācijas telpu aprīko ar akreditētu informācijas iznīcināšanas ierīci, kas apstiprināta visaugstākā līmeņa klasifikācijai, kā minēts apstrādes instrukcijās. Informācijas, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL EU, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai līdzvērtīga līmeņa informācijas tulkošanu veic reģistrācijas telpā, izmantojot atbilstīgo un akreditēto sistēmu. Reģistrācijas telpā iekārto darba vietas, ko vienlaikus izmanto ne vairāk kā divi tulkotāji vienam un tam pašam dokumentam. Tulkošana notiek viena KIN personāla locekļa klātbūtnē;

e) lasītava, kur ar klasificētu informāciju var iepazīties individuālas personas, kurām ir atbilstošas atļaujas. Lasītavā ir pietiekami daudz vietas divām personām, kā arī KIN personāla loceklim, kurš tur uzturas visu laiku, kad notiek iepazīšanās ar katru atsevišķo dokumentu. Šīs telpas drošības līmenis ir paredzēts informācijai, kas klasificēta kā CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai līdzvērtīga līmeņa informācijai. Lasītavu var aprīkot ar TEMPEST iekārtu, lai vajadzības gadījumā nodrošinātu iepazīšanos ar dokumentiem elektroniskā veidā atbilstīgi attiecīgās informācijas klasifikācijas līmenim;

f) sanāksmju telpa, kura paredzēta ne vairāk kā 25 personām informācijas, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL un SECRET EU/EU SECRET, vai līdzvērtīgas informācijas apspriešanai. Sanāksmju telpa ir aprīkota ar nepieciešamo tehnisko drošības un sertificēto aprīkojumu mutiskai tulkošanai no un uz divām valodām. Kad sanāksmju telpa netiek izmantota sanāksmēm, to kā papildu lasītavu var izmantot arī individuālas personas, lai iepazītos ar dokumentiem. Izņēmuma gadījumā KIN var atļaut iepazīties ar klasificētu informāciju vairāk kā vienai personai, kurai ir piešķirta atļauja, ja visām personām šajā telpā ir viens un tas pats drošības pielaides līmenis un tāda pati vajadzība pēc informācijas. Iepazīties ar klasificētu informāciju vienlaikus nav atļauts vairāk nekā četrām personām. KIN personāla klātbūtni pastiprina;

g) tehniskās drošības telpas, kurās glabājas viss tehniskais aprīkojums, kas savienots ar visas drošības zonas apsardzi un IT drošības serveriem.

20. Drošības zona atbilst piemērojamiem starptautiskajiem drošības standartiem un to sertificē Drošības un riska novērtēšanas direktorāts. Drošības zonā ir šāds minimālais drošības tehniskais aprīkojums:

a) signalizācijas un novērošanas sistēmas;

b) drošības aprīkojums un ārkārtēju situāciju sistēmas (divu posmu brīdinājuma sistēma);

c) videonovērošanas sistēma (CCTV);

d) pretielaušanās sistēma;

e) piekļūšanas kontrole (tostarp biometriskā drošības sistēma);

f) konteineri;

g) slēdzami skapīši:

h) aizsardzība pret elektromagnētiskajām emisijām.

21. Ja vajadzīgi papildu tehniskie drošības pasākumi, tos var noteikt DAI ciešā sadarbībā ar KIN ar DI apstiprinājumu.

22. Infrastruktūras iekārtas var tikt savienotas ar tās ēkas vispārējās pārvaldības sistēmām, kurā atrodas drošības zona. Tomēr drošības iekārtas, kas paredzētas piekļūšanas kontrolei un KIS, ir neatkarīgas no jebkurām citām Eiropas Parlamentā esošajām sistēmām.

H. **DROŠĪBAS ZONAS PĀRBAUDES**

23. DAI regulāri pārbauda drošības zonu, pārbaudes veic arī pēc KIN pieprasījuma.

24. DAI izstrādā un atjaunina tādu priekšmetu drošības pārbaudes kontrolsarakstu, kuri jāpārbauda pārbaužu laikā atbilstīgi apstrādes instrukcijām.

I. **KONFIDENCIĀLAS INFORMĀCIJAS TRANSPORTĒŠANA**

25. Kad konfidenciālu informāciju transportē, to atbilstīgi apstrādes instrukcijām dara aizklātā veidā bez norādēm par satura konfidenciālo būtību.

26. Informāciju, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai līdzvērtīga līmeņa informāciju, var transportēt tikai kurjeri vai darbinieki, kuriem ir atbilstoša drošības līmeņa atļauja.

27. Konfidenciālu informāciju var sūtīt ar ārējo pastu vai rokas bagāžu dokumentu transportēšanai ārpus ēkas vienīgi saskaņā ar nosacījumiem, kas noteikti apstrādes instrukcijās.

28. Informāciju, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai līdzvērtīga līmeņa informāciju nekādā gadījumā nesūta pa elektronisko pastu vai pa faksu, pat ja uzstādīta droša e-pasta sistēma vai kriptofakss. Informāciju, kura klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai līdzvērtīgu un citu konfidenciālu informāciju, var nosūtīt pa e-pastu, izmantojot akreditētu kriptogrāfijas sistēmu.

J. **KONFIDENCIĀLAS INFORMĀCIJAS GLABĀŠANA**

29. Konfidenciālai informācijai piešķirtais klasifikācijas vai marķējuma līmenis nosaka aizsardzības līmeni, ko piemēro tās glabāšanai. To glabā iekārtās, kas sertificētas minētajam nolūkam atbilstīgi apstrādes instrukcijām.

30. Informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai līdzvērtīgu informāciju un citu konfidenciālu informāciju:

a) glabā tērauda aizslēdzamā standartizstrādājuma skapī vai nu birojā, vai darba telpā, kad materiālus faktiski neizmanto;

b) neatstāj bez uzraudzības, ja materiāls nav atbilstoši ieslēgts un uzglabāts;

c) neatstāj uz rakstāmgalda, galda u. tml. tā, ka jebkura persona, kurai nav piešķirta atļauja, piemēram, apmeklētāji, apkopēji, apkalpojošais personāls u. tml., var to izlasīt vai iznest;

d) nerāda nevienai personai vai to neapspriež ar nevienu personu, kurai nav piešķirta atļauja.

31. Informāciju, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, vai līdzvērtīgu informāciju un citu konfidenciālu informāciju glabā vienīgi Parlamenta struktūras / pilnvarotās personas sekretariāts vai KIN atbilstīgi apstrādes instrukcijām.

32. Informāciju, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET vai TRÈS SECRET UE/EU TOP SECRET vai līdzvērtīgu informāciju:

a) glabā drošības zonā seifā vai glabātuvē. Izņēmuma gadījumā, piemēram, ja KIN ir slēgta, to var uzglabāt apstiprinātā un sertificētā seifā apsardzes dienesta telpās;

b) nekādā gadījumā drošības zonā neatstāj bez uzraudzības, to vispirms neieslēdzot apstiprinātā seifā (pat uz visīsāko prombūtnes brīdi);

c) neatstāj uz rakstāmgalda, galda u. tml. tā, ka persona, kurai nav piešķirta atļauja, varētu izlasīt vai to iznest, pat ja atbildīgais KIN personāla loceklis uzturas telpā.

Ja dokumentu, kurā ir klasificēta informācija, drošības zonā sagatavo elektroniski, laikā, kad dokumenta sagatavotājs vai atbildīgais KIN personāla loceklis atstāj telpu (pat uz visīsāko brīdi), datoru bloķē, un ekrānu padara nepieejamu. Automātiskā drošības slēdzene, kas noslēdz datoru pēc dažām minūtēm, nav uzskatāma par pietiekamu līdzekli.

DROŠĪBAS PAZIŅOJUMS Nr. 5

INDUSTRIĀLĀ DROŠĪBA

A. **IEVADS**

1. Šis drošības paziņojums attiecas tikai uz klasificētu informāciju.

2. Tajā izklāstīti noteikumi šā lēmuma I pielikuma 1. daļā paredzēto kopējo obligāto standartu īstenošanai.

3. "Industriālā drošība" ir pasākumu piemērošana, lai nodrošinātu, ka līgumslēdzējs vai apakšlīgumslēdzējs aizsargā klasificētu informāciju sarunu laikā pirms klasificēta līguma slēgšanas un klasificēto līgumu aprites laikā. Tādi līgumi nav saistīti ar piekļuvi informācijai, kas klasificēta līmenī TRES SECRET UE/EU TOP SECRET .

4. Eiropas Parlaments kā līgumslēdzēja iestāde nodrošina, ka, piešķirot klasificētu līgumu rūpniecības vai citām struktūrām, tiek ievēroti šajā lēmumā izklāstītie un attiecīgajā līgumā minētie industriālās drošības obligātie standarti.

B. **KLASIFICĒTA LĪGUMA DROŠĪBAS ELEMENTI**

B.1. ***Drošības klasifikācijas rokasgrāmata (DKR)***

5. Pirms konkursu izsludināšanas vai pirms klasificētu līgumu piešķiršanas Eiropas Parlaments kā līgumslēdzēja iestāde nosaka tās informācijas drošības klasifikāciju, kuru sniedz pretendentiem un līgumslēdzējiem, kā arī tās informācijas drošības klasifikāciju, ko sastādīs līgumslēdzējs. Šim nolūkam Eiropas Parlaments sagatavo drošības klasifikācijas metodisko līdzekli (DKML), kas jāizmanto līguma izpildei.

6. Lai noteiktu dažādu klasificēta līguma elementu drošības klasifikācijas līmeni, piemēro šādus principus:

a) izstrādājot DKR, Eiropas Parlaments ņem vērā visus attiecīgos drošības aspektus, tostarp drošības klasifikāciju, ko uz informāciju attiecinājis un apstiprinājis informācijas sagatavotājs;

b) vispārējais līguma klasifikācijas līmenis nedrīkst būt zemāks par augstāko jebkura tā elementa klasifikācijas līmeni.

B.2. ***Drošības aspektu vēstule (DAV)***

7. Ar attiecīgo līgumu saistītās drošības prasības izklāsta drošības aspektu vēstulē (DAV). Vajadzības gadījumā DAV iekļauj DKR, un tas ir neatņemama klasificēta līguma vai apakšlīguma daļa.

8. DAV iekļauj nosacījumus par to, ka līgumslēdzējam un/vai apakšlīgumslēdzējam ir jānodrošina atbilsme saskaņā ar šajā lēmumā noteiktajiem obligātajiem standartiem. Neatbilstība šiem obligātajiem standartiem var būt pietiekams pamats līguma izbeigšanai.

B.3. ***Programmas/projekta drošības instrukcijas (PDI)***

9. Atkarībā no to projektu vai programmu darbības jomas, kurās vajadzīga piekļuve ESKI, vai kurās tā jāapstrādā vai jāglabā, līgumslēdzēja iestāde, kurai uzticēta atbildība par attiecīgās programmas vai projekta pārvaldību, var izstrādāt programmas/projekta drošības instrukcijas (PDI).

C. **IESTĀDES DROŠĪBAS PIELAIDE (IDP)**

10. IDP piešķir dalībvalsts VDI vai jebkura cita kompetentā iestāde, lai atbilstīgi valsts normatīvajiem aktiem apliecinātu, ka rūpniecības vai cita struktūra savās telpās spēj nodrošināt pietiekamu ESKI aizsardzību attiecīgā klasifikācijas līmenī CONFIDENTIEL UE/EU CONFIDENTIAL vai SECRET UE/EU SECRET vai līdzvērtīgā līmenī. Apliecinājumu par IDP piešķiršanu iesniedz Eiropas Parlamentam kā līgumslēdzējai iestādei, pirms līgumslēdzējam vai apakšlīgumslēdzējam vai iespējamam līgumslēdzējam vai apakšlīgumslēdzējam var piešķirt vai nodrošināt piekļuvi ESKI.

11. Piešķirot IDP:

a) novērtē rūpniecības vai citas struktūras integritāti;

b) novērtē atbildību, kontroli un/vai iespējas izdarīt neatļautu ietekmi, ko var uzskatīt par drošības apdraudējumu;

c) pārbauda, vai rūpniecības vai cita struktūra iestādē ir izveidojusi drošības sistēmu, kurā ietverti visi atbilstīgie drošības pasākumi, kas vajadzīgi, lai aizsargātu informāciju vai materiālus, kas atbilstīgi šajā lēmumā izklāstītajām prasībām ir klasificēti līmenī CONFIDENTIEL UE/EU CONFIDENTIAL vai SECRET UE/EU SECRET ;

d) pārbauda, vai to vadības, īpašnieku un darbinieku personāla drošības statuss, kuriem vajadzīga piekļuve informācijai, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL vai SECRET UE/EU SECRET, ir noteikts saskaņā ar šajā lēmumā noteiktajām prasībām;

e) pārbauda, vai rūpniecības vai cita struktūra ir iecēlusi iestādes drošības ierēdni, kurš ir atbildīgs savas vadības priekšā par drošības pienākumu īstenošanu šajā vienībā.

12. Ja vajadzīgs, Eiropas Parlaments kā līgumslēdzēja iestāde paziņo attiecīgajai VDI vai jebkurai citai kompetentai drošības iestādei, ka IDP ir vajadzīga pirms līguma parakstīšanas vai līguma pildīšanas laikā. Pirms līguma parakstīšanas pieprasa IDP vai personāla drošības pielaidi (PDP), ja priekšlikuma iesniegšanas procesā ir jāsniedz informācija, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL vai SECRET UE/EU SECRET .

13. Līgumslēdzēja iestāde nepiešķir klasificētu līgumu izraudzītajam pretendentam pirms nav saņemts tās dalībvalsts VDI vai kādas citas kompetentas drošības iestādes apstiprinājums, kurā reģistrēti iesaistītie līgumslēdzēji vai apakšlīgumslēdzēji, ka viņiem ir izsniegta atbilstīga IDP, ja tas vajadzīgs.

14. Jebkura kompetentā drošības iestāde, kas izsniegusi IDP, paziņo Eiropas Parlamentam kā līgumslēdzējai iestādei par jebkādām izmaiņām, kas ietekmē IDP. Apakšlīguma gadījumā attiecīgi informē kompetento drošības iestādi.

15. Ja attiecīgā VDI vai kāda cita kompetenta drošības iestāde atceļ IDP, tas ir pietiekams pamats Eiropas Parlamentam kā līgumslēdzējai iestādei izbeigt klasificētu līgumu vai izslēgt attiecīgo pretendentu no konkursa.

D. **KLASIFICĒTI LĪGUMI UN APAKŠLĪGUMI**

16. Ja pretendentam sniedz klasificētu informāciju pirms līguma parakstīšanas, aicinājumā piedalīties iekļauj prasību, ka ikvienam potenciālajam pretendentam, kurš neiesniedz priekšlikumu vai kuru neizvēlas, noteiktā laikposmā ir jāatdod atpakaļ visi klasificētie dokumenti.

17. Kad klasificētais līgums vai apakšlīgums ir piešķirts, Eiropas Parlaments kā līgumslēdzēja iestāde paziņo līgumslēdzēja vai apakšlīgumslēdzēja VDI un/vai jebkurai citai kompetentai drošības iestādei klasificētā līguma drošības noteikumus.

18. Kad šāds līgums tiek izbeigts, Eiropas Parlaments kā līgumslēdzēja iestāde (un/vai kompetentā drošības iestāde apakšlīguma gadījumā) nekavējoties par to paziņo tās dalībvalsts VDI vai jebkurai citai kompetentai drošības iestādei, kurā līgumslēdzējs vai apakšlīgumslēdzējs reģistrēts.

19. Parasti līgumslēdzējam vai apakšlīgumslēdzējam jāpieprasa atdot viņa rīcībā esošo klasificēto informāciju līgumslēdzējai iestādei, ja šāda informācija ir viņa rīcībā laikā, kad beidzas klasificēta līguma vai apakšlīguma darbība.

20. Drošības aspektu vēstulē ir paredzēti konkrēti noteikumi attiecībā uz klasificētas informācijas iznīcināšanu līguma darbības laikā vai pēc tā darbības beigām.

21. Ja līgumslēdzējam vai apakšlīgumslēdzējam ir atļauts saglabāt klasificētu informāciju pēc līguma darbības beigām, viņam joprojām ir japiemēro šajā lēmumā noteiktie obligātie standarti un jāsargā ESKI konfidencialitāte.

22. Nosacījumus par kārtību, kādā līgumslēdzējs var slēgt apakšlīgumu, definē gan uzaicinājumā uz konkursu, gan līgumā.

23. Pirms līgumslēdzējs atsevišķas klasificēta līguma daļas nodod apakšlīgumslēdzējam, tas saņem atļauju no Eiropas Parlamenta kā līgumslēdzējas iestādes. Nedrīkst piešķirt apakšlīgumu rūpniecības vai citām struktūrām, kas reģistrētas trešā valstī, ja tā nav noslēgusi informācijas drošības nolīgumu ar Savienību.

24. Līgumslēdzējs ir atbildīgs par to, lai visas apakšlīgumslēdzēja darbības tiktu veiktas saskaņā ar šajā lēmumā noteiktiem obligātajiem standartiem un ESKI netiktu nodota apakšlīgumslēdzējam bez iepriekšējas rakstiskas līgumslēdzējas iestādes piekrišanas.

25. Attiecībā uz klasificētu informāciju, ko sagatavo vai apstrādā līgumslēdzējs vai apakšlīgumslēdzējs, līgumslēdzēja iestāde piemēro informācijas sagatavotāja tiesības.

E. **AR KLASIFICĒTIEM LĪGUMIEM SAISTĪTI APMEKLĒJUMI**

26. Ja Eiropas Parlaments, līgumslēdzēji vai apakšlīgumslēdzēji lūdz piekļuvi informācijai, kas klasificēta līmenī CONFIDENTIEL UE/EU CONFIDENTIAL vai SECRET UE/EU SECRET, viens otra telpās klasificēta līguma darbības laikā, apmeklējumus organizē sadarbībā ar Valsts drošības iestādi (VDI) vai jebkuru citu attiecīgo kompetento drošības iestādi. Tomēr noteiktu projektu gadījumā VDI var vienoties arī par kārtību, ar ko tādus apmeklējumus var organizēt tieši.

27. Visiem apmeklētājiem ir attiecīgā PDP un tiem ir atbilstoša "vajadzība zināt", lai varētu piekļūt klasificētai informācijas, kas saistīta ar Eiropas Parlamenta līgumu.

28. Apmeklētājiem nodrošina piekļuvi tikai tai klasificētajai informācijai, kura saistīta ar apmeklējuma mērķi.

F. **KLASIFICĒTAS INFORMĀCIJAS NOSŪTĪŠANA UN PĀRVIETOŠANA**

29. Attiecībā uz klasificētas informācijas elektronisku nosūtīšanu piemēro drošības paziņojuma Nr. 3 attiecīgos noteikumus.

30. Attiecībā uz klasificētas informācijas pārvietošanu piemēro drošības paziņojuma Nr. 4 attiecīgos noteikumus un attiecīgās apstrādes instrukcijas.

31. Nosakot drošības pasākumus klasificēto materiālu pārvietošanai ar kravu pārvadājumiem, piemēro šādus principus:

a) drošību garantē visos posmos sūtīšanas laikā no sagatavošanas vietas līdz galamērķim;

b) sūtījumam piešķirto drošības līmeni nosaka augstākais iekļauto materiālu klasifikācijas līmenis;

c) uzņēmumiem, kas nodrošina sūtīšanu, veic piemērotā līmeņa IDP. Šajos gadījumos personālam, kas apstrādā sūtījumu, veic drošības pārbaudi atbilstīgi I pielikumam;

d) pirms materiālu, kas klasificēts līmenī CONFIDENTIEL UE/EU CONFIDENTIAL vai SECRET UE/EU SECRET, vai līdzvērtīgu materiālu pārvieto pāri robežām, sūtītājs sagatavo pārsūtīšanas plānu, un ģenerālsekretārs to apstiprina;

e) maršrutus, cik vien iespējams, veic tieši no noteiktas izbraukšanas vietas līdz noteiktam galamērķim, un tos veic tik ātri, cik to apstākļi pieļauj;

f) izmantotie maršruti, kad vien iespējams, ved caur dalībvalstu teritorijām.

G. **KLASIFICĒTAS INFORMĀCIJAS PĀRSŪTĪŠANA LĪGUMSLĒDZĒJIEM TREŠĀS VALSTĪS**

32. Klasificētu informāciju pārsūta līgumslēdzējiem vai apakšlīgumslēdzējiem, kas atrodas trešās valstīs, atbilstīgi drošības pasākumiem, par kuriem vienojies Eiropas Parlaments kā līgumslēdzēja iestāde un tā trešā valsts, kurā līgumslēdzējs reģistrēts.

H. **INFORMĀCIJAS, KAS KLASIFICĒTA LĪMENĪ RESTREINT UE / EU RESTRICTED, APSTRĀDE UN GLABĀŠANA**

33. Attiecīgā gadījumā sadarbībā ar dalībvalsts VDI Eiropas Parlaments kā līgumslēdzēja iestāde, pamatojoties uz līguma noteikumiem, var apmeklēt līgumslēdzēja/apakšlīgumslēdzēja telpas, lai pārbaudītu, vai tiek īstenoti līgumā noteiktie vajadzīgie drošības pasākumi, lai aizsargātu ESKI, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED .

34. Ciktāl tas vajadzīgs atbilstīgi valsts normatīvajiem aktiem, Eiropas Parlaments kā līgumslēdzēja iestāde informē VDI vai jebkuras citas kompetentās drošības iestādes par līgumiem vai apakšlīgumiem, kuros ir iekļauta līmenī RESTREINT UE/EU RESTRICTED klasificēta informācija.

35. Līgumslēdzējam vai apakšlīgumslēdzējam un viņu personālam nav vajadzīga IDP vai PDP attiecībā uz līgumiem, ko piešķīris Eiropas Parlaments un kuros iekļauta informācija, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED .

36. Eiropas Parlaments kā līgumslēdzēja iestāde izskata iesniegtos pieteikumus līgumiem, kuros vajadzīga piekļuve līmenī RESTREINT UE/EU RESTRICTED klasificētai informācijai, neskarot prasības saistībā ar IDP vai PDP, kas var būt noteiktas valsts normatīvajos aktos.

37. Nosacījumus par kārtību, kādā līgumslēdzējs var slēgt apakšlīgumu, definē gan izsludinātajā konkursā, gan līgumā.

38. Ja līgumslēdzēja izmantotās komunikāciju un informācijas sistēmās ir ar līgumu saistīta informācija, kas klasificēta līmenī RESTREINT UE/EU RESTRICTED, tad Eiropas Parlaments kā līgumslēdzēja iestāde nodrošina, ka līgumā vai katrā apakšlīgumā ir noteiktas nepieciešamās tehniskās un administratīvās prasības attiecībā uz komunikāciju un informācijas sistēmu akreditāciju, kas ir samērīgas ar novērtēto apdraudējumu, ņemot vērā visus atbilstīgos faktorus. Līgumslēdzēja iestāde un attiecīgā VDI/IDI savstarpēji vienojas par tādu komunikāciju un informācijas sistēmu akreditācijas darbības jomu.

DROŠĪBAS PAZIŅOJUMS Nr. 6

DROŠĪBAS PĀRKĀPUMI ATTIECĪBĀ UZ KONFIDENCIĀLU INFORMĀCIJU, TĀS ZUDUMS VAI APDRAUDĒŠANA

1. Drošība tiek pārkāpta, ja tādas darbības vai bezdarbības rezultātā, kas ir pretrunā ar šo lēmumu, tiek apdraudēta vai kompromitēta konfidenciāla informācija.

2. Konfidenciālas informācijas apdraudējums notiek, ja tā ir pilnībā vai daļēji nonākusi nepiederošu personu rokās, proti, tādu personu, kurām nav nedz atbilstošas drošības pielaides, nedz vajadzības pēc informācijas, vai, ja pastāv iespēja, ka šāds gadījums ir noticis.

3. Konfidenciāla informācija var būt apdraudēta paviršības, neuzmanības vai neapdomības rezultātā, kā arī tādu dienestu darbību rezultātā, kuri vēršas pret Savienību, vai graujošu organizāciju darbības rezultātā.

4. Ja ģenerālsekretārs konstatē vai ja viņu informē par pierādītu drošības pārkāpumu vai aizdomām, ka ir zudusi vai ir apdraudēta konfidenciāla informācija, viņš:

a) konstatē faktus;

b) izvērtē un mazina nodarīto kaitējumu;

c) veic attiecīgus pasākumus, lai novērstu atkārtošanos;

d) paziņo par to trešās puses vai tās dalībvalsts kompetentajai iestādei, kura konfidenciālo informāciju sagatavojusi vai pārsūtījusi.

Ja gadījums attiecas uz Eiropas Parlamenta deputātu, ģenerālsekretārs rīkojas sadarbībā ar Parlamenta priekšsēdētāju.

Ja informāciju saņem no citas Savienības iestādes, ģenerālsekretārs rīkojas saskaņā ar atbilstīgajiem drošības pasākumiem attiecībā uz klasificētu informāciju, kā arī atbilstīgi kārtībai, kāda paredzēta Pamatnolīgumā ar Komisiju vai Iestāžu nolīgumā ar Padomi.

5. Visas personas, kuru uzdevums ir apstrādāt konfidenciālu informāciju, tiek detalizēti iepazīstinātas ar drošības procedūrām, draudiem drošībai, ko izraisa neapdomīgas sarunas un personu attiecības ar plašsaziņas līdzekļiem, un minētās personas attiecīgā gadījumā paraksta deklarāciju, ka tās ievēros pienākumus aizsargāt klasificētu informāciju un apzinās sekas, ja tos neievēros. Piekļuvi klasificētai informācijai un tās izmantošanu uzskata par drošības pārkāpumu, ja persona nav iepazīstināta ar nosacījumiem un nav parakstījusi attiecīgo deklarāciju.

6. Jebkurš Eiropas Parlamenta deputāts, Parlamenta ierēdnis un citi Parlamenta darbinieki, kas strādā politiskajās grupās vai kā līgumdarbinieki, nekavējoties ziņo ģenerālsekretāram par jebkādiem drošības pārkāpumiem, konfidenciālas informācijas zudumu vai apdraudēšanu, kas būtu kļuvuši tām zināmi.

7. Personai, kas atbildīga par konfidenciālas informācijas apdraudējumu, piemēro disciplināru atbildību saskaņā ar attiecīgiem noteikumiem. Šāda atbildība neskar nekādu tiesisku darbību, kādu var veikt saskaņa ar piemērojamiem tiesību aktiem.

8. Neskarot citu juridisku darbību, ja šādus pārkāpumus izdarījis kāds no Parlamenta ierēdņiem vai citiem Parlamenta darbiniekiem, kuri strādā politiskajās grupās, piemēro procedūras un sodus, kas paredzēti Civildienesta noteikumu VI sadaļā.

9. Neskarot citu juridisku darbību, pārkāpumus, ko izdarījuši Eiropas Parlamenta deputāti, izskata atbilstīgi Parlamenta Reglamenta 9. panta 2. punktam, 152., 153. un 154. pantam.