IV

(Paziņojumi)

EIROPAS SAVIENĪBAS IESTĀŽU UN STRUKTŪRU SNIEGTI PAZIŅOJUMI

EIROPAS PARLAMENTS

EIROPAS PARLAMENTA PREZIDIJA LĒMUMS

(2011. gada 6. jūnijs)

par noteikumiem par rīcību ar konfidenciālu informāciju Eiropas Parlamentā

(2011/C 190/02)

EIROPAS PARLAMENTA PREZIDIJS,

ņemot vērā Reglamenta 23. panta 12. punktu,

tā kā:

(1) Sakarā 2010. gada 20. oktobrī parakstīto pamatnolīgumu par attiecībām starp Eiropas Parlamentu un Eiropas Komisiju [1] ("pamatnolīgums") ir nepieciešams pārskatīt Prezidija 2006. gada 13. novembra lēmumu par noteikumiem par administratīvo procedūru attiecībā uz konfidenciāliem dokumentiem.

(2) Lisabonas līgumā Eiropas Parlamentam noteikti jauni uzdevumi, un, lai aktīvāk veiktu Eiropas Parlamenta darbības jomās, kurās nepieciešama konfidencialitāte, nepieciešams noteikt pamatprincipus, obligātos drošības standartus un atbilstīgas procedūras rīcībai ar konfidenciālu, tostarp klasificētu, informāciju Eiropas Parlamentā.

(3) Šī 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) Šī Lēmuma noteikumus pieņem, neierobežojot Līguma par Eiropas Savienības darbību (LESD) 15. pantu un Eiropas Parlamenta un Padomes 2001. gada 30. maija Regulu (EK) Nr. 1049/2001 par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem [2].

(5) Šī Lēmuma noteikumus pieņem, neierobežojot LESD 16. pantu un Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regulu (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti [3],

IR PIEŅĒMIS ŠĀDU LĒMUMU:

1. pants

Mērķis

Šis Lēmums nosaka kārtību, kādā veic konfidenciālas informācijas sagatavošanu, saņemšanu, pārsūtīšanu un glabāšanu Eiropas Parlamentā, lai nodrošinātu tās konfidenciālā rakstura atbilstīgu aizsardzību. Ar to jo īpaši īsteno 2. pielikumu pamatnolīgumā.

[1] OV L 304, 20.11.2010., 47. lpp.

[2] OV L 145, 31.5.2001., 43. lpp.

[3] OV L 8, 12.1.2001., 1. lpp.

2. pants

Definīcijas

Šajā Lēmumā:

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

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

c) "ES klasificēta informācija" (ESKI) ir visu veidu informācija un materiāli, kas ir klasificēti kā "ES SEVIŠĶI SLEPENI", "ES SLEPENI", "ES KONFIDENCIĀLI" vai "ES DIENESTA VAJADZĪBĀM", un kuru neatļauta izpaušana varētu radīt dažādas pakāpes kaitējumu Savienības vai vienas vai vairāku dalībvalstu interesēm neatkarīgi no tā, vai šāda informācija ir sagatavota kādā no ES iestādēm, struktūrām, pārvaldēm un aģentūrām, kas izveidotas saskaņā ar Līgumiem, vai arī tā ir saņemta no dalībvalstīm, trešām valstīm vai starptautiskām organizācijām. Šajā sakarā:

— "ES SEVIŠĶI SLEPENI" ir klasifikācija informācijai un materiāliem, kuru neatļauta izpaušana varētu nodarīt ārkārtīgi smagu kaitējumu Savienības vai vienas vai vairāku dalībvalstu būtiskām interesēm,

— "ES SLEPENI" ir klasifikācija informācijai un materiāliem, kuru neatļauta izpaušana varētu nodarīt nopietnu kaitējumu Savienības vai vienas vai vairāku dalībvalstu būtiskām interesēm,

— "ES KONFIDENCIĀLI" ir klasifikācija informācijai un materiāliem, kuru neatļauta izpaušana varētu nodarīt kaitējumu Eiropas Savienības vai vienas vai vairāku dalībvalstu būtiskām interesēm,

— "ES DIENESTA VAJADZĪBĀM" ir klasifikācija informācijai un materiāliem, kuru neatļauta publiskošana varētu būt nevēlama Savienības vai vienas vai vairāku dalībvalstu interesēm.

d) "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 tam no citām ES iestādēm, struktūrām, pārvaldēm un aģentūrām, kas izveidotas saskaņā ar Līgumiem, vai arī no dalībvalstīm;

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

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

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

h) "atļaujas piešķiršana" ir lēmums (lēmums par pielaidi), ko pieņem priekšsēdētājs, ja tas attiecas uz Eiropas Parlamenta deputātiem un ģenerālsekretārs, ja tas attiecas uz Parlamenta ierēdņiem un citiem Parlamenta darbiniekiem, kuri strādā politiskajās grupās, lai piešķirtu individuālu pieeju ESKI 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;

i) "klasifikācijas samazināšana" ir klasifikācijas līmeņa pazemināšana;

j) "deklasificēšana" ir jebkāda klasifikācijas līmeņa atcelšana;

k) "autors" ir pienācīgi pilnvarots ESKI vai jebkāda cita veida konfidenciālas informācijas autors;

l) "drošības paziņojumi" ir tehniski īstenošanas pasākumi, kā noteikts II pielikumā [1].

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 vadības sistēmu *(ISMS)* saskaņā ar pamatprincipiem un obligātajiem standartiem, kuras mērķis ir veicināt parlamentāro un administratīvo darbu, vienlaikus nodrošinot jebkuras Eiropas Parlamentā apstrādātās konfidenciālās informācijas aizsardzību, pilnībā ievērojot šīs informācijas autora drošības paziņojumos paredzētos noteikumus.

Konfidenciālas informācijas apstrāde ar Eiropas Parlamenta automatizētām informācijas sistēmām (IS) notiek saskaņā ar koncepciju par informācijas aizsardzību (IA) un ir noteikta drošības paziņojumos.

[1] Šo pielikumu vēl pieņems.

3. Eiropas Parlamenta deputāti bez drošības pielaides var iepazīties ar klasificēto informāciju līdz un ieskaitot līmeni "ES KONFIDENCIĀLI". Attiecībā uz informāciju, kas klasificēta kā "ES KONFIDENCIĀLI" viņi paraksta oficiālu apliecinājumu, ka neizpaudīs šīs informācijas saturu trešajām personām. Informācija, kas klasificēta augstāk par līmeni "ES KONFIDENCIĀLI" ir pieejama tikai tiem deputātiem, kuriem ir atbilstīgs drošības pielaides līmenis.

4. Eiropas Parlamenta ierēdņi un citi Parlamenta darbinieki, kas strādā politiskajās grupās, var iepazīties ar konfidenciālu informāciju, ja ir apliecināta viņu vajadzība pēc informācijas, ka arī ar informāciju, kas klasificēta augstāk par līmeni "ES DIENESTA VAJADZĪBĀM", ja viņiem ir atbilstīgs drošības pielaides līmenis.

4. pants

Konfidenciālas informācijas sagatavošana un administratīvā pārvaldība Eiropas Parlamentā

1. Eiropas Parlamenta priekšsēdētājs, attiecīgo Parlamenta komiteju priekšsēdētāji un ģenerālsekretārs, un/vai jebkura cita persona, kuru viņš ir pienācīgi pilnvarojis rakstiski, var sagatavot konfidenciālu informāciju un/vai klasificētu informāciju, kā noteikts drošības paziņojumos.

2. Sagatavojot klasificētu informāciju, autors piemēro atbilstoša līmeņa klasifikāciju saskaņā ar starptautiskiem standartiem un definīcijām, kas izklāstītas I pielikumā. Autors parasti nosaka arī adresātus, kuriem ir atļauts iepazīties ar šo informāciju atbilstoši tās klasifikācijas līmenim. Šo informāciju paziņo Konfidenciālās informācijas dienestam (KID), kad dokuments tam tiek nodots.

3. Ar konfidenciālu informāciju, uz kuru attiecas dienesta noslēpums, rīkojas saskaņā ar pārvaldības instrukcijām, kuras noteiktas drošības paziņojumos.

5. pants

Konfidenciālas informācijas saņemšana Eiropas Parlamentā

1. Par Eiropas Parlamentā saņemtu konfidenciālu informāciju paziņo:

— par ESKI "ES DIENESTA VAJADZĪBĀM" līmeņa informāciju un citu konfidenciālu informāciju – tās Parlamenta struktūras sekretariātam/pilnvarotajai personai, kura iesniegusi pieprasījumu,

— par ESKI "ES KONFIDENCIĀLI" un augstāka līmeņa informāciju – KID.

2. Konfidenciālas informācijas reģistrāciju, glabāšanu un izsekojamību nodrošina vai nu Parlamenta struktūras sekretariāts/-pilnvarotā persona, kas saņēmuši informāciju, vai KID.

3. Ja konfidenciālu informāciju nosūtījusi Komisija saskaņā ar pamatnolīgumu, panāktās vienošanās pamatnolīguma 2. pielikuma 3.2. punkta izpratnē (kopēja vienošanās par adresātiem, apspriežu procedūru, t. i. drošu lasītavu un tikšanos aiz slēgtām durvīm, vai citi jautājumi), kuras paredzētas, lai saglabātu informācijas konfidencialitāti, uzglabā kopā ar Parlamenta struktūras sekretariāta/pilnvarotās personas vai KID konfidenciālo informāciju, ja šī nosūtītā informācija tiek klasificēta "ES KONFIDENCIĀLI" vai augstākā līmenī.

4. 3. punktā minēto kārtību konfidenciālas informācijas izplatīšani *mutatis mutandis* var piemērot arī citās ES iestādēs, organizācijās, pārvaldēs un aģentūrās, kas izveidotas saskaņā ar Līgumiem vai arī izveidotas dalībvalstīs.

5. ESKI "ES SEVIŠĶI SLEPENI" līmeņa informāciju nosūta Eiropas Parlamentam saskaņā ar turpmāku kārtību, par kuru vienojas Parlamenta struktūra/pilnvarotā persona, kas iesniedza pieprasījumu un tā ES iestāde, struktūra un aģentūra vai arī dalībvalsts, kas šo informāciju izplata. Priekšsēdētāju konference izveido uzraudzības komiteju. Tās mērķis ir nodrošināt klasifikācijas līmenim atbilstošu aizsardzības līmeni.

6. pants

Eiropas Parlamenta veikta ESKI nosūtīšana trešām personām

Ja autors piekrīt, Eiropas Parlaments var nosūtīt ESKI citām ES iestādēm, struktūrām, pārvaldēm un aģentūrām, kas izveidotas saskaņā ar Līgumiem, vai arī dalībvalstīm ar nosacījumu, ka, rīkojoties ar ESKI, tās attiecībā uz savām darbībām un telpām nodrošina tādu noteikumu ievērošanu, kas ir līdzvērtīgi šajā Lēmumā minētajiem.

7. pants

Konfidenciālas informācijas uzglabāšana un iepazīšanās ar to drošās telpās (drošās lasītavas)

1. Drošās lasītavās nodrošina dokumentu drošu uzglabāšanu un tajās nav kopēšanas iekārtu, telefonu, faksa aparātu, skeneru vai citu tehnisku iekārtu dokumentu kopēšanai un pārraidīšanai.

2. Uz piekļuvi drošai lasītavai attiecas šādi noteikumi:

a) drošo lasītavu drīkst apmeklēt tikai šādas personas:

— Eiropas Parlamenta deputāti, Eiropas Parlamenta ierēdņi un citi Parlamenta politisko grupu darbinieki, kuri pienācīgi identificēti saskaņā ar kārtību, kas minēta 4. panta 2. punktā vai 5. panta 3. un 4. punktā,

— Eiropas Parlamenta ierēdņi, kuri atbildīgi par KID pārvaldību,

— nepieciešamības gadījumā – Eiropas Parlamenta ierēdņi, kuri atbildīgi par drošību un ugunsdrošību.

Tīrīšana drošības zonā notiek tikai KID darbinieka klātbūtnē un stingrā uzraudzībā;

b) katrai personai, kura vēlas piekļūt konfidenciālai informācijai, ir pienākums savlaicīgi darīt zināmu savu vārdu KID. KID pārbauda katras personas identitāti, kura iesniedz pieteikumu iepazīties ar konfidenciālu informāciju, kā arī nepieciešamības gadījumā pārbauda, vai šai personai ir vajadzīgais drošības pielaides līmenis un vai tā ir pilnvarota šādi rīkoties saskaņā ar noteikumiem, kas minēti 4. panta 2. punktā vai 5. panta 3. un 4. punktā;

c) KID ir pilnvarots atteikt piekļuvi lasītavai jebkurai personai, kura tur nedrīkst iekļūt atbilstoši šā punkta a) un b) apakšpunktiem. Eiropas Parlamenta deputātu iebildumi par KID lēmumu iesniedzami Eiropas Parlamenta priekšsēdētājam, savukārt ierēdņu un citu darbinieku iebildumi – ģenerālsekretāram.

3. Uz iepazīšanos ar konfidenciālo informāciju drošajā lasītavā attiecas šādi noteikumi:

a) personām, kurām atļauts iepazīties ar informāciju un kuras ir iesniegušas 2. punkta b) apakšpunktā paredzēto pieteikumu, ir jāierodas KID.

Izņemot ārkārtas apstākļus (piemēram, saņemti daudzi lūgumi iepazīties ar informāciju īsā laikā), atrasties drošajā lasītavā un iepazīties ar konfidenciālo informāciju drīkst tikai viena persona, turklāt KID amatpersonas klātbūtnē.

Minētā amatpersona informē personu, kura ir pilnvarota iepazīties ar konfidenciālo informāciju, par viņas pienākumiem, un jo īpaši lūdz parakstīt oficiālu deklarāciju par apņemšanos neizpaust informācijas saturu trešai personai;

b) kamēr notiek iepazīšanās ar konfidenciālo informāciju, aizliegts sazināties ar ārpasauli (tai skaitā aizliegta telefona vai citu saziņas tehnoloģiju lietošana), norakstīt un kopēt vai fotografēt minēto informāciju;

c) pirms dot atļauju pamest drošo lasītavu, a) apakšpunktā minētā KID atbildīgā amatpersona pārliecinās, vai tā konfidenciālā informācija, ar kuru notika iepazīšanās, atrodas savā vietā, ir neskarta un pilnīga.

4. Ja minētie noteikumi tiek pārkāpti, KID atbildīgā amatpersona informē ģenerālsekretāru, kurš gadījumā, ja pārkāpumus ir veicis deputāts, šo informāciju nodod Eiropas Parlamenta priekšsēdētājam.

8. pants

Obligātie standarti attiecībā uz cita veida iepazīšanos ar konfidenciālu informāciju

1. Gadījumā, ja konfidenciālu informāciju izskata sanāksmē aiz slēgtām durvīm, Parlamenta struktūras sekretariāts/pilnvarotā persona, kas atbild par sanāksmi nodrošina, ka:

— sanāksmē var piedalīties tikai uzaicinātās personas un tikai tad, ja tām ir nepieciešamais drošības pielaides līmenis, kas ļauj iekļūt sanāksmes telpā,

— 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,

— sanāksmes protokolā nekādā veidā netiek pieminēts diskusiju saturs par informāciju, uz kuru attiecas konfidencialitātes procedūra,

— uz konfidenciālu informāciju, kas saņēmējiem Eiropas Parlamentā sniegta mutiski, attiecas rakstiskā veidā sniegtai konfidenciālai informācijai līdzvērtīgs aizsardzības līmenis. Uz to var arī attiekties prasība saņēmējam oficiāli apliecināt, ka viņš neizpaudīs tās saturu trešai personai.

2. Ja Parlamenta struktūra/pilnvarotā persona rīkojas ar konfidenciālu informāciju ārpus sanāksmes, kas notiek aiz slēgtām durvīm:

— dokumentu kopijas papīra formātā personīgi nodod sekretariāta vadītājam, kurš tās reģistrē un sniedz apstiprinājumu par saņemšanu,

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

— neskarot 1. punktā izklāstīto administratīvo procedūru gadījumā, ja konfidenciālu informāciju izskata sanāksmē aiz slēgtām durvīm, nekādā gadījumā tos nedrīkst kopēt, saglabāt citā datu nesējā vai nosūtīt citai personai,

— piekļuve šādiem dokumentiem atļauta tikai to adresātiem un tā notiek saskaņā ar kārtību, kas minēta 4. panta 2. punktā, 5. panta 3. punktā vai 5. panta 4. punktā, turklāt sekretariāta uzraudzībā,

— sekretariāts reģistrē personas, kuras ir iepazinušās ar dokumentiem, un reģistrē arī laiku un datumu, kad šāda iepazīšanās notikusi. Šo informāciju, gatavojot 12. pantā minēto gada pārskatu, nosūta KID.

9. pants

Konfidenciālas informācijas arhivēšana

1. Eiropas Parlamenta telpās nodrošina drošu informācijas arhivēšanu.

Konfidenciālu informāciju, ko galīgi deponē KID vai Parlamenta struktūras sekretariātā / pie pilnvarotās personas, nodod drošā KID arhīvā sešu mēnešu laikā pēc tam, kad ar to pēdējo reizi notikusi iepazīšanās, un, vēlākais, vienu gadu pēc tam, kad tā tikusi deponēta.

2. Par drošu arhīvu pārvaldību ir atbildīgs KID, rīkojoties saskaņā ar standarta arhivēšanas kritērijiem.

3. Ar drošos arhīvos glabātu konfidenciālu informāciju var iepazīties, ievērojot šādus nosacījumus:

— ar informāciju var iepazīties tikai tās personas, kuru vārds un uzvārds vai amats minēts dokumentā, kas sastādīts konfidenciālas informācijas deponēšanas brīdī,

— pieteikumu par iepazīšanos ar konfidenciālu informāciju iesniedz KID, kas nodrošina attiecīgā dokumenta pārvietošanu uz drošo lasītavu,

— piemēro visas 7. pantā noteiktās procedūras un nosacījumus attiecībā uz iepazīšanos ar konfidenciālu informāciju.

10. pants

ESKI klasifikācijas līmeņa pazemināšana un deklasificēšana

1. ESKI klasificētas informācijas klasifikācijas līmeni var pazemināt vai šo informāciju deklasificēt tikai ar autora piekrišanu un, vajadzības gadījumā, pēc apspriešanās ar citām ieinteresētajām pusēm. Klasifikācijas līmeņa pazemināšanu vai deklasificēšanu apstiprina rakstiski. Autors atbild par izmaiņu paziņošanu adresātiem un tie, savukārt, atbild par izmaiņu paziņošanu citiem tālākajiem adresātiem, kuriem tie ir nosūtījuši vai nokopējuši dokumentu. Ja iespējams, autori uz klasificētiem dokumentiem norāda datumu, laika posmu vai notikumu, pēc kuriem to klasifikācijas līmeni var pazemināt vai informāciju deklasificēt. Pretējā gadījumā tie dokumentus pārskata vēlākais ik pēc pieciem gadiem, lai pārliecinātos, ka sākotnējā klasifikācija vēl arvien ir nepieciešama.

2. Drošos arhīvos glabāto dokumentu deklasificēšana notiek ne vēlāk kā pēc 30 gadiem saskaņā ar noteikumiem Padomes 1983. gada 1. februāra Regulā (EEK, Euratom) Nr. 354/83 par Eiropas Ekonomikas kopienas un Eiropas Atomenerģijas kopienas vēsturisko arhīva materiālu nodošanu atklātībai [1]. Deklasificēšanu veic klasificētās informācijas autors vai dienests, kurš par to atbildīgs saskaņā ar I pielikuma 1. daļas 10. pantu.

11. pants

Pārkāpumi attiecībā uz konfidenciālu informāciju

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

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

3. Priekšsēdētājs un ģenerālsekretārs organizē jebkādu nepieciešamo izmeklēšanu.

12. 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 iesniedz Prezidijam gada pārskatu par šā lēmuma piemērošanu.

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

13. pants

Pārejas un nobeiguma noteikumi

1. Konfidenciālā informācija, kas jau atrodas KID vai arhīvos pirms šā lēmuma piemērošanas, automātiski tiek klasificēta kā "ES DIENESTA VAJADZĪBĀM" līmeņa informācija, ja vien tās autors viena gada laikā no šā lēmuma spēkā stāšanās dienas nolemj vai nu to neklasificēt, vai klasificēt augstākā klasifikācijas līmenī vai arī marķēt šo informāciju.

2. Ja konfidenciālās informācijas autors nolemj piešķirt tai augstāku klasifikācijas līmeni, autors vai tā pārstāvji dokumentus klasificē pēc iespējas zemākā līmenī, sadarbojoties ar KID un saskaņā ar šā lēmuma I pielikumā noteiktajiem kritērijiem.

3. Atceļ Prezidija 2006. gada 13. novembra Lēmumu par noteikumiem, kas reglamentē administratīvo procedūru attiecībā uz konfidenciāliem dokumentiem.

4. Atceļ Prezidija 2005. gada 24. oktobra lēmumu, ar kuru ģenerālsekretāru pilnvaro izveidot deklasificēšanas komiteju un pieņemt lēmumus jautājumos par deklasificēšanu.

14. pants

Stāšanās spēkā

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

2. Tos piemēro no 2011. gada 1. jūlija.

I PIELIKUMS

1. DAĻA

DROŠĪBAS PAMATPRINCIPI UN OBLIGĀTIE STANDARTI KONFIDENCIĀLAS INFORMĀCIJAS AIZSARDZĪBAI

1. **Ievads**

Ar šiem noteikumiem nosaka drošības pamatprincipus un obligātos standartus, kuri pienācīgi jāievēro gan Eiropas Parlamentam visās tā darba vietās, gan arī visiem ESKI un citas konfidenciālas informācijas saņēmējiem, lai aizsargātu drošību un ikviens būtu pārliecināts, ka ir izstrādāti vienoti aizsardzības standarti. Tos papildina ar noteikumiem, kas reglamentē to, kā konfidenciālu informāciju apstrādā Parlamenta komitejas un citas Parlamenta struktūras/pilnvarotās personas.

2. **Vispārēji principi**

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. Tā nozīmē arī to, ka 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 jārīkojas veidā, kas atbilst Eiropas Parlamenta politikai disciplināro pasākumu jomā.

Pārredzamības princips paredz skaidrību attiecībā uz visiem drošības noteikumiem un nosacījumiem, lai tādējādi nodrošinātu līdzsvaru starp dažādiem dienestiem un dažādām jomām (fiziskā drošība pret informācijas aizsardzību u. c.), gan arī konsekventa un strukturēta drošības izpratnes politika. Turklāt tā nozīmē arī nepieciešamību noteikt precīzas rakstiskas pamatnostādnes drošības pasākumu īstenošanai.

Atbildības princips nozīmē to, ka skaidri tiks noteikti pienākumi drošības jomā. Turklāt tā nozīmē arī to, ka ir nepieciešams regulāri pārbaudīt šo pienākumu pareizu izpildi.

Subsidiaritātes princips nozīmē to, ka drošību organizē iespējami zemākā līmenī un pēc iespējas ciešākā saiknē ar ģenerāldirektorātiem un Eiropas Parlamenta dienestiem. Samērīguma princips nozīmē to, ka drošības darbībās iekļauj tikai to, kas patiešām ir nepieciešams un ka drošības pasākumiem jābūt samērīgiem ar aizsargājamām interesēm un faktiskiem vai iespējamiem draudiem šīm interesēm, sniedzot tādu aizsardzību, kas izraisa vismazāko iespējamo traucējumu.

3. **Informācijas drošības pamati**

Efektīvas informācijas drošības pamati ir:

a) Eiropas Parlamentā – *INFOSEC* (informācijas drošības) nodrošināšanas pakalpojumu iestāde, kas atbild par sadarbību ar attiecīgo drošības iestādi, lai sniegtu informāciju un konsultācijas par tehniskiem draudiem drošībai un veidiem, kā pret tiem aizsargāties;

b) cieša sadarbība starp Eiropas Parlamenta atbildīgajiem dienestiem un citu Eiropas iestāžu drošības dienestiem.

4. **Informācijas drošības principi**

4.1. *Mērķi*

Galvenie informācijas drošības mērķi ir šādi:

a) aizsargāt ESKI un citu klasificēto informāciju no spiegošanas, apdraudējuma vai neatļautas atklāšanas;

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

c) aizsargāt Eiropas Parlamenta telpas, kurās atrodas ESKI, 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 nepieciešamos pasākumus stāvokļa uzlabošanai.

4.2. *Klasificēšana*

4.2.1. Attiecībā uz konfidencialitāti nepieciešama rūpība un pieredze, izvēloties informāciju un materiālu, kas ir jāaizsargā, un izvērtējot tiem piemērojamo aizsardzības pakāpi. Ir būtiski, lai aizsardzības pakāpe atbilstu konkrētās aizsargājamās informācijas vai materiāla drošības nozīmībai. Lai nodrošinātu vienmērīgu informācijas plūsmu, veic pasākumus, lai izvairītos no pārlieku augstas vai zemas klasifikācijas pakāpes piešķiršanas.

4.2.2. Klasifikācijas sistēma ir šajā nodaļā minēto principu īstenošanas instruments; līdzīgu klasifikācijas sistēmu ievēro, plānojot un organizējot veidus, lai apkarotu spiegošanu, sabotāžu, terorismu un citus draudus un lai attiecībā uz vissvarīgākajām telpām, kurās atrodas ESKI, un visjutīgākajām to vietām piemērotu vislielākos aizsardzības pasākumus.

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

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

4.2.5. Ja ir grupētas vairākas ziņas, klasifikācijas pakāpe, ko piešķir visam kopumam, ir vismaz tik augsta kā visaugstākā individuāli piešķirtā klasifikācija. Grupētai informācijai tomēr 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 ESKI, ESKI nesējiem un citai konfidenciālai informācijai, ka arī visām telpām, kurās atrodas šāda informācija, un svarīgām iekārtām;

b) ir izveidoti tā, lai atpazītu personas, kuru stāvoklis var apdraudēt šādas informācijas drošību un svarīgas iekārtas, kas satur šādu informāciju un kas paredzētas to izslēgšanai vai iznīcināšanai;

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

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

e) nodrošina integritāti (piemēram, korupcijas novēršanu vai neatļautu izmaiņu veikšanu vai neatļautas izdzēšanas novēršanu) un pieejamību (piemēram, piekļuve netiek liegta tiem, kam tā ir nepieciešama un kam tā ir atļauta) visai konfidenciālajai informācijai, vai tā ir klasificēta vai nav, jo īpaši tādai informācijai, kas ir uzglabāta, apstrādāta vai pārsūtīta elektromagnētiskā formā.

5. **Kopējie obligātie standarti**

Eiropas Parlaments nodrošina to, ka kopējos obligātos drošības standartus ievēro visi ESKI 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 iekļauj kritērijus drošības atļauju izsniegšanai Eiropas Parlamenta ierēdņiem un citiem Parlamenta darbiniekiem, kuri strādā politiskajās grupās, un procedūrām konfidenciālas informācijas aizsardzībai.

Eiropas Parlaments ļauj piekļūt šai informācijai ārējām struktūrām 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 piešķir uzdevumus, kuru veikšanai nepieciešama konfidenciāla informācija par rūpniecības vai citām vienībām.

6. **Eiropas Parlamenta ierēdņu un citu Parlamenta darbinieku, kuri strādā politiskās grupās, drošība**

6.1. *Drošības instrukcijas 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 ESKI, stājoties amatā un pēc regulāriem starplaikiem, rūpīgi instruē par nepieciešamību ievērot drošību un tās nodrošināšanas procedūrām. Šādas personas rakstiski apliecina, ka tās ir izlasījušas un pilnīgi saprot piemērojamos drošības noteikumus.

6.2. *Vadītāju atbildība*

Vadītāju pienākums ir apzināt tos sev pakļautos darbiniekus, kuri ir iesaistīti darbā ar klasificētu informāciju vai kuriem ir piekļuve slepenai saziņai 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 un citu Parlamenta darbinieku, kas strādā politiskajās grupās, nosaka, vai šī indivīda darbs ir saistīts ar klasificētu informāciju un vai viņam ir piekļuve slepenai saziņai vai informācijas sistēmām, par ko informē Eiropas Parlamenta attiecīgo dienestu. Ja konstatē, ka šāds indivīds apdraud drošību, to atceļ no tādiem darbiem vai liedz pildīt uzdevumus, kuros viņš var apdraudēt drošību.

7. **Fiziskā drošība**

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

7.1. *Vajadzība pēc aizsardzības*

ESKI aizsardzības nodrošināšanai piemēroto fiziskās drošības pasākumu pakāpe ir samērīga ar uzglabātās informācijas un materiāla klasifikāciju, apjomu un apdraudējumu. Visi ESKI 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 iziet no zonām, kurās atrodas ESKI, atbildīgās personas nodrošina to, ka tā tiek droši uzglabāta un darbojas visas drošības ierīces (slēdzenes, trauksmes signāli u. c.). Papildu neatkarīgu pārbaudi veic pēc darba dienas beigām.

7.3. *Ēku drošība*

Ēkas, kurās atrodas ESKI vai slepenas komunikācijas un informācijas sistēmas, aizsargā pret neatļautu piekļuvi.

ESKI nodrošinātais aizsardzības raksturs, piemēram, logu aizrestošana, durvju slēdzenes, durvju apsardze, automatizētas iekļūšanas kontroles sistēmas, drošības pārbaudes un patruļas, signalizācijas sistēmas, iekļūšanas noteikšanas sistēmas un sargsuņi, ir atkarīgs 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.

Tāpat komunikācijas un informācijas sistēmām piešķirtā aizsardzība ir atkarīga 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 ārkārtējas situācijas gadījumā.

8. **Drošības apzīmējumi, marķējums, piešķiršana un klasifikācijas pārvaldība**

8.1. *Drošības apzīmējumi*

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

Lai ierobežotu klasifikācijas derīgumu (klasificētai informācijai, kas paredz automātisku klasifikācijas līmeņa pazemināšanu vai deklasificēšanu), var izmantot norunātus drošības apzīmējumus, par kuriem panākta vienošanās. Šādi apzīmējumi ir vai nu "LĪDZ (laiks/diena)" vai "LĪDZ (notikums)".

Piemēro papildu drošības apzīmējumus, tādus kā *CRYPTO* vai jebkuru citu ES atzītu drošības apzīmējumu, ja ir nepieciešams ierobežot izplatīšanu un veikt īpašu apstrādi papildus tai, kas ir norādīta drošības klasifikācijā.

Drošības apzīmējumus izmanto tikai kopā ar klasifikāciju.

8.2. *Marķējums*

Marķējumu var izmantot, lai norādītu jomu, uz ko attiecas dokumenti, vai īpašu izplatīšanu, pamatojoties uz vajadzību pēc informācijas, vai (neklasificētai informācijai) lai norādītu aizlieguma beigas.

Ar marķējumu neklasificē un to nedrīkst lietot klasifikācijas aizstāšanai.

8.3. *Klasifikācijas piešķiršana un drošības apzīmējumi*

Klasifikāciju piešķir šādi:

a) ES DIENESTA VAJADZĪBĀM klasificētiem dokumentiem – mehāniski vai elektroniski;

b) ES KONFIDENCIĀLI klasificētiem dokumentiem – mehāniski vai ar roku, vai drukājot uz iepriekš apzīmogota, reģistrēta papīra;

c) ES SLEPENI un ES SEVIŠĶI SLEPENI klasificētiem dokumentiem – mehāniski vai ar roku.

Drošības apzīmējumus norāda tieši zem klasifikācijas tādā pašā veidā kā apzīmējumus, ar kuriem norāda klasifikāciju.

8.4. *Klasifikācijas pārvaldība*

8.4.1. Vispārējs pārskats

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

Par informācijas klasificēšanu un tās tālāku klasifikācijas līmeņa pazemināšanu vai deklasificēšanu atbild tās autors.

Eiropas Parlamenta ierēdņi klasificē, ierindo zemākā līmenī vai deklasificē informāciju pēc ģenerālsekretāra norādījuma vai ar viņa piekrišanu.

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

Personu skaitu, kurām ir atļauts izstrādāt ES SEVIŠĶI SLEPENI dokumentus, pēc iespējas vairāk ierobežo un viņu vārdus ieraksta KID sagatavotajā sarakstā.

8.4.2. Klasifikācijas piemērošana

Dokumenta klasifikāciju nosaka pēc dokumenta satura jutības pakāpes saskaņā ar 2. panta c) apakšpunktā doto definīciju. Ir svarīgi, lai klasifikāciju izmantotu pareizi un ierobežoti. Tas īpaši attiecas uz ES SEVIŠĶI SLEPENI klasifikāciju.

Vēstules vai piezīmes klasifikācija ir tikpat augsta, kā tai pievienoto dokumentu visaugstākā klasifikācija. Autors skaidri norāda, kāds klasifikācijas līmenis tam piešķirams, kad to atdala no tam pievienotajiem dokumentiem.

Tāda dokumenta autors, kuram tiks piešķirta klasifikācija, patur prātā 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 par drošību atbildīgais direktorāts, kuram šā uzdevuma īstenošanā var palīdzēt KID, periodiski pārbauda ESKI aizsardzībai paredzētos drošības pasākumus.

Parlamenta Drošības par drošību atbildīgais direktorāts un citu ES iestāžu, struktūru, pārvalžu un aģentūru, kas izveidotas saskaņā ar Līgumiem, kuru rīcībā ir ESKI, drošības dienesti var arī vienoties veikt ESKI aizsardzībai paredzēto drošības pasākumu salīdzinošo novērtēšanu.

10. **Deklasificēšanas procedūra**

10.1. KID izvērtē ESKI un sagatavos deklasifikācijas priekšlikumus dokumenta autoram, bet ne vēlāk kā 25. gadā pēc dokumenta sagatavošanas. Dokumentus, kuru klasifikācijas pakāpe nav atcelta pirmajā pārbaudē, regulāri un vismaz reizi piecos gados pārbauda..

10.2. Deklasificēšanas procedūra attiecas ne tikai uz dokumentiem, kas atrodas drošos arhīvos un ir pienācīgi klasificēti, bet arī uz citu konfidenciālu informāciju, kas uzkrāta vai nu drošos arhīvos, vai Eiropas Parlamenta Arhīvu un dokumentācijas centrā (*CARDOC*).

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

10.4. Deklasificēšana neskar marķējumus, kas var parādīties uz dokumenta.

10.5. Svītro sākotnējo klasifikāciju, kas ir norādīta katras lappuses augšā un apakšā. Uz dokumenta pirmās lapas (titullapas) uzliek zīmogu un papildina ar KID norādi.

10.6. Deklasificētā 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) attiecībā uz iesaistīto trešo pušu dokumentiem, pirms uzsākt deklasificēšanu, KID apspriežas ar konkrēto trešo pusi. Minētajai trešai pusei ir astoņas nedēļas piezīmju iesniegšanai;

b) attiecībā uz izņēmumiem, kas saistās ar privātumu un indivīda neaizskaramību, deklasificēšanā jo īpaši ņem vērā attiecīgās personas piekrišanu, nespēju noteikt attiecīgo personu un faktu, ka šī persona ir mirusi;

c) attiecībā uz izņēmumu, kas saistās ar kādas fiziskas vai juridiskas personas komerciālām interesēm, informāciju par attiecīgo personu varētu 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. Ņemot vērā Eiropas Parlamenta prerogatīvas un pilnvaras, Eiropas Parlamenta deputātiem var tik sniegta piekļuve ESKI līdz pat līmenim "ES KONFIDENCIĀLI" ieskaitot, neizsniedzot drošības pielaidi. Attiecībā uz informāciju, kas klasificēta kā "ES KONFIDENCIĀLI", viņi paraksta oficiālu deklarāciju par apņemšanos neizpaust šīs informācijas saturu trešai personai.

11.2. Lai piekļūtu informācijai, kas klasificēta kā "ES SEVIŠĶI SLEPENI" vai "ES SLEPENI", Eiropas Parlamenta deputātiem jābūt piešķirtai atļaujai atbilstoši procedūrai, kas ir minētas šīs 11.3. un 11.4. punktā.

11.3. Atļauju var piešķirt tikai tiem deputātiem, kuri izturējuši dalībvalstu kompetentās iestādes (nacionālās drošības iestādes) veiktu drošības pārbaudi saskaņā ar procedūru, kas minēta 11.9. līdz 11.14. punktā. Par atļaujas piešķiršanu deputātiem atbild priekšsēdētājs.

11.4. Priekšsēdētājs piešķir atļauju pēc dalībvalstu kompetento nacionālo iestāžu atzinuma, kas pamatojas uz drošības pārbaudi, kura ir veikta saskaņā ar 11.8. līdz 11.13. punktu.

11.5. Eiropas Parlamenta par drošību atbildīgais direktorāts uzglabā atjauninātu visu to Eiropas Parlamenta deputātu sarakstu, kuriem ir piešķirta atļauja, tostarp pagaidu atļauja 11.15. punkta nozīmē.

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 minēto procedūru.

11.7. Priekšsēdētājs atsauc atļauju, ja viņš uzskata, ka tam ir pamatoti iemesli. Ikvienu lēmumu par atļaujas atsaukšanu dara zināmu attiecīgajam Eiropas Parlamenta deputātam, kurš pirms atsaukuma stāšanās spēkā var lūgt, lai viņu uzklausa priekšsēdētājs un kompetentā valsts 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 pilsonis ir deputāts, kam tiek piešķirta atļauja.

11.9. Veicot pārbaudes procedūru, attiecīgais Eiropas Parlamenta deputāts aizpilda personas informācijas veidlapu.

11.10. Pieprasījumā valsts kompetentai iestādei priekšsēdētājs norāda konkrētu klasificētās informācijas līmeni, kas jādara pieejams attiecīgajam Eiropas Parlamenta deputātam, lai tās varētu veikt pārbaudes procedūru.

11.11. Uz visu drošības pārbaudes procedūru, ko veic valsts 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. Valsts kompetento iestāžu negatīvu atzinumu dara zināmu attiecīgajam Eiropas Parlamenta deputātam, kurš var lūgt, lai viņu uzklausa priekšsēdētājs. Ja priekšsēdētājs uzskata par vajadzīgu, viņš var lūgt valsts kompetentajām iestādēm veikt visu iespējamo turpmāko lietas noskaidrošanu. Ja negatīvu atzinumu apstiprina, atļauju nepiešķir.

11.14. Visi deputāti, kuriem ir piešķirta atļauja 11.3. punkta izpratnē, atļaujas piešķiršanas laikā un turpmāk regulāri saņem visu nepieciešamās vadlīnijas par klasificētas informācijas aizsargāšanu un šādas aizsardzības nodrošināšanas līdzekļiem. Šādi deputāti paraksta deklarāciju par minēto vadlīniju saņemšanu.

11.15. Izņēmuma gadījumā priekšsēdētājs pēc paziņojuma nosūtīšanas valsts kompetentajām iestādēm un ar nosacījumu, ka tās mēneša laikā nesniedz atbildi, var piešķirt Eiropas Parlamenta deputātam pagaidu atļauju uz laiku, kas nepārsniedz sešus mēnešus, līdz būs zināmi 11.11. punktā minētās pārbaudes rezultāti. Šādi piešķirtās pagaidu atļaujas nedod piekļuvi informācijai, kas klasificēta kā "ES SEVIŠĶI SLEPENI".

12. **Drošības pielaides izsniegšanas procedūra Parlamenta ierēdņiem un citiem Eiropas Parlamenta darbiniekiem, kas strādā politiskajās grupās**

12.1. Piekļuve šādai informācijai ir tikai Eiropas Parlamenta ierēdņiem un citiem Eiropas Parlamenta darbiniekiem, kas strādā politiskajās grupās, kuriem saistībā ar to pienākumiem vai darba prasībām ir nepieciešams zināt vai izmantot klasificētu informāciju.

12.2. Lai piekļūtu informācijai, kas klasificēta kā "ES SEVIŠĶI SLEPENI" un "ES KONFIDENCIĀLI", 12.1. punktā minētajām personām ir piešķirta 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 (nacionālā drošības iestāde) saskaņā ar 12.9. līdz 12.14. punktā minēto procedūru. Par atļaujas piešķiršanu Eiropas Parlamenta ierēdņiem un Eiropas Parlamenta darbiniekiem, kas strādā politiskajās grupās, atbild ģenerālsekretārs.

12.4. Ģenerālsekretārs piešķir atļauju pēc tam, kad ir saņemts dalībvalstu kompetento nacionālo iestāžu atzinums, kas pamatojas uz drošības pārbaudi, kura ir veikta saskaņā ar šīs daļas 12.8. līdz 12.13. punkta noteikumiem.

12.5. Eiropas Parlamenta par drošību atbildīgais direktorāts uzglabā atjauninātu 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 minēto procedūru.

12.7. Ģenerālsekretārs atsauc atļauju, ja viņš uzskata, ka tam ir pamatoti iemesli. Ikviens lēmums atsaukt atļauju tiek darīts zināms attiecīgajam Eiropas Parlamenta ierēdnim un citam Parlamenta darbiniekam, kurš strādā kādā no politiskajām grupām, un šis ierēdnis vai darbinieks pirms atsaukšanas stāšanās spēkā var lūgt, lai viņu uzklausa ģenerālsekretārs un kompetentā valsts iestāde.

12.8. Drošības pārbaudi veic ar attiecīgās personas palīdzību un pēc ģenerālsekretāra pieprasījuma. Par pārbaudi ir atbildīga tās dalībvalsts nacionālā iestāde, kuras pilsonis ir attiecīgā persona. Valsts drošības iestādes vai citas valsts kompetentās iestādes, ja to paredz valsts tiesību akti, var veikt izmeklēšanu par ārvalstniekiem, kuri pieprasa piekļūšanu informācijai, kas klasificēta kā "ES KONFIDENCIĀLI", vai vēl slepenākai informācijai.

12.9. Veicot pārbaudes procedūru, attiecīgajam Eiropas Parlamenta ierēdnim un citam Parlamenta darbiniekam, kurš strādā kādā no politiskajām grupām, pieprasa aizpildīt personas informācijas veidlapu.

12.10. Ģenerālsekretārs savā pieprasījumā valsts kompetentajai iestādei precizē klasificētās informācijas, kas jādara pieejama attiecīgajai personai, veidu un pakāpi, lai tā varētu veikt pārbaudi un sniegt atzinumu par to, kāda līmeņa atļauju šai personai varētu piešķirt.

12.11. Uz visu drošības pārbaudes procedūru, ko veic valsts 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, ģenerālsekretārs var sniegt attiecīgajai personai atļauju.

12.13. Par kompetentu valsts iestāžu sniegtu negatīvu atzinumu paziņo attiecīgajam Eiropas Parlamenta ierēdnim vai Parlamenta darbiniekam, kurš strādā kādā no politiskajām grupām, un šis ierēdnis vai darbinieks var lūgt, lai viņu uzklausa ģenerālsekretārs. Ja ģenerālsekretārs uzskata par vajadzīgu, viņš var lūgt valsts kompetentajām iestādēm veikt visu iespējamo turpmāko lietas noskaidrošanu. 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 12.4. un 12.5. punkta izpratnē, atļaujas piešķiršanas laikā un turpmāk regulāri saņem visas nepieciešamās instrukcijas par slepenas informācijas aizsargāšanu un šādas aizsardzības nodrošināšanas līdzekļiem. Šādi ierēdņi un darbinieki, kuri strādā politiskajās grupās, paraksta deklarāciju par instrukciju saņemšanu un uzņemas saistības tās ievērot.

12.15. Izņēmuma gadījumā ģenerālsekretārs pēc paziņojuma nosūtīšanas valsts kompetentajām iestādēm un ar nosacījumu, ka tās mēneša laikā nesniedz atbildi, var piešķirt Eiropas Parlamenta ierēdnim vai citam Parlamenta darbiniekam, kurš strādā kādā no poliskajām grupām, 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 kā "ES SEVIŠĶI SLEPENI".