KOMISIJAS LĒMUMS (ES, Euratom) 2015/443

(2015. gada 13. marts)

par drošību Komisijā

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 249. pantu,

ņemot vērā Eiropas Atomenerģijas kopienas dibināšanas līgumu,

ņemot vērā 7. Protokolu par privilēģijām un imunitāti Eiropas Savienībā, kas pievienots Līgumiem, un jo īpaši tā 18. pantu,

tā kā:

(1) Komisijā drošības mērķis ir ļaut Komisijai darboties drošā un aizsargātā vidē, izveidojot saskaņotu un integrētu pieeju tās drošībai, nodrošinot pienācīgu aizsardzības līmeni personām, aktīviem un informācijai, kas ir samērīga ar noteiktajiem riskiem, un panākot, ka drošība tiek īstenota efektīvi un savlaicīgi.

(2) Komisija, tāpat kā citas starptautiskās organizācijas, saskaras ar nopietniem draudiem un problēmām drošības jomā, jo īpaši attiecībā uz terorismu, kiberuzbrukumiem un politisku un komerciālu spiegošanu.

(3) Eiropas Komisija kopā ar Beļģijas, Luksemburgas un Itālijas valdību piedalās vairākos ar drošības jautājumiem saistītos pasākumos tās struktūru galvenajās atrašanās vietās ([1]). Šie pasākumi apliecina, ka Komisija ir atbildīga par savu drošību.

(4) Lai nodrošinātu personu, aktīvu un informācijas drošību, Komisijai, iespējams, vajadzēs veikt pasākumus tādās jomās, ko aizsargā pamattiesības, kas noteiktas Eiropas Savienības Pamattiesību hartā un Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijā, kā to atzinusi Eiropas Savienības Tiesa.

(5) Tāpēc visiem šiem pasākumiem jābūt attaisnotiem, pamatojoties uz to, cik būtiskas ir intereses, kuru aizsardzībai tie ir paredzēti, samērīgiem un jānodrošina, ka tiek pilnībā ievērotas pamattiesības, tostarp it īpaši tiesības uz privātās dzīves neaizskaramību un datu aizsardzību.

(6) Sistēmā, kurā valda tiesiskums un pamattiesību ievērošana, Komisijai ir jācenšas panākt atbilstīgu drošības līmeni saviem darbiniekiem, aktīviem un informācijai, kas nodrošina, ka tā var veikt savu darbību, vienlaikus neierobežojot pamattiesības vairāk nekā tas ir absolūti nepieciešams.

(7) Drošība Komisijā pamatojas uz likumības, pārredzamības, proporcionalitātes un atbildības principiem.

(8) Darbiniekus, kas pilnvaroti veikt drošības pasākumus, nedrīkst viņu darbības dēļ nostādīt neizdevīgā stāvoklī, izņemot ja viņi ir rīkojušies ārpus savas kompetences vai pārkāpuši tiesību aktus un tādēļ šis lēmums ir jāuzskata par dienesta instrukciju Civildienesta noteikumu nozīmē.

(9) Komisijai būtu jāuzņemas attiecīgas iniciatīvas, lai veicinātu un nostiprinātu savu drošības kultūru, nodrošinot, ka drošība tiek īstenota efektīvi, uzlabojot tās drošības pārvaldību, vēl vairāk stiprinot sadarbības tīklus un sadarbību ar attiecīgajām iestādēm starptautiskā, Eiropas un valstu līmenī, un uzlabojot drošības pasākumu īstenošanas uzraudzību un kontroli.

(10) Eiropas Ārējās darbības dienesta (EĀDD) izveide, kas ir funkcionāli autonoma Savienības struktūra, ievērojami ietekmēja Komisijas intereses drošības jomā, un tādēļ ir nepieciešams izveidot noteikumus un procedūras EĀDD un Komisijas sadarbībai drošuma un drošības jautājumos, jo īpaši, lai izpildītu Komisijas pienākumu rūpēties par Komisijas darbiniekiem Savienības delegācijās.

([1]) Sal. ar 2004. gada 31. decembra *Arrangement entre le Gouvernement belge et le Parlement européen, le Conseil, la Commission, le Comité économique et social européen, le Comité des régions, la Banque européenne d'investissement en matière de sécurité*, 2007. gada 20. janvāra *Accord de sécurité signé entre la Commission et le Gouvernement luxembourgeois* un 1959. gada 22. jūlija *Accordo tra il Governo italiano e la Commissione europea dell'energia atomica (Euratom) per l'istituzione di un Centro comune di ricerche nucleari di competenza generale*.

(11) Komisijas drošības politika būtu jāīsteno saderīgi ar citiem iekšējiem procesiem un procedūrām, kuras var būt saistītas ar drošības jautājumiem. Jo īpaši tas attiecas uz Darbības nepārtrauktības pārvaldību, kuras mērķis ir saglabāt Eiropas Komisijas būtisko funkciju izpildi darbības traucējumu gadījumā, kā arī daudznozaru krīžu koordinācijas procesu *ARGUS*.

(12) Neatkarīgi no pasākumiem, kuri jau ir spēkā šā lēmuma pieņemšanas laikā un par kuriem jau ir paziņots Eiropas Datu aizsardzības uzraudzītājam ([1]), visiem saskaņā ar šo lēmumu noteiktajiem pasākumiem, kas ietver personas datu apstrādi, saskaņā ar 21. pantu piemēro īstenošanas noteikumus, kas paredz atbilstošus aizsardzības pasākumus datu subjektiem.

(13) Tādēļ Komisijai ir jāpārskata, jāatjaunina un jākonsolidē spēkā esošais drošības regulējuma pamats Komisijā.

(14) Tāpēc būtu jāatceļ Komisijas Lēmums C(94) 2129 ([2]),

IR PIEŅĒMUSI ŠO LĒMUMU.

1. NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Definīcijas

Šajā lēmumā piemēro šādas definīcijas:

1) "aktīvi" ir visu veidu kustamā un nekustamā manta, kas atrodas Komisijas īpašumā vai turējumā;

2) "Komisijas dienests" ir Komisijas ģenerāldirektorāts vai dienests vai Komisijas locekļa kabinets;

3) "komunikācijas un informācijas sistēma" vai "KIS" ir jebkura sistēma, kas ļauj rīkoties ar informāciju elektroniskā formā, ietverot visus aktīvus, kas nepieciešami tās darbībai, kā arī infrastruktūras, organizācijas, personāla un informācijas resursus;

4) "risku kontrole" ir jebkurš drošības pasākums, ko var pamatoti uzskatīt par tādu, kas efektīvi kontrolē risku drošībai – profilakses, ietekmes mazināšanas, izvairīšanās vai nodošanas veidā;

5) "krīzes situācija" ir apstākļi, notikums, starpgadījums vai ārkārtas situācija (kā arī to virkne vai kombinācija), kas rada nopietnus vai tūlītējus draudus drošībai Komisijā neatkarīgi no tās izcelsmes;

6) "dati" ir informācija tādā formā, kas ļauj to paziņot, ierakstīt vai apstrādāt;

7) "par drošību atbildīgais Komisijas loceklis" ir Komisijas loceklis, kura atbildības jomā ietilpst Cilvēkresursu un drošības ģenerāldirektorāts;

8) "personas dati" nozīmē personas datus, kas definēti Eiropas Parlamenta un Padomes Regulas (EK) Nr. 45/2001 ([3]) 2. panta a) punktā;

9) "telpas" ir visa veida nekustamā vai tai pielīdzināma manta, kas atrodas Komisijas īpašumā vai turējumā;

10) "riska profilakse" ir drošības pasākumi, ko var pamatoti uzskatīt par tādiem, kas traucē, kavē vai aptur drošības risku;

11) "drošības risks" ir kāda notikuma draudu pakāpes, neaizsargātības pakāpes un iespējamās ietekmes apvienojums;

12) "drošība Komisijā" ir personu, aktīvu un informācijas drošība Komisijā un jo īpaši personu un aktīvu fiziskā integritāte, informācijas kā arī informācijas un komunikācijas sistēmu integritāte, konfidencialitāte un pieejamība, kā arī Komisijas darbību nekavēta norise;

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.

([2]) Komisijas 1994. gada 8. septembra Lēmums C(94) 2129 par Drošības biroja uzdevumiem.

([3]) Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti (OV L 8, 12.1.2001., 1. lpp.).

13) "drošības pasākums" ir pasākums, ko pieņem saskaņā ar šo lēmumu, lai kontrolētu drošības riskus;

14) "Civildienesta noteikumi" ir Eiropas Savienības Civildienesta noteikumi, kas noteikti ar Padomes Regulu (EEK, Euratom, EOTK) Nr. 259/68 ([1]) un tās grozījumiem;

15) "draudi drošībai" ir notikums vai aģents, ko var pamatoti uzskatīt par tādu, kas var negatīvi ietekmēt drošību, ja uz to nereaģē un to nekontrolē;

16) "tūlītēji draudi drošībai" ir draudi drošībai, kas rodas bez iepriekšēja brīdinājuma vai ārkārtīgi īsā laikposmā pēc iepriekšējā brīdinājuma; un

17) "nopietni draudi drošībai" ir draudi drošībai, ko var pamatoti uzskatīt par tādiem, kas var izraisīt nāvi, nopietnu ievainojumu vai kaitējumu, ievērojamus bojājumus īpašumam, kaitēt īpaši sensitīvai informācijai, pārraut IT sistēmu darbību vai būtiskas Komisijas darbības spējas;

18) "neaizsargātība" ir jebkura vājā vieta, ko var pamatoti uzskatīt par tādu, kas var negatīvi ietekmēt drošību Komisijā, ja to pakļauj vienam vai vairākiem draudiem.

2. pants

Priekšmets

1. Šajā lēmumā ir noteikti mērķi, pamatprincipi, organizācija un pienākumi attiecībā uz drošību Komisijā.

2. Šo lēmumu piemēro visiem Komisijas dienestiem un visās Komisijas telpās. Komisijas darbiniekiem, kas strādā Savienības delegācijās, piemēro Eiropas Ārējās darbības dienesta drošības noteikumus ([2]).

3. Neatkarīgi no īpašām norādēm attiecībā uz konkrētām darbinieku grupām, šo lēmumu piemēro Komisijas locekļiem, Komisijas darbiniekiem, kuriem ir piemērojami Civildienesta noteikumi un Eiropas Savienības pārējo darbinieku nodarbināšanas kārtība, darbam Komisijā norīkotajiem valsts ekspertiem (NVE), pakalpojumu sniedzējiem un viņu darbiniekiem, stažieriem un ikvienai personai, kurai ir piekļuve Komisijas ēkām vai citiem aktīviem vai informācijai, ko izmanto Komisija.

4. Šā lēmuma noteikumi neskar Komisijas Lēmumu 2002/47/EK, EOTK, Euratom ([3]) un Komisijas Lēmumu 2004/563/EK, Euratom ([4]), Komisijas Lēmumu C(2006) 1623 ([5]) un Komisijas Lēmumu C(2006) 3602 ([6]).

2. NODAĻA

PRINCIPI

3. pants

Principi drošībai Komisijā

1. Īstenojot šo lēmumu, Komisija ievēro Līgumus un jo īpaši Pamattiesību hartu un 7. protokolu Par privilēģijām un imunitāti Eiropas Savienībā, aktus, kas minēti 2. apsvērumā, visus piemērojamo valsts tiesību aktu noteikumus, kā arī šā lēmuma noteikumus. Ja nepieciešams, saskaņā ar 21. panta 2. punktu pieņem drošības paziņojumu, kas sniedz norādes šajā sakarā.

2. Drošība Komisijā pamatojas uz likumības, pārredzamības, proporcionalitātes un atbildības principu.

3. Likumības princips nozīmē, ka, īstenojot šo lēmumu, nedrīkst pārkāpt tiesiskā satvara robežas un ir jāievēro tiesiskās prasības.

([1]) Padomes 1968. gada 29. februāra Regula (EEK, Euratom, EOTK) Nr. 259/68, ar ko nosaka Eiropas Kopienu Civildienesta noteikumus un Pārējo darbinieku nodarbināšanas kārtību un nosaka pagaidu pasākumus, kas piemērojami Komisijas ierēdņiem (Pārējo darbinieku nodarbināšanas kārtība) (OV L 56, 4.3.1968., 1. lpp.).

([2]) Savienības Augstā pārstāvja ārlietās un drošības politikas jautājumos 2013. gada 19. aprīļa Lēmums 2013/C 190/01 par Eiropas Ārējās darbības dienesta drošības noteikumiem (OV C 190, 29.6.2013., 1. lpp.).

([3]) Komisijas 2002. gada 23. janvāra Lēmums 2002/47/EK, EOTK, Euratom, ar ko groza Komisijas reglamentu (OV L 21, 24.1.2002., 23. lpp.), pievienojot noteikumus par dokumentvedību.

([4]) Komisijas 2004. gada 7. jūlija Lēmums 2004/563/EK, EOTK, Euratom par grozījumiem tās reglamentā (OV L 251, 27.7.2004., 9. lpp.), pievienojot noteikumus par elektroniskajiem un digitālajiem dokumentiem.

([5]) Komisijas 2006. gada 21. aprīļa Lēmums C(2006) 1623, ar ko nosaka saskaņotu politiku veselības un darba drošības jomā attiecībā uz visiem Eiropas Komisijas darbiniekiem.

([6]) Komisijas 2006. gada 16. augusta Lēmums C(2006) 3602 par informācijas sistēmu drošību, ko izmanto Eiropas Komisija.

4. Drošības pasākumu veic atklāti, izņemot gadījumus, ja var pamatoti gaidīt, ka tas mazinās drošības pasākuma ietekmi. Drošības pasākuma adresātu iepriekš informē par iemesliem un pasākuma ietekmi, izņemot, ja var pamatoti gaidīt, ka, sniedzot šādu informāciju, pasākuma ietekme samazināsies. Šādā gadījumā drošības pasākuma adresātu informē pēc tam, kad vairs nepastāv risks, ka drošības pasākuma ietekme samazinājusies.

5. Komisijas dienesti nodrošina, ka drošības jautājumi tiek ņemti vērā jau sākot izstrādāt un īstenot Komisijas politikas virzienus, lēmumus, programmas, projektus un darbības, par kurām tie ir atbildīgi. Lai to paveiktu, dienesti iesaista Cilvēkresursu un drošības ģenerāldirektorātu vispārīgi un Komisijas galveno informācijas drošības ierēdni attiecībā uz IT sistēmām jau pašā sagatavošanas posma sākumā.

6. Komisija attiecīgos gadījumos meklē sadarbības iespējas ar kompetentām iestādēm uzņēmējā valstī, citās dalībvalstīs un citās ES iestādēs, aģentūrās vai vienībās, ja iespējams, ņemot vērā pasākumus, ko šīs struktūras jau veic vai plāno, lai risinātu attiecīgo drošības risku.

4. pants

Ievērošanas pienākums

1. Šā lēmuma, tā īstenošanas noteikumu, drošības pasākumu un attiecīgi pilnvarotu darbinieku norādījumu ievērošana ir obligāta.

2. Drošības noteikumu neievērošana var būt par pamatu saukšanai pie disciplināratbildības saskaņā ar Līgumiem un Civildienesta noteikumiem, līgumiskām sankcijām un/vai tiesvedībai saskaņā ar valsts tiesību aktiem un noteikumiem.

3. NODAĻA

DROŠĪBAS ĪSTENOŠANA

5. pants

Pilnvaroti darbinieki

1. Tikai tiem darbiniekiem, kuri ir pilnvaroti, pamatojoties uz konkrētajam darbiniekam adresētu Cilvēkresursu un drošības ģenerāldirektora pilnvarojumu, ņemot vērā darbinieka pašreizējos pienākumus, var piešķirt tiesības īstenot vienu vai vairākus no šādiem pasākumiem:

1) nēsāt pie jostas ieročus;

2) veikt drošības izmeklēšanu, kā minēts 13. pantā;

3) īstenot drošības pasākumus, kas minēti 12. pantā, kā norādīts pilnvarojumā.

2. Pilnvaras, kas minētas 1. punktā, piešķir uz laikposmu, kas nav ilgāks par periodu, kurā attiecīgā persona ieņem amatu vai pilda funkciju, saistībā ar kuru ir izdots pilnvarojums. Tās piešķir saskaņā ar piemērojamiem noteikumiem, kas ir izklāstīti 3. panta 1. punktā.

3. Attiecībā uz pilnvarotiem darbiniekiem šis lēmums ir dienesta instrukcija Civildienesta noteikumu 21. panta nozīmē.

6. pants

Vispārīgi noteikumi par drošības pasākumiem

1. Īstenojot drošības pasākumus, Komisija jo īpaši iespēju robežās nodrošina, ka:

a) tā vēršas pēc atbalsta vai palīdzības tikai pie attiecīgās valsts ar nosacījumu, ka šī valsts ir Eiropas Savienības dalībvalsts vai, ja tā nav, tad – Eiropas Cilvēktiesību konvencijas dalībvalsts, vai garantē tiesības, kas ir vismaz līdzvērtīgas tiesībām, kas ir garantētas šajā konvencijā;

b) saņēmējiem, kas nav Kopienas iestādes un struktūras un kas nav pakļauti valsts tiesību aktiem, kuri pieņemti saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK ([1]), informāciju par personu tā nosūta tikai saskaņā ar Regulas (EK) Nr. 45/2001 9. pantu;

([1]) Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV L 281, 23.11.1995., 31. lpp.).

c) ja persona rada draudus drošībai, drošības pasākumu vērš pret šo personu un šai personai var uzlikt pienākumu segt radušās izmaksas. Drošības pasākumus var vērst pret citām personām tikai tad, ja nepieciešams kontrolēt tūlītējus vai nopietnus draudus drošībai un ir izpildīti šādi nosacījumi:

a) paredzētos pasākumus pret personu, kas rada draudus drošībai, nevar īstenot vai tie visticamāk nebūs efektīvi;

b) Komisija nevar kontrolēt draudus drošībai pati ar savu rīcību vai nevar to izdarīt laicīgi;

c) pasākums nav uzskatāms par nesamērīgu šīs citas personas un viņas tiesību apdraudējumu.

2. Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorāts izstrādā pārskatu par drošības pasākumiem, kuriem var būt nepieciešams tiesneša rīkojums saskaņā ar spēkā esošajiem tiesību aktiem un noteikumiem dalībvalstīs, kurās atrodas Komisijas telpas.

3. Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorāts ar drošību saistītu uzdevumu veikšanu Drošības direktorāta vadībā un pārraudzībā var uzdot darbuzņēmējam.

7. pants

Drošības pasākumi attiecībā uz personām

1. Komisijas telpās personām nodrošina atbilstīgu aizsardzības līmeni, ņemot vērā drošības un drošuma prasības.

2. Nopietnu drošības risku gadījumā Cilvēkresursu un drošības ģenerāldirektorāts nodrošina stingru Komisijas locekļu vai citu darbinieku aizsardzību, ja draudu novērtējums liecina, ka šāda aizsardzība ir nepieciešama, lai nodrošinātu viņu drošumu un drošību.

3. Nopietnu drošības risku gadījumā Komisija var norīkot evakuāciju no telpām.

4. Personas, kas cietušas negadījumos vai uzbrukumos Komisijas telpās, saņem palīdzību.

5. Lai novērstu un kontrolētu drošības riskus, pilnvaroti darbinieki var veikt iepriekšējās darbības pārbaudes par personām, kurām piemērojams šis Lēmums, lai noteiktu, vai, piešķirot šīm personām piekļuvi Komisijas telpām vai informācijai, tiek radīti draudi drošībai. Šajā nolūkā un saskaņā ar Regulu (EK) Nr. 45/2001 un noteikumiem, kas minēti 3. panta 1. punktā, attiecīgais pilnvarotais darbinieks var:

a) izmantot visus Komisijai pieejamos informācijas avotus, ņemot vērā informācijas avota uzticamību;

b) pienācīgi pamatotos gadījumos piekļūt personas lietai vai datiem, kas ir Komisijas rīcībā par personām, ko tā nodarbina vai plāno nodarbināt, vai par darbuzņēmēja darbiniekiem.

8. pants

Drošības pasākumi attiecībā uz fizisko drošību un aktīviem

1. Aktīvu drošību nodrošina, izmantojot atbilstīgus fiziskos un tehniskos aizsardzības pasākumus un attiecīgas procedūras, turpmāk "fiziskā drošība", radot daudzpakāpju sistēmu.

2. Pasākumus var pieņemt saskaņā ar šo pantu, lai aizsargātu personas vai informāciju Komisijā, kā arī lai aizsargātu aktīvus.

3. Fiziskajai drošībai ir šādi mērķi:

— novērst vardarbības aktus pret Komisijas locekļiem vai personām, kurām piemērojams šis lēmums,

— novērst sensitīvas vai klasificētas informācijas izspiegošanu un slepenu noklausīšanos,

— novērst zādzības, vandālismu, sabotāžas un citas vardarbīgas darbības, kas bojā vai iznīcina Komisijas ēkas un aktīvus,

— nodrošināt ar drošību saistītu starpgadījumu izmeklēšanu un izpēti, tostarp pārbaudot piekļuves un izejas kontroles žurnālu datnes, nodrošinot slēgta tīkla kameru pārklājumu, telefonsarunu un tamlīdzīgu datu ierakstus, kā minēts 22. panta 2. punktā, un izmantojot citus informācijas avotus.

4. Fiziskā drošība ietver:

— piekļuves politiku, ko piemēro jebkurai personai vai transportlīdzeklim, kas vēlas piekļūt Komisijas telpām, ieskaitot stāvvietas,

— piekļuves kontroles sistēmu, kas ietver apsargus, tehnisko aprīkojumu un pasākumus, informācijas sistēmas vai visu šos elementu apvienojumu.

5. Lai nodrošinātu fizisko drošību, var īstenot šādus pasākumus:

— reģistrēt personu, transportlīdzekļu, preču un iekārtu iekļūšanu Komisijas telpās un izkļūšanu no tām,

— veikt identitātes pārbaudes Komisijas telpās,

— veikt transportlīdzekļu, preču un iekārtu vizuālu pārbaudi vai pārbaudi ar tehnisku līdzekļu palīdzību,

— novērst nepiederošu personu, transportlīdzekļu un preču iekļūšanu Komisijas telpās.

9. pants

Drošības pasākumi attiecībā uz informāciju

1. Informācijas drošība attiecas uz visu informāciju, kas ir Komisijas rīcībā.

2. Informācijas drošība, neatkarīgi no tās veida, ir līdzsvara ar pārredzamību, proporcionalitāti, atbildību un efektivitāti ar vajadzību aizsargāt informāciju no neatļautas piekļuves, izmantošanas, nodošanas atklātībai, sagrozīšanas vai iznīcināšanas.

3. Informācijas drošības mērķis ir aizsargāt konfidencialitāti, integritāti un pieejamību.

4. Tāpēc, lai klasificētu informācijas aktīvus un izstrādātu proporcionālus drošības pasākumus, procedūras un standartus, izmanto riska pārvaldības procesus, tostarp riska mazināšanas pasākumus.

5. Šos vispārīgos principus, kas ir informācijas drošības pamatā, jo īpaši piemēro šādai informācijai:

a) "Eiropas Savienības klasificēta informācija" (turpmāk – ESKI), proti, jebkura informācija vai materiāli, kuriem piemērota ES drošības klasifikācija un kuru neatļauta izpaušana var izraisīt dažāda līmeņa kaitējumu Eiropas Savienības vai vienas vai vairāku tās dalībvalstu interesēm;

b) "sensitīva neklasificēta informācija", proti, informācija vai materiāli, kas Komisijai ir jāaizsargā līgumos vai aktos, kas pieņemti to īstenošanai, noteikto tiesisko pienākumu ietvaros un/vai informācijas vai materiālu sensitivitātes dēļ. Sensitīva neklasificēta informācija, neaprobežojoties ar šeit uzskaitīto, ietver informāciju un materiālus, uz ko attiecas dienesta noslēpuma glabāšanas pienākums, kā noteikts LESD 339. pantā, informāciju, uz kuru attiecas intereses, kas aizsargātas Eiropas Parlamenta un Padomes Regulas (EK) Nr. 1049/2001 ([1]) 4. pantā, skatot to kopā ar attiecīgo Eiropas Savienības Tiesas judikatūru, vai personas datus, kas ietilpst Regulas (EK) Nr. 45/2001 piemērošanas jomā.

6. Sensitīvai neklasificētai informācijai piemēro noteikumus par rīcību ar to un tās glabāšanu. To izpauž tikai tām personām, kurām ir "vajadzība pēc informācijas". Ja uzskata, ka tas ir vajadzīgs, lai efektīvi aizsargātu tās konfidencialitāti, tai nosaka drošības marķējumu un atbilstīgas instrukcijas rīcībai ar to, ko apstiprina Cilvēkresursu un drošības ĢD ģenerāldirektors. Ja šādu informāciju apstrādā vai glabā komunikācijas un informācijas sistēmās, to aizsargā arī saskaņā ar Lēmumu C(2006) 3602, tā īstenošanas noteikumiem un attiecīgajiem standartiem.

7. Ikvienu personu, kura ir atbildīga par to, ka tiek apdraudēta vai zaudēta ESKI vai sensitīva neklasificēta informācija, kas ir identificēta kā šāda veida informācija noteikumos par rīcību ar to un tās glabāšanu, var saukt pie disciplināras atbildības saskaņā ar Civildienesta noteikumiem. Šādi disciplināri pasākumi neskar nekādu cita veida tiesvedību, tostarp krimināltiesvedību, ko var ierosināt kompetentas valsts iestādes dalībvalstīs saskaņā ar valsts normatīvajiem aktiem, un neskar līgumiskos tiesiskās aizsardzības līdzekļus.

([1]) Eiropas Parlamenta un Padomes 2001. gada 30. maija Regula (EK) Nr. 1049/2001 par publisku piekļuvi Eiropas Parlamenta, Padomes un Komisijas dokumentiem (OV L 145, 31.5.2001., 43. lpp.).

10. pants

Drošības pasākumi attiecībā uz komunikācijas un informācijas sistēmām

1. Visas komunikācijas un informācijas sistēmas (KIS), ko izmanto Komisija, atbilst Komisijas informācijas sistēmu drošības politikai, kā izklāstīts Lēmumā C(2006) 3602, tā īstenošanas noteikumos un attiecīgajos drošības standartos.

2. Komisijas dienesti, kam pieder KIS, vai kuri pārvalda vai darbojas ar KIS, šīm sistēmām ļauj piekļūt tikai citām ES iestādēm, aģentūrām, struktūrām vai citām organizācijām ar nosacījumu, ka šīs Savienības iestādes, aģentūras, struktūras vai citas organizācijas var sniegt pamatotu pārliecību, ka to IT sistēmas ir aizsargātas tādā līmenī, kas ir līdzvērtīgs Komisijas informācijas sistēmu drošības politikai, kas izklāstīta Lēmumā C(2006) 3602, tās īstenošanas noteikumos un attiecīgajos drošības standartos. Komisija uzrauga šādu atbilstību, un, konstatējusi smagu neatbilstība vai atkārtotu neievērošanu, ir tiesīga aizliegt piekļuvi.

11. pants

Kriminālistiskā kiberdrošības ekspertīze

Cilvēkresursu un drošības ģenerāldirektorāts jo īpaši ir atbildīgs par kriminālistiskās tehnikas ekspertīzēm sadarbībā ar kompetentajiem Komisijas dienestiem, lai atbalstītu drošības izmeklēšanu, kā minēts 13. pantā, saistībā ar pretizlūkošanu, datu noplūdi, kiberuzbrukumiem un informācijas sistēmu drošību.

12. pants

Drošības pasākumi attiecībā uz personām un lietām

1. Lai nodrošinātu drošību Komisijā un novērstu un kontrolētu riskus, darbinieki, kas pilnvaroti saskaņā ar 5. pantu, var, ievērojot 3. pantā noteiktos principus, īstenot cita starpā vienu vai vairākus šādus aizsardzības pasākumus:

a) nodrošināt pierādījumus un notikuma vietu, tostarp piekļuves un izejas kontroles žurnālu datnes, slēgta tīkla kameru pārklājuma materiālus un attēlus, ja norisinās starpgadījumi vai rīcība, kas var būt par pamatu administratīvai, disciplinārai, civiltiesiskai vai krimināltiesiskai procedūrai;

b) veikt ierobežotus pasākumus attiecībā uz personām, kas rada draudus drošībai, tostarp liekot personām atstāt Komisijas telpas, eskortējot personas no Komisijas telpās, liedzot personām uzturēties Komisijas telpās uz laiku, ko nosaka saskaņā ar kritērijiem, kas paredzēti īstenošanas noteikumos;

c) veikt ierobežotus pasākumus attiecībā uz priekšmetiem, kas rada draudus drošībai, tostarp, aizvācot, izņemot vai likvidējot šos priekšmetus;

d) pārmeklēt Komisijas telpas, tostarp birojus, kas atrodas šādās telpās;

e) pārmeklēt KIS un iekārtas, tālruņu un telekomunikācijas datu plūsmu, žurnālu datnes, lietotāju kontus utt.;

f) veikt citus īpašus drošības pasākumus ar tamlīdzīgu ietekmi, lai novērstu vai kontrolētu drošības riskus, jo īpaši saistībā ar Komisijas tiesībām, kas tai piemīt kā īpašniekam vai kā darba devējam saskaņā ar piemērojamiem valsts tiesību aktiem.

2. Ārkārtējos gadījumos Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorāta darbinieki, kas pilnvaroti saskaņā ar 5. pantu, var veikt nepieciešamos steidzamos pasākumus, stingri ievērojot 3. pantā noteiktos principus. Iespējami drīz pēc šo pasākumu īstenošanas tie informē Drošības direktorāta direktoru, kas vēršas pie Cilvēkresursu un drošības ĢD ģenerāldirektora, lai saņemtu attiecīgu pilnvarojumu, kas apstiprina īstenotos pasākumus un atļauj turpmākas nepieciešamās darbības, un attiecīgā gadījumā uztur sakarus ar kompetentām valsts iestādēm.

3. Drošības pasākumus, ko īsteno saskaņā ar šo pantu, dokumentē brīdī, kad tie tiek īstenoti, bet tūlītēja riska vai krīzes situācijā – saprātīgā termiņā pēc tam, kad tie ir īstenoti. Pēdējā minētajā gadījumā dokumentācijā jāiekļauj arī aspekti, uz ko pamatojas novērtējums, ka pastāv tūlītējs risks vai krīzes situācija. Dokumentācija var būt kodolīga, bet tai jābūt veidotai tā, lai personai, kurai piemēro pasākumu, būtu nodrošinātas tiesības uz aizstāvību un personas datu aizsardzību saskaņā ar Regulu (EK) Nr. 45/2001, un lai būtu iespējams noteikt, vai pasākums bija likumīgs. Informāciju par īpašiem drošības pasākumiem, kas adresēti kādam darbiniekam, neiekļauj personas lietā.

4. Īstenojot aizsardzības pasākumus saskaņā ar b) apakšpunktu, Komisija turklāt garantē, ka attiecīgajai personai tiek dota iespēja sazināties ar advokātu vai uzticības personu un to informē par tiesībām vērsties pie Eiropas datu aizsardzības uzraudzītāja.

13. pants

Izmeklēšana

1. Neskarot Civildienesta noteikumu 86. pantu un IX pielikumu un neskarot īpašo kārtību, kas pastāv starp Komisiju un EĀDD, piemēram, īpašo vienošanos, ko 2014. gada 28. maijā parakstīja Eiropas Komisijas Cilvēkresursu un drošības ģenerāldirektorāts un Eiropas Ārējās darbības dienests par pienākumu rūpēties par Komisijas darbiniekiem, kas strādā Savienības delegācijās, drošības izmeklēšanu var veikt:

a) incidenta gadījumā, kas ietekmē drošību Komisijā, tostarp, ja ir aizdomas par noziedzīgu nodarījumu;

b) sensitīvas neklasificētas informācijas, ESKI vai Euratom klasificētas informācijas iespējamas noplūdes, nepareizas rīcības ar to vai apdraudējuma gadījumā;

c) pretizlūkošanas un terorisma apkarošanas kontekstā;

d) nopietnu kiberincidentu gadījumā.

2. Lēmumu veikt drošības izmeklēšanu pieņem Cilvēkresursu un drošības ĢD ģenerāldirektors, kurš kļūst arī par izmeklēšanas ziņojuma saņēmēju.

3. Drošības izmeklēšanu veic tikai īpaši tam paredzēti Cilvēkresursu un drošības ģenerāldirektorāta darbinieki, kas pienācīgi pilnvaroti saskaņā ar 5. pantu.

4. Pilnvarotie darbinieki savas drošības izmeklēšanas pilnvaras īsteno neatkarīgi, kā noteikts pilnvarojumā, un tiem ir 12. pantā uzskaitītās tiesības.

5. Pilnvaroti darbinieki, kas ir kompetenti veikt drošības izmeklēšanu, var vākt informāciju no visiem pieejamiem avotiem, kas saistīti ar administratīvu pārkāpumu vai noziedzīgu nodarījumu, kas izdarīti Komisijas telpās vai kuros iesaistītas 2. panta 3. punktā minētās personas vai nu kā cietušie, vai kā šādu nodarījumu izdarītāji.

6. Cilvēkresursu un drošības ģenerāldirektorāts attiecīgos gadījumos informē uzņēmējas dalībvalsts vai jebkuras citas iesaistītās dalībvalsts kompetentās iestādes un jo īpaši tad, ja izmeklēšanā ir atklājušās pazīmes, kas liecina, ka ir izdarīts noziedzīgs nodarījums. Šajā sakarā Cilvēkresursu un drošības ģenerāldirektorāts attiecīgā gadījumā vai ja tas nepieciešams, var sniegt atbalstu uzņēmējas dalībvalsts vai jebkuras citas iesaistītās dalībvalsts iestādēm.

7. Nopietna kiberincidenta gadījumā Informātikas ģenerāldirektorāts cieši sadarbojas ar Cilvēkresursu un drošības ģenerāldirektorātu, lai sniegtu atbalstu visos tehniskajos jautājumos. Cilvēkresursu un drošības ģenerāldirektorāts, apspriežoties ar Informātikas ģenerāldirektorātu, lemj par to, kad ir lietderīgi informēt uzņēmējas valsts vai jebkuras citas iesaistītās dalībvalsts kompetentās iestādes. Lai atbalstītu citas ES iestādes un aģentūras, kuras varētu būt skartas, tiks izmantoti Eiropas iestāžu, struktūru un aģentūru Datorapdraudējumu reaģēšanas vienības incidentu koordinācijas dienesti (*CERT-EU*).

8. Drošības izmeklēšanu dokumentē.

14. pants

Kompetenču sadalījums attiecībā uz drošības izmeklēšanu un cita veida izmeklēšanu

1. Ja Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorāts veic drošības izmeklēšanu, kā minēts 13. pantā, un ja šāda izmeklēšana ietilpst Eiropas Biroja krāpšanas apkarošanai (*OLAF*) vai Komisijas Izmeklēšanas un disciplīnas biroja (*IDOC*) kompetencē, tas nekavējoties uzņem sakarus ar šīm struktūrām, jo īpaši, lai neapdraudētu turpmāko *OLAF* vai *IDOC* rīcību. Attiecīgā gadījumā Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorāts aicina *OLAF* vai *IDOC* iesaistīties izmeklēšanā.

2. Drošības izmeklēšana, kas minēta 13. pantā, neskar *OLAF* un *IDOC* pilnvaras, kas paredzētas noteikumos, kuri regulē šīs struktūras. Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorātam var lūgt sniegt tehnisko palīdzību attiecībā uz izmeklēšanām, ko sācis *OLAF* vai *IDOC*.

3. Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorātam var lūgt palīdzību *OLAF* pārstāvjiem, kad tie piekļūst Komisijas telpām saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES, Euratom) Nr. 883/2013 [1] 3. panta 5. punktu un 4. panta 4. punktu, lai atvieglotu viņu uzdevumu izpildi. Drošības direktorāts par šādiem palīdzības

[1] Eiropas Parlamenta un Padomes 2013. gada 11. septembra Regula (ES, Euratom) Nr. 883/2013 par izmeklēšanu, ko veic Eiropas Birojs krāpšanas apkarošanai (*OLAF*), un ar ko atceļ Eiropas Parlamenta un Padomes Regulu (EK) Nr. 1073/1999 un Padomes Regulu (Euratom) Nr. 1074/1999 (OV L 248, 18.9.2013., 1. lpp.).

lūgumiem informē ģenerālsekretāru un Cilvēkresursu un drošības ĢD ģenerāldirektoru vai, ja šāda izmeklēšana tiek veikta Komisijas telpās, kurās atrodas tās locekļi vai ģenerālsekretārs, – Komisijas priekšsēdētāju un Komisāru, kura atbildības jomā ir cilvēkresursi.

4. Neskarot Civildienesta noteikumu 22. panta a) punktu, ja jautājums ir gan Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorāta, gan *IDOC* kompetencē, Drošības direktorāts, ziņojot Cilvēkresursu ĢD ģenerāldirektoram saskaņā ar 13. pantu, pēc iespējas agrīnā posmā informē, vai ir pamatoti iemesli, kāpēc lieta būtu jānodod *IDOC*. Jo īpaši tiek uzskatīts, ka šis agrīnais posms ir sācies, ja tūlītējie draudi drošībai ir beigušies. Šo jautājumu izlemj Cilvēkresursu un drošības ĢD ģenerāldirektors.

5. Ja jautājums var būt gan Cilvēkresursu un drošības ģenerāldirektorāta Drošības direktorāta, gan *OLAF* kompetencē, Drošības direktorāts nekavējoties ziņo Cilvēkresursu un drošības ĢD ģenerāldirektoram un informē *OLAF* ģenerāldirektoru pēc iespējas agrīnā posmā. Jo īpaši tiek uzskatīts, ka šis agrīnais posms ir sācies, ja tūlītējie draudi drošībai ir beigušies.

15. pants

Drošības pārbaudes

1. Cilvēkresursu un drošības ģenerāldirektorāts veic drošības pārbaudes, lai pārbaudītu, vai Komisijas dienesti un personas ievēro šo lēmumu un tā īstenošanas noteikumus, un formulētu ieteikumus, ja to uzskata par vajadzīgu.

2. Attiecīgā gadījumā Cilvēkresursu un drošības ģenerāldirektorāts veic drošības pārbaudes vai drošības uzraudzības vai izvērtējuma apmeklējumus, lai pārbaudītu, vai Komisijas darbinieku, aktīvu un informācijas, par kuru atbild citas Savienības iestādes, aģentūras vai struktūras, dalībvalstis, trešās valstis vai starptautiskas organizācijas, drošība ir pienācīgi aizsargāta saskaņā ar drošības noteikumiem un standartiem, kas ir vismaz līdzvērtīgi Komisijas noteikumiem un standartiem. Attiecīgā gadījumā un ievērojot pārvaldības labas sadarbības principu, šīs drošības pārbaudes ietver arī pārbaudes, ko veic saistībā ar klasificētas informācijas apmaiņu ar citām Savienības iestādēm, struktūrām un aģentūrām, dalībvalstīm vai trešām valstīm vai starptautiskām organizācijām.

3. Šo pantu piemēro pēc analoģijas Komisijas darbiniekiem Savienības pārstāvniecībās, neskarot, īpašo kārtību, kas pastāv starp Komisiju un EĀDD, piemēram, īpašo vienošanos, ko 2014. gada 28. maijā parakstīja Eiropas Komisijas Cilvēkresursu un drošības ģenerāldirektorāts un Eiropas Ārējās darbības dienests par pienākumu rūpēties par Komisijas darbiniekiem, kas strādā Savienības pārstāvniecībās

16. pants

Trauksmes stāvokļi un krīzes situāciju pārvaldība

1. Cilvēkresursu un drošības ģenerāldirektorāts ir atbildīgs par atbilstošu trauksmes stāvokļa pasākumu ieviešanu, lai sagatavotos vai reaģētu uz draudiem un incidentiem, kas ietekmē drošību Komisijā, un par pasākumiem, kas vajadzīgi, lai pārvaldītu krīzes situācijas.

2. Trauksmes stāvokļa pasākumi, kas minēti šā panta 1. punktā, ir samērīgi ar draudu līmeni drošībai. Trauksmes stāvokļa līmeņus nosaka ciešā sadarbībā ar citu Savienības iestāžu, aģentūru un struktūru un dalībvalsts vai dalībvalstu, kurās atrodas Komisijas telpas, kompetentajiem dienestiem.

3. Cilvēkresursu un drošības ģenerāldirektorāts ir kontaktpunkts trauksmes stāvokļu un krīzes situāciju pārvaldības jautājumos.

4. NODAĻA

ORGANIZĀCIJA

17. pants

Komisijas dienestu vispārīgi pienākumi

1. Komisijas pienākumus, kas minēti šajā lēmumā, veic Cilvēkresursu un drošības ģenerāldirektorāts tā Komisijas locekļa pakļautībā un viņa atbildības ietvaros, kurš ir atbildīgs par drošības jautājumiem.

2. Īpašā kārtība attiecībā uz kiberdrošību ir noteikta Lēmumā C(2006) 3602.

3. Atbildību par šā lēmuma un tā īstenošanas noteikumu īstenošanu un ikdienas ievērošanu var uzticēt citiem Komisijas dienestiem gadījumos, kad decentralizēta drošības īstenošana nozīmē ievērojamu efektivitāti, resursu un laika ietaupījumus, piemēram, attiecīgo dienestu ģeogrāfiskās atrašanās vietas dēļ.

4. Ja piemēro 3. punktu, Cilvēkresursu un drošības ĢD ģenerāldirektors un attiecīgā gadījumā Informātikas ĢD ģenerāldirektors, vienojas ar atsevišķiem Komisijas dienestiem par uzdevumu un pienākumus skaidru sadali drošības politikas īstenošanai un uzraudzībai.

18. pants

Cilvēkresursu un drošības ģenerāldirektorāts

1. Cilvēkresursu un drošības ģenerāldirektorāts jo īpaši ir atbildīgs par:

1) Komisijas drošības politikas, īstenošanas noteikumu un drošības paziņojumu izstrādi;

2) informācijas vākšanu ar mērķi izvērtēt draudus un drošības riskus un par visiem jautājumiem, kas var ietekmēt drošību Komisijā;

3) elektroniskās pretuzraudzības un aizsardzības nodrošināšanu visās Komisijas atrašanās vietās, pienācīgi ņemot vērā draudu novērtējumus un pierādījumus par neatļautām darbībām pret Komisijas interesēm;

4) Diennakts ārkārtas dienesta nodrošināšanu Komisijas dienestiem un darbiniekiem saistībā ar visiem drošuma un drošības jautājumiem;

5) drošības pasākumu veikšanu, lai mazinātu drošības riskus un izstrādātu un uzturētu operatīvajām vajadzībām atbilstīgu KIS jo īpaši tādās jomās kā fiziskās piekļuves kontrole, drošības pilnvaru pārvaldība un rīcība ar sensitīvu un ES klasificētu informāciju;

6) informētības palielināšanu, rīkojot mācības un treniņus un nodrošinot apmācību un konsultācijas par visiem jautājumiem, kas saistīti ar drošību Komisijā, lai veicinātu drošības kultūru un izveidotu drošības jautājumos pienācīgi apmācīta personāla kopu.

2. Cilvēkresursu un drošības ģenerāldirektorāts, neskarot citu Komisijas dienestu kompetenci un pienākumus, nodrošina ārējos sakarus:

1) ar citu Savienības iestāžu, aģentūru un struktūru drošības dienestiem par jautājumiem, kas saistīti ar personu, aktīvu un informācijas drošību Komisijā;

2) ar drošības, izlūkošanas un draudu novērtēšanas dienestiem, tostarp ar dalībvalstu, trešo valstu un starptautisko organizāciju un struktūru drošības iestādēm, par jautājumiem, kas skar personu, aktīvu un informācijas drošību Komisijā;

3) ar policiju un citiem operatīvajiem dienestiem par visiem ikdienas un ārkārtas jautājumiem, kas skar Komisijas drošību;

4) ar drošības iestādēm citās Savienības iestādēs, aģentūrās un struktūrās, dalībvalstīs un trešās valstīs par reaģēšanu tādu kiberuzbrukumu gadījumā, kas varētu ietekmēt drošību Komisijā;

5) par izlūkdatu saņemšanu, izvērtēšanu un izplatīšanu attiecībā uz draudiem, ko rada teroristu un spiegošanas darbības, kas skar drošību Komisijā;

6) par jautājumiem, kas saistīti ar klasificētu informāciju, kā noteikts Komisijas Lēmumā (ES, Euratom) 2015/444 ([1]).

3. Cilvēkresursu un drošības ģenerāldirektorāts ir atbildīgs par to, lai saskaņā ar šo pantu tiktu droši nosūtīta informācija, tostarp par personas dati.

19. pants

Komisijas drošības ekspertu grupa (*ComSEG*)

Izveido Komisijas drošības ekspertu grupu ar pilnvarām konsultēt Komisiju attiecīgos gadījumos par jautājumiem, kas saistīti ar tā iekšējo drošības politiku un it īpaši ar ES klasificētas informācijas aizsardzību.

([1]) Komisijas 2015. gada 13. marta Lēmums (ES, Euratom) 2015/444 par drošības noteikumiem ES klasificētas informācijas aizsardzībai (skatīt šā *Oficiālā Vēstneša* 53. lpp.).

20. pants

Vietējie drošības speciālisti (*LSOs*)

1. Katrs Komisijas dienests vai kabinets ieceļ vietējo drošības inspektoru (*LSO*), kas darbojas kā galvenais kontaktpunkts starp viņa pārstāvēto dienestu un Cilvēkresursu un drošības ģenerāldirektorātu par visiem jautājumiem, kas saistīti ar drošību Komisijā. Vajadzības gadījumā var iecelt vienu vai vairākus *LSO* vietniekus. *LSO* ir ierēdnis vai pagaidu darbinieks.

2. Kā galvenais kontaktpunkts drošības jautājumos savā Komisijas dienestā vai kabinetā *LSO* regulāri atskaitās Cilvēkresursu un drošības ģenerāldirektorātam un savam tiešajam vadītājam par drošības jautājumiem, kas skar viņa pārstāvēto Komisijas dienestu un nekavējoties ziņo par visiem drošības incidentiem, tostarp, ja varētu būt apdraudēta ESKI vai sensitīva neklasificēta informācija.

3. Attiecībā uz jautājumiem, kas saistīti ar komunikācijas un informācijas sistēmu drošību, *LSO* sadarbojas ar vietējo IT drošības speciālistu (*LISO*) savā Komisijas dienestā, kura loma un pienākumi ir noteikti Lēmumā C(2006) 3602.

4. Viņš līdzdarbojas drošības mācībās un informatīvajos pasākumos, kas pievēršas darbinieku, darbuzņēmēju un citu personu, kas strādā viņa Komisijas dienesta pakļautībā, konkrētajām vajadzībām.

5. *LSO* var uzticēt veikt īpašus uzdevumus nopietnu vai tūlītēju risku drošībai gadījumā vai ārkārtas situācijās pēc Cilvēkresursu un drošības ģenerāldirektorāta lūguma. *LSO* pārstāvētā ĢD ģenerāldirektoru vai Cilvēkresursu departamenta direktoru par šiem īpašajiem uzdevumiem informē Cilvēkresursu un drošības ģenerāldirektorāts.

6. *LSO* pienākumi neskar uzdevumus un pienākumus, kas uzticēti vietējiem IT drošības speciālistiem (*LISOs*), veselības un drošības speciālistiem, reģistra kontrolieriem vai jebkuras citas funkcijas veicējiem saistībā ar drošības vai drošuma pienākumiem. *LSO* uztur kontaktus ar tiem, lai nodrošinātu saskaņotu un konsekventu pieeju drošības jautājumiem un efektīvu informācijas plūsmu par jautājumiem saistībā ar drošību Komisijā.

7. *LSO* ir tieša piekļuve viņa ģenerāldirektoram vai dienesta vadītājam, informējot viņa tiešo vadību. Viņam ir drošības atļauja piekļūt ESKI vismaz līdz *SECRET UE/EU SECRET* līmenim.

8. Lai veicinātu informācijas un paraugprakses apmaiņu, Cilvēkresursu un drošības ģenerāldirektorāts organizē vismaz divreiz gadā *LSO* konferenci. Šajās konferencēs *LSO* dalība ir obligāta.

5. NODAĻA

ĪSTENOŠANA

21. pants

Īstenošanas noteikumi un drošības paziņojumi

1. Ja nepieciešams pieņemt šā lēmuma īstenošanas noteikumus, par to, pilnībā ievērojot iekšējo reglamentu, tiks pieņemts atsevišķs Komisijas pilnvarojošs lēmums tam Komisijas loceklim, kas ir atbildīgs par drošības jautājumiem,.

2. Kad saskaņā ar iepriekš minēto Komisijas lēmumu saņemts pilnvarojums, Komisijas loceklis, kas ir atbildīgs par drošības jautājumiem, var izstrādāt drošības paziņojumus, kuros izklāstītas drošības norādes un paraugprakse šā lēmuma un tā īstenošanas noteikumu piemērošanas jomā.

3. Komisija var deleģēt uzdevumus, kas minēti šā panta pirmajā un otrajā punktā, Cilvēkresursu un drošības ĢD ģenerāldirektoram ar atsevišķu deleģēšanas lēmumu pilnībā ievērojot iekšējo reglamentu.

6. NODAĻA

DAŽĀDI NOTEIKUMI UN NOBEIGUMA NOTEIKUMI

22. pants

Personas datu apstrāde

1. Komisija apstrādā personu datus, kas vajadzīgi, lai īstenotu šo lēmumu saskaņā ar Regulu (EK) Nr. 45/2001.

2. Neatkarīgi no pasākumiem, kas jau ir spēkā šā lēmuma pieņemšanas laikā un ir paziņoti Eiropas Datu aizsardzības uzraudzītājam ([1]), visus saskaņā ar šo lēmumu veiktos pasakumus, kas ietver personas datu apstrādi, piemēram, saistībā ar piekļuves un izejas kontroles žurnāliem, slēgta tīkla kameru pārklājuma ierakstiem, tālruņa zvaniem uz dežūrdienestiem vai sadales centriem vai tamlīdzīgiem datiem, kas nepieciešami drošības nolūkos vai reaģēšanai krīzes situācijā, piemēro īstenošanas noteikumus saskaņā ar 21. pantu, kas paredz atbilstošus aizsardzības pasākumus datu subjektiem.

3. Cilvēkresursu un drošības ĢD ģenerāldirektors ir atbildīgs par ikvienu personas datu apstrādi, ko veic saskaņā ar šo lēmumu.

4. Minētos īstenošanas noteikumus un procedūras pieņem pēc apspriešanās ar datu aizsardzības inspektoru un Eiropas Datu aizsardzības uzraudzītāju saskaņā ar Regulu (EK) Nr. 45/2001.

23. pants

Pārskatāmība

Šo lēmumu un tā īstenošanas noteikumus paziņo Komisijas darbiniekiem un visām personām, kurām tie ir piemērojami.

24. pants

Iepriekšējo lēmumu atcelšana

Atceļ Lēmumu C(94) 2129.

25. pants

Stāšanās spēkā

Šī regula stājas spēkā nākamajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Briselē, 2015. gada 13. martā

Komisijas vārdā –
priekšsēdētājs
Jean-Claude JUNCKER

([1]) DPO-914.2, DPO-93.7, DPO-153.3, DPO-870.3, DPO-2831.2, DPO-1162.4, DPO-151.3, DPO-3302.1, DPO-508.6, DPO-2638.3, DPO-544.2, DPO-498.2, DPO-2692.2, DPO-2823.2.