KOMISIJAS LĒMUMS

(2010. gada 4. maijs)

par drošības plānu Vīzu informācijas sistēmas darbībai

(2010/260/ES)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Eiropas Parlamenta un Padomes 2008. gada 9. jūlija Regulu (EK) Nr. 767/2008 par Vīzu informācijas sistēmu (VIS) un datu apmaiņu starp dalībvalstīm saistībā ar īstermiņa vīzām (VIS regula) [1] un jo īpaši tās 32. pantu,

tā kā:

(1) Regulas (EK) Nr. 767/2008 32. panta 3. punktā noteikts, ka vadības iestāde veic vajadzīgos pasākumus, lai sasniegtu 32. panta 2. punktā izklāstītos mērķus drošības jomā attiecībā uz VIS darbību, tostarp pieņem drošības plānu.

(2) Saskaņā ar Regulas (EK) Nr. 767/2008 26. panta 4. punktu pārejas laikposmā, pirms vadības iestāde sāk pildīt savus pienākumus, par VIS darbības pārvaldību atbild Komisija.

(3) Eiropas Parlamenta un Padomes Regula (EK) Nr. 45/2001 [2] attiecas uz personas datu apstrādi, ko veic Komisija, pildot pienākumus VIS darbības pārvaldības jomā.

(4) Ar Regulas (EK) Nr. 767/2008 26. panta 7. punktu paredzēts, ka, ja Komisija deleģē savu atbildību pārejas laikposmā, pirms vadības iestāde sāk pildīt savus pienākumus, tā nodrošina, ka ar šo deleģēšanu nelabvēlīgi neietekmē nevienu ar Eiropas Savienības tiesību aktiem izveidotu spēkā esošu kontroles mehānismu, ko īsteno Tiesa, Revīzijas palāta vai Eiropas Datu aizsardzības uzraudzītājs.

(5) Tiklīdz vadības iestāde sāk pildīt savus pienākumus, tai jāizveido drošības plāns attiecībā uz VIS.

(6) Komisijas 2008. gada 17. jūnija Lēmumā 2008/602/EK par valsts saskarņu un komunikācijas infrastruktūras starp centrālo VIS un valsts saskarnēm uzbūvi un tām piemērojamām prasībām izveides posmā [3] aprakstīti nepieciešamie drošības pakalpojumi, kuri jāpiemēro VIS tīklam.

(7) Regulas (EK) Nr. 767/2008 27. pantā noteikts, ka galvenā Centrālā VIS, ar ko veic tehniskās pārraudzības un administrācijas funkcijas, atrodas Strasbūrā (Francijā) un Centrālās VIS dublējums, kas spēj nodrošināt visas galvenās Centrālās VIS funkcijas šīs sistēmas avārijas gadījumā, atrodas *Sankt Johann im Pongau* (Austrijā).

(8) Jānosaka drošības inspektoru pienākumi, lai nodrošinātu efektīvu un tūlītēju reakciju uz drošības incidentiem un sniegtu par tiem ziņojumus.

(9) Jāizstrādā drošības politika, kurā saskaņā ar šā lēmuma noteikumiem sīki izklāsta visus tehniskos un organizatoriskos jautājumus.

(10) Jādefinē pasākumi, lai nodrošinātu pienācīgu drošības līmeni VIS darbībai,

IR PIEŅĒMUSI ŠO LĒMUMU.

I NODAĻA

VISPĀRĪGI NOTEIKUMI

1. pants

Temats

Šajā lēmumā paredzēta drošības organizācija un pasākumi (drošības plāns) Regulas (EK) Nr. 767/2008 32. panta 3. punkta nozīmē.

II NODAĻA

ORGANIZĀCIJA, PIENĀKUMI UN INCIDENTU PĀRVALDĪBA

2. pants

Komisijas uzdevumi

1. Komisija īsteno un uzrauga Centrālās VIS, kā arī šajā lēmumā minētās sakaru infrastruktūras drošības pasākumu efektivitāti.

[1] OV L 218, 13.8.2008., 60. lpp.
[2] OV L 8, 12.1.2001., 1. lpp.
[3] OV L 194, 23.7.2008., 3. lpp.

2. Komisija ieceļ sistēmas drošības inspektoru, izraugoties to no savu ierēdņu vidus. Sistēmas drošības inspektoru ieceļ Komisijas Tiesiskuma, brīvības un drošības ģenerāldirektorāta ģenerāldirektors. Sistēmas drošības inspektora pienākumos ietilpst jo īpaši:

a) sagatavot, atjaunināt un pārskatīt drošības politiku, kā aprakstīts šā lēmuma 7. pantā;

b) uzraudzīt Centrālās VIS un sakaru infrastruktūras drošības procedūru īstenošanas efektivitāti;

c) piedalīties ar drošību saistīto ziņojumu sagatavošanā, kā minēts Regulas (EK) Nr. 767/2008 50. panta 3. un 4. punktā;

d) veikt koordinēšanas un palīdzības uzdevumus, piedaloties pārbaudēs un revīzijās, ko veic Eiropas Datu aizsardzības uzraudzītājs, kā norādīts Regulas (EK) Nr. 767/2008 42. pantā;

e) uzraudzīt, lai šo lēmumu un drošības politiku pareizi un pilnībā piemēro visi līgumslēdzēji, tostarp apakšuzņēmēji, kuri jebkādā veidā iesaistīti VIS pārvaldībā un darbībā;

f) uzturēt VIS drošības valsts vienoto kontaktpunktu sarakstu, kā arī darīt to pieejamu vietējiem drošības inspektoriem, kuri ir atbildīgi par Centrālo VIS un sakaru infrastruktūru.

3. pants

Par Centrālo VIS atbildīgais vietējais drošības inspektors

1. Neskarot 8. pantu, Komisija ieceļ par Centrālo VIS atbildīgu vietējo drošības inspektoru, izraugoties to no savu ierēdņu vidus. Novērš interešu konfliktus starp vietējā drošības inspektora pienākumiem un jebkādiem citiem oficiālajiem pienākumiem. Par Centrālo VIS atbildīgo vietējo drošības inspektoru ieceļ Komisijas Tiesiskuma, brīvības un drošības ģenerāldirektorāta ģenerāldirektors.

2. Par Centrālo VIS atbildīgais vietējais drošības inspektors nodrošina, ka tiek īstenoti šajā lēmumā minētie drošības pasākumi un galvenajā Centrālajā VIS tiek ievērotas drošības procedūras. Attiecībā uz Centrālās VIS dublējumu par Centrālo VIS atbildīgais vietējais drošības inspektors nodrošina, ka tiek īstenoti šajā lēmumā minētie drošības pasākumi, izņemot 10. pantā minētos pasākumus, un tiek ievērotas attiecīgās drošības procedūras.

3. Par Centrālo VIS atbildīgais vietējais drošības inspektors var deleģēt savus uzdevumus padotajam personālam. Novērš interešu konfliktus starp pienākumu veikt minētos uzdevumus un jebkādiem citiem oficiālajiem pienākumiem. Izmantojot atsevišķu kontakttālruņa numuru un adresi, ar vietējo drošības inspektoru vai tā pienākumu izpildītāju var sazināties jebkurā laikā.

4. Par Centrālo VIS atbildīgais vietējais drošības inspektors veic uzdevumus drošības pasākumu ietvaros galvenās VIS un VIS dublējuma vietās, nepārsniedzot 1. punktā noteiktās robežas, jo īpaši:

a) veic vietējos operatīvos drošības uzdevumus, tostarp ugunsmūra revīziju, regulāru drošības pārbaudi, revīziju un ziņošanu;

b) uzrauga darbības nepārtrauktības plāna efektivitāti un nodrošina, ka notiek regulāras mācības;

c) nodrošina pierādījumus par visiem incidentiem, kas var ietekmēt Centrālās VIS vai sakaru infrastruktūras drošību, un ziņo par tiem sistēmas drošības inspektoram;

d) informē sistēmas drošības inspektoru, ja jāveic grozījumi drošības politikā;

e) uzrauga, lai šo lēmumu un drošības politiku pareizi un pilnībā piemēro visi līgumslēdzēji, tostarp apakšuzņēmēji, kuri jebkādā veidā iesaistīti Centrālās VIS pārvaldībā un darbībā;

f) nodrošina, ka darbiniekus informē par to pienākumiem, un uzrauga drošības politikas piemērošanu;

g) uzrauga jaunākās attīstības tendences IT drošības jomā un nodrošina, ka darbiniekus attiecīgi apmāca;

h) sagatavo pamatinformāciju un iespējas drošības politikas izveidei, atjaunināšanai un pārskatīšanai saskaņā ar 7. pantu.

4. pants

Par sakaru infrastruktūru atbildīgais vietējais drošības inspektors

1. Neskarot 8. pantu, Komisija ieceļ par sakaru infrastruktūru atbildīgo vietējo drošības inspektoru, izraugoties to no savu ierēdņu vidus. Novērš interešu konfliktus starp vietējā drošības inspektora pienākumiem un jebkādiem citiem oficiālajiem pienākumiem. Par sakaru infrastruktūru atbildīgo vietējo drošības inspektoru ieceļ Komisijas Tiesiskuma, brīvības un drošības ģenerāldirektorāta ģenerāldirektors.

2. Par sakaru infrastruktūru atbildīgais vietējais drošības inspektors uzrauga tās darbību un nodrošina, ka tiek īstenoti drošības pasākumi un tiek ievērotas drošības procedūras.

3. Par sakaru infrastruktūru atbildīgais vietējais drošības inspektors var deleģēt savus uzdevumus padotajam personālam. Novērš interešu konfliktus starp pienākumu veikt minētos uzdevumus un jebkādiem citiem oficiālajiem pienākumiem. Izmantojot atsevišķu kontakttālruņa numuru un adresi, ar vietējo drošības inspektoru vai tā pienākumu izpildītāju var sazināties jebkurā laikā.

4. Par sakaru infrastruktūru atbildīgais vietējais drošības inspektors veic ar drošības pasākumiem saistītos uzdevumus, kuri attiecas uz sakaru infrastruktūru, jo īpaši:

a) veic visus operatīvos drošības uzdevumus, kuri attiecas uz sakaru infrastruktūru, piemēram, ugunsmūra revīziju, regulāras drošības pārbaudes, revīziju, ziņošanu;

b) uzrauga darbības nepārtrauktības plāna efektivitāti un nodrošina, ka notiek regulāras mācības;

c) nodrošina pierādījumus par visiem incidentiem, kas var ietekmēt sakaru infrastruktūras vai Centrālās VIS, vai valstu sistēmu drošību, un ziņo par tiem sistēmas drošības inspektoram;

d) informē sistēmas drošības inspektoru, ja jāveic grozījumi drošības politikā;

e) uzrauga, lai šo lēmumu un drošības politiku pareizi un pilnībā piemēro visi līgumslēdzēji, tostarp apakšuzņēmēji, kuri jebkādā veidā iesaistīti sakaru infrastruktūras pārvaldībā;

f) nodrošina, ka darbiniekus informē par to pienākumiem, un uzrauga drošības politikas piemērošanu;

g) uzrauga jaunākās attīstības tendences IT drošības jomā un nodrošina, ka darbiniekus attiecīgi apmāca;

h) sagatavo pamatinformāciju un iespējas drošības politikas izveidei, atjaunināšanai un pārskatīšanai saskaņā ar 7. pantu.

5. pants

Drošības incidenti

1. Jebkurš notikums, kurš ietekmē vai var ietekmēt VIS darbības drošību un var kaitēt vai radīt zaudējumus VIS, ir uzskatāms par drošības incidentu, jo īpaši, ja ir radusies piekļuve datiem vai ir apdraudēta vai var tikt apdraudēta datu pieejamība, integritāte un konfidencialitāte.

2. Drošības politikā nosaka procedūras, kuras veic, lai atgūtos no incidenta. Drošības incidentus pārvalda, lai nodrošinātu ātru, efektīvu un pareizu reakciju atbilstīgi drošības politikai.

3. Attiecīgajai dalībvalstij sniedz informāciju par drošības incidentu, kas ietekmē vai var ietekmēt VIS darbību dalībvalstī vai dalībvalstī reģistrēto VIS datu pieejamību, integritāti un konfidencialitāti. Par drošības incidentiem paziņo Komisijas datu aizsardzības inspektoram.

6. pants

Incidentu pārvaldība

1. Visiem darbiniekiem un līgumslēdzējiem, kas iesaistīti VIS attīstībā, pārvaldībā vai darbībā, jāņem vērā visas novērotās vai iespējamās drošības nepilnības VIS darbībā un jāziņo par tām sistēmas drošības inspektoram vai par Centrālo VIS atbildīgajam vietējam drošības inspektoram vai, attiecīgā gadījumā, par sakaru infrastruktūru atbildīgajam vietējam drošības inspektoram.

2. Ja konstatēts incidents, kas ietekmē vai var ietekmēt VIS darbības drošību, par Centrālo VIS atbildīgais vietējais drošības inspektors vai par sakaru infrastruktūru atbildīgais vietējais drošības inspektors pēc iespējas drīzāk rakstiski, vai ārkārtas gadījumā izmantojot citus saziņas līdzekļus, informē sistēmas drošības inspektoru un, ja vajadzīgs, VIS drošības vienoto valsts kontaktpunktu, ja attiecīgajā dalībvalstī šāds kontaktpunkts darbojas. Ziņojumā ietver drošības incidenta aprakstu, riska līmeni, iespējamās sekas un pasākumus, kuri būtu jāveic vai kurus būtu bijis jāveic, lai mazinātu risku.

3. Visus ar drošības incidentu saistītos pierādījumus nekavējoties saglabā attiecīgi par Centrālo VIS atbildīgais vietējais drošības inspektors vai par sakaru infrastruktūru atbildīgais vietējais drošības inspektors. Saskaņā ar piemērojamajiem noteikumiem par datu aizsardzību šādus pierādījumus pēc iespējas lielākā mērā dara pieejamus sistēmas drošības inspektoram pēc tā pieprasījuma.

4. Īsteno atgriezeniskās saiknes procesus, lai nodrošinātu, ka tiek nodota informācija par rezultātiem, tiklīdz incidents ir atrisināts un beidzies.

III NODAĻA

DROŠĪBAS PASĀKUMI

7. pants

Drošības politika

1. Tiesiskuma, brīvības un drošības ģenerāldirektorāta ģenerāldirektors saskaņā ar šo lēmumu izveido, atjaunina un regulāri pārskata saistošu drošības politiku. Drošības politikā paredz detalizētas procedūras un pasākumus, lai aizsargātu pret VIS pieejamības, integritātes un konfidencialitātes apdraudējumiem, tostarp tajā ietver ārkārtas situāciju plānošanu, lai nodrošinātu pienācīgu drošības līmeni, kā paredzēts šajā lēmumā. Drošības politika atbilst šā lēmuma noteikumiem.

2. Drošības politikas pamatā ir riska novērtējums. Drošības politikā aprakstītie pasākumi ir proporcionāli identificētajiem riskiem.

3. Riska novērtējumu un drošības politiku atjaunina, ja to pieprasa tehnoloģiskas pārmaiņas, jauni identificēti apdraudējumi vai citi apstākļi. Drošības politiku jebkurā gadījumā pārskata katru gadu, lai nodrošinātu, ka tā aizvien atbilst jaunākajam riska novērtējumam vai jebkādām citām nesen identificētām tehnoloģiskajām pārmaiņām, apdraudējumiem vai citiem būtiskiem apstākļiem.

4. Drošības politiku izstrādā sistēmas drošības inspektors sadarbībā ar VIS vietējo drošības inspektoru un par sakaru infrastruktūru atbildīgo vietējo drošības inspektoru.

8. pants

Drošības pasākumu īstenošana

1. Šajā lēmumā un drošības politikā noteikto uzdevumu un prasību īstenošanai, tostarp vietējā drošības inspektora iecelšanai, var noslēgt līgumus vai to uzticēt privātām vai valsts iestādēm.

2. Šajā gadījumā Komisija, noslēdzot juridiski saistošu nolīgumu, nodrošina, ka tiek pilnībā izpildītas šajā lēmumā un drošības politikā izklāstītās prasības. Ja Komisija deleģē uzdevumu iecelt vietējo drošības inspektoru vai noslēdz par to līgumu ar apakšuzņēmēju, tā, noslēdzot juridiski saistošu nolīgumu, nodrošina, ka ar Komisiju konsultēsies par cilvēku, ko paredzēts iecelt par vietējo drošības inspektoru.

9. pants

Iekārtu piekļuves kontrole

1. Lai aizsargātu zonas, kurās atrodas datu apstrādes iekārtas, izmanto drošības robežas, uzstādot atbilstīgas barjeras, un veic iebraukšanas kontroli.

2. Drošības robežu ietvaros atdala drošas zonas, lai aizsargātu fiziskās daļas (pamatlīdzekļus), tostarp aparatūru, datu nesējus un konsoles, plānus un citus dokumentus par VIS, kā arī birojus un citas VIS darbībā iesaistītā personāla darba vietas. Šādas drošās zonas aizsargā, veicot pienācīgas iebraukšanas kontroles, lai nodrošinātu, ka piekļuve atļauta tikai pilnvarotam personālam. Darbu drošajās zonās var veikt, tikai ievērojot drošības politikā izklāstītos precīzos drošības noteikumus.

3. Tiks paredzēti un uzstādīti fiziskās drošības elementi birojos, telpās un iekārtās. Piekļuves vietas, piemēram, piegādes un izkraušanas zonas un citas telpas, kurās var ienākt nepilnvarotas personas, tiek kontrolētas un, ja iespējams, izolētas no datu apstrādes iekārtām, lai novērstu neatļautu piekļuvi.

4. Proporcionāli riskam izstrādā un piemēro drošības perimetru fizisku aizsardzību pret dabas vai cilvēku izraisītu katastrofu rezultātā radītiem bojājumiem.

5. Aprīkojumu aizsargā pret fiziskiem un vides apdraudējumiem, kā arī pret neatļautas piekļuves mēģinājumiem.

6. Ja šāda informācija nonāk Komisijas rīcībā, tā 2. panta 2. punkta f) apakšpunktā minētajā sarakstā pievieno atsevišķu kontaktpunktu šajā pantā paredzēto noteikumu īstenošanas uzraudzībai vietās, kur atrodas VIS dublējums.

10. pants

Datu nesēju un pamatlīdzekļu kontrole

1. Pārnēsājamos datu nesējus, kuros ievadīti dati, aizsargā pret neatļautu piekļuvi, ļaunprātīgu izmantošanu vai uzlaušanu, un nodrošina, ka datus var nolasīt visu to dzīves laiku.

2. Ja datu nesēji vairs nav vajadzīgi, no tiem atbrīvojas drošā veidā saskaņā ar sīki izstrādātām procedūrām, kuras jāietver drošības politikā.

3. Veicot inventarizāciju, nodrošina, ka ir pieejama informācija par datu glabāšanas vietu, piemērojamo datu uzglabāšanas periodu un piekļuves pilnvarām.

4. Tiek identificēti visi būtiskie Centrālās VIS un sakaru infrastruktūras pamatlīdzekļi, lai tos varētu aizsargāt atbilstīgi to nozīmei. Tiek glabāts atjaunināts attiecīgā IT aprīkojuma reģistrs.

5. Ir pieejama atjaunināta dokumentācija par Centrālo VIS un sakaru infrastruktūru. Šāda dokumentācija jāaizsargā pret neatļautu piekļuvi.

11. pants

Uzglabāšanas kontrole

1. Veic piemērotus pasākumus, lai nodrošinātu pareizu informācijas uzglabāšanu un novērstu neatļautu piekļuvi tai.

2. Visas aprīkojuma vienības, kuras ietver datu uzglabāšanas nesējus, pārbauda, lai nodrošinātu, ka konfidenciāli dati pirms aprīkojuma vienību izņemšanas no lietošanas ir izdzēsti vai pilnībā pārrakstīti, vai tās drošā veidā iznīcina.

12. pants

Paroles kontrole

1. Visas paroles uzglabā drošā veidā, un tās ir uzskatāmas par konfidenciālām. Ja rodas aizdomas, ka parole ir atklāta, tā nekavējoties jānomaina vai jāanulē lietotāja konts. Izmanto unikālas un individuālas lietotāju identitātes.

2. Lai novērstu neatļautu piekļuvi, drošības politikā nosaka procedūras, ar kurām pieslēdzas kontam un no tā atslēdzas.

13. pants

Piekļuves kontrole

1. Drošības politikā paredz darbinieku oficiālu reģistrēšanas procedūru attiecīgajā vietā un reģistrēšanas anulēšanas procedūru, lai darbības pārvaldības nolūkos Centrālajā VIS piešķirtu piekļuves atļauju VIS aparatūrai un programmatūrai un to anulētu. Atbilstīgu piekļuves pilnvaru (paroļu vai citu piemērotu instrumentu) piešķiršanu un izmantošanu kontrolē, izmantojot oficiālu pārvaldības procesu, kā noteikts drošības politikā.

2. Piekļuve VIS aparatūrai un programmatūrai Centrālajā VIS:

i) ir atļauta tikai pilnvarotajām personām;

ii) ir atļauta tikai gadījumos, kad var identificēt likumīgu nolūku saskaņā ar Regulas (EK) Nr. 767/2008 42. pantu un 50. panta 2. punktu;

iii) nepārsniedz piekļuves nolūkam vajadzīgo apmeklējuma ilgumu un darbības jomu; kā arī

iv) tiek īstenota tikai saskaņā ar piekļuves kontroles politiku, kas jānosaka drošības politikā.

3. Centrālajā VIS izmanto tikai tās konsoles un programmatūru, ko pilnvarojis par Centrālo VIS atbildīgais vietējais drošības inspektors. Tādu sistēmas iekārtu izmantošana, kuras spēj ignorēt sistēmas un lietojumprogrammu kontroli, ir ierobežota un kontrolēta. Tiek ieviestas procedūras, lai kontrolētu programmatūras uzstādīšanu.

14. pants

Sakaru kontrole

Sakaru struktūru uzrauga, lai nodrošinātu informācijas apmaiņas pieejamību, integritāti un konfidencialitāti. Lai aizsargātu sakaru infrastruktūras ietvaros pārsūtītos datus, izmanto kriptogrāfiskos līdzekļus.

15. pants

Datu reģistrēšanas kontrole

To personu kontus, kuriem piešķirtas pilnvaras piekļuvei VIS programmatūrai no Centrālās VIS, uzrauga par Centrālo VIS atbildīgais vietējais drošības inspektors. Tiek reģistrēta minēto kontu izmantošana, tostarp izmantošanas laiks un lietotāja identitāte.

16. pants

Pārraides kontrole

1. Drošības politikā nosaka piemērotus pasākumus, lai novērstu personas datu neatļautu lasīšanu, kopēšanu, izmainīšanu vai dzēšanu laikā, kad datus pārsūta uz VIS vai no tās vai transportē datu nesējus. Drošības politikā paredz noteikumus attiecībā uz pieļaujamajiem nosūtīšanas vai transportēšanas veidiem, kā arī attiecībā uz vienību transportēšanas un to galamērķa sasniegšanas pārskata procedūrām. Datu nesējā ietver tikai tos datus, kuri paredzēti nosūtīšanai.

2. Attiecībā uz pakalpojumiem, kurus sniedz trešās personas un kuros iesaistīta piekļuve datiem, to apstrāde, nosūtīšana un datu apstrādes iekārtu pārvaldība vai produktu vai pakalpojumu pievienošana datu apstrādes iekārtām, attiecīgi veic integrētas drošības kontroles.

17. pants

Sakaru infrastruktūras drošība

1. Sakaru infrastruktūru atbilstoši pārvalda un kontrolē, lai aizsargātu to pret apdraudējumiem un nodrošinātu pašas sakaru infrastruktūras un centrālās VIS, tostarp tās ietvaros veiktās datu apmaiņas drošību.

2. Visi tīkla pakalpojumu drošības elementi, drošības līmeņi un pārvaldības prasības ir identificētas tīkla pakalpojumu nolīgumā, kas noslēgts ar attiecīgo pakalpojumu sniedzēju.

3. Papildus VIS piekļuves punktu aizsardzībai aizsargā arī visus pārējos pakalpojumus, kurus izmanto sakaru infrastruktūras ietvaros. Drošības politikā nosaka attiecīgus pasākumus.

18. pants

Uzraudzība

1. Ierakstus ar Regulas (EK) Nr. 767/2008 34. panta 1. punktā minēto informāciju, kas attiecas uz katru piekļuvi datiem un visām datu apstrādes darbībām Centrālajā VIS, drošā veidā uzglabā telpās, kurās atrodas Centrālā VIS un VIS dublējums, un tiem var piekļūt uz laikposmu, kas minēts Regulas (EK) Nr. 767/2008 34. panta 2. punktā.

2. Informācijas apstrādes iekārtu izmantošanas vai kļūdu novēršanas uzraudzības procedūras izklāsta drošības politikā, un uzraudzības darbību rezultāti tiek regulāri pārskatīti. Nepieciešamības gadījumā seko piemērota rīcība.

3. Reģistrācijas iekārtas un ierakstus aizsargā pret krāpnieciskām darbībām un neatļautu piekļuvi, lai izpildītu datu apkopošanas un uzglabāšanas prasības pierādījumu uzglabāšanas periodā.

19. pants

Kriptogrāfiskie pasākumi

Vajadzības gadījumā informācijas aizsardzības nolūkā izmanto kriptogrāfiskus pasākumus. Šādu pasākumu izmantošanai, tostarp precizējot konkrētus nolūkus un apstākļus, jāsaņem iepriekšējs apstiprinājums no sistēmas drošības inspektora.

IV NODAĻA

CILVĒKRESURSU DROŠĪBA

20. pants

Darbinieku apraksti

1. Drošības politikā definē to personu funkcijas un pienākumus, kuriem sniegta atļauja piekļūt VIS, kā arī sakaru infrastruktūrai.

2. Informāciju par Komisijas darbinieku, līgumslēdzēju un darbības pārvaldībā iesaistīto darbinieku uzdevumiem un pienākumiem drošības jomā definē, dokumentē un dara zināmu attiecīgajām personām. Komisijas darbinieku un līgumslēdzēju uzdevumus un pienākumus izklāsta darba aprakstā un tā mērķos, attiecībā uz līgumslēdzējiem – pakalpojumu līmeņa nolīgumos.

3. Ar visām personām, uz kurām neattiecas Eiropas Savienības vai dalībvalstu civildienesta noteikumi, noslēdz konfidencialitātes un dienesta noslēpumu glabāšanas nolīgumus. Darbiniekiem, kuriem jāstrādā ar VIS datiem, veic vajadzīgo drošības pārbaudi vai sertifikāciju saskaņā ar precīzām procedūrām, kuras jāietver drošības politikā.

21. pants

Informācija personālam

1. Visi darbinieki un vajadzības gadījumā līgumslēdzēji saņem atbilstošu apmācību par drošības izpratnes, juridisko prasību, politikas virzienu un procedūru jautājumiem tādā apjomā, kādā tas ir nepieciešams pienākumu izpildei.

2. Attiecībā uz darba līguma vai līgumsaistību termiņa beigām drošības politikā nosaka ar darba maiņu vai darba attiecību izbeigšanu saistītos pienākumus darbiniekiem vai līgumslēdzējiem, un tajā arī izklāsta procedūras, lai pārvaldītu līdzekļu atgriešanu un piekļuves tiesību anulēšanu.

V NODAĻA

NOBEIGUMA NOTEIKUMI

22. pants

Piemērojamība

1. Šo lēmumu sāk piemērot dienā, ko Komisija nosaka saskaņā ar Regulas (EK) Nr. 767/2008 48. panta 1. punktu.

2. Lēmuma darbības termiņš beidzas dienā, kad vadības iestāde sāk pildīt savus pienākumus.

Briselē, 2010. gada 4. maijā

Komisijas vārdā –
priekšsēdētājs
José Manuel BARROSO