KOMISJONI OTSUS,

4. mai 2010,

viisainfosüsteemi turvakava kohta

(2010/260/EL)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 9. juuli 2008. aasta määrust (EÜ) nr 767/2008, mis käsitleb viisainfosüsteemi (VIS) ja liikmesriikidevahelist teabevahetust lühiajaliste viisade kohta (VIS määrus), [1] eriti selle artikli 32,

ning arvestades järgmist:

(1) Määruse (EÜ) nr 767/2008 artikli 32 lõikes 3 on sätestatud, et korraldusasutus võtab vajalikke meetmeid, et saavutada artikli 32 lõikes 2 esitatud eesmärgid seoses VISi kasutamisega, kaasa arvatud turvakava vastuvõtmine.

(2) Määruse (EÜ) nr 767/2008 artikli 26 lõikes 4 on sätestatud, et üleminekuperioodil enne seda, kui korraldusasutus asub oma ülesandeid täitma, vastutab VISi operatiivjuhtimise eest komisjon.

(3) Euroopa Parlamendi ja nõukogu määrust (EÜ) nr 45/2001 [2] kohaldatakse isikuandmete töötlemise suhtes, mida teostab komisjon VISi operatiivjuhtimisega seotud kohustuste täitmisel.

(4) Määruse (EÜ) nr 767/2008 artikli 26 lõikes 7 on sätestatud, et juhul kui komisjon delegeerib üleminekuperioodi vältel oma kohustused enne seda, kui korraldusasutus hakkab täitma oma kohustusi, tagab ta, et kõnealune delegeerimine ei avaldaks ebasoovitavat mõju ühelegi Euroopa Liidu õiguse alusel loodud tõhusale kontrollimehhanismile, olgu selleks siis Euroopa Kohus, kontrollikoda või Euroopa andmekaitseinspektor.

(5) Korraldusasutus peaks vastu võtma VISi turvakava pärast seda, kui ta on asunud täitma oma kohustusi.

(6) Komisjoni 17. juuni 2008. aasta otsuses 2008/602/EÜ (millega määratakse väljatöötamisetapiks kindlaks VISi riikide liideste ning keskinfosüsteemi ja riikide liideste vahelise sideinfrastruktuuri füüsiline ülesehitus ning neile esitatavad nõuded) [3] kirjeldatakse VIS võrgu suhtes kohaldatavaid turvateenuseid.

(7) Määruse (EÜ) nr 767/2008 artiklis 27 on sätestatud, et keskne VIS põhisüsteem, mis teostab tehnilist järelevalvet ja täidab haldusfunktsiooni, asub Prantsusmaal Strasbourgis ja keskne VIS varusüsteem, mis suudab tagada keskse VIS põhisüsteemi kõik funktsioonid viimase rikke korral, asub Austrias Sankt Johann im Pongaus.

(8) Turvaametnike tööülesanded tuleks kindlaks määrata, et tagada tõhus ja kiire reageerimine turvaintsidentidele ja nendest teatamine.

(9) Sätestada tuleks turbepoliitika, mis hõlmaks kõiki käesoleva otsuse kohaseid tehnilisi ja korralduslikke üksikasju.

(10) Tuleks kindlaks määrata meetmed, et tagada VISi toimimise piisav turvalisus,

ON VASTU VÕTNUD JÄRGMISE OTSUSE:

I PEATÜKK

ÜLDSÄTTED

Artikkel 1

Sisu

Käesoleva otsusega kehtestatakse turvalisuse kord ja meetmed (turvakava) määruse (EÜ) nr 767/2008 artikli 32 lõike 3 tähenduses.

II PEATÜKK

KORRALDUS, KOHUSTUSED JA INTSIDENTIDE HALDAMINE

Artikkel 2

Komisjoni ülesanded

1. Komisjon rakendab keskse VISi ja sideinfrastruktuuri turvalisuse tagamiseks käesolevas otsuses nimetatud meetmeid ja kontrollib nende tõhusust.

[1] ELT L 218, 13.8.2008, lk 60.
[2] ELT L 8, 12.1.2001, lk 1.
[3] ELT L 194, 23.7.2008, lk 3.

2. Komisjon määrab oma ametnike hulgast süsteemi turvalisuse eest vastutava ametniku. Süsteemi turvalisuse eest vastutava ametniku nimetab ametisse komisjoni õigus-, vabadus- ja turvalisusküsimuste peadirektoraadi peadirektor. Süsteemi turvalisuse eest vastutava ametniku ülesannete hulka kuuluvad eelkõige järgmised ülesanded:

a) turbepoliitika ettevalmistamine, ajakohastamine ja läbivaatamine käesoleva otsuse artikli 7 kohaselt;

b) keskse VISi ja sideinfrastruktuuri turvamenetluse rakendamise tõhususe kontrollimine;

c) määruse (EÜ) nr 767/2008 artikli 50 lõigetes 3 ja 4 nimetatud turvalisusega seotud aruannete ettevalmistamisele kaasaaitamine;

d) määruse (EÜ) nr 767/2008 artiklis 42 nimetatud Euroopa andmekaitseinspektori kontrollide ja auditite kooskõlastamine ja abistamine;

e) selle kontrollimine, et tööettevõtja, sealhulgas alltöövõtja, kes osaleb mis tahes moel VISi juhtimises ja toimimises, kohaldab käesolevat otsust ja turbepoliitikat nõuetekohaselt ja täielikult;

f) VISi turvalisusega tegelevate riiklike kontaktpunktide nimekirja haldamine ja sellise nimekirja jagamine keskse VISi ja sideinfrastruktuuri kohalike turvaametnikega.

Artikkel 3

Keskse VISi kohalik turvaametnik

1. Ilma et see piiraks artikli 8 kohaldamist, määrab komisjon oma ametnike hulgast keskse VISi kohaliku turvaametniku. Välistatakse huvide konflikt kohaliku turvaametniku kohustuste ja mis tahes muude ametikohustuste vahel. Keskse VISi kohaliku turvaametniku nimetab ametisse komisjoni õigus-, vabadus- ja turvalisusküsimuste peadirektoraadi peadirektor.

2. Keskse VISi kohalik turvaametnik tagab, et keskse VISi põhisüsteemis rakendatakse käesolevas otsuses nimetatud turvameetmeid ja järgitakse turvamenetlust. Keskse VISi varusüsteemi puhul tagab keskse VISi kohalik turvaametnik ka, et rakendatakse käesolevas otsuses nimetatud turvameetmeid, välja arvatud artiklis 10 nimetatud meetmed, ja järgitakse nendega seotud turvamenetlust.

3. Keskse VISi kohalik turvaametnik võib delegeerida mis tahes tööülesande oma alluvatele. Välistatakse huvide konflikt kõnealuste tööülesannete täitmise kohustuste ja mis tahes muude ametikohustuste vahel. Üks kontakttelefon ja -aadress võimaldavad võtta kohaliku turvaametniku või tema parajasti tööl oleva alluvaga ühendust mis tahes ajahetkel.

4. Keskse VISi kohalik turvaametnik täidab ülesandeid, mis tulenevad turvameetmetest, mida võetakse keskse VISi põhi- ja varusüsteemi asukohas lõikes 1 sätestatud piirangute raames, sealhulgas eelkõige järgmisi ülesandeid:

a) süsteemi toimimise turvalisusega seotud kohalikud ülesanded, sealhulgas tulemüüri audit, korrapärane turvalisuse kontroll, auditeerimine ja aruandlus;

b) talituspidevuse kava tõhususe kontrollimine ja korrapäraste õppuste korraldamise tagamine;

c) tõendite kogumine selliste intsidentide kohta, mis võivad mõjutada keskse VISi või sideinfrastruktuuri turvalisust, ja nendest intsidentidest teatamine süsteemi turvalisuse eest vastutavale ametnikule;

d) süsteemi turvalisuse eest vastutava ametniku teavitamine juhul, kui turbepoliitika vajab muutmist;

e) selle kontrollimine, et tööettevõtja, sealhulgas alltöövõtja, kes osaleb mis tahes moel keskse VISi juhtimises ja toimimises, kohaldab käesolevat otsust ja turbepoliitikat;

f) selle tagamine, et personal oleks teadlik oma kohustustest, ja turbepoliitika kohaldamise kontrollimine;

g) infotehnoloogiaalase turvalisuse arengu kontrollimine ja selle tagamine, et personali koolitatakse asjakohaselt;

h) turbepoliitika väljatöötamise, ajakohastamise ja läbivaatamise aluseks oleva teabe ja lahenduste ettevalmistamine kooskõlas artikliga 7.

Artikkel 4

Sideinfrastruktuuri kohalik turvaametnik

1. Ilma et see piiraks artikli 8 kohaldamist, määrab komisjon oma ametnike hulgast sideinfrastruktuuri kohaliku turvaametniku. Välistatakse huvide konflikt kohaliku turvaametniku kohustuste ja mis tahes muude ametikohustuste vahel. Sideinfrastruktuuri kohaliku turvaametniku nimetab ametisse komisjoni õigus-, vabadus- ja turvalisusküsimuste peadirektoraadi peadirektor.

2. Sideinfrastruktuuri kohalik turvaametnik kontrollib sideinfrastruktuuri toimimist ja tagab, et kohaldatakse turvameetmeid ja järgitakse turvamenetlust.

3. Sideinfrastruktuuri kohalik turvaametnik võib delegeerida mis tahes tööülesande oma alluvatele. Välistatakse huvide konflikt kõnealuste tööülesannete täitmise kohustuste ja mis tahes muude ametikohustuste vahel. Üks kontakttelefon ja -aadress võimaldavad võtta kohaliku turvaametniku või tema parajasti tööl oleva alluvaga ühendust mis tahes ajahetkel.

4. Sideinfrastruktuuri kohalik turvaametnik täidab ülesandeid, mis tulenevad turvameetmetest, mida võetakse seoses sideinfrastruktuuriga, sealhulgas eelkõige järgmisi ülesandeid:

a) kõik sideinfrastruktuuri toimimise turvalisusega seotud kohalikud ülesanded, sealhulgas tulemüüri audit, korrapärane turvalisuse kontroll, auditeerimine ja aruandlus;

b) talituspidevuse kava tõhususe kontrollimine ja korrapäraste õppuste korraldamise tagamine;

c) tõendite kogumine selliste intsidentide kohta, mis võivad mõjutada keskse VISi või sideinfrastruktuuri või riiklike süsteemide turvalisust, ja nendest intsidentidest teatamine süsteemi turvalisuse eest vastutavale ametnikule;

d) süsteemi turvalisuse eest vastutava ametniku teavitamine juhul, kui turbepoliitika vajab muutmist;

e) selle kontrollimine, et tööettevõtja, sealhulgas alltöövõtja, kes osaleb mis tahes moel sideinfrastruktuuri juhtimises, kohaldab käesolevat otsust ja turbepoliitikat;

f) selle tagamine, et personal oleks teadlik oma kohustustest, ja turbepoliitika kohaldamise kontrollimine;

g) infotehnoloogiaalase turvalisuse arengu kontrollimine ja selle tagamine, et personali koolitatakse asjakohaselt;

h) turbepoliitika väljatöötamise, ajakohastamise ja läbivaatamise aluseks oleva teabe ja lahenduste ettevalmistamine kooskõlas artikliga 7.

Artikkel 5

Turvaintsidendid

1. Mis tahes sündmust, mis mõjutab või võib mõjutada VISi toimimise turvalisust ning mis võib VISile kaasa tuua kahju või andmete kadu, peetakse turvaintsidendiks, eelkõige juhul, kui leidis aset juurdepääs andmetele või kui andmete kättesaadavus, terviklikkus ja konfidentsiaalsus on sattunud või võib sattuda ohtu.

2. Turbepoliitikaga kehtestatakse kord, mida kohaldada pärast turvaintsidentide esinemist. Turvaintsidentidele reageeritakse kooskõlas turbepoliitikaga kiirelt, tõhusalt ja nõuetekohaselt.

3. Teave turvaintsidendi kohta, mis mõjutab või võib mõjutada VISi toimimist liikmesriigis või liikmesriigi saadetud andmete kättesaadavust, terviklikkust või konfidentsiaalsust, saadetakse asjaomasele liikmesriigile. Turvaintsidentidest teatatakse komisjoni andmekaitseametnikule.

Artikkel 6

Intsidentide haldamine

1. Kogu personalilt ja kõikidelt tööettevõtjatelt, kes osalevad VISi arendamises, haldamises ja juhtimises, nõutakse, et nad märgiksid üles kõik täheldatud või võimalikud turvalisuse puudused VISi toimimises ja teataksid nendest süsteemi turvalisuse eest vastutavale ametnikule, keskse VISi kohalikule turvaametnikule või sideinfrastruktuuri kohalikule turvaametnikule.

2. Sellise intsidendi avastamise korral, mis mõjutab või võib mõjutada VISi toimimise turvalisust, teatab keskse VISi kohalik turvaametnik või sideinfrastruktuuri kohalik turvaametnik sellest kirjalikult või väga kiireloomulise juhtumi puhul muude sidekanalite kaudu nii kiiresti kui võimalik süsteemi turvalisuse eest vastutavale ametnikule ning vajaduse korral VISi turvalisuse eest vastutavale riiklikule kontaktpunktile, juhul kui selline kontaktpunkt on asjaomases liikmesriigis loodud. Aruanne sisaldab turvaintsidendi kirjeldust, riskitaset, võimalikke tagajärgi ja meetmeid, mida on võetud või mida tuleks võtta, et riski vähendada.

3. Keskse VISi kohalik turvaametnik või sideinfrastruktuuri kohalik turvaametnik peab kohe kokku koguma kõik turvaintsidendiga seotud tõendid. Niivõrd kui see on kohaldatavate andmekaitsesätete kohaselt võimalik, tehakse kõnealused tõendid kättesaadavaks süsteemi turvalisuse eest vastutavale ametnikule, kui ta seda taotleb.

4. Et tagada turvaintsidentide tagajärgi käsitleva teabe edastamine siis, kui turvaintsident on lahendatud ja selle menetlemine lõpetatud, kohaldatakse tagasiside andmise korda.

III PEATÜKK

TURVAMEETMED

Artikkel 7

Turbepoliitika

1. Õigus-, vabadus- ja turvalisusküsimuste peadirektoraadi peadirektor kehtestab, ajakohastab ja vaatab kooskõlas käesoleva otsusega korrapäraselt läbi siduva turbepoliitika. Turbepoliitikas nähakse ette üksikasjalik menetlus ja üksikasjalikud meetmed, et kaitsta VISi selle kättesaadavust, terviklikkust ja konfidentsiaalsust ähvardavate ohtude eest, sealhulgas hädaolukorra lahendamise plaan, et tagada nõuetekohane turvalisuse tase vastavalt käesolevale otsusele. Turbepoliitika peab olema kooskõlas käesoleva otsusega.

2. Turbepoliitika põhineb riskihindamisel. Turbepoliitikas kirjeldatud meetmed on proportsionaalsed tuvastatud riskidega.

3. Riskihindamist ja turbepoliitikat ajakohastatakse juhul, kui tehnoloogilised muutused, tuvastatud uued ohud või mis tahes muud asjaolud seda nõuavad. Igal juhul vaadatakse turbepoliitika läbi kord aastas, tagamaks, et see vastab jätkuvalt nõuetekohaselt kõige viimasele riskihindamisele või mis tahes muule äsja tuvastatud tehnoloogilisele muutusele, ohule või muule asjaomasele asjaolule.

4. Turbepoliitika valmistab ette süsteemi turvalisuse eest vastutav ametnik koostöös VISi kohaliku turvaametnikuga ja sideinfrastruktuuri kohaliku turvaametnikuga.

Artikkel 8

Turvameetmete rakendamine

1. Käesolevas otsuses ja turbepoliitikas ettenähtud ülesannete ja nõuete rakendamist, sealhulgas kohaliku turvaametniku määramist, võib korraldada allhanke korras või usaldada need era- või avalik-õiguslikule asutusele.

2. Sellisel juhul tagab komisjon õiguslikult siduva lepingu kaudu, et käesolevas otsuses ja turbepoliitikas ettenähtud nõuded on täielikult täidetud. Kohaliku turvaametniku määramise ülesande delegeerimise või allhanke korras korraldamise korral tagab komisjon õiguslikult siduva lepingu kaudu, et komisjoniga peetakse nõu kohalikuks turvaametnikuks määratava inimese küsimuses.

Artikkel 9

Rajatistele juurdepääsu kontroll

1. Andmetöötlusrajatiste asukoha kaitsmiseks kasutatakse turvapiirdeid koos asjakohaste tõkete ja sisenemiskontrollidega.

2. Turvapiirete raames määratakse kindlaks turvaala, et kaitsta füüsilisi elemente (varad), sealhulgas tarkvara, andmekandjad ja konsoolid, VISi käsitlevad kavad ja muud dokumendid ning VISi juhtimises osalevate töötajate kabinetid ja muud töökohad. Kõnealust turvaala kaitstakse asjakohaseid sisenemiskontrolle kasutades, et tagada ainult volitatud töötajate juurdepääs turvaalale. Turvaalal toimuva tegevuse suhtes kohaldatakse üksikasjalikke turvaeeskirju, mis on sätestatud turbepoliitikas.

3. Nähakse ette ja võetakse kasutusele füüsilised turvameetmed kabinettide, ruumide ja rajatiste kaitseks. Kontrollitakse selliseid juurdepääsupunkte nagu tarnealad, laadimisalad ja muud kohad, kus volitamata isikutel võib olla võimalik ruumidesse siseneda; võimaluse korral isoleeritakse sellised punktid andmetöötlusrajatistest, et vältida loata juurdepääsu.

4. Töötatakse välja turvapiirete füüsiline kaitse loodus- ja inimtegevusest põhjustatud suurõnnetustega seotud kahju eest ning seda kaitset rakendatakse proportsionaalselt riskidega.

5. Seadmeid kaitstakse füüsiliste ja keskkonnaohtude eest ning loata juurdepääsu võimaluste eest.

6. Juhul kui komisjonil on sellist teavet, lisab ta artikli 2 lõike 2 alapunktis f nimetatud nimekirja kontaktpunkti, kes kontrollib käesoleva artikli rakendamist keskse VISi varusüsteemi asukohas.

Artikkel 10

Andmekandjate ja varade kontroll

1. Andmeid sisaldavaid eemaldatavaid andmekandjaid kaitstakse loata juurdepääsu, väärkasutamise ja andmelaostuse eest ning nende loetavus tagatakse kogu andmete kasutusaja jooksul.

2. Kui andmekandjaid enam vaja ei ole, kõrvaldatakse need kasutusest turvaliselt ja ohutult kooskõlas turbepoliitikas ettenähtud üksikasjaliku korraga.

3. Inventuuridega tagatakse, et teave säilituskoha, kohaldatava säilitamisaja ja juurdepääsulubade kohta oleks kättesaadav.

4. Tuvastatakse keskse VISi ja sideinfrastruktuuri kõik olulised varad, et neid oleks vastavalt nende olulisusele võimalik kaitsta. Peetakse ajakohastatud registrit asjaomastest infotehnoloogilistest seadmetest.

5. Tehakse kättesaadavaks keskse VISi ja sideinfrastruktuuri ajakohastatud dokumendid. Selliseid dokumente tuleb loata juurdepääsu eest kaitsta.

Artikkel 11

Säilitamise kontroll

1. Võetakse asjaomaseid meetmeid, et tagada andmete nõuetekohane säilitamine ja vältida loata juurdepääsu säilitatavatele andmetele.

2. Kontrollitakse kõiki säilitatud andmeid sisaldavaid seadmeid, tagamaks, et kõik delikaatsed andmed on enne seadmete kasutusest kõrvaldamist kustutatud või täies ulatuses üle kirjutatud, või hävitatakse vastavad seadmed turvaliselt.

Artikkel 12

Salasõnade kontroll

1. Kõiki salasõnasid säilitatakse turvaliselt ja käsitletakse konfidentsiaalsetena. Juhul kui on kahtlus, et salasõna on kolmandatele isikutele avaldatud, tuleb see kohe ära vahetada või peatada asjaomase konto kasutamine. Kasutatakse unikaalseid ja isiklikke kasutajatunnuseid.

2. Turbepoliitikas nähakse ette sisse- ja väljaregistreerimise kord, et vältida loata juurdepääsu.

Artikkel 13

Juurdepääsu kontroll

1. Turbepoliitikas nähakse ette ametlik töötajate sisse- ja väljaregistreerimise kord, et anda ja tühistada süsteemi operatiivjuhtimise eesmärgil juurdepääs keskses VISis VISi riist- ja tarkvarale. Asjakohase juurdepääsu volituste määramist ja kasutamist (salasõna ja muud asjaomased vahendid) kontrollitakse turbepoliitikas ettenähtud ametliku halduskorra abil.

2. Juurdepääs VISi riist- ja tarkvarale keskses VISis:

i) on ainult volitatud töötajatel;

ii) antakse vaid juhul, kui on võimalik tuvastada õiguspärane eesmärk kooskõlas määruse (EÜ) nr 767/2008 artikliga 42 ja artikli 50 lõikega 2;

iii) ei ületa kestuselt ega ulatuselt seda, mida on vaja juurdepääsu andmise eesmärgi täitmiseks, ning

iv) leiab aset vaid kooskõlas turbepoliitikas ettenähtud juurdepääsu kontrolli korraga.

3. Keskses VISis kasutatakse ainult keskse VISi kohaliku turvaametniku poolt heakskiidetud konsoole ja tarkvara. Selliste süsteemiutiliitide kasutamist, mille abil võib mööda minna süsteemi ja rakenduste kontrollimisest, piiratakse ja kontrollitakse. Tarkvara paigalduse kontrollimiseks kehtestatakse vastav kord.

Artikkel 14

Andmeedastuse kontroll

Sideinfrastruktuuri jälgitakse selleks, et tagada vahetatava teabe kättesaadavus, terviklikkus ja konfidentsiaalsus. Sideinfrastruktuuris edastatavate andmete kaitseks kasutatakse krüptograafilisi vahendeid.

Artikkel 15

Sisestamise kontroll

Nende isikute kasutajakontosid, kellel on luba VISi tarkvarale juurdepääsuks keskse VISi kaudu, kontrollib keskse VISi kohalik turvaametnik. Selliste kontode kasutamine, sealhulgas kellaeg ja kasutaja isik, registreeritakse.

Artikkel 16

Transpordikontroll

1. Turbepoliitikas nähakse ette asjakohased meetmed, et ära hoida isikuandmete loata lugemine, kopeerimine, muutmine või kustutamine nende VISi süsteemi või süsteemist edastamise või andmekandjate transportimise ajal. Turbepoliitikas nähakse ette sätted seoses andmete lähetamise või transportimise vastuvõetavate liikidega ning andmete transportimisest ja nende sihtkohta saabumisest aruandmise korraga. Andmekandja ei sisalda muid andmeid kui need, mida soovitakse süsteemi edastada.

2. Kolmandate isikute osutatud teenuste suhtes, mis on seotud andmetele juurdepääsu, nende töötlemise ja edastamise ning andmetöötlusrajatiste haldamise või andmetöötlusrajatistele toodete või teenuste lisamisega, rakendatakse asjakohaseid integreeritud turvakontrolle.

Artikkel 17

Sideinfrastruktuuri turvalisus

1. Sideinfrastruktuuri hallatakse ja kontrollitakse nõuetekohaselt, et kaitsta seda ohtude eest ning tagada sideinfrastruktuuri ja keskse VISi, sealhulgas süsteemi kaudu edastatavate andmete turvalisus.

2. Kõikide võrguteenuste turvaelemendid, teenusetase ja haldusnõuded määratakse kindlaks teenuseosutajaga sõlmitavas võrguteenuste osutamise lepingus.

3. Lisaks VISi juurdepääsupunktide kaitsmisele kaitstakse ka mis tahes muid teenuseid, mida sideinfrastruktuuris kasutatakse. Turbepoliitikas nähakse ette asjakohased meetmed.

Artikkel 18

Kontroll

1. Register, millesse on kantud määruse (EÜ) nr 767/2008 artikli 34 lõikes 1 nimetatud teave, mis käsitleb iga juurdepääsu keskses VISis hoitavatele isikuandmetele ja nende andmete igasugust töötlemist, säilitatakse turvaliselt ning sellele võimaldatakse keskse VISi põhi- ja varusüsteemi asukohas juurdepääs maksimaalselt määruse (EÜ) nr 767/2008 artikli 34 lõikes 2 sätestatud ajavahemiku jooksul.

2. Turbepoliitikas nähakse ette andmetöötlusrajatiste kasutamise ja nendes esinevate vigade kontrollimine ning selliste kontrollide tulemuste korrapärane läbivaatamine. Vajaduse korral võetakse asjakohaseid meetmeid.

3. Registreid ja rajatisi, kus neid säilitatakse, kaitstakse mis tahes rikkumise või loata juurdepääsu eest, et täita säilitamisaja jooksul tõendite kogumise ja säilitamisega seotud nõudeid.

Artikkel 19

Krüptograafilised vahendid

Vajaduse korral kasutatakse teabe kaitsmiseks krüptograafilisi vahendeid. Süsteemi turvalisuse eest vastutav ametnik peab eelnevalt heaks kiitma nende kasutamise, eesmärgid ja tingimused.

IV PEATÜKK

PERSONALIGA SEOTUD TURVALISUSKÜSIMUSED

Artikkel 20

Personali profiilid

1. Turbepoliitikas nähakse ette nende isikute ülesanded ja kohustused, kellel on luba juurdepääsuks VISile, sealhulgas sideinfrastruktuurile.

2. Komisjoni ametnike, tööettevõtjate ja operatiivjuhtimisega seotud personali turvalisusega seotud ülesanded ja kohustused määratakse kindlaks, dokumenteeritakse ja nendest teavitatakse asjaomaseid isikuid. Komisjoni personali puhul on kõnealused ülesanded ja kohustused kirjas ametijuhendis ja tööeesmärkides; tööettevõtjate puhul on need kirjas lepingutes või teenuse taseme kokkulepetes.

3. Konfidentsiaalsus- ja saladuse hoidmise lepingud sõlmitakse kõigi nende töötajatega, kelle suhtes ei kohaldata Euroopa Liidu või liikmesriigi avaliku teenistuse eeskirju. Töötajatele, kes peavad töötama VISi andmetega, antakse vajalik luba või sertifikaat kooskõlas turbepoliitikas ettenähtud üksikasjaliku korraga.

Artikkel 21

Teave personali kohta

1. Kogu personali ja vajaduse korral kõiki tööettevõtjaid koolitakse asjakohaselt seoses turvateadlikkuse, õigusnormide, poliitika ja menetlustega ulatuses, mida nõuavad nende kohustused.

2. Töösuhte või lepingu lõppemisel määratakse turbepoliitikas kindlaks töötajate ja tööettevõtjate kohustused seoses töömuutuse või töösuhte lõppemisega ning varade tagastamise ja juurdepääsuloa tühistamise kord.

V PEATÜKK

LÕPPSÄTE

Artikkel 22

Kohaldamine

1. Käesolevat otsust hakatakse kohaldama kuupäevast, mille määrab kindlaks komisjon kooskõlas määruse (EÜ) nr 767/2008 artikli 48 lõikega 1.

2. Käesolev otsus kaotab kehtivuse, kui korraldusasutus asub täitma oma ülesandeid.

Brüssel, 4. mai 2010

Komisjoni nimel

president

José Manuel BARROSO