KOMISJONI OTSUS,

4. mai 2010,

keskse SIS II ja sideinfrastruktuuri turvakava kohta

(2010/261/EL)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut,

võttes arvesse Euroopa Parlamendi ja nõukogu 20. detsembri 2006. aasta määrust (EÜ) nr 1987/2006, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist, [1] eriti selle artiklit 16,

võttes arvesse nõukogu 12. juuni 2007. aasta otsust 2007/533/JSK, mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist, [2] eriti selle artiklit 16,

ning arvestades järgmist:

(1) Määruse (EÜ) nr 1987/2006 artiklis 16 ja otsuse 2007/533/JSK artiklis 16 on sätestatud, et korraldusasutus võtab seoses keskse SIS II ning komisjon seoses sideinfrastruktuuriga vastu vajalikud meetmed, sealhulgas turvakava.

(2) Määruse (EÜ) nr 1987/2006 artikli 15 lõikes 4 ja otsuse 2007/533/JSK artikli 15 lõikes 4 on sätestatud, et üleminekuperioodil enne seda, kui korraldusasutus asub oma ülesandeid täitma, vastutab keskse SIS II operatiivjuhtimise eest komisjon.

(3) Et korraldusasutust ei ole veel loodud, tuleks komisjoni vastuvõetavat turvakava üleminekuperioodil kohaldada ka keskse SIS II suhtes.

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

(5) Määruse (EÜ) nr 1987/2006 artikli 15 lõikes 7 ja otsuse 2007/533/JSK artikli 15 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 avalda ebasoovitavat mõju ühelegi Euroopa Liidu õiguse alusel loodud tõhusale kontrollimehhanismile, olgu selleks siis Euroopa Kohus, kontrollikoda või Euroopa Andmekaitseinspektor.

(6) Korraldusasutus peaks vastu võtma keskse SIS II turvakava pärast seda, kui ta on asunud täitma oma kohustusi. Käesolev turvakava peaks seega kaotama kehtivuse keskse SIS II osas siis, kui korraldusasutus asub oma kohustusi täitma.

(7) Määruse (EÜ) nr 1987/2006 artikli 4 lõikes 3 ja otsuse 2007/533/JSK artikli 4 lõikes 3 on sätestatud, et CS-SISi põhisüsteem, mis teostab tehnilist järelevalvet ja haldusfunktsioone, hakkab asuma Strasbourgis (Prantsusmaal) ja CS-SISi varusüsteem, mis suudab tagada põhisüsteemi kõik funktsioonid viimase rikke korral, hakkab asuma Sankt Johann im Pongaus (Austrias).

(8) Turvakavas tuleks ette näha üks süsteemi turvalisuse eest vastutav ametnik, kes täidab turvalisusega seotud ülesandeid nii keskse SIS II kui ka sideinfrastruktuuri puhul, ning kaks kohalikku turvaametnikku, kes täidavad turvalisusega seotud ülesandeid vastavalt keskse SIS II või sideinfrastruktuuri puhul. 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 keskse SIS II ja sideinfrastruktuuri toimimise piisav turvalisus,

[1] ELT L 381, 28.12.2006, lk 4.
[2] ELT L 205, 7.8.2007, lk 63.
[3] ELT L 8, 12.1.2001, lk 1.

ON VASTU VÕTNUD KÄESOLEVA OTSUSE:

I. PEATÜKK

ÜLDSÄTTED

Artikkel 1

Sisu

1. Käesoleva otsusega kehtestatakse üleminekuperioodiks turvalisuse kord ja meetmed (turvakava), et kaitsta keskset SIS II ja selles töödeldavaid andmeid nende kättesaadavust, terviklikkust ja konfidentsiaalsus ähvardavate ohtude eest määruse (EÜ) nr 1987/2006 artikli 16 lõike 1 ja otsuse 2007/533/JSK (mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist) artikli 16 lõike 1 tähenduses enne seda, kui korraldusasutus asub oma kohustusi täitma.

2. Käesoleva otsusega kehtestatakse turvakorraldus ja -meetmed (turvakava), et kaitsta sideinfrastruktuuri selle kättesaadavust, terviklikkust ja konfidentsiaalsust ähvardavate ohtude eest määruse (EÜ) nr 1987/2006 artikli 16 ja otsuse 2007/533/JSK (mis käsitleb teise põlvkonna Schengeni infosüsteemi (SIS II) loomist, toimimist ja kasutamist) artikli 16 tähenduses.

II. PEATÜKK

KORRALDUS, KOHUSTUSED JA INTSIDENTIDE HALDAMINE

Artikkel 2

Komisjoni ülesanded

1. Komisjon rakendab keskse SIS II turvalisuse tagamiseks käesolevas otsuses nimetatud meetmeid ja kontrollib nende tõhusust.

2. Komisjon rakendab käesolevas otsuses nimetatud sideinfrastruktuuri turvalisuse tagamiseks ette nähtud meetmeid ja kontrollib nende tõhusust.

3. 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 käesoleva otsuse artikli 7 kohaselt;

b) keskse SIS II turvamenetluse rakendamise tõhususe kontrollimine;

c) sideinfrastruktuuri turvamenetluse rakendamise tõhususe kontrollimine;

d) määruse (EÜ) nr 1987/2006 artiklis 50 ja otsuse 2007/533/JSK artiklis 66 nimetatud turvalisusega seotud aruannete ettevalmistamisele kaasaaitamine;

e) määruse (EÜ) nr 1987/2006 artiklis 45 ja otsuse 2007/533/JSK artiklis 61 nimetatud Euroopa Andmekaitseinspektori kontrollide ja auditite kooskõlastamine ja abistamine ning komisjoni andmekaitseametnikule artikli 5 lõike 2 kohastest intsidentidest teatamine;

f) selle kontrollimine, et tööettevõtja, sealhulgas alltöövõtja, kes osaleb mis tahes moel keskse SIS II juhtimises, kohaldab käesolevat otsust ja turbepoliitikat nõuetekohaselt ja täielikult;

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

h) SIS II turvalisusega tegelevate riiklike kontaktpunktide nimekirja haldamine ja sellise nimekirja jagamine sideinfrastruktuuri kohaliku turvaametnikuga;

i) alapunktis h nimetatud nimekirja jagamine keskse SIS II kohaliku turvaametnikuga.

Artikkel 3

Keskse SIS II kohalik turvaametnik

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

2. Keskse SIS II kohalik turvaametnik tagab, et CS-SISi põhisüsteemis rakendatakse käesolevas otsuses nimetatud turvameetmeid ja järgitakse turvamenetlust. CS-SISi varusüsteemi puhul tagab keskse SIS II kohalik turvaametnik ka, et CS-SISi varusüsteemis rakendatakse käesolevas otsuses nimetatud turvameetmeid, välja arvatud artiklis 9 nimetatud meetmed, ja järgitakse nendega seotud turvamenetlust.

3. Keskse SIS II 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 SIS II kohalik turvaametnik täidab ülesandeid, mis tulenevad turvameetmetest, mida võetakse CS-SISi 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 SIS II 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 SIS II operatiivjuhtimises, 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 sideinfrastruktuuris toimunud intsidentide kohta, mis võivad mõjutada keskse SIS II 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 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 SIS II turvalisust ning mis võib SIS II-le 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. Turvaintsidentidele reageeritakse kooskõlas turbepoliitikaga kiirelt, tõhusalt ja nõuetekohaselt. Kehtestatakse kord, mida kohaldada pärast turvaintsidentide esinemist.

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

Artikkel 6

Intsidentide haldamine

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

2. Sellise intsidendi avastamise korral, mis mõjutab või võib mõjutada SIS II turvalisust, teatab 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 SIS II 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. 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. Turbepoliitikas nähakse ette tagasiside andmise kord, tagamaks, et turvaintsidentide liiki, nendele reageerimist ja nende tagajärgi käsitlev teave edastatakse süsteemi turvalisuse eest vastutavale ametnikule ja sideinfrastruktuuri kohalikule turvaametnikule siis, kui turvaintsident on lahendatud ja selle menetlemine lõpetatud.

5. Lõikeid 1–4 kohaldatakse *mutatis mutandis* keskses SIS II toimunud intsidentide suhtes. Sellisel juhul käsitletakse lõigetes 1–4 esitatud viiteid sideinfrastruktuuri kohalikule turvaametnikule viidetena keskse SIS II kohalikule turvaametnikule.

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 sideinfrastruktuuri 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 keskse SIS II kohaliku turvaametnikuga ja sideinfrastruktuuri kohaliku turvaametnikuga.

5. Lõikeid 1–4 kohaldatakse *mutatis mutandis* keskse SIS II turbepoliitika suhtes. Sellisel juhul käsitletakse lõigetes 1–4 esitatud viiteid sideinfrastruktuuri kohalikule turvaametnikule viidetena keskse SIS II kohalikule turvaametnikule.

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, SIS II käsitlevad kavad ja muud dokumendid ning SIS II 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 3 alapunktis h nimetatud nimekirja kontaktpunkti, kes kontrollib käesoleva artikli rakendamist CS-SISi 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 sideinfrastruktuuri kõik olulised varad, et neid oleks vastavalt nende olulisusele võimalik kaitsta. Peetakse ajakohastatud registrit asjaomastest infotehnoloogilistest seadmetest.

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

6. Lõikeid 1–5 kohaldatakse *mutatis mutandis* keskse SIS II suhtes. Sellisel juhul käsitletakse viiteid sideinfrastruktuurile viidetena kesksele SIS II-le.

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 SIS II riist- ja tarkvarale. Asjakohase juurdepääsu volituste määramist ja kasutamist (salasõna ja muud asjaomased vahendid) kontrollitakse turbepoliitikas ettenähtud ametliku halduskorra abil.

2. Juurdepääs SIS II riist- ja tarkvarale CS-SISi süsteemis

i) on ainult volitatud töötajatel;

ii) antakse vaid juhul, kui on võimalik tuvastada õiguspärane eesmärk kooskõlas määruse (EÜ) nr 1987/2006 artikliga 45 ja otsuse 2007/533/JSK artikliga 61 või määruse (EÜ) nr 1987/2006 artikli 50 lõikega 2 ja otsuse 2007/533/JSK artikli 66 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. CS-SISi süsteemis kasutatakse ainult keskse SIS II 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 SIS II tarkvarale juurdepääsuks CS-SISi süsteemi kaudu, kontrollib keskse SIS II 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 SIS II süsteemi või SIS II 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 SIS II, sealhulgas süsteemi kaudu edastatavate andmete turvalisus.

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

3. Lisaks SIS II 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 1987/2006 artikli 18 lõikes 1 ja otsuse 2007/533/JSK artikli 18 lõikes 1 nimetatud teave, mis käsitleb iga juurdepääsu CS-SISis hoitavatele isikuandmetele ja nende andmete igasugust vahetamist CS-SISi raames, säilitatakse turvaliselt ning sellele võimaldatakse CS-SIS põhi- ja varusüsteemi asukohas juurdepääs maksimaalselt määruse (EÜ) nr 1987/2006 artikli 18 lõikes 3 ja otsuse 2007/533/JSK artikli 18 lõikes 3 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 keskkele SIS II-le.

2. Turbepoliitikas nähakse ette nende isikute ülesanded ja kohustused, kellel on luba juurdepääsuks sideinfrastruktuurile.

3. 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.

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

Artikkel 21

Teave personali kohta

1. Kogu personali ja 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 töö muutuse 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 nõukogu kooskõlas määruse (EÜ) nr 1987/2006 artikli 55 lõikega 2 ja otsuse 2007/533/JSK artikli 71 lõikega 2.

2. Artikli 1 lõige 1, artikli 2 lõige 1, artikli 2 lõike 3 punktid b, d, f ja i, artikkel 3, artikli 6 lõige 5, artikli 7 lõige 5, artikli 9 lõige 6, artikli 10 lõige 6, artikli 13 lõiked 2 ja 3, artiklid 15 ja 18 ning artikli 20 lõige 1 kaotavad kehtivuse, kui korraldusasutus asub täitma oma ülesandeid.

Brüssel, 4. mai 2010

Komisjoni nimel

president

José Manuel BARROSO