SKLEP KOMISIJE

z dne 4. maja 2010

o varnostnem načrtu za centralni SIS II in komunikacijsko infrastrukturo

(2010/261/EU)

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe (ES) št. 1987/2006 Evropskega parlamenta in Sveta z dne 20. decembra 2006 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II) [1] ter zlasti člena 16 Uredbe,

ob upoštevanju Sklepa Sveta 2007/533/PNZ z dne 12. junija 2007 o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II) [2] ter zlasti člena 16 Sklepa,

ob upoštevanju naslednjega:

(1) Člen 16 Uredbe (ES) št. 1987/2006 in člen 16 Sklepa 2007/533/PNZ določata, da upravljavski organ sprejme potrebne ukrepe, vključno z varnostnim načrtom, v zvezi s centralnim SIS II, Komisija pa to stori v zvezi s komunikacijsko infrastrukturo.

(2) Člen 15(4) Uredbe (ES) št. 1987/2006 in člen 15(4) Sklepa 2007/533/PNZ določata, da je v prehodnem obdobju, dokler upravljavski organ ne prevzame svojih nalog, Komisija odgovorna za operativno upravljanje centralnega SIS II.

(3) Ker upravljavski organ še ni bil ustanovljen, je treba varnostni načrt, ki ga bo sprejela Komisija, v prehodnem obdobju uporabiti tudi za centralni SIS II.

(4) Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta [3] se uporablja za obdelavo osebnih podatkov, ki jo izvaja Komisija v okviru svojih nalog operativnega upravljanja SIS II.

(5) Člen 15(7) Uredbe (ES) št. 1987/2006 in člen 15(7) Sklepa 2007/533/PNZ določata, da Komisija ob prenosu svojih pristojnosti v prehodnem obdobju, dokler upravljavski organ ne prevzame svojih nalog, zagotovi, da ta prenos ne vpliva škodljivo na noben veljavni nadzorni mehanizem po zakonodaji Unije, naj bo to mehanizem Sodišča, Računskega sodišča ali Evropskega nadzornika za varstvo podatkov.

(6) Ko upravljavski organ prevzame svoje naloge, mora oblikovati lasten varnostni načrt v zvezi s centralnim SIS II. Ko upravljavski organ prevzame svoje naloge, mora ta varnostni načrt prenehati veljati, kar zadeva centralni SIS II.

(7) Člen 4(3) Uredbe (ES) št. 1987/2006 in člen 4(3) Sklepa 2007/533/PNZ določata, da je glavni CS-SIS, ki zagotavlja tehnični nadzor in upravljanje, v Strasbourgu (Francija), varnostna kopija CS-SIS, ki lahko ob odpovedi delovanja glavnega CS-SIS zagotavlja vse njegove funkcije, pa je v kraju Sankt Johann im Pongau (Avstrija).

(8) V varnostnem načrtu je treba predvideti enega sistemskega varnostnega uradnika, ki opravlja naloge v zvezi z varnostjo centralnega SIS II in komunikacijske infrastrukture, ter dva lokalna varnostna uradnika, ki opravljata naloge v zvezi z varnostjo centralnega SIS II oziroma komunikacijske infrastrukture. Da se zagotovita učinkovito in takojšnje odzivanje na incidente v zvezi z varnostjo ter poročanje o njih, je treba določiti vloge varnostnih uradnikov.

(9) Oblikovati je treba varnostno politiko, v kateri so opisane vse tehnične in organizacijske podrobnosti v skladu z določbami tega sklepa.

(10) Določiti je treba ukrepe za zagotavljanje ustrezne ravni varnosti delovanja centralnega SIS II in komunikacijske infrastrukture –

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

SPREJELA NASLEDNJI SKLEP:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Vsebina

1. Ta sklep določa organizacijo varnosti in varnostne ukrepe (varnostni načrt) za zaščito centralnega SIS II in podatkov, ki se v njem obdelujejo, pred nevarnostmi za njihovo razpoložljivost, celovitost in zaupnost v smislu člena 16(1) Uredbe (ES) št. 1987/2006 in člena 16(1) Sklepa 2007/533/PNZ o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II) , in sicer v prehodnem obdobju, dokler upravljavski organ ne prevzame svojih nalog.

2. Ta sklep določa organizacijo varnosti in varnostne ukrepe (varnostni načrt) za zaščito komunikacijske infrastrukture pred nevarnostmi za njeno razpoložljivost, celovitost in zaupnost v smislu člena 16 Uredbe (ES) št. 1987/2006 in člena 16 Sklepa 2007/533/PNZ o vzpostavitvi, delovanju in uporabi druge generacije schengenskega informacijskega sistema (SIS II).

POGLAVJE II

ORGANIZACIJA, NALOGE IN OBVLADOVANJE INCIDENTOV

Člen 2

Naloge Komisije

1. Komisija izvaja varnostne ukrepe za centralni SIS II in komunikacijsko infrastrukturo iz tega sklepa ter spremlja njihovo učinkovitost.

2. Komisija izvaja varnostne ukrepe za komunikacijsko infrastrukturo iz tega sklepa in spremlja njihovo učinkovitost.

3. Komisija izmed svojih uradnikov določi sistemskega varnostnega uradnika. Sistemskega varnostnega uradnika imenuje generalni direktor Generalnega direktorata Komisije za pravosodje, svobodo in varnost. Naloge sistemskega varnostnega uradnika vključujejo zlasti:

(a) pripravo varnostne politike, kot je opisano v členu 7 tega sklepa;

(b) spremljanje učinkovitosti izvajanja varnostnih postopkov centralnega SIS II;

(c) spremljanje učinkovitosti izvajanja varnostnih postopkov komunikacijske infrastrukture;

(d) prispevanje k pripravi poročil o varnosti iz člena 50 Uredbe (ES) št. 1987/2006 in člena 66 Sklepa 2007/533/PNZ;

(e) usklajevanje in pomoč pri preverjanjih in revizijah, ki jih po členu 45 Uredbe (ES) št. 1987/2006 in členu 61 Sklepa 2007/533/PNZ izvaja Evropski nadzornik za varstvo podatkov, ter sporočanje incidentov v smislu člena 5(2) pooblaščencu Komisije za varstvo podatkov;

(f) nadzorovanje, da vsi izvajalci in podizvajalci, ki so kakor koli vključeni v upravljanje centralnega SIS II, ustrezno in v celoti upoštevajo ta sklep in varnostno politiko;

(g) nadzorovanje, da vsi izvajalci in podizvajalci, ki so kakor koli vključeni v upravljanje komunikacijske infrastrukture, ustrezno in v celoti upoštevajo ta sklep in varnostno politiko;

(h) urejanje seznama enotnih nacionalnih kontaktnih točk za varnost SIS II in omogočanje souporabe tega seznama lokalnemu varnostnemu uradniku za komunikacijsko infrastrukturo;

(i) omogočanje souporabe seznama iz točke (h) lokalnemu varnostnemu uradniku za centralni SIS II.

Člen 3

Lokalni varnostni uradnik za centralni SIS II

1. Brez poseganja v člen 8 Komisija izmed svojih uradnikov imenuje lokalnega varnostnega uradnika za centralni SIS II. Navzkrižja interesov med dolžnostjo lokalnega varnostnega uradnika in katero koli drugo uradno dolžnostjo se preprečijo. Lokalnega varnostnega uradnika za centralni SIS II določi generalni direktor Generalnega direktorata Komisije za pravosodje, svobodo in varnost.

2. Lokalni varnostni uradnik za centralni SIS II zagotavlja, da se v glavnem CS-SIS izvajajo varnostni ukrepi iz tega sklepa in upoštevajo varnostni postopki. V zvezi z varnostno kopijo CS-SIS lokalni varnostni uradnik za centralni SIS II zagotavlja, da se varnostni ukrepi iz tega sklepa izvajajo, razen tistih iz člena 9, in da se upoštevajo s tem povezani varnostni postopki.

3. Lokalni varnostni uradnik za centralni SIS II lahko katero koli svojo nalogo dodeli podrejenemu osebju. Navzkrižja interesov med dolžnostjo izpolnjevanja teh nalog in katero koli drugo uradno dolžnostjo se preprečijo. Lokalnega varnostnega uradnika ali njegovega dežurnega podrejenega je mogoče kadar koli doseči na enotni kontaktni telefonski številki ali naslovu.

4. Lokalni varnostni uradnik za centralni SIS II opravlja naloge, ki so posledica varnostnih ukrepov, ki jih je treba sprejeti na lokacijah glavnega centralnega CS-SIS in varnostne kopije CS-SIS, in sicer v okviru omejitev iz odstavka 1, še zlasti pa:

(a) lokalne operativne varnostne naloge, vključno z revizijo požarnega zidu, rednimi preskusi in revizijami varnosti ter poročanjem o njej;

(b) spremljanje učinkovitosti načrta neprekinjenega delovanja in zagotavljanje rednega izvajanja vaj;

(c) zavarovanje dokazov o vseh incidentih v centralnem SIS II, ki bi lahko vplivali na varnost centralnega SIS II ali komunikacijske infrastrukture, in poročanje sistemskemu varnostnemu uradniku o takih incidentih;

(d) obveščanje sistemskega varnostnega uradnika o morebitni potrebi po spremembi varnostne politike;

(e) nadzorovanje, da vsi izvajalci in podizvajalci, ki so kakor koli vključeni v operativno upravljanje centralnega SIS II, upoštevajo ta sklep in varnostno politiko;

(f) zagotavljanje, da so zaposleni seznanjeni s svojimi obveznostmi, in nadzorovanje izvajanja varnostne politike;

(g) spremljanje razvoja IT-varnosti in zagotavljanje ustreznega usposabljanja zaposlenih;

(h) pripravljanje osnovnih informacij in možnosti za oblikovanje, posodabljanje in revidiranje varnostne politike v skladu s členom 7.

Člen 4

Lokalni varnostni uradnik za komunikacijsko infrastrukturo

1. Brez poseganja v člen 8 Komisija izmed svojih uradnikov imenuje lokalnega varnostnega uradnika za komunikacijsko infrastrukturo. Navzkrižja interesov med dolžnostjo lokalnega varnostnega uradnika in katero koli drugo uradno dolžnostjo se preprečijo. Lokalnega varnostnega uradnika za komunikacijsko infrastrukturo določi generalni direktor Generalnega direktorata Komisije za pravosodje, svobodo in varnost.

2. Lokalni varnostni uradnik za komunikacijsko infrastrukturo nadzoruje delovanje komunikacijske infrastrukture ter zagotavlja izvajanje varnostnih ukrepov in upoštevanje varnostnih postopkov.

3. Lokalni varnostni uradnik za komunikacijsko infrastrukturo lahko katero koli svojo nalogo dodeli podrejenemu osebju. Navzkrižja interesov med dolžnostjo izpolnjevanja teh nalog in katero koli drugo uradno dolžnostjo se preprečijo. Lokalnega varnostnega uradnika ali njegovega dežurnega podrejenega je mogoče kadar koli doseči na enotni kontaktni telefonski številki ali naslovu.

4. Lokalni varnostni uradnik za komunikacijsko infrastrukturo opravlja naloge, ki izhajajo iz varnostnih ukrepov v zvezi s komunikacijsko infrastrukturo, in zlasti:

(a) vse operativne varnostne naloge v zvezi s komunikacijsko infrastrukturo, kot so revizija požarnega zidu, redni preskusi in revizije varnosti ter poročanje o njej;

(b) spremljanje učinkovitosti načrta neprekinjenega delovanja in zagotavljanje rednega izvajanja vaj;

(c) zavarovanje dokazov o vseh incidentih v komunikacijski infrastrukturi, ki bi lahko vplivali na varnost centralnega SIS II ali komunikacijske infrastrukture, in poročanje sistemskemu varnostnemu uradniku o takih incidentih;

(d) obveščanje sistemskega varnostnega uradnika o morebitni potrebi po spremembi varnostne politike;

(e) nadzorovanje, da vsi izvajalci in podizvajalci, ki so kakor koli vključeni v upravljanje komunikacijske infrastrukture, upoštevajo ta sklep in varnostno politiko;

(f) zagotavljanje, da so zaposleni seznanjeni s svojimi obveznostmi, in nadzorovanje izvajanja varnostne politike;

(g) spremljanje razvoja IT-varnosti in zagotavljanje ustreznega usposabljanja zaposlenih;

(h) pripravljanje osnovnih informacij in možnosti za oblikovanje, posodabljanje in revidiranje varnostne politike v skladu s členom 7.

Člen 5

Incidenti v zvezi z varnostjo

1. Za incident v zvezi z varnostjo se šteje vsak dogodek, ki vpliva ali bi lahko vplival na varnost SIS II in bi lahko temu sistemu povzročil škodo ali izgubo, zlasti v primeru morebitnega dostopa do podatkov ali kadar so bile ali bi lahko bile ogrožene razpoložljivost, celovitost in zaupnost podatkov.

2. Incidenti v zvezi z varnostjo se obvladujejo tako, da se zagotovi hitro, učinkovito in ustrezno odzivanje v skladu z varnostno politiko. Določijo se postopki za odpravo posledic incidenta.

3. Informacije o incidentu v zvezi z varnostjo, ki vpliva ali bi lahko vplival na delovanje SIS II v državi članici ali na razpoložljivost, celovitost in zaupnost podatkov, ki jih je vnesla ali poslala država članica, se sporočijo zadevni državi članici. Incidenti v zvezi z varnostjo se sporočijo pooblaščencu Komisije za varstvo podatkov.

Člen 6

Obvladovanje incidentov

1. Če zaposleni in izvajalci, vključeni v razvoj, upravljanje ali delovanje SIS II opazijo kakršne koli varnostne pomanjkljivosti v komunikacijski infrastrukturi ali sumijo, da te obstajajo, jih morajo evidentirati in o njih poročati sistemskemu varnostnemu uradniku ali lokalnemu varnostnemu uradniku za komunikacijsko infrastrukturo.

2. Če se ugotovi kakršen koli incident, ki vpliva ali bi lahko vplival na varnost SIS II, lokalni varnostni uradnik za komunikacijsko infrastrukturo čim prej pisno ali, če je zadeva izredno nujna, po drugih komunikacijskih poteh o tem obvesti sistemskega varnostnega uradnika in po potrebi enotno nacionalno kontaktno točko za varnost SIS II, če v zadevni državi članici taka kontaktna točka obstaja. Poročilo vsebuje opis incidenta v zvezi z varnostjo, raven tveganja, morebitne posledice in ukrepe, ki so bili ali bi morali biti sprejeti za zmanjšanje tveganja.

3. Lokalni varnostni uradnik za komunikacijsko infrastrukturo nemudoma zavaruje vse dokaze o incidentu v zvezi z varnostjo. Ti dokazi se dajo na voljo sistemskemu varnostnemu uradniku na njegovo zahtevo, kolikor je mogoče na podlagi veljavnih določb o varstvu podatkov.

4. V varnostni politiki se določijo postopki pridobivanja povratnih informacij, da se zagotovi sporočanje informacij o vrsti, obvladovanju in posledicah incidenta v zvezi z varnostjo sistemskemu varnostnemu uradniku in lokalnemu varnostnemu uradniku za komunikacijsko infrastrukturo, ko se incident obvlada in je končan.

5. Odstavki 1 do 4 se smiselno uporabljajo za incidente v centralnem SIS II. Tako se vsako sklicevanje na lokalnega varnostnega uradnika za komunikacijsko infrastrukturo v odstavkih 1 do 4 razume kot sklicevanje na lokalnega varnostnega uradnika za centralni SIS II.

POGLAVJE III

VARNOSTNI UKREPI

Člen 7

Varnostna politika

1. Generalni direktor Generalnega direktorata za pravosodje, svobodo in varnost oblikuje, posodablja in redno revidira zavezujočo varnostno politiko v skladu s tem sklepom. V varnostni politiki so določeni podrobni postopki in ukrepi za zaščito pred nevarnostmi za razpoložljivost, celovitost in zaupnost komunikacijske infrastrukture, vključno z načrtovanjem ravnanja v izrednih razmerah, da se zagotovi ustrezna raven varnosti, predpisana s tem sklepom. Varnostna politika je usklajena s tem sklepom.

2. Varnostna politika temelji na oceni tveganja. Ukrepi, opisani v varnostni politiki, so sorazmerni z opredeljenimi tveganji.

3. Ocena tveganja in varnostna politika se po potrebi posodabljata zaradi tehnoloških sprememb, odkritja novih nevarnosti ali kakršnih koli drugih okoliščin. Varnostna politika se v vsakem primeru revidira letno, s čimer se zagotovi, da vedno ustreza najnovejši oceni tveganja ali kateri koli drugi novi tehnološki spremembi, novoodkriti nevarnosti ali drugi pomembni okoliščini.

4. Varnostno politiko pripravi sistemski varnostni uradnik ob usklajevanju z lokalnim varnostnim uradnikom za centralni SIS II in lokalnim varnostnim uradnikom za komunikacijsko infrastrukturo.

5. Odstavki 1 do 4 se smiselno uporabljajo za varnostno politiko centralnega SIS II. Tako se vsako sklicevanje na lokalnega varnostnega uradnika za komunikacijsko infrastrukturo v odstavkih 1 do 4 razume kot sklicevanje na lokalnega varnostnega uradnika za centralni SIS II.

Člen 8

Izvajanje varnostnih ukrepov

1. Izpolnjevanje nalog in zahtev, določenih v tem sklepu in varnostni politiki, vključno z nalogo imenovanja lokalnega varnostnega uradnika, se lahko odda zunanjim izvajalcem ali poveri zasebnim ali javnim organizacijam.

2. V tem primeru Komisija s pravno zavezujočim dogovorom zagotovi, da se zahteve, določene v tem sklepu in varnostni politiki, v celoti upoštevajo. Če se naloga imenovanja lokalnega varnostnega uradnika delegira ali se njeno izvajanje odda zunanjim izvajalcem, Komisija s pravno zavezujočim dogovorom zagotovi, da se bo izvajalec naloge s Komisijo posvetoval o osebi, imenovani za lokalnega varnostnega uradnika.

Člen 9

Nadzor dostopa do opreme

1. Za zavarovanje krajev, kjer je nameščena oprema za obdelavo podatkov, se postavijo varnostna območja z ustreznimi zaporami in vstopnimi kontrolami.

2. Znotraj varnostnih območij se določijo varovana območja, da se zaščitijo fizične komponente (sredstva), vključno s strojno opremo, nosilci podatkov in konzolami, načrti in drugimi dokumenti o SIS II ter pisarnami in drugimi delovnimi mesti osebja, vključenega v delovanje SIS II. Ta varovana območja se zavarujejo z ustreznimi vstopnimi kontrolami, da se zagotovi, da lahko do varovanih območij dostopa samo pooblaščeno osebje. Za delo v varovanih območjih veljajo podrobna varnostna pravila, določena v varnostni politiki.

3. Fizično varovanje se predvidi in namesti za pisarne, sobe in opremo. Dostopne točke, kot so območja za dostavo in natovarjanje, ter druge točke, kjer lahko v prostore vstopajo nepooblaščene osebe, se nadzorujejo in so po možnosti ločene od območij z opremo za obdelavo podatkov, da se prepreči nepooblaščen dostop.

4. Oblikuje in uporablja se tveganju sorazmerna fizična zaščita varnostnih območij pred naravnimi nesrečami in nesrečami, ki jih povzroči človek.

5. Oprema se zaščiti pred fizičnimi in okoljskimi nevarnostmi ter možnostmi za nepooblaščeni dostop.

6. Če ima Komisija take informacije na voljo, doda seznamu iz člena 2(3)(h) enotno kontaktno točko za nadzor izvajanja določb tega člena v prostorih varnostne kopije CS-SIS.

Člen 10

Nadzor nosilcev podatkov in sredstev

1. Odstranljivi nosilci podatkov, ki vsebujejo podatke, se zaščitijo pred nepooblaščenim dostopom, zlorabo ali poškodovanjem, njihova berljivost pa se zagotavlja skozi celotno življenjsko dobo podatkov.

2. Ko nosilci podatkov niso več potrebni, se zavržejo varno v skladu s podrobnimi postopki, ki se določijo v varnostni politiki.

3. Z evidencami se zagotavljajo informacije o lokacijah, kjer so podatki shranjeni, veljavnih obdobjih shranjevanja in dovoljenjih za dostop.

4. Vsa pomembna sredstva komunikacijske infrastrukture se določijo, da se jih zaščiti glede na njihovo pomembnost. Vodi se register pomembne opreme IT, ki se stalno posodablja.

5. Na voljo je dokumentacija o komunikacijski infrastrukturi, ki se stalno posodablja. To dokumentacijo je treba zaščititi pred nepooblaščenim dostopom.

6. Odstavki 1 do 5 se smiselno uporabljajo za centralni SIS II. Tako se vsako sklicevanje na komunikacijsko infrastrukturo razume kot sklicevanje na centralni SIS II.

Člen 11

Nadzor shranjevanja

1. Sprejmejo se ustrezni ukrepi, da se zagotovi ustrezno shranjevanje informacij in prepreči nepooblaščen dostop do njih.

2. Vsi elementi opreme, ki vsebujejo nosilce za shranjevanje podatkov, se varno uničijo ali pa se pred zavrženjem pregledajo, da se zagotovi, da so bili vsi občutljivi podatki odstranjeni ali v celoti prepisani z drugimi podatki.

Člen 12

Nadzor gesel

1. Vsa gesla se hranijo na varnem in obravnavajo zaupno. Če se pojavi sum, da je bilo geslo razkrito, je treba to geslo nemudoma zamenjati ali onemogočiti uporabniški račun. Uporabljajo se enolične in individualne uporabniške identitete.

2. V varnostni politiki se opredelijo postopki za prijavljanje in odjavljanje, da se prepreči vsak nepooblaščen dostop.

Člen 13

Nadzor dostopa

1. Z varnostno politiko se določi postopek za uradno registracijo in preklic registracije zaposlenih, s katerim se za namene operativnega upravljanja odobri ali prekliče dostop do strojne in programske opreme SIS II. Dodeljevanje in uporaba ustreznih poverilnic za dostop (gesel ali drugih ustreznih sredstev) se nadzorujeta z uradnim upravljavskim postopkom, kot je določen v varnostni politiki.

2. Dostop do strojne in programske opreme SIS II pri CS-SIS:

(i) je dovoljen samo pooblaščenim osebam;

(ii) je omejen na primere, ko je mogoče ugotoviti legitimen interes v skladu s členom 45 Uredbe (ES) št. 1987/2006 in členom 61 Sklepa 2007/533/PNZ ali s členom 50(2) Uredbe (ES) št. 1987/2006 in členom 66(2) Sklepa 2007/533/PNZ;

(iii) ne traja dlje in ni obsežnejši, kot je potrebno za namen dostopa, in

(iv) se omogoča samo v skladu s politiko nadzora dostopa, ki se določi v varnostni politiki.

3. Pri CS-SIS se uporabljajo samo konzole in programska oprema, ki jih je odobril lokalni varnostni uradnik za centralni SIS II. Uporaba sistemskih pripomočkov, ki bi lahko obšli sistemski in programski nadzor, se omeji in nadzoruje. Uvedejo se postopki za nadzor nameščanja programske opreme.

Člen 14

Nadzor sporočanja

Komunikacijska infrastruktura se nadzoruje, da se zagotovijo razpoložljivost, celovitost in zaupnost izmenjave podatkov. Za zaščito podatkov, ki se prenašajo po komunikacijski infrastrukturi, se uporabljajo šifrirna sredstva.

Člen 15

Nadzor vnosa

Račune oseb, ki jim je bil odobren dostop do programske opreme SIS II prek CS-SIS, nadzoruje lokalni varnostni uradnik za centralni SIS II. Uporaba teh računov, vključno s časom in uporabniško identiteto, se evidentira.

Člen 16

Nadzor prenosa

1. V varnostni politiki se določijo ustrezni ukrepi, da se preprečijo nepooblaščeno branje, kopiranje, spreminjanje ali brisanje osebnih podatkov med njihovim prenosom v SIS II ali iz njega ali med prenosom nosilcev podatkov. Varnostna politika vsebuje določbe o dovoljenih oblikah pošiljanja ali prenosa ter o postopkih glede odgovornosti za prenos predmetov in njihov prihod v namembni kraj. Nosilec podatkov ne vsebuje nobenih drugih podatkov, razen tistih, ki jih je treba poslati.

2. Storitve, ki jih zagotavljajo tretje osebe in vključujejo dostop, obdelavo in sporočanje podatkov ali upravljanje opreme za obdelavo podatkov ali dodajanje proizvodov ali storitev opremi za obdelavo podatkov, imajo nameščene ustrezne varnostne kontrole.

Člen 17

Varnost komunikacijske infrastrukture

1. Komunikacijska infrastruktura se ustrezno upravlja in nadzoruje, da se zaščiti pred nevarnostmi ter da se zagotovi varnost komunikacijske infrastrukture in centralnega SIS II, vključno s podatki, ki se izmenjujejo skozi njiju.

2. Varnostni elementi, ravni storitev in zahteve upravljanja za vse omrežne storitve se opredelijo v dogovoru o zagotavljanju omrežnih storitev s ponudnikom storitev.

3. Poleg dostopnih točk SIS II se zaščitijo tudi vse dodatne storitve, ki jih uporablja komunikacijska infrastruktura. Ustrezni ukrepi se določijo v varnostni politiki.

Člen 18

Spremljanje

1. V prostorih glavnega CS-SIS in varnostne kopije CS-SIS se za najdaljše obdobje iz člena 18(3) Uredbe (ES) št. 1987/2006 in člena 18(3) Sklepa 2007/533/PNZ varno hranijo in so iz teh prostorov dostopne evidence s podatki iz člena 18(1) Uredbe (ES) št. 1987/2006 in člena 18(1) Sklepa 2007/533/PNZ, ki se nanašajo na vsak dostop do podatkov v CS-SIS in na vsak postopek njihove obdelave.

2. V varnostni politiki se določijo postopki za spremljanje uporabe ali okvar opreme za obdelavo podatkov, rezultati dejavnosti spremljanja pa se redno pregledujejo. Po potrebi se ustrezno ukrepa.

3. Sredstva za vodenje evidenc in evidence se zaščitijo pred nedovoljenimi posegi in nepooblaščenim dostopom, da se izpolnijo zahteve glede zbiranja podatkov in shranijo dokazi za obdobje shranjevanja.

Člen 19

Šifrirni ukrepi

Za zaščito informacij se po potrebi uporabljajo šifrirni ukrepi. Uporabo ter namene in pogoje uporabe mora vnaprej odobriti sistemski varnostni uradnik.

POGLAVJE IV

VARNOST ČLOVEŠKIH VIROV

Člen 20

Profili osebja

1. V varnostni politiki se določijo naloge in pristojnosti oseb, ki jim je bil odobren dostop do centralnega SIS II.

2. V varnostni politiki se določijo naloge in pristojnosti oseb, ki jim je bil odobren dostop do komunikacijske infrastrukture.

3. Varnostne vloge in odgovornosti osebja Komisije, izvajalcev in zaposlenih, vključenih v operativno upravljanje, se opredelijo, zapišejo in sporočijo zadevnim osebam. Za osebje Komisije so te vloge in odgovornosti navedene v opisu dela in nalog ter ciljih; za izvajalce so te vloge in odgovornosti navedene v pogodbah ali dogovorih o ravni storitev.

4. Z vsemi osebami, za katere ne veljajo pravila javnih služb Evropske unije ali držav članic, se sklenejo dogovori o zaupnosti in tajnosti. Zaposleni, ki morajo delati s podatki SIS II, imajo potrebno dovoljenje ali potrdilo v skladu s podrobnimi postopki, ki se določijo v varnostni politiki.

Člen 21

Informacije osebja

1. Vsem zaposlenim in izvajalcem se zagotovi ustrezno usposabljanje o varnostni ozaveščenosti, pravnih zahtevah, politikah in postopkih, in sicer v obsegu, ki ga zahtevajo njihove dolžnosti.

2. V varnostni politiki se za osebje in izvajalce, ki jim preneha zaposlitev ali se jim izteče pogodba, določijo odgovornosti, povezane z menjavo ali prenehanjem zaposlitve, ter postopki za upravljanje vračila sredstev in odvzema pravic dostopa.

POGLAVJE V

KONČNE DOLOČBE

Člen 22

Veljavnost

1. Ta sklep začne veljati z datumom, ki ga določi Svet v skladu s členom 55(2) Uredbe (ES) št. 1987/2006 in členom 71(2) Sklepa 2007/533/PNZ.

2. Člen 1(1), člen 2(1) ter 2(3)(b), (d), (f) in (i), člen 3, členi 6(5), 7(5), 9(6), 10(6), člen 13(2) in (3), člena 15 in 18 ter člen 20(1) prenehajo veljati, ko upravljavski organ prevzame svoje naloge.

V Bruslju, 4. maja 2010

Za Komisijo

Predsednik

José Manuel BARROSO