NORTH ATLANTIC COUNCIL

CONSEIL DE L'ATLANTIQUE NORD

25. november 2020

DOKUMENT
AC/35-D/2000-REV8

JULGEOLEKUKOMITEE

PERSONALIJULGEOLEKU DIREKTIIV
Eesistuja kohusetäitja märkus

Käesoleva dokumendi lisas 1 avaldatakse kaheksas redaktsioon normdokumenti CM(2002)49-REV1 „Turvalisus Põhja-Atlandi lepingu organisatsioonis“ täiendavast personalijulgeoleku direktiivist. Redaktsioon on olemuselt siduv ja kohustuslik. Käesolev dokument asendab dokumendi AC/35-D/2000-REV7, mis kuulub hävitamisele.

Käesolev redaktsioon kajastab NATO Security Policy tervikliku läbivaatuse (AC/35-N(2015)0025-AS1, vastu võetud 21. detsembril 2015) tulemusi.

Käesoleva normdokumendi on heaks kiitnud julgeolekukomitee (AC/35-N(2020)0004-AS1, vastu võetud 4. novembril 2020) ning dokumendile rakendatakse korralist ülevaatamist.

(allkiri) Marco Criscuolo

Lisasid: 1

nõunik: M. Rožaj, NOS (sisetel. 4084)

algteksti keel: inglise

NHQD207444

Lisa 1
AC/35-D/2000-REV8

PERSONALIJULGEOLEKU DIREKTIIV
SISUKORD

Käesoleva direktiivi järgnevates liidetes käsitletakse menetluslikke ja korralduslikke üksikasju ning näidisdokumente:
a) LIIDE 1 – Taotlus juurdepääsuõiguse kinnituse saamiseks
b) LIIDE 2 – Kinnitus isiku juurdepääsuõiguse kohta

SISSEJUHATUS

1. Julgeolekukomitee (AC/35) avaldab käesoleva personalijulgeoleku direktiivi NATO Security Policy (dokument C-M(2002)49) lisa C täiendusena. Käesolev direktiiv sisaldab kohustuslikke sätteid ja samuti nimetatud sätteid selgitavat teavet. Direktiiv käsitleb järgnevaid küsimusi:

a) juurdepääsuload (PSC);

b) personalijulgeolekuga seotud kohustused;

c) isiku nõuetelevastavuse hindamine PSC andmiseks;

d) salastatustasemega NATO CONFIDENTIAL (NC), NATO SECRET (NS) ja COSMIC TOP SECRET (CTS) teabele juurdepääsuloa andmisega seotud julgeolekukontrolli nõuded;

e) PSC kehtivuse pikendamise nõuded ja kord;

f) PSC-d omava isiku usaldamise vastu rääkiva teabe käsitlemise reeglid ja kord;

g) PSC-de arvestuse pidamine ning isikul nõutava PSC olemasolu kinnitamise võimalused;

h) järelkontrolli meetmed ning julgeolekukoolitus ja -teadlikkus;

i) juurdepääs NATO salastatud teabele erandjuhtudel ning

j) NATO liikmesriikide tsiviil- või sõjalistes organites töötavate NATOsse mittekuuluvate riikide kodanike juurdepääs NATO salastatud teabele.

JUURDEPÄÄSULUBA (PSC)

2. Vastavalt NATO Security Policy nõuetele tuleb kokkulepitud tasemel tagada NC ja kõrgema salastatustasemega NATO teabele juurdepääsu omavate või oma töökohustustest või -ülesannetest tulenevalt juurdepääsu saada võivate isikute lojaalsus, usaldusväärsus ja -kindlus. Selleks nõutakse, et isikul, kes vajab või võib oma töökohustustest tulenevalt saada juurdepääsu NC ja kõrgema salastatustasemega NATO teabele, oleks nõutava taseme PSC, mis kehtib seni, kuni isikule on juurdepääs lubatud. Lisaks peab:

a) isikul olema teadmisvajadus;

b) isikule olema tutvustatud tema NATO salastatud teabe kaitsega seotud kohustusi ning

c) isik olema kinnitanud oma kohustusi kirjalikult või muul samaväärsel salgamist mittevõimaldaval viisil.

3. PSC antakse pärast kõigile NATO Security Policy-s sätestatud nõuetele vastava julgeolekukontrolli läbiviimist, mis hõlmab asjaomase riigi julgeoleku volitatud esindaja (inglise keeles *National Security Authority (NSA))* või volitatud julgeolekuasutuse (inglise keeles *Designated Security Authority (DSA)*) või muu pädeva julgeolekuasutuse kinnitust selle kohta, et isikule võib lubada juurdepääsu NATO salastatud teabele.

4. Võib esineda olukordi, kus mõnda ülalpool esitatud nõuetest ei saa täita. Sellisel juhul saab kohaldada NATO salastatud teabele juurdepääsu erandjuhtudel andmist käsitlevat korda (vastavalt punktidele 40–48).

5. NATO Security Policy kohaselt ei ole PSC nõutav juurdepääsuks teabele salastatustasemega NATO RESTRICTED (NR). Isikutele, kes vajavad juurdepääsu üksnes teabele salastatustasemega NR, tutvustatakse nende julgeolekukohustusi ning neil peab olema teadmisvajadus. Isikud peavad salgamist mittevõimaldaval viisil olema liikmesriigi õigusaktide kohaselt andnud kinnituse selle kohta, et on teadlikud oma julgeolekukohustustest.

PSC andmine kõrgematele riigiametnikele

6. Kõrgemate riigiametnike (inglise keeles *Senior Governmental Officials (SGO)*), nt riigipead ja valitsusjuhid, ministrid, parlamendiliikmed, kohtunikud) juurdepääs NATO salastatud teabele määratakse kindlaks liikmesriigi õigusaktide kohaselt; SGO-le tutvustatakse tema julgeolekukohustusi ning tal peab olema teadmisvajadus. Kui tekib vajadus otsustada, kas PSC-ta SGO-le saab võimaldada juurdepääsu NATO salastatud teabele, võib selleks konsulteerida SGO osas pädevust omava NSA/DSA või muu julgeolekuasutusega[1].

PSC andmine lepinglase töötajale, kes teostab töid või osutab teenust NATO tsiviil- või sõjalisele organile

7. PSC andmist NATO asutustes töid teostavale lepinglase töötajale, kelle puhul on nõutav PSC, või nimetatud töötaja PSC olemasolu kinnitamist käsitletakse salastatud projekte ja tööstusjulgeolekut käsitlevas direktiivis (AC/35-D/2003).

PSC olemasolu kinnitamine

8. Olukorras, kus isik osaleb üritusel, mis nõuab juurdepääsu NATO salastatud teabele NC ja kõrgemal salastatustasemel (nt konverents, koosolek, kursus, seminar), on nõutav kinnituse esitamine isiku PSC olemasolu kohta.

9. Kinnitus isiku PSC olemasolu kohta edastatakse läbi ametlike kanalite (nt NSA/DSA poolt NATO tsiviil või sõjalisele organile), kinnituse kohaletoimetamine isiku enda poolt on lubatav üksnes erandjuhtudel. NATO liikmesriik ja NATO tsiviil- või sõjaline organ võib kinnitada isiku PSC olemasolu ühel järgnevatest viisidest:

a) PSC kinnitus, mille vorm on esitatud käesoleva lisa liites 2;
b) külastustaotlus (inglise keeles *Request for Visit (RfV)),* mille vorm on kinnitatud salastatud projekte ja tööstusjulgeolekut käsitlevas direktiivis (AC/35-D/2003);
c) erandkorras, kui isiku PSC kinnitus on ülesande täitmise seisukohast ülitähtis, – muul viisil vahetu teateedastusena NSA/DSA või muu pädeva julgeolekuasutuse poolt NATO sõjalise või tsiviilorgani julgeolekuüksusele.

10. Liikmesriikide PSC-toiminguid ja -nõudeid käsitlevas dokumendis (AC/35-D/1043) on esitatud pädevate julgeolekuasutuste nimistu (ja kontaktid), kel on õigus esitada kinnitus isiku NATO salastatud teabele NC ja kõrgemal salastatustasemel juurdepääsuloa kohta.

11. Kui isiku PSC tunnistatakse kehtetuks või peatatakse või seda muudetakse (nt muudetakse selle kehtivusaega või taset), teavitab vastutav NATO liikmesriik ja/või NATO tsiviil- või sõjaline organ kõiki isiku PSC kinnituse saanuid asjaomasest muudatusest.

[1] NSA/DSA poolt volitatud ja liikmesriikide PSC-toiminguid ja -nõudeid käsitlevas tugidokumendis (AC/35-D/1043) esitatud nimistusse kantud asutus.

NATOs töötava isiku PSC kinnitus

12. Kui isik võetakse tööle NATO tsiviil- või sõjalisse organisse või lähetatakse nimetatud organi juurde või määratakse NATO liikmesriigi poolt vastava riigi delegatsiooni/esindusse NATO juures, tuleb saada kinnitus isiku PSC olemasolu kohta. Kinnitus edastatakse ühel järgnevatest viisidest:

a) asjaomase NATO organi konkreetse päringu põhjal, kasutades PSC kinnituse päringu vormi (käesoleva lisa liide 1) või
b) vahetult NATO liikmesriigi NSA/DSA või muu pädeva julgeolekuasutuse poolt, kasutades PSC kinnituse vormi (liide 2).

13. Isiku suhtes pädevust omavalt NSA-lt/DSA-lt või muult julgeolekuasutuselt taotletakse isiku PSC jätkuva kehtivuse kohta kinnitust kui:

a) isik ei asu tööle NATO tsiviil- või sõjalises organis uue PSC väljastamisele järgneva 12 kuu jooksul;
b) isiku töö katkeb 12 kuuks ning vastava aja jooksul isik ei tööta NATO või NATO liikmesriigi tsiviil- või sõjalise organi ametikohal.

VASTUTUSALA

14. NSA/DSA või muu pädeva julgeolekuasutuse vastutusalasse kuulub:

a) oma kodanike[2] ja oma riigi õigusaktide kohaselt teiste tema vastutusalasse jäävate isikute suhtes, kes vajavad juurdepääsu NC või kõrgema salastatustasemega teabele, julgeolekukontrolli teostamine ning vastavalt käesolevas direktiivis esitatud põhimõtetele otsuse tegemine selle kohta, kas isikule tuleks juurdepääsuluba anda, selle andmisest keelduda või isikule antud juurdepääsuluba kehtetuks tunnistada;
b) julgeolekukontrolli teostamine isiku teadmisel ja nõusolekul – niivõrd, kuivõrd seda võimaldavad riigisisesed õigusaktid;
c) PSC kehtivuse pikendamine ja PSC olemasolu kinnitamine;
d) isiku PSC kinnituse saanud isikute teavitamine PSC kehtetuks tunnistamisest, peatamisest või muutmisest ning
e) koostöö tegemine teiste NSAde/DSAde ja muude pädevate julgeolekuasutustega nende poolt teostatava julgeolekukontrolli läbiviimisel.

15. NATO liikmesriigi ning NATO tsiviil- ja sõjalise organi juhi vastutusalasse kuulub:

a) PSC olemasolu nõudvate ametikohtade kindlaksmääramine;
b) oma vastutusalas NATO salastatud teabele juurdepääsu andmine, sealhulgas käesoleva direktiivi punktides 40–48 kirjeldatud olukordades;
c) käesolevas direktiivis sätestatud personalijulgeoleku standarditest kinnipidamise tagamine;
d) oma töötajate NATO salastatud teabele juurdepääsu andmise nõuetele vastavuse hindamine;

[2] Tööstusjulgeoleku valdkonnas (salastatud projekte ja tööstusjulgeolekut käsitlev direktiiv (AC/35-D/2003)) kehtib säte, mis lubab NSA-l/DSA-l või muul pädeval julgeolekuasutusel väljastada PSC teise NATO liikmesriigi kodanikule.

e) asjaomase NSA/DSA teavitamine, kui isikul ei ole enam vaja PSC-d ja/või juurdepääsu NATO salastatud teabele (liikmesriikide PSC-toiminguid ja -nõudeid käsitlevas tugidokumendis (AC/35-D/1043) esitatakse riikide nimistu, kes nõuavad nimetatud teavitust);
f) NSAde/DSAde või muude pädevate julgeolekuasutuste toetamine asjakohase teabe andmisega asutuse abistamiseks julgeolekukontrolli läbiviimisel ning
g) asjaomasele pädevatele julgeolekuasutusele PSC-d omava isikuga seotud tegelikust või võimalikust julgeolekuprobleemist teatamine vastavalt käesoleva direktiivi punktidele 31, 32 ja 38.

PSC vajadusega ametikohtade kindlaksmääramine

16. Konkreetse ametikoha, millel töötamine nõuab PSC olemasolu, kindlaksmääramiseks kaasab NATO liikmesriik ja NATO tsiviil- ja sõjaline organ ametikohta hõlmava asutuse juhtkonna esindajad, kes üldjuhul omavad parimat ettekujutust sellest, mis tasemel juurdepääsuluba sellel ametikohal vajatakse.
17. Asutuse juhtkonna vastutusalasse kuulub ka asutuse töötajatele nende tööülesannete täitmiseks vajaliku tasemega PSC olemasolu ning teadmisvajaduse nõude rakendamise tagamine. Isiku PSC korralisel kehtivuse pikendamisel või ametikohta täitva isiku vahetumisel on asjaomase juhi ülesanne hinnata, kas ametikohal on jätkuvalt vajalik senise tasemega PSC omamine.

ISIKU NÕUETELE VASTAVUSE HINDAMINE JUURDEPÄÄSULOA ANDMISEKS

18. Järgnevates punktides esitatakse peamised kriteeriumid, mille põhjal tuvastatakse isiku lojaalsus, usaldusväärsus ja -kindlus isikule PSC andmiseks ja isikul PSC säilimiseks. Kriteeriumid arvestavad isiku iseloomuomadusi ja potentsiaalseid julgeolekuprobleeme põhjustada võivaid asjaolusid ning hinnatakse kooskõlas riigisiseste õigusaktidega järgneva tuvastamiseks:
a) kas isik on toime pannud salakuulamis-, terrorismi-, sabotaaži-, riigireetmis- või mässukuriteo või sellise kuriteo toimepanemise katse või on kaasa aidanud teise isiku poolt sellise kuriteo (või kuriteokatse) toimepanemisele;
b) kas isik on või on olnud seotud salakuulaja, terroristi või sabotööriga või isikuga, keda on põhjendatult alust kahtlustada salakuulamises, terrorismis või saboteerimises, või NATO ja/või NATO liikmesriigi julgeolekut ohustada võiva välisriigi organisatsiooni, sealhulgas välisriigi luureteenistuse, esindajaga, välja arvatud juhul, kui seotus oli lubatud seoses isiku ametiülesannetega;
c) kas isik kuulub või on kuulunud organisatsiooni, mis püüab vägivalla või õõnestustegevuse abil või muul õigusvastasel viisil kukutada NATO liikmesriigi valitsust või muuta NATO liikmesriigi valitsuskorda;
d) kas isik on või on olnud käesoleva punkti alapunktis c nimetatud organisatsiooni toetaja või kaasa aidanud sellise organisatsiooni tegevusele või on või on olnud tihedalt seotud sellise organisatsiooni liikmega;
e) kas isik on teadvalt jätnud avaldamata olulisi andmeid või avaldanud neid eksitavalt või võltsinud, iseäranis juhul, kui tegemist on julgeolekualaste andmetega, või on oma juurdepääsuloa taotluse täitmisel või julgeolekuvestlusel teadvalt valetanud;
f) kas isik on süüdi mõistetud kuriteos või on toime pannud süütegusid, mis osutavad isiku kuritegelikele kalduvustele;
g) kas isiku suhtes on tuvastatud varasemaid alkoholi väärtarvitamise juhtumeid;
h) kas isiku suhtes on tuvastatud varasemaid ebaseadusliku narkootilise aine tarvitamise ja/või seadusliku narkootilise aine väärtarvitamise juhtumeid;

i) kas isik osaleb või on osalenud tegevuses, sealhulgas seksuaalkäitumises, mis võib tekitada ohu isiku haavatavaks muutumiseks väljapressimise või surveavalduste suhtes;
j) kas isik on teos või sõnas näidanud ennast ebaausa, ebalojaalse, vastutustundetu, ebausaldusväärse või ebadiskreetsena;
k) kas isik on oluliselt või korduvalt rikkunud julgeolekualast korda või on püüdnud teostada või teostanud side- ja infosüsteemi või süsteemide suhtes toiminguid, milleks tal puudub luba;
l) kas isik võib sugulaste või lähedalt seotud isikute kaudu olla haavatav või survestatav välisriikide luureteenistuste, terrorirühmituste või muude õõnestusega tegelevate organisatsioonide või isikute poolt, kelle huvid võivad ohustada NATO ja/või NATO liikmesriikide julgeolekuhuve;
m) kas isik on tõsistes rahalistes raskustes või seletamatult jõukas ning
n) kas isik põeb või on põdenud mis tahes haigust või tal esineb või on esinenud vaimseid või emotsionaalseid häireid, mis võib põhjustada olulisi kõrvalekaldeid tema otsustusvõimes või usaldusväärsuses või muuta ta tahtmatult võimalikuks julgeolekuriskiks.

19. Kuigi ülalpool esitatud kriteeriume kohaldatakse kontrollitava isiku suhtes, võivad asjakohasel juhul ning kooskõlas liikmesriigi õigusaktidega osutuda asjassepuutuvaks ka isiku pereliikmed ning teised kontrollitavat isikut mõjutada võivad isikud, kellega sellisel juhul tuleks nimetatud isikule PSC andmise otsustamisel arvestada.

Topeltkodakondsusega isikud

20. Isiku PSC andmise nõuetele vastavuse hindamisel tuleb erilist tähelepanu pöörata isikutele, kellel on mitme riigi kodakondsus, kui ühe riigi näol võib tegemist olla NATOsse mittekuuluva riigiga. Kui isikule PSC-d andva riigi NSA/DSA või muu pädev julgeolekuasutus on veendunud lojaalsuskonflikti või niisuguse konflikti võimaluse puudumises, ei ole esmapilgul alust PSC andmisest keelduda.[3]

Julgeolekukontrollinõuded PSC andmisel NATO CONFIDENTIAL, NATO SECRET ja COSMIC TOP SECRET salastatustasemega teabele

21. Esmane julgeolekukontroll juurdepääsuks teabele salastatustasemega NC või NS tugineb päringutele, mis hõlmavad lühemat kahest ajavahemikust – vähemalt viimased viis aastat või isiku 18. eluaastast kuni päringu tegemiseni ulatuv vahemik – ning hõlmab järgnevat:

a) füüsilise isiku julgeolekuküsimustikule vastamine (võib olla kas NATO või liikmesriigi küsimustik);
b) isikusamasuse / kodakondsuse / riikliku kuuluvuse kontrollimine – kontrollitakse isiku sünniaega ja kohta ning isikusamasust; selgitatakse välja isiku kodakondsusseisund ja/või riiklik kuuluvus päringute tegemise ja sellele eelneval ajal, kusjuures hinnatakse isiku haavatavust välisriigist pärinevale survele, näiteks tulenevalt varasemast elukohast või endisaegsetest sidemetest ning
c) riiklike ja kohalike registrite andmete pärimine – tehakse päringud riiklikku julgeoleku- ja olemasolu korral keskkaristusregistrisse ja/või muusse samaväärsesse haldus- või politseiregistrisse.

[3] Näide: tööstusjulgeoleku valdkonnas (salastatud projekte ja tööstusjulgeolekut käsitlev direktiiv (AC/35-D/2003)) kehtib säte, mis lubab NSA-l/DSA-l või muul pädeval julgeolekuasutusel väljastada PSC isikule, kellel on enam kui üks kodakondsus.

22. Esmane julgeolekukontroll juurdepääsuks teabele salastatustasemega CTS tugineb päringutele, mis hõlmavad lühemat kahest ajavahemikust – vähemalt viimased kümme aastat või isiku 18. eluaastast kuni päringu tegemiseni ulatuv vahemik. Käesoleva punkti alapunkti e lõigetes i ja ii sätestatud vestluste läbiviimise korral päritakse lühema kohta kahest ajavahemikust – vähemalt viimased seitse aastat või isiku 18. eluaastast kuni päringu tegemiseni ulatuv vahemik. Lisaks käesoleva direktiivi punktis 21 esitatud nõuetele on salastatustasemega CTS teabele juurdepääsuloa andmiseks vajalikud (ning võivad olla asjakohased ka NC ja NS teabele juurdepääsuloa andmisel, kui see on kooskõlas liikmesriigi õigusaktidega) veel:

a) andmed varalise seisundi kohta: isiku vara kohta kogutakse teavet, hindamaks isiku haavatavust välis- või koduriigist pärinevale survele tõsistes rahalistes raskustes olemise tõttu või tuvastamaks seletamatu jõukuse olemasolu;

b) andmed hariduskäigu kohta: teavet kogutakse isiku õpingute kohta koolides, ülikoolides ja muudes haridusasutustes alates tema 18. sünnipäevast või uurimist läbiviiva julgeolekuasutuse äranägemisel muu asjakohase ajavahemiku vältel;

c) andmed töökäigu kohta: teavet kogutakse isiku praeguse ja varasema töötamise kohta; allikad, millele tuginetakse, hõlmavad töötamisega seotud dokumente, aruandeid töö tulemuslikkuse või tõhususe kohta ning tööandjaid või vahetuid juhte;

d) andmed sõjaväeteenistuse kohta: asjakohasel juhul kontrollitakse isiku teenimist relvajõududes ning teenistusest vabastamise alust ning

e) vestlused:
   i. asjaomase isikuga viiakse läbi vestlus(ed), iseäranis, kui esmaste päringute põhjal on ilmnenud teave, mis võib isiku vastu rääkida ning
   ii. vestlused viiakse läbi ka isikutega, kellel on võimalik anda erapooletu hinnangu uuritava isiku taustale, tegevusele, lojaalsusele, usaldusväärsusele ja usalduskindlusele. Kui liikmesriigis on tavaks nõuda uuritavalt soovituste esitamist, siis viiakse vestlused läbi ka soovitajatega, kui puudub mõjuv põhjus vestluse läbiviimisest loobumiseks. Isiku kohta kogutud olulise teabega seotud üksikasjade selgitamiseks ning isiku vastu rääkiva teabe põhistamiseks või ümber lükkamiseks tehakse piisavas mahus täiendavad päringud.

23. Andmete ebapiisavus uuritavas andmevaldkonnas korvatakse muude uurimisvahenditega kooskõlas liikmesriigi õigusaktidega. See võib hõlmata päringutaotlusi riigile, kus asjaomane isik on töötanud või elanud.

PSC andmine

24. NSA/DSA või muu pädev julgeolekuasutus arvestab PSC andmise otsustamisel kogu olemasolevat teavet ning hindab iga juhtumiga seotud riske. Arvestada tuleb, et isiku võimalikule survestatavusele viitavad märgid (näiteks võlad või abikaasa, elukaaslase või lähedase pereliikme võimalik survestatavus) ei või olla juurdepääsuloa andmisest keeldumise aluseks, kui isiku lojaalsus, usaldusväärsus ja usalduskindlus on muus osas vaieldamatu.

25. PSC andmisel kehtib see juurdepääsuks NC ja NS salastatustasemega teabele mitte kauem kui 10 aastat, juurdepääsuks CTS salastatustasemega teabele mitte kauem kui 7 aastat.

PSC kehtivuse pikendamine

26. PSC kehtivuse pikendamisega alustatakse enne PSC kehtivustähtaja lõppemist. Liikmesriikide PSC-toiminguid ja -nõudeid käsitlevas tugidokumendis (AC/35-D/1043) toodud tabelis esitatakse PSC kehtivuse pikendmise taotlus isiku osas pädevale NSA-le/DSA-le või muule pädevale julgeolekusasutusele vastavalt taotluse menetlusajale.

27. NC ja NS salastatustasemega teabe kohta antud PSC kehtivuse pikendmisel viiakse läbi vähemalt järgmised toimingud:

a) isik täidab julgeolekuküsimustiku (küsimustikuna võib kasutada kas NATO täiendavate isikuandmete vormi või muud sarnast liikmesriigi asjaomase asutuse vormi);
b) NATO tsiviil- või sõjalises organis töötavate isikute puhul võrreldakse isiku julgeolekuküsimustikus antud vastuseid vastava NATO organi julgeoleku- ja isikuregistrites olevate andmetega;
c) kui juurdepääsuloa kehtivuse pikendamist taotleb NATO tsiviil- või sõjaline organ oma töötaja kohta, saadetakse käesoleva punkti alapunktis a nimetatud julgeolekuküsimustik ning alapunktis b nõutava registritega võrdlemise tulemused isiku osas pädevust omava riigi NSA-le/DSA-le või muule pädevale julgeolekuasutusele;
d) riik, mille territooriumil NATO organ asub (st organi asukohariik), vaatab isiku osas pädevust omava NSA/DSA või muu pädeva julgeolekuasutuse taotlusel läbi oma riigisisesed registrid;
e) vajadusel ja isiku osas pädevust omava NSA/DSA või muu pädeva julgeolekuasutuse taotlusel vaatab oma riigisisesed registrid sarnaselt käesoleva punkti alapunktis d sätestatuga läbi ka muu NATO liikmesriik, kus töötaja on elanud ning
f) PSC kehtivuse pikendamise taotlemisel isiku osas pädevalt NSA-lt/DSA-lt või muult pädevalt julgeolekuasutuselt esitab asjaomane NATO tsiviil- või sõjaline organ koos taotlusega ka uuritava ajavahemiku vältel organis töötamise ajal isiku julgeolekukäitumist kajastavad üksikasjalikud andmed.

28. Isiku osas pädevust omav NSA/DSA või muu pädev julgeolekuasutus vaatab läbi esitatud teabe ning viib läbi liikmesriigi õigusaktidega nõutavad vajalikud kontrollimistoimingud. Otsuse tegemisel PSC kohta teavitab ta tulemusest taotluse esitanud NATO tsiviil- või sõjalist organit. Positiivse otsuse korral kinnitatakse PSC käesoleva direktiivi punkti 9 kohaselt.

29. CTS-taseme PSC kehtivuse pikendamisel võib lisaks käesoleva direktiivi punktis 27 esitatud tavapärastele kontrollitoimingutele viia läbi ka vestluse isikuga ning viimasele isiku osas läbiviidud uurimisele või isikuga läbiviidud vestlusele järgneva ajavahemiku osas nõutakse:

a) isikuomadusi käsitlevaid soovitusi – kui oma julgeolekuküsimustikku kasutav NATO liikmesriik seda nõuab;
b) kui on vajalik üksikasjalikum uurimine, tuleb viia läbi vestlus vähemalt kahe isikuga, kellel on võimalik anda erapooletu hinnang isiku taustale, tegevusele, lojaalsusele, usaldusväärsusele ja -kindlusele;
c) kui välismaal teenistuses oleva isiku PSC kehtivust on vaja pikendada teist või enamat korda katkematu välismaal viibimise ajal, tuleb kaaluda käesoleva punkti alapunktis b nimetatud üksikasjaliku uurimise läbiviimist;

d) vajaduse korral teeb asukohariigi NSA/DSA või muu pädev julgeolekuasutus isiku osas pädevust omava NSA/DSA või muu pädeva julgeolekuasutuse nimel täiendavaid päringuid tulenevalt teabest, mis võib ilmneda käesoleva direktiivi punktis 27 ning punkti 29 alapunktides a–c nimetatud toimingute tulemusel;
e) isiku suhtes pädevust omava NSA/DSA või muu pädeva julgeolekuasutuse poolt talle käesoleva punkti alapunkti d alusel saadetud teabe läbivaatamine ja kõrvutamine oma registrite andmetega ning
f) isiku suhtes pädevust omava NSA/DSA või muu pädeva julgeolekuasutuse poolt PSC kehtivuse uuendamise kohta tehtud otsuse kinnitamine taotluse esitanud NATO tsiviil- või sõjalisele organile.

30. Erandlikel asjaoludel, kui PSC kehtivust ei pikendata enne selle kehtivuse lõppemise kuupäeva, siis NATO tsiviil- või sõjaline organ, mis on isiku tööandja:

a) taotleb isiku suhtes pädevust omavalt NSA-lt/DSA-lt või muult pädevalt julgeolekuasutuselt kehtiva juurdepääsuloa kehtivuse jätkamist, kui see on lubatud liikmesriigi õigusaktide kohaselt;[4]
b) taotleb isiku suhtes pädevust omavalt NSA-lt/DSA-lt või muult julgeolekuasutuselt isikule menetlusaegset või ajutist juurdepääsuluba, kui see on lubatud liikmesriigi õigusaktide kohaselt[4] või
c) võib PSC kehtivuse lõppemisel anda jätkuvalt juurdepääsu NATO salastatud teabele tingimusel, et:
    i. isiku NSA/DSA või muu pädev julgeolekuasutus on kinnitanud juurdepääsuloa kehtivuse pikendamise menetluse jätkumist;
    ii. isiku tööandjaks olev NATO tsiiviil- või sõjaline asutus on nõus kandma riski, mis tuleneb isiku jätkuvast juurdepääsust NATO salastatud teabele ning
    iii. NATO salastatud teabele juurdepääsuloa andmise otsus vaadatakse üle iga 6 kuu möödumisel, kuni PSC kehtivuse pikendamiseni.[5]

PSC muutmine

31. Isiku osas pädevust omav NSA/DSA või muu pädev julgeolekuasutus teavitab isiku tööandjaks olevat organit asjakohastest muudatustest isiku PSCs. Vajadusel tagab organ, et kõiki asjakohaseid üksusi, kellele on kinnitatud isiku PSC olemasolu, teavitatakse isiku PSC muutmisest. Kui ilmneb isiku vastu rääkiv teave, otsustab isiku PSC kehtimajäämise isiku osas pädevust omav NSA/DSA või muu pädev julgeolekuasutus.

32. Kui PSC peatatakse või tunnistatakse kehtetuks, teavitab isiku osas pädevust omav NSA/DSA või muu pädev julgeolekusasutus asjaomasest otsusest viivitamata isiku tööandjaks olevat organit. Organ välistab isiku juurdepääsu NATO salastatud teabele. Lisaks teavitatakse isikut tema jätkuvast kohustusest kaitsta teavet, millele tal juurdepääs oli, ning samuti kohustuse rikkumise tagajärgedest. Kohustuse jätkumise tutvustamise kinnitamiseks tuleb isikult võtta kirjalik või muus samaväärses salgamist mittevõimaldavas vormis kinnitus.

[4] Liikmesriikide PSC-toiminguid ja -nõudeid käsitlevas tugidokumendis (AC/35-D/1043) esitatakse riikide loend, kes, vastavalt oma õigusaktidele, saavad pikendada PSC kehtivust või väljastada menetlusaegse või ajutise PSC.

[5] Kehtivuse pikendamise menetluse puhul on nõutav tööandjaks oleva NATO tsiviil- või sõjalise organi ühenduse võtmine NSA/DSA või muu pädeva julgeolekuasutusega PSC kehtivuse pikendamise menetluse jätkumise kohta kinnituse saamiseks.

PSC-de arvestus

33. NATO liikmesriik ja isiku tööandjaks olev NATO tsiviil- või sõjaline organ peavad arvestust NATO salastatud teabele juurdepääsu omavatele isikutele antud PSC-de kohta. Arvestus (asjakohasel juhul koos kinnitustega) sisaldab üksikasjalikke andmeid juurdepääsuloa taseme, kuupäeva ja kehtivuse kohta.

Julgeolekukoolitus ja -teadlikkus

34. Kõigile isikutele, kes töötavad salastatustasemega NR teabele juurdepääsu võimaldaval ametikohal või kellele on antud PSC juurdepääsuks NC või kõrgema salastatustasemega teabele, tutvustatakse NATO salastatud teabe kaitse aluseks olevaid julgeolekumeetmeid ja isiku julgeolekukohustusi. Isik annab kirjaliku või samaväärses salgamist mittevõimaldavas vormis kinnituse selle kohta, et mõistab täies ulatuses oma kohustusi ning tema poolt NATO salastatud teabe volitamata isikule tahtlikult või hooletusest üleandmise võimaldamise tuvastamisest temale tulenevaid tagajärgi vastavalt isiku liikmesriigi õigusaktidele. Kinnituse dokumenteerib NATO salastatud teabele juurdepääsuks luba andev NATO liikmesriik või NATO tsiviil- või sõjaline organ.

35. NATO liikmesriigi või NATO tsiviil- või sõjalise organi vastutusalas on asjakohase julgeolekukoolitus- ja -teadlikkuskava koostamine isikutele, kellele on antud juurdepääsuõigus NATO salastatud teabele.[6] Isikuid kohustatakse regulaarselt osalema julgeolekukoolitustel või muudel julgeolekuteadlikkuse tõstmiseks korraldatavatel üritustel.

36. Julgeolekukoolitus- ja -teadlikkusmeetmed kujundatakse konkreetset sihtrühma arvestades, kuid peavad hõlmama vähemalt:

a) asjakohaseid NATO salastatud teabe kaitsmisele kohaldatavaid õigusakte ning nende rikkumise tagajärgi;

b) vaenulikust luuretegevusest tulenevaid ohte, teabe kogumise võtteid ja viise, samuti ohu tõrjumiseks rakendatavaid kaitsemeetmeid;

c) teavet side- ja infosüsteeme puudutavate enimlevinud ohtude ning lõppkasutaja poolt nende tõrjumiseks rakendatavate elementaarsete meetmete kohta ning

d) nõudest viivitamatult teavitada asjakohast pädevat julgeolekuasutust NATO salastatud teavet puudutavatest julgeolekurikkumistest, teabe volitamata avaldamisest või võimalikust salastatuse ohtu seadmisest.[7]

37. Isikuid, kes ei vaja enam juurdepääsu NATO salastatud teabele, teavitatakse nende jätkuvast kohustusest nimetatud teavet kaitsta ning samuti kohustuse rikkumise tagajärgedest. Kooskõlas liikmesriigi õigusaktidega tuleb kohustuse jätkumise tutvustamise kohta võtta isikult kirjalik või muus samaväärses salgamist mittevõimaldavas vormis kinnitus.

---

[6] Liikmesriigid võivad kasutada NATO tarbeks koostatud tutvustusi või samaväärseid liikmesriigi enda tarbeks koostatud materjale, kui viimases juhitakse tähelepanu nende kahe julgeolekuraamistiku erisustele.

[7] Täiendvad juhised põhjaliku julgeolekukoolitus- ja -teadlikkuskava koostamiseks on esitatud julgeolekukoolitust ja -teadlikkust käsitlevas tugideokumendis (AC/35-D/1029).

JÄTKUMEETMED

38. Kui isiku nõuetele vastavuse hindamine PSC andmiseks on NSA/DSA või muu pädeva julgeolekuasutuse vastutusalas, siis isiku NATO salastatud teabe kaitse jätkuva teadlikkuse tagamine on siseohu[8] tõrjumise kontekstis isiku tööandjaks oleva organisatsiooni vastutusalas. Tööandjaks olev organ teavitab PSC-d omava isikuga seotud asjakohastest julgeolekualastest küsimustest isikule PSC andnud NSA-d/DSA-d või muud pädevat julgeolekuasutust isiku PSC säilitamise otsustamiseks.

39. Lisaks tuleb siseohu tõrjumiseks rakendada mitmetasandiline vastumeetmete[9] süsteem. Vastumeetmed peavad hõlmama:

a) tõhusat esmatasandi juhtimist, mis võimaldab tuvastada käitumisviisid, mis võivad mõjutada julgeolekut, ning nendega tegeleda;
b) head juhtimispraktikat, mis suurendab töötajate pühendumust ja lojaalsust;
c) tulemuslikkuse hindamise korda, mis hõlmab tegelemist konkreetse isiku, ametikoha või organisatsiooniga seotud julgeolekuprobleemidega;
d) tõhusat kontrolli turvaaladele sissepääsu üle ning side- ja infosüsteeme, mis võimaldab tuvastada lubamatud toimingud;
e) kohustuslikku teavitamist muudatustest PSC-d omava isiku eraelulistes asjaoludes, iseäranis juhul, kui tegemist on isikuga, kellel on CTS-taseme PSC või kes töötab kõrge julgeolekuriskiga ametikohal ning
f) korralisi julgeolekuteadlikkuskoolitusi ning turvameetmete täpset järgimist nõudva julgeolekukultuuri kujundamist.

JUURDEPÄÄS NATO SALASTATUD TEABELE ERANDJUHTUDEL

Menetlusaegne või ajutine juurdepääs

40. Olukorras, kus algset kontrollimenetlust on alustatud, aga ei ole veel lõpule viidud, või isiku PSC kehtivus on pikendamisel, võib NATO salastatud teabele juurdepääsu vajavale isikule, kellel puhul isiku suhtes pädevust omav NSA/DSA või muu pädev julgeolekuasutus on otsustanud, et isik ei kujuta endast ilmset ohtu, lubada nimetatud juurdepääsu menetlusaegse või ajutise PSC alusel, mis antakse kooskõlas liikmesriigi õigusaktidega (liikmesriikide PSC-toiminguid ja -nõudeid käsitlevas tugidokumendis (AC/35-D/1043) loetletakse riigid, kes saavad anda menetlusaegse või ajutise PSC).

41. Isiku suhtes pädevust omav NSA/DSA või muu julgeolekuasutus tagab, et:

a) isikul on teadmisvajadus;
b) isikule on tutvustatud tema julgeolekukohustusi NATO salastatud teabe kaitsmisel ning

---

[8] Siseoht lähtub töötajatest, kellele on antud õigus juurdepääsuks NATO salastatud teabele ja/või NATO varadele tulenevalt nende ülesannetest organisatsioonis ning kellel on võimalik antud juurdepääsu tahtlikult või hooletusest väärkasutada teabe ja/või varade hävitamiseks, kahjustamiseks, kõrvaldamiseks või avalikustamiseks.

[9] Täiendavad juhised mitmetasandilise lähenemise rakendamiseks organisatsiooni seest tuleneva ohu tõrjumisel on esitatud julgeolekukoolitust ja -teadlikkust käsitlevas tugidokumendis (AC/35-D/1029-REV1).

c) isik on kinnitanud oma kohustusi kirjalikult või sellega samaväärsel salgamist mittevõimaldaval viisil.

Ajutine juurdepääs ametisse nimetamisel

42. Kui kavandatakse isiku nimetamist ametikohale, mis nõuab kõrgema taseme PSC-d kui isikul hetkel on, võib isiku erandkorras ajutiselt ametisse nimetada järgmistel tingimustel:

a) isikul on kehtiv PSC;
b) julgeolekukontrollimenetlust ametikohal vajaliku tasemega PSC saamiseks on juba alustatud ning
c) isiku tööandjaks olev NATO tsiviil- või sõjaline organ on sooritanud piisavad kontrollitoimingud, mis näitavad, et isik ei ole oluliselt või korduvalt rikkunud julgeolekualast korda.

43. Arvestust isikute üle, kellele on antud juurdepääs käesoleva direktiivi punktide 40 kuni 42 alusel peab vastutav turvateenistus ning see edastatakse korraliselt NOSile. NATO tsiviil- või sõjalise organi juht teavitab isiku suhtes pädevust omavat NSA-d/DSA-d või muud julgeolekuasutust isikule nimetatud juurdepääsu andmisest.

Ühekordne juurdepääs

44. Erandkorras võib isikule ühekordselt lubada juurdepääsu NATO salastatud teabele, mille salastatustase on ühe taseme võrra kõrgem isiku kehtiva PSC tasemest. Juurdepääsu lubamiseks peavad olema täidetud järgnevad tingimused:

a) isiku vahetu juht peab kirjalikult põhjendama täidetava ülesande seisukohast kaalukat vajadust juurdepääsu lubamiseks;
b) juurdepääs lubatakse üksnes konkreetsetele vahetu juhi poolt nimetatud ülesandega seotud NATO salastatud teabele;
c) isiku tööandjaks olev NATO tsiviil- või sõjaline organ on sooritanud piisavad kontrollitoimingud, mis näitavad, et isik ei ole oluliselt või korduvalt rikkunud julgeolekualast korda;
d) loa annab OF6 (brigaadikindrali auaste või samaväärne tsiviilamet) taseme ametnik pärast asjaomaselt pädevalt julgeolekuasutuselt kooskõlastuse saamist ning
e) vastutav turvateenistus dokumenteerib erandi, muuhulgas kirjeldades teavet, millele juurdepääs lubati.

45. NATO salastatud teabele juurdepääsu lubamiseks ei või käesolevat menetlust korduvalt kasutada. Vajaduse korral või kui juurdepääs on vajalik enam kui 6 kuuks hangitakse kõrgema taseme PSC ning ajakohastatakse ametikohaga seotud PSC-nõuded.

Tõlgi kasutamine

46. Erandkorras võib kirjaliku või suulise tõlke tegemiseks NATO liikmesriigi või NATO-sse mittekuuluva riigi tõlgi poolt, kellel ei ole vastava tõlke tegemiseks vajalikku PSC-d, lubada juurdepääsu NATO salastatud teabele järgneval juhul kui:

a) keel, millest suulist tõlkimist vajatakse, nõuab emakeelena kõnelejat ning muudab isiku teostatava tegevuse seisukohalt oluliseks/elutähtsaks;

b) juurdepääsu lubab NATO peakorteri divisjonijuht või NATO tsiviil- või sõjaline organ kaaluka kirjaliku põhjenduse alusel;
c) juurdepääs lubatakse üksnes konkreetsetele NATO peakorteri osakonnajuhi või NATO tsiviil- või sõjalise organi poolt nimetatud ülesandega seotud NATO teabele, mille salastatustase ulatub tasemeni CTS ning hõlmab seda
d) juurdepääsu ei lubata NATO salastatud teavet töötlevale side- ja infosüsteemile, välja arvatud sellistele side- ja infosüsteemidele, mis on ette nähtud üksnes isiku teostatava tegevuse toetamiseks;
e) vastutav turvateenistus dokumenteerib erandi, muuhulgas kirjeldades taristut ja teavet, millele juurdepääs lubati, ning edastab selle perioodiliselt NOSile;
f) isikule on tutvustatud asjaomaseid turbetingimusi ning isik on kirjalikult kinnitanud, et mõistab täies ulatuses oma kohustusi ning võimalikke tagajärgi juhul, kui tahtlikult või hooletusest leiab aset teabe lubamatu avaldamine.

Juurdepääs eriolukorras

47. Sõja, riikidevaheliste pingete kasvu või rahvusvaheliste hädaoperatsioonide ajal või, kui eriolukorra meetmed seda nõuavad, rahuajal võivad NATO liikmesriigid ning NATO tsiviil- ja sõjaliste organite juhid erandjuhtudel anda kirjaliku loa juurdepääsuks NATO salastatud teabele isikule, kellel ei ole nõutavat PSC-d, tingimusel, et loa andmine on tingimata vajalik ning puudub mõistlik alus kahelda isiku lojaalsuses, usaldusväärsuses ja -kindluses. Vastutav turvateenistus dokumenteerib loa, kirjeldades teavet, millele juurdepääs lubati.

48. CTS-tasemega teabe puhul antakse juurdepääs võimalusel vaid isikutele, kellel on luba juurdepääsuks liikmesriigi täiesti sajalase või NS-taseme teabele.

NATO SALASTATUD TEABELE JUURDEPÄÄSU ANDMINE NATOSSE MITTEKUULUVA RIIGI KODANIKULE, KES ON NATO LIIKMESRIIGI TSIVIIL- VÕI SÕJALISE ORGANI LÕIMITUD TÖÖTAJA

49. NATO-sse mittekuuluva riigi kodanikule[10], kes teenib lõimitud töötajana[11] NATO liikmesriigi tsiviil- või sõjalises organis (nt relvajõududes, riigiasutustes), võib lubada juurdepääsu NATO salastatud teabele, kui juurdepääs on vajalik seoses konkreetse NATO operatsiooni, ülesande, toimingu või programmiga. Enne juurdepääsu andmist teabele on NATO liikmesriigi NSA/DSA või muu pädev julgeolekuasutus kohustatud veenduma järgnevate tingimuste täitmises ning hankima selle kohta asjakohase kinnituse:

a) liikmesriik on valmis lõimitud töötaja kodakondsusriigiga, mis ei ole NATO liige, jagama juurdepääsu riigisisesele samaliigilisele ja sama salastatustasemega teabele;
b) isikule on antud PSC julgeolekukontrolli põhjal, mis on vähemalt sama range, kui kontroll, mida nõutakse NATO liikmesriigi kodaniku puhul tulenevalt NATO Security Policy julgeolekutingimustest ja nendega seotud direktiividest; märkides, et PSC ei ole nõutav juurdepääsuks NR taseme teabele;

[10] Asjaomaseid sätteid ei kohaldata Kanada alalistele elanikele. Käesoleva direktiivi raames käsitletakse neid NATO kodanikena.

[11] NATO-sse mittekuuluva riigi kodanik loetakse NATO liikmesriigi tsiviil- või sõjalise organi lõimitud liikmeks, kui ta on lülitatud organi koosseisu organit moodustava liikmena ning organ loeb ta igas aspektis samaväärseks, kui isiku PSC pärineb isiku suhtes pädevust omavalt riigilt või asjaomaselt NATO liikmesriigilt, kusjuures viimase puhul on sellega kaasnevad õiguslikud kohustused samad, mis NATO liikmesriigi kodaniku puhul.

c) liikmesriigil on piisav reaalne ja õiguslik võim isiku üle asjakohaste õiguslike meetmete rakendamiseks ning isiku vastutusele võtmiseks NATO salastatud teabe mittenõuetekohase käsitlemise eest ning
d) juurdepääsu ei anta ATOMAL või muusse eriliiki kuuluvale teabele.

50. Üksikasjalik käsitlus muudest juhtudest, mille puhul NATO-sse mittekuuluva riigi kodanikud või rahvusvahelise organisatsiooni kuuluvusega isikud vajavad juurdepääsu NATO salastatud teabele, esitatakse C-M(2002)49 lisas H ning sellega seotud direktiivides.

Kuupäev: (pp/kk/aaaa) __/__/____
Vajadusel (viitenumber): ……

TAOTLUS JUURDEPÄÄSUÕIGUSE KINNITUSE SAAMISEKS

1. **Palume kinnitada, kas allpool näidatud isikul on juurdepääsuõigus (PSC) salastatud teabele osundatud tasemel.**

Perenimi:

……

Eesnimi (eesnimed) (passi/isikutunnistuse järgi):

……

Sünnikuupäev (pp/kk/aaaa) __/__/____

Sünnikoht:

…..……

Kodakondsus:

……...……

Passi või isikutunnistuse number (vajadusel)

……

Väljastaja: ……

Väljastatud: (pp/kk/aaaa) __/__/____

2. **Nõutav PSC:**

Märkida asjakohane valik (üks või mitu):

[ ] CTS ……[1]

[ ] NS ……[1]

[ ] NC ……[1]

3. **Taotluse põhjus[2]:**

……

……

……

……

4. **Taotlev asutus:**

……

Julgeolekuametniku nimi: ……..

Telefoninumber: ……..

E-post: ……..

[1] Asjakohasel juhul lisada eriliigitähis (nt ATOMAL, BOHEMIA, CRYPTO)
[2] PSC-d nõudev toiming, selle ajaraam/kestus, muu oluline teave
(*) Tähistatud märge ei ole vormi osa.

Kuupäev: (pp/kk/aaaa) __/__/____
Vajadusel (viitenumber): …….

KINNITUS ISIKU JUURDEPÄÄSUÕIGUSE KOHTA

1. Käesolevaga kinnitatakse, et isikule:

perenimi:

eesnimi (eesnimed) (passi/isikutunnistuse järgi):

sünnikuupäev (pp/kk/aaaa) __/__/____

sünnikoht:

kodakondsus:

on antud juurdepääsuõigus …… valitsuse poolt kooskõlas NATO kehtiva julgeolekueeskirjaga, sealhulgas ATOMAL-teabe puhul dokumendi C-M(64)39 julgeolekulisaga, ning isik on sellega tunnistatud sobivaks temale tasemeni (sealhulgas nimetatud tasemel salastatud teave) …… salastatud teabe usaldamiseks.

Märkused:

2. **Käesolev kinnitus kaotab kehtivuse hiljemalt (pp/kk/aaaa) __/__/____**
3. **Kinnitav asutus (NSA/DSA või muu pädev julgeolekuasutus):**

Nimi:

……

……

……

Telefoninumber: ……..

E-post: ……..

Kuupäev: (pp/kk/aaaa) __/__/____ Allkiri/pitser (kui on nõutav)[2]

[1] Märkida vastavalt asjaoludele üks või mitu järgnevatest:
CTS
NS
NC
lisades asjakohasel juhul eriliigitähise (nt ATOMAL, BOHEMIA, CRYPTO)

[2] Liikmesriikide PSC-toiminguid ja -nõudeid käsitlevas tugideokumendis esitatakse riikide loend, mille puhul on nõutav allkiri või pitser.

(*) Tähistatud märge ei ole vormi osa.