



KAITSEMINISTEERIUM



KAITSEMINISTEERIUM

**EL Nõukogu otsus
EL salastatud teabe kaitseks vajalike
julgeolekueeskirjade kohta**

15.01.2010

Hetkel kehtivad ...



KAITSEMINISTEERIUM

... nõukogu julgeolekueeskirjad, mis on vastu võetud Euroopa Liidu Nõukogu 19. märtsi 2001 otsusega.

Eeskirjade muutmise vajadus



KAITSEMINISTEERIUM

2007. aasta lõpus anti EL Nõukogu Julgeolekukomiteele ülesanne 2001. aasta eeskirjad üle vaadata, kuna need jäid ajale jalgu ning teatud küsimustes puudus paindlikkus.

Uue eeskirja jõustumine



KAITSEMINISTEERIUM

Uus eeskiri võetakse vastu 2010. a alguses.

PS! Uus eeskiri asendab jõustudes terviktekstina 2001. aasta eeskirja.

Eeskirja paneme üles meie kodulehele
www.nsa.ee.

Eeskirja eesmärk on ...



KAITSEMINISTEERIUM

... kehtestada Euroopa Liidu salastatud teabe kaitseks vajalikud julgeoleku aluspõhimõtted ja miinimumstandardid.

Kellele eeskiri kohaldub



KAITSEMINISTEERIUM

ELi salastatud teabe töötlemisel liikmesriikide pädevate asutuste poolt peaksid liikmesriigid järgima seda eeskirja kooskõlas oma riigisiseste õigusaktidega, et iga liikmesriik võiks olla kindel ELi salastatud teabe suhtes samaväärse kaitse kohaldamises.

Kellele eeskiri kohaldub (2)



KAITSEMINISTEERIUM

Liikmesriigid peavad tagama, et eeskirja järgivad nii ELi alalistes esindustes töötavad isikud, nõukogu istungitel osalevad delegatsiooni liikmed kui muud isikud, kellel on liikmesriikides oma tööülesannete tõttu volitused juurdepääsuks ELi salastatud teabele.

Uue eeskirja struktuur



KAITSEMINISTEERIUM

Uues eeskirjas on:

- **üldine osa**, mis koosneb 18 artiklist
- **6 erinevat julgeolekuvaldkonda reguleerivat lisa:**
 - töötajatega seotud julgeolek (lisa 1)
 - füüsiline julgeolek (lisa 2)
 - salastatud teabe haldamine (lisa 3)
 - side- ja infosüsteemides töödeldava ELi salastatud teabe kaitse (lisa 4)
 - tööstusjulgeolek (lisa 5)
 - salastatud teabe vahetamine kolmandate riikide ja rahvusvaheliste organisatsioonidega (lisa 6)

Uue eeskirja struktuur (2)



KAITSEMINISTEERIUM

Lõpus on 4 liidet:

- mõisted
- tabel salastatuse tasemete vastavuse kohta
- riiklike julgeolekuasutuste loetelu ja kontaktandmed
- lühendite loetelu

EL salastatud teabe märgistuse kord



KAITSEMINISTEERIUM

Uues eeskirjas kasutatakse prantsuse ja inglise keelset märgistusviisi (näiteks RESTREINT UE / EU RESTRICTED). Praegu kehtivas eeskirjas on mõlemakeelne märgistus ainult täiesti salajase taseme puhul ja kolm alumist taset on märgistatud ainult prantsuse keelse märkega (näiteks RESTREINT UE).

EL salastatud teabe märgistuse kord (2)



KAITSEMINISTEERIUM

Lühemate kui ühe lehekülje pikkuste tekstilõikude salastatuse taseme märkimisel ELi salastatud dokumentides võib kasutada järgmisi standardlühendeid:

- TS-UE/EU-TS
- S-UE/EU-S
- C-UE/EU-C
- R-UE/EU-R

EL salastatud teabe märgistuse kord (3)



KAITSEMINISTEERIUM

Lisaks salastuse märkele võib ELi salastatud teave kanda täiendavat märget, näiteks teabe koostajale viitav tunnus, kasutuspiirangud, vajadusel kuupäev või konkreetne sündmus, pärast mida võib salastatuse taset alandada või salastatuse kustutada.

Lisa 1 - Töötajatega seotud julgeolek



KAITSEMINISTEERIUM

Sätetatakse kriteeriumid, mille alusel on võimalik kindlaks teha, kas isikule võib tema lojaalsust ja usaldusväarsust arvesse võttes anda loa juurdepääsuks ELi salastatud teabele, ning uurimis- ja haldusmenetlused, mida tuleb sellisel juhul järgida.

On täpsustatud julgeolekuloa andmisest keeldumise aluseid.

Lisa 1 - Töötajatega seotud julgeolek (2)



KAITSEMINISTEERIUM

Toonitatakse, et kõik liikmesriigid peavad määrama oma struktuurides kindlaks need ametikohad, mis eeldavad juurdepääsu CONFIDENTIEL / UE / EU CONFIDENTIAL või kõrgemal tasemel salastatud teabele ja seetõttu eeldavad asjakohase tasemega juurdepääsuloa olemasolu.

Lisa 1 - Töötajatega seotud julgeolek (3)



KAITSEMINISTEERIUM

Liikmesriigid peavad Euroopa Liidu juurdepääsulubade kohta vastavaid registreid, et omada ülevaadet isikutest, kellel on õigus ELi salastatud teabele juurde pääseda.

Lisa 2 - Füüsiline julgeolek



KAITSEMINISTEERIUM

Füüsiline julgeolek on füüsiliste ja tehniliste kaitsemeetmete rakendamine, et vältida volitamata juurdepääsu ELi salastatud teabele.

Lisas sätestatakse miinimumnõuded objektide ja ruumide, kus toimub ELi salastatud teabe töötlemine ja säilitamine, füüsiliseks kaitsmiseks.

Lisa 2 - Füüsiline julgeolek (2)



KAITSEMINISTEERIUM

Pädev julgeolekuasutus peab tagama ELi salastatud teabe füüsiliseks kaitseks vajalike seadmete (seifid, paberi-purustajad, ukسلukud, häiresüsteemid jne) hankimisel, et nimetatud seadmed vastavad heakskiidetud tehnilistele standarditele.

Lisa 2 - Füüsiline julgeolek (3)



KAITSEMINISTEERIUM

ELi salastatud teabe füüsiliseks kaitsmiseks luuakse kaht tüüpi alad või riigisisese süsteemi kohaselt samaväärsed alad:

- a) haldustegevuse alad
- b) turvaalad (sealhulgas tehniliselt kaitstud turvaalad).

Välja on toodud nõuded, millele need alad peavad vastama.

Lisa 2 - Füüsiline julgeolek (4)



KAITSEMINISTEERIUM

Uues eeskirjas ei kasutata I ja II klassi turvaala mõistet, kuid sätestatakse eraldi nõuded alale, millele sisenemine tähendab praktiliselt otsest juurdepääsu alal asuvale salastatud teabele.

Lisa 3 - Salastatud teabe haldamine



KAITSEMINISTEERIUM

Sätetatakse haldusmeetmed ELi salastatud teabe kontrollimiseks kogu selle kasutusaja jooksul, et aidata ära hoida ja avastada sellise teabe teadlik või juhuslik ohtusattumine või kadumine.

Lisa 3 - Salastatud teabe haldamine (2)



KAITSEMINISTEERIUM

Enne iga kalendriaasta lõppu võtab nõukogu vastu kontrollimiskava järgmiseks aastaks, et tagada ELi salastatud teabe kaitseks kehtestatud nõutavate miinimumstandardite järgimine.

Lisa 3 - Salastatud teabe haldamine (3)



KAITSEMINISTEERIUM

Eeskiri sätestab kohustuse registreerida ELi salastatud teavet alates CONFIDENTIEL UE / EU CONFIDENTIAL tasemest.

Lisa 3 - Salastatud teabe haldamine

(4)



KAITSEMINISTEERIUM

CONFIDENTIEL UE / EU
CONFIDENTIAL tasemel salastatud
teavet võib vedada ka postiteenuste või
kommerts-kullerteenuste abil, kui vedu
toimub ühest liikmesriigist teise ja kui
seda lubavad antud riigi seadused ning
kohaldatakse asjakohaseid kaitse-
meetmeid.

Lisa 4 - Side- ja infosüsteemides töödeldava ELi salastatud teabe kaitse



Tuuakse sisse infokindluse (Information Assurance = IA) mõiste.

Infokindlus side- ja infosüsteemide valdkonnas tähendab kindlust, et sellised süsteemid kaitsevad neis töödeldavat teavet ning toimivad ettenähtud korras, ettenähtud ajal ja õiguspäraste kasutajate kontrolli all.

Lisa 5 - Tööstusjulgeolek



KAITSEMINISTEERIUM

- Sätestatakse üldised julgeolekunõuded, mida kohaldatakse ettevõtetele lepingueelsetel läbirääkimistel ja nõukogu peasekretariaadi poolt sõlmitud EL salastatud teavet sisaldavatele lepingutele kogu kehtivusaja jooksul.
- Kirjeldatakse, mida peab asjaomane riiklik julgeolekuasutus enne töötlemisloa väljastamist hindama ja kontrollima.

Lisa 6 - Salastatud teabe vahetamine kolmandate riikide ja rahvusvaheliste organisatsioonidega



KAITSEMINISTEERIUM

Kui nõukogu otsustab, et on pikaajaline vajadus vahetada ELi salastatud teavet kolmanda riigi või rahvusvahelise organisatsiooniga, sõlmitakse haldus-kokkulepe (kui avalikustatav ELi salastatud teave ei ole kõrgemal salastatuse tasemel kui RESTREINT UE / EU RESTRICTED) või salastatud teabe kaitse leping.

Lisa 6 - Salastatud teabe vahetamine kolmandate riikide ja rahvusvaheliste organisatsioonidega (2)



KAITSEMINISTEERIUM

Halduskokkuleppe või salastatud teabe kaitse lepingu sätted tagavad, et kui kolmandad riigid või rahvusvahelised organisatsioonid saavad ELi salastatud teavet, kaitstakse kõnealust teavet vastavalt eeskirjas kehtestatud miinimum-standarditele.

Lisa 6 - Salastatud teabe vahetamine kolmandate riikide ja rahvusvaheliste organisatsioonidega (3)



KAITSEMINISTEERIUM

Nõukogu teeb otsuse nõukogust pärineva ELi salastatud teabe avaldamise kohta igal üksikjuhul eraldi.

Kui salastatud teave ei ole pärit nõukogust, küsib nõukogu peasekretariaat avaldamiseks teabe koostaja kirjalikku nõusolekut.



KAITSEMINISTEERIUM

Täna!