

SUOMEN SÄÄDÖSKOKOELMA

Julkaistu Helsingissä 2 päivänä joulukuuta 2019

1101/2019

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa

Valtioneuvoston päätöksen mukaisesti säädetään julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 18 §:n 4 momentin ja kansainvälisistä tietoturvaluusvelvoitteista annetun lain (588/2004) 8 §:n 2 momentin nojalla:

1 §

Soveltamisala

Tässä asetuksessa säädetään julkisen hallinnon tiedonhallinnasta annetun lain (906/2019), jäljempänä *tiedonhallintalaki*, 18 §:n 1 momentissa tarkoitettujen asiakirjojen turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä sekä turvallisuusluokiteltujen asiakirjojen käsittelyä koskevista tietoturvaluusvelvoitteista valtionhallinnon viranomaisissa.

Viranomaisen asiakirjan julkisuudesta ja asiakirjan saamista koskevan pyynnön käsittelystä säädetään viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999).

Kansainvälisten tietoturvaluusvelvoitteiden mukaisesti turvallisuusluokitellun asiakirjan salassapitovelvollisuudesta ja kansainvälisten tietoturvaluusvelvoitteiden toteuttamisesta säädetään kansainvälisistä tietoturvaluusvelvoitteista annetussa laissa (588/2004). Tätä asetusta sovelletaan toisen maan viranomaiselta tai kansainväliseltä toimielimeltä saadun turvallisuusluokiteltavan asiakirjan käsittelyyn, jollei mainitun lain mukaisesta kansainvälisestä tietoturvaluusvelvoitteesta muuta johdu.

2 §

Määritelmät

Tässä asetuksessa tarkoitetaan:

- 1) *valtionhallinnon viranomaisella* valtion virastoissa ja laitoksissa toimivia viranomaisia, tuomioistuimia ja valitusasioita käsittelemään perustettuja lautakuntia;
- 2) *asiakirjan käsittelyllä* asiakirjan vastaanottamista, laatimista, tallentamista, katse-lua, muuttamista, luovuttamista, kopiointia, siirtoa, välittämistä, tuhoamista, säilyttämistä ja arkistointia sekä muita asiakirjaan kohdistuvia toimenpiteitä;
- 3) *päätelaitteella* tietojärjestelmää tai sen osaa, jota yleensä yksi henkilö käyttää työtehtäviensä tai muiden valtionhallinnon viranomaisen tehtävien hoitamiseen liittyvään sähköiseen tietojenkäsittelyyn.

Sen lisäksi, mitä tässä asetuksessa erikseen säädetään asiakirjan kopioimisesta tai asiakirjan kopiosta, asiakirjan kopioon sovelletaan, mitä asiakirjasta säädetään.

Turvallisuusluokittelu ja turvallisuusluokan merkitseminen

Tiedonhallintalain 18 §:n 1 momentissa tarkoitettut turvallisuusluokiteltavat asiakirjat jaetaan seuraaviin turvallisuusluokkiin:

1) turvallisuusluokan I asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa tiedonhallintalain 18 §:n 1 momentissa tarkoitettulle suojattavalle edulle;

2) turvallisuusluokan II asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa tiedonhallintalain 18 §:n 1 momentissa tarkoitettulle suojattavalle edulle;

3) turvallisuusluokan III asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa tiedonhallintalain 18 §:n 1 momentissa tarkoitettulle suojattavalle edulle;

4) turvallisuusluokan IV asiakirja, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa lievää vahinkoa tiedonhallintalain 18 §:n 1 momentissa tarkoitettulle suojattavalle edulle.

Edellä 1 momentissa tarkoitettut turvallisuusluokat merkitään asiakirjaan seuraavasti: turvallisuusluokan I asiakirjaan tehdään merkintä "ERITTÄIN SALAINEN", turvallisuusluokan II asiakirjaan merkintä "SALAINEN", turvallisuusluokan III asiakirjaan merkintä "LUOTTAMUKSELLINEN" ja turvallisuusluokan IV asiakirjaan merkintä "KÄYTTÖ RAJOITETTU". Mainitun merkinnän lisäksi voidaan käyttää merkintää "TL I", "TL II", "TL III" ja "TL IV".

Turvallisuusluokka merkitään 2 momentissa säädetystä poiketen ruotsiksi asiakirjoihin, jotka on laadittu ruotsinkielisinä tai käännetty ruotsiksi. Merkintä voidaan tehdä muulloinkin, jos viranomainen pitää sitä tarpeellisenä. Turvallisuusluokan I asiakirjaan tehdään merkintä "YTTERST HEMLIG", turvallisuusluokan II asiakirjaan merkintä "HEMLIG", turvallisuusluokan III asiakirjaan merkintä "KONFIDENTIELL" ja turvallisuusluokan IV asiakirjaan merkintä "BEGRÄNSAD TILLGÅNG".

Asiakirjan turvallisuusluokan tulee käydä ilmi myös tiedonhallintalain 25 §:ssä tarkoitettun asiarekisterin ja muun viranomaisen yleisesti tiedonhallintaan käyttämän tietovarannon asiakirjaa koskevista tiedoista.

Merkintä voidaan tehdä asiakirjaan liitettävään erilliseen asiakirjaan, jos merkintöjen tekeminen asiakirjaan tai merkinnän muuttaminen ei ole teknisesti mahdollista tai jos turvallisuusluokkaa vastaavat käsittelyvaatimukset ovat tarpeen vain tietyn lyhyehkön ajan.

Turvallisuusluokituksen vastaavuus kansainvälisiä tietoturvallisuusvelvoitteita toteutettaessa

Jollei kansainvälisestä tietoturvallisuusvelvoitteesta muuta johdu, turvallisuusluokitusmerkintää "ERITTÄIN SALAINEN" tai "YTTERST HEMLIG" vastaa englanninkielinen turvallisuusluokitusmerkintä "TOP SECRET" tai sitä vastaava muun kielinen merkintä; merkintää "SALAINEN" tai "HEMLIG" vastaa merkintä "SECRET" tai sitä vastaava muun kielinen merkintä; merkintää "LUOTTAMUKSELLINEN" tai "KONFIDENTIELL" vastaa merkintä "CONFIDENTIAL" tai sitä vastaava muun kielinen merkintä; merkintää "KÄYTTÖ RAJOITETTU" tai "BEGRÄNSAD TILLGÅNG" vastaa merkintä "RESTRICTED" tai sitä vastaava muun kielinen merkintä.

5 §

Turvallisuusluokkaa koskevan merkinnän poistaminen tai muuttaminen

Jos asiakirjan turvallisuusluokittelulle ei enää ole perusteita lain mukaan tai turvallisuusluokkaa on tarpeen muuttaa, 3 §:ssä tarkoitetun merkinnän poistamisesta tai muuttamisesta on tehtävä asianmukainen merkintä asiakirjaan, johon alkuperäinen merkintä on tehty sekä asiakirjan 3 §:n 4 momentissa tarkoitettuihin tietoihin. Merkinnän asianmukaisuus on tarkistettava viimeistään asiakirjaa ulkopuoliselle annettaessa.

Jos asiakirja on saatu toiselta viranomaiselta, turvallisuusluokkaa koskevan merkinnän saa poistaa tai muuttaa ainoastaan asiakirjan laatineen viranomaisen tai sen viranomaisen luvalla, jonka käsiteltäväksi asia kokonaisuudessaan kuuluu, jollei ole selvää, ettei perusteita turvallisuusluokan käytölle enää ole.

6 §

Turvallisuusluokitellun asiakirjan antamisen edellytykset

Valtionhallinnon viranomaisen on ennakolta varmistuttava siitä, että turvallisuusluokitellun asiakirjan suojaamisesta huolehditaan asianmukaisesti, jos se antaa turvallisuusluokitellun asiakirjan muulle kuin valtionhallinnon viranomaiselle. Vaatimus ei koske asianosaisen tiedonsaantioikeuteen perustuvaa tiedon antamista asiakirjan sisällöstä.

Viranomaisen velvollisuudesta huolehtia tietojen salassapidosta ja suojaamisesta luovutettaessa salassa pidettäviä tietoja toimeksiantotehtävän suorittamista varten säädetään viranomaisten toiminnan julkisuudesta annetun lain 26 §:n 3 momentissa.

7 §

Monitasoinen suojaus

Tiedonhallintayksikön on toteutettava turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyn tietojärjestelmän, tietoliikennejärjestelyn ja 9 §:ssä tarkoitetun turvallisuusalueen suojausta vaarantavia tekoja ennaltaehkäiseviä, estäviä ja rajaavia toimenpiteitä, toimenpiteitä suojausta vaarantavien tekojen havaitsemiseksi ja jäljittämiseksi sekä toimenpiteitä vaarantanutta tekoa edeltäneen turvallisuustason palauttamiseksi viipymättä.

8 §

Käsittelyoikeudet ja niiden luettelointi

Turvallisuusluokitellun asiakirjan käsittelyoikeus voidaan antaa vain sille, jolla työtehtäviensä tai muiden valtionhallinnon viranomaisen tehtävien hoitamiseen liittyvän tarpeen vuoksi on tarve saada tietoja asiakirjasta tai muutoin käsitellä sitä ja jolle on selvitetty turvallisuusluokiteltujen tietojen suojaamista koskevat ohjeet ja menettelyt ja joka tuntee asiakirjojen käsittelyä koskevat velvoitteet.

Valtionhallinnon viranomaisen on pidettävä luetteloa henkilöistä, joilla on oikeus käsitellä turvallisuusluokan I, II tai III asiakirjoja. Luettelossa on mainittava henkilön tehtävä, johon turvallisuusluokitellun tiedon käsittelytarve perustuu.

Valtionhallinnon viranomaisen on pidettävä huolta, että se, joka ei enää toimi tehtävissä, joihin oikeus luokiteltujen asiakirjojen käsittelyyn perustuu, palauttaa asiakirjat tai tuhoaa ne asianmukaisella tavalla.

9 §

Turvallisuusalueet

Tiedonhallintayksikön on määritettävä seuraavat fyysisesti suojatut *turvallisuusalueet* turvallisuusluokiteltujen asiakirjojen käsittelyn ja tietojärjestelmien suojaamiseksi 10 §:ssä tarkoitetulla tavalla:

1) hallinnolliset alueet, joilla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamalla henkilöillä on pääsy ilman saattajaa;

2) *turva-alueet*, joilla on selkeästi määritetyt ja suojatut rajat, joilla valvotaan kaikkea kulkua sisään ja ulos kulkuluvuin tai henkilökohtaisesti tunnistamalla ja joihin on pääsy ilman saattajaa vain henkilöillä, joiden luotettavuus on varmistettu ja joilla on erityinen lupa tulla alueelle.

10 §

Asiakirjan käsittelyn ja tietojärjestelmien suojaaminen turvallisuusalueiden avulla

Turvallisuusluokiteltuja asiakirjoja on turvallisuusalueilla ja niiden ulkopuolella käsiteltävä siten, että pääsy turvallisuusluokiteltuihin tietoihin suojataan sivullisilta.

Turvallisuusluokan I asiakirjaa saa säilyttää tai muutoin käsitellä ainoastaan turva-alueilla.

Turvallisuusluokan II–IV asiakirjaa saa käsitellä turvallisuusalueilla ja niiden ulkopuolella kuitenkin siten, että:

1) turvallisuusluokan II tai III asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turva-alueelle;

2) turvallisuusluokan II ja III paperiasiakirjat on säilytettävä turva-alueella;

3) turvallisuusluokan IV asiakirjoja sisältävät tietovarannot ja näiden asiakirjojen käsittelyyn käytetyt tietojärjestelmät on sijoitettava turvallisuusalueelle;

4) turvallisuusluokan IV paperiasiakirjat on säilytettävä turvallisuusalueella.

Sen estämättä, mitä 3 momentin 1 ja 3 kohdassa säädetään tietojärjestelmän sijoittamisesta turvallisuusalueille, turvallisuusluokan II–IV asiakirjoja saa käsitellä myös 9 §:n 1 kohdassa tarkoitetuilla hallinnollisilla alueilla ja niiden ulkopuolella 11 ja 12 §:n vaatimukset täyttävän päätelaitteen ja tietoliikennejärjestelyn avulla. Turvallisuusluokan II asiakirjan käsittelyyn käytetty päätelaite on kuitenkin säilytettävä turva-alueella. Jos turvallisuusluokan III tai IV sähköisiä asiakirjoja säilytetään päätelaitteessa turva-alueiden ulkopuolella, ne on suojattava turvallisuusluokalle riittävän turvallisella salausratkaisulla. Päätelaitteen tietoturvallisuudesta on huolehdittava.

11 §

Tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset

Turvallisuusluokiteltujen asiakirjojen käsittelyyn käytetyt tietojärjestelmät ja tietoliikennejärjestelyt on toteutettava siten, että:

1) ne erotetaan niissä käsiteltävien asiakirjojen turvallisuusluokka huomioon ottaen riittävän luotettavasti alemman turvallisuustason tietojärjestelmistä ja tietoliikennejärjestelyistä;

2) tietoturvallisuutta vaarantavia sähköisiä viestejä vastaan suojaudutaan ja suojauksista sekä niiden toiminnasta huolehditaan tietojärjestelmän ja tietoliikennejärjestelyn koko elinkaaren ajan;

3) tietojärjestelmien käyttäjille annetaan vain ne tiedot, oikeudet tai valtuudet, jotka ovat tehtävien suorittamiseksi välttämättömät;

4) niiden eheys varmistetaan riittävästi;

5) niitä käyttävät henkilöt, laitteet ja tietojärjestelmät tunnistetaan riittävän luotettavasti;

6) niissä otetaan käyttöön vain käyttövaatimusten kannalta välttämättömät toiminnallisuudet;

7) käytetyt salausratkaisut ovat tietojärjestelmässä tai tietoliikennejärjestelyssä käsiteltävien asiakirjojen turvallisuusluokka huomioon ottaen riittävän turvallisia.

Käsiteltäessä turvallisuusluokan I–III asiakirjoja sähköisesti, on pidettävä huolta, että hajasäteilyyn ja elektroniseen tiedusteluun liittyviä riskejä on pienennetty riittävästi. Riskien pienentämiseksi toteutettavat tietoturvallisuustoimenpiteet on suhteutettava tietojen hyväksikäytön riskiin ja turvallisuusluokan tasoon.

12 §

Asiakirjan siirtäminen tietoverkon kautta

Salassa pidettävien tietojen siirtämisestä yleisessä tietoverkossa säädetään tiedonhallintalain 14 §:ssä.

Turvallisuusluokiteltuja asiakirjoja saa siirtää muussa kuin yleisessä tietoverkossa viranomaisen turvallisuusalueiden ulkopuolelle tai kyseistä turvallisuusluokkaa alemman turvallisuustason tietojärjestelmän tai tietoliikennejärjestelyn kautta vain salatussa muodossa. Jos turvallisuusluokiteltujen asiakirjojen siirtäminen tapahtuu turvallisuusalueella muussa kuin yleisessä tietoverkossa ja tietojen riittävä suojaus voidaan toteuttaa fyysisen suojaamisen menetelmin, voidaan käyttää salaamatonta siirtoa tai alemman turvallisuustason salausta.

13 §

Asiakirjan kuljettaminen

Turvallisuusluokiteltuja asiakirjoja saa kuljettaa turvallisuusalueiden ulkopuolelle suojaamalla sähköiset tietovälineet riittävällä salauksella.

Turvallisuusluokan I–III salaamaton asiakirja on kuljettamista varten pakattava asianmukaisesti sekä kuljetettava se jatkuvan valvonnan alaisuudessa vastaanottajalle. Mainittu asiakirjan saa kuljettaa vastaanottajalle myös muulla valtionhallinnon viranomaisen hyväksymällä turvallisella tavalla, jolla asiakirjan luottamuksellisuus ja eheys varmistetaan kyseiselle turvallisuusluokalle riittävällä tavalla.

14 §

Asiakirjan käsittelyn seuraaminen

Turvallisuusluokiteltujen asiakirjojen käsittelyn seuraamiseksi valtionhallinnon viranomaisen on toteutettava seuraavat toimenpiteet:

1) turvallisuusluokan I–III asiakirjan käsittely on rekisteröitävä sähköiseen lokiin, tietojärjestelmään, asiarekisteriin tai asiakirjaan;

2) turvallisuusluokan I–III asiakirjan lähettäminen ja vastaanottaminen on rekisteröitävä;

3) turvallisuusluokan I ja II asiakirjan kopiointia varten on hankittava asiakirjan laatineen viranomaisen lupa;

4) turvallisuusluokan I ja II asiakirjojen kopiot ja niiden käsittelijät on luetteloitava.

Asiakirjojen rekisteröinnistä asiarekisteriin säädetään tiedonhallintalain 25 §:ssä.

1101/2019

15 §

Asiakirjan tuhoaminen

Tarpeettomaksi käynyt turvallisuusluokiteltu asiakirja on tuhottava tavalla, jolla kyseiselle turvallisuusluokalle riittävän luotettavasti estetään tietojen palauttaminen sekä koaminen uudelleen kokonaan tai osittain.

Jos asiakirjan on laatinut toinen viranomainen, tarpeettomaksi käyneen turvallisuusluokan I ja II asiakirjan tuhoamisesta on ilmoitettava asiakirjan laatineelle viranomaiselle, jollei sitä palauteta asiakirjan laatineelle viranomaiselle. Turvallisuusluokan I ja II asiakirjan tuhoamisen saa suorittaa vain henkilö, jonka viranomainen on tähän tehtävään määrännyt. Asiakirjan valmisteluvaiheen versiot voi tuhota ne laatinut henkilö.

16 §

Voimaantulo ja siirtymäsäännökset

Tämä asetus tulee voimaan 1 päivänä tammikuuta 2020.

Turvallisuusluokittelua koskevan 3 §:n mukaisen merkinnän tarve arkistoitujen tai valtionhallinnon viranomaisella säilytettävänä olevien asiakirjojen osalta on arvioitava, jos valtionhallinnon viranomainen ottaa asiakirjan muuhun käsittelyyn.

Jos valtionhallinnon viranomainen ei ole tehnyt tietoturvallisuudesta valtionhallinnossa annetun valtioneuvoston asetuksen (681/2010) 7 §:n mukaista luokittelupäätöstä, sen on saatettava turvallisuusluokiteltujen asiakirjojen käsittely vastaamaan tämän asetuksen 6–15 §:ssä säädettyjä käsittelyvaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta.

Helsingissä 28 päivänä marraskuuta 2019

Kunta- ja omistajaohjausministeri Sirpa Paatero

Lainsäädäntöneuvos Eeva Lantto