Otteita laista tieturvalinjauksiin tutustumisen yhteydessä selailtavaksi.

Finlex › Lainsäädäntö › Säädökset alkuperäisinä › 2019 › 906/2019

906/2019

Laki julkisen hallinnon tiedonhallinnasta

Helsinki

www.finlex.fi

1 §

Lain tarkoitus

Tämän lain tarkoituksena on:

1) varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi;

2) mahdollistaa viranomaisten tietoaineistojen turvallinen ja tehokas hyödyntäminen, jotta viranomainen voi hoitaa tehtävänsä ja tarjota palvelunsa hallinnon asiakkaille hyvää hallintoa noudattaen tuloksellisesti ja laadukkaasti;

3) edistää tietojärjestelmien ja tietovarantojen yhteentoimivuutta.

2 §
Määritelmät

Tässä laissa tarkoitetaan:

8) *tietoturvallisuustoimenpiteillä* tietoaineistojen saatavuuden, eheyden ja luottamuksellisuuden varmistamista hallinnollisilla, toiminnallisilla ja teknisillä toimenpiteillä;

9) *tiedonhallinnalla* viranomaisen tehtävien hoidossa tai sen muussa toiminnassa syntyviin tarpeisiin perustuvia toimia ja tietoturvallisuustoimenpiteitä viranomaisen tietoaineistojen, niiden käsittelyvaiheiden ja tietoaineistoihin sisältyvien tietojen hallinnoimiseksi riippumatta tietoaineistojen tallentamistavasta ja muista käsittelytavoista;

4 §

Tiedonhallinnan järjestäminen tiedonhallintayksikössä

Tässä laissa tarkoitettuja tiedonhallintayksikkojä ovat:

5) kunnat;

Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on:

1) määritelty tässä ja muussa laissa säädettyjen tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut;

2) ajantasaiset ohjeet tietoaineistojen käsittelystä, tietojärjestelmien käytöstä, tietojenkäsittelyoikeuksista, tiedonhallinnan vastuiden toteuttamisesta, tiedonsaantioikeuksien toteuttamisesta, tietoturvallisuustoimenpiteistä sekä poikkeusoloihin varautumisesta;

3) tarjolla koulutusta, jolla varmistetaan, että henkilöstöllä ja tiedonhallintayksikön lukuun toimivilla on riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista;

4) asianmukaiset työvälineet tiedonhallintaa koskevien velvollisuuksien toteuttamiseksi;

5) järjestetty riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta.

5 §

Tiedonhallintamalli ja muutosvaikutuksen arviointi

Tiedonhallintayksikössä on ylläpidettävä sen toimintaympäristön tiedonhallintaa määrittelevää ja kuvaavaa tiedonhallintamallia. Tiedonhallintamallia ylläpidetään palvelujen, asiankäsittelyn ja tietoaineistojen hallinnan suunnittelemiseksi ja toteuttamiseksi, tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttamiseksi, moninkertaisen tietojen keruun vähentämiseksi, tietojärjestelmien ja tietovarantojen yhteentoimivuuden toteuttamiseksi sekä tietoturvallisuuden ylläpitämiseksi.

Tiedonhallintamallin on sisällettävä vähintään tiedot:

5) tietoturvallisuustoimenpiteistä.

Suunniteltaessa tiedonhallintamallin sisältöön vaikuttavia olennaisia hallinnollisia uudistuksia ja tietojärjestelmien käyttöönottoa tiedonhallintayksikössä on arvioitava näihin kohdistuvat muutokset ja niiden vaikutukset suhteessa tiedonhallinnan vastuisiin, 4 luvussa säädettyihin tietoturvallisuusvaatimuksiin ja -toimenpiteisiin.

10 §

Julkisen hallinnon tiedonhallintalautakunta

Valtiovarainministeriön yhteydessä toimii julkisen hallinnon tiedonhallintalautakunta (*tiedonhallintalautakunta*), jonka tehtävänä on:

2) edistää tässä laissa säädettyjen tiedonhallinnan ja tietoturvallisuuden menettelytapojen ja tämän lain vaatimusten toteuttamista.

4 luku
Tietoturvallisuus

12 §
Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen

Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. Henkilöturvallisuusselvityksen laatimisen edellytyksistä säädetään turvallisuusselvityslaissa (726/2014). Työnantajan oikeudesta selvittää työntekijän luotettavuuden arvioimiseksi häntä koskevat luottotiedot ja käsitellä huumausainetestejä koskevia tietoja säädetään yksityisyyden suojasta työelämässä annetussa laissa (759/2004).

13 §

Tietoaineistojen ja tietojärjestelmien tietoturvallisuus

Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan. Tiedonhallintayksikön on selvitettävä olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet riskiarvioinnin mukaisesti.

Viranomaisen tehtävien hoitamisen kannalta olennaisten tietojärjestelmien vikasietoisuus ja toiminnallinen käytettävyys on varmistettava riittävällä testauksella säännöllisesti.

Viranomaisen on suunniteltava tietojärjestelmät, tietovarantojen tietorakenteet ja niihin liittyvä tietojenkäsittely siten, että asiakirjojen julkisuus voidaan vaivatta toteuttaa.

Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet.

Viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista säädetään erikseen.

14 §

Tietojen siirtäminen tietoverkossa

Viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä. Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja.

Käyttäjän tunnistamisesta yleisölle tarjottavissa digitaalisissa palveluissa säädetään digitaalisten palvelujen tarjoamisesta annetussa laissa (306/2019).

15 §

Tietoaineistojen turvallisuuden varmistaminen

Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein, että sen:

1) tietoaineistojen muuttumattomuus on riittävästi varmistettu;

2) tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta;

3) tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys on varmistettu;

4) tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu;

5) tietoaineistojen saatavuutta rajoitetaan vain, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu;

6) tietoaineistot voidaan tarvittavilta osin arkistoida.

Tietoaineistoja on käsiteltävä ja säilytettävä toimitiloissa, jotka ovat tietoaineiston luottamuksellisuuteen, eheyteen ja saatavuuteen liittyvien vaatimusten toteuttamiseksi riittävän turvallisia.

16 §

Tietojärjestelmien käyttöoikeuksien hallinta

Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet. Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina.

17 §

Lokitietojen kerääminen

Viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista. Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.

18 §

Turvallisuusluokiteltavat asiakirjat valtionhallinnossa

Valtion virastoissa ja laitoksissa toimivien viranomaisten, tuomioistuimien ja valitusasioita käsittelemään perustettujen lautakuntien on turvallisuusluokiteltava asiakirjat ja tehtävä niihin turvallisuusluokkaa koskeva merkintä sen osoittamiseksi, minkälaisia tietoturvallisuustoimenpiteitä asiakirjaa käsiteltäessä noudatetaan. Turvallisuusluokkaa koskeva merkintä on tehtävä, jos asiakirja tai siihen sisältyvä tieto on salassa pidettävä viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2, 5 tai 7–11 kohdan perusteella ja asiakirjaan sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa maanpuolustukselle, poikkeusoloihin varautumiselle, kansainvälisille suhteille, rikosten torjunnalle, yleiselle turvallisuudelle tai valtion- ja kansantalouden toimivuudelle taikka muulla niihin rinnastettavalla tavalla Suomen turvallisuudelle.

Turvallisuusluokkaa koskevaa merkintää ei saa käyttää muissa kuin 1 momentissa tarkoitetuissa tapauksissa, ellei merkinnän tekeminen ole tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai asiakirja muutoin liity kansainväliseen yhteistyöhön.

Kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa (588/2004) tarkoitettuihin asiakirjoihin on tehtävä turvallisuusluokituksesta merkintä siten kuin mainitussa laissa säädetään.

Turvallisuusluokittelusta, turvallisuusluokiteltaviin asiakirjoihin tehtävistä merkinnöistä ja turvallisuusluokiteltujen asiakirjojen käsittelyyn liittyvistä tietoturvallisuustoimenpiteistä säädetään tarkemmin valtioneuvoston asetuksella. Asiakirjoihin tehtävistä salassapitoa koskevista merkinnöistä säädetään viranomaisten toiminnan julkisuudesta annetun lain 25 §:ssä.

19 §

Tietoaineistojen sähköiseen muotoon muuttaminen ja saatavuus

Jos asiakirja saapuu viranomaiselle muussa kuin sähköisessä muodossa, on se muutettava sähköiseen muotoon, jos asiakirja on säädetty pysyvästi säilytettäväksi taikka lailla tai lain nojalla arkistoitavaksi. Viranomainen vastaa siitä, että sähköiseen muotoon muutetun asiakirjan luotettavuus ja eheys varmistetaan. Viranomaisen laatimat asiakirjat säilytetään sähköisesti. Sähköiseen muotoon muuttamisesta ja säilyttämisestä voidaan poiketa, jos se on välttämätöntä turvallisuusluokiteltavien asiakirjojen käsittelyä koskevien vaatimusten, muiden tietoturvallisuusvaatimusten tai muun asiakirjan luonteeseen liittyvän välttämättömän syyn vuoksi.

21 §

Tietoaineistojen säilytystarpeen määrittäminen

Jos tietoaineistojen tai asiakirjojen säilytysajasta ei ole säädetty laissa, säilytysaikoja määritettäessä on otettava huomioon:

Säilytysajan päättymisen jälkeen tietoaineistot on arkistoitava tai tuhottava viipymättä tietoturvallisella tavalla.

30 §
Siirtymäsäännökset

Tiedonhallintayksikköjen on laadittava 5 §:n mukainen tiedonhallintamalli 12 kuukauden kuluessa tämän lain voimaantulosta.

Muiden kuin valtion virastoissa ja laitoksissa toimivien viranomaisten on toteutettava 12–16 §:ssä säädetyt vaatimukset 36 kuukauden kuluessa tämän lain voimaantulosta.

Tämän lain 17 ja 22–24 §:n säännöksiä sovelletaan lain voimaantulon jälkeen hankittaviin tietojärjestelmiin. Ennen tämän lain voimaantuloa hankittuihin tietojärjestelmiin sovelletaan 22–24 §:ssä säädettyjä tietojen sähköistä luovutustapaa koskevia vaatimuksia päivitettäessä tietojärjestelmien teknisiä rajapintoja tai katseluyhteyksiä, kuitenkin viimeistään 48 kuukauden kuluttua lain voimaantulosta, ja 17 §:ssä edellytettyjä lokitietojen keräämistä koskevia vaatimuksia 24 kuukauden kuluttua tämän lain voimaantulosta.

29 §

Voimaantulo

Tämä laki tulee voimaan 1 päivänä tammikuuta 2020.

Voimaantulo ja siirtymäsäännökset