VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tietoturvallisuusvaatimukset viranomaistoiminnassa

Kirsi Janhunen, erityisasiantuntija, CISM, CRISC
26.2.2020
Tiedonhallintalain aluekierros, Helsinki

Aiheet

- Keskeisiä käsitteitä
- Mikä muuttuu aikaisemmasta ja mikä pysyy
- Keskeiset tietoturvallisuuteen liittyvät kohdat laissa
- Tukea toimeenpanoon

Tietoturvallisuudessa ja tiedonhallinnassa kokenutkin asiantuntija joutuu varmistamaan, että puhuu toisen kanssa samoilla käsitteillä.

Keskeisiä käsitteitä tiedonhallintalain kannalta

Tietoturvallisuus on tietojen saatavuutta, eheyttä ja luottamuksellisuutta varmistamista.

Tietoturvallisuustoimenpiteillä tarkoitetaan hallinnollisia, toiminnallisia ja teknisiä toimenpiteitä tietoturvallisuuden varmistamiseksi.

Riski on todennäköisyyden ja seurauksen yhdistelmä.

Riskienhallinta on seurauksiltaan merkittävien ei-toivottujen tapahtumien (riskien) järjestelmällistä määrittelyä ja niihin varautumista.

Jäännösriski on jäljelle jäävä riski, jota ei voida tai haluta poistaa.

Keskeisiä käsitteitä tiedonhallintalain kannalta

Asiakirjalla tarkoitetaan kirjallisen ja kuvallisen esityksen lisäksi sellaista käyttönsä vuoksi yhteen kuuluviksi tarkoitetuista merkeistä muodostuvaa tiettyä kohdetta tai asiaa koskevaa viestiä, joka on saatavissa selville vain automaattisen tietojenkäsittely tai äänen- ja kuvantoistolaitteen taikka muiden apuvälineiden avulla. (JulkL 5.1 §)

Salassapidolla tarkoitetaan tiedon suojaamista oikeudettomalta käsittelyltä tai paljastumiselta.

Salassa pidettävä viranomaisen asiakirja (ellei erikseen toisin säädetty) JulkL 24 § 1-31 kohtien perusteella salassa pidettävä asiakirja.

Mikä muuttuu ja mikä pysyy tietoturvallisuuden osalta?

Mikä mm. muuttuu aikaisemmasta ja mikä pysyy

- Tiedonhallintalaki koskee koko julkista hallintoa (yleislaki)
- Riskienhallinnan merkitys kasvaa tietoturvatoimenpiteiden suunnittelussa.
- Valtionhallinnossa käytössä ollut suojaustasoluokitus (STIV-STI) häviää, asiakirjojen suojaamisessa korostuu riskienhallinta
- Valtionhallintoa koskeva turvallisuusluokitusasetus edelleen neliportainen (TLIV-TLI)
- Julkisuusperiaate säilyy, tiedon salassapidolle tulee aina löytyä säädösperuste

Tietoturvallisuuteen liittyvät keskeiset kohdat tiedonhallintalaissa

Tiedonhallinnan vastuiden määrittely

Tiedonhallintamallin ylläpitovastuu

Muutosvaikutusarvioinnista vastaavat tiedonhallintayksikön toiminnot

Asiakirjajulkisuuskuvauksen ylläpidosta vastaavat toimijat

Tietoturvallisuustoimenpiteistä vastaavat toimijat

Tietojärjestelmien toiminnasta ja laadunvarmistamisesta vastaavat virkamiehet

Asianhallinnasta vastaava virkamies

Säilytysaikojen määrittelystä vastaava virkamies

Valvonnan toteuttamisvastuu

Asiakirjapyyntöihin vastaavat virkamiehet

Asiakirjojen antamista koskevat päätöksentekovastuut

Tietosuojavastaava

Rekisterinpitäjät ja niiden edustajat

Arkistotoimesta vastaava virkamies tai toimihenkilö

Tiedonhallintalaki

Tietosuoja-asetus

Julkisuuslaki

Arkistolaki

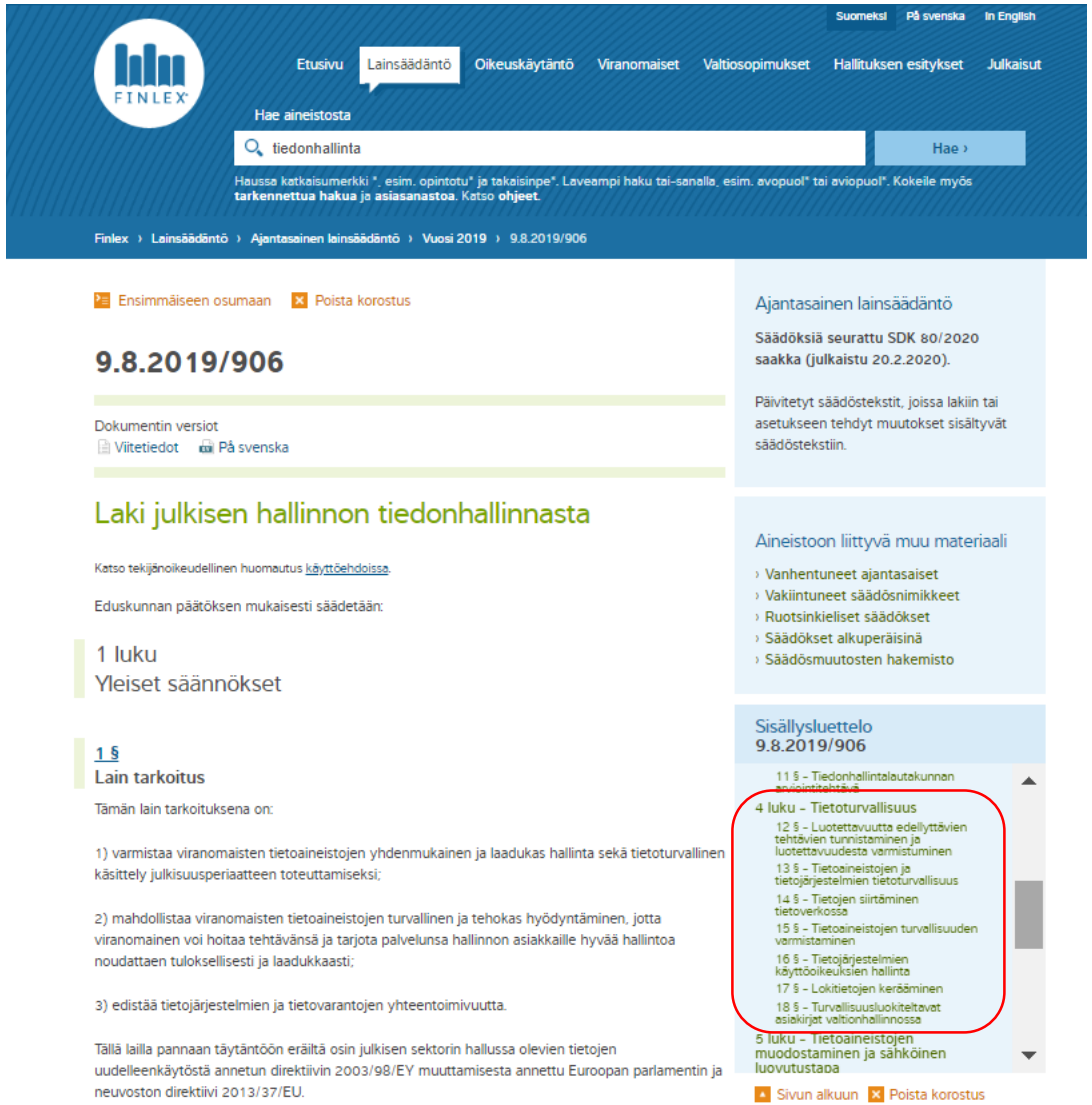
VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Lain rakenne karkeasti

- **1 luku (1-3 §) Yleiset säännökset**
- **2 luku (4-5 §) Tiedonhallinnan järjestäminen**
  - tiedonhallintayksikön johdon vastuut
- **3 luku (6-11 §) Julkisen hallinnon tiedonhallinnan yleinen ohjaus**
  - 6-7 § VM:n vastuut, ministeriöiden vastuut omalla toimialallaan
  - 8-9 § valtion tiedonhallintayksiköiden vastuut muutosten arvioinneissa
  - 10-11 § tiedonhallintalautakunta ja sen tehtävät
- **4 luku (12-18 §) Tietoturvallisuus**
  - 12-13 § tiedonhallintayksikön vastuut
  - 14-18 § viranomaistason vastuut
- **5 luku (19-24 §) Tietoaineistojen muodostaminen ja sähköinen luovutustapa**
  - Viranomaistason vastuut
- **6 luku (25-28 §) Asianhallinta ja palvelujen tiedonhallinta**
  - Tiedonhallintayksikön vastuut
- **7 luku (29-30 §) Erinäiset säännökset**
  - Voimaantulo, siirtymäsäännökset

Tietoturvatoimenpiteistä vastaavalle vinkkejä lain läpikäyntiin

www.finlex.fi



VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

4 luku
Tietoturvallisuus

12 §
Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen

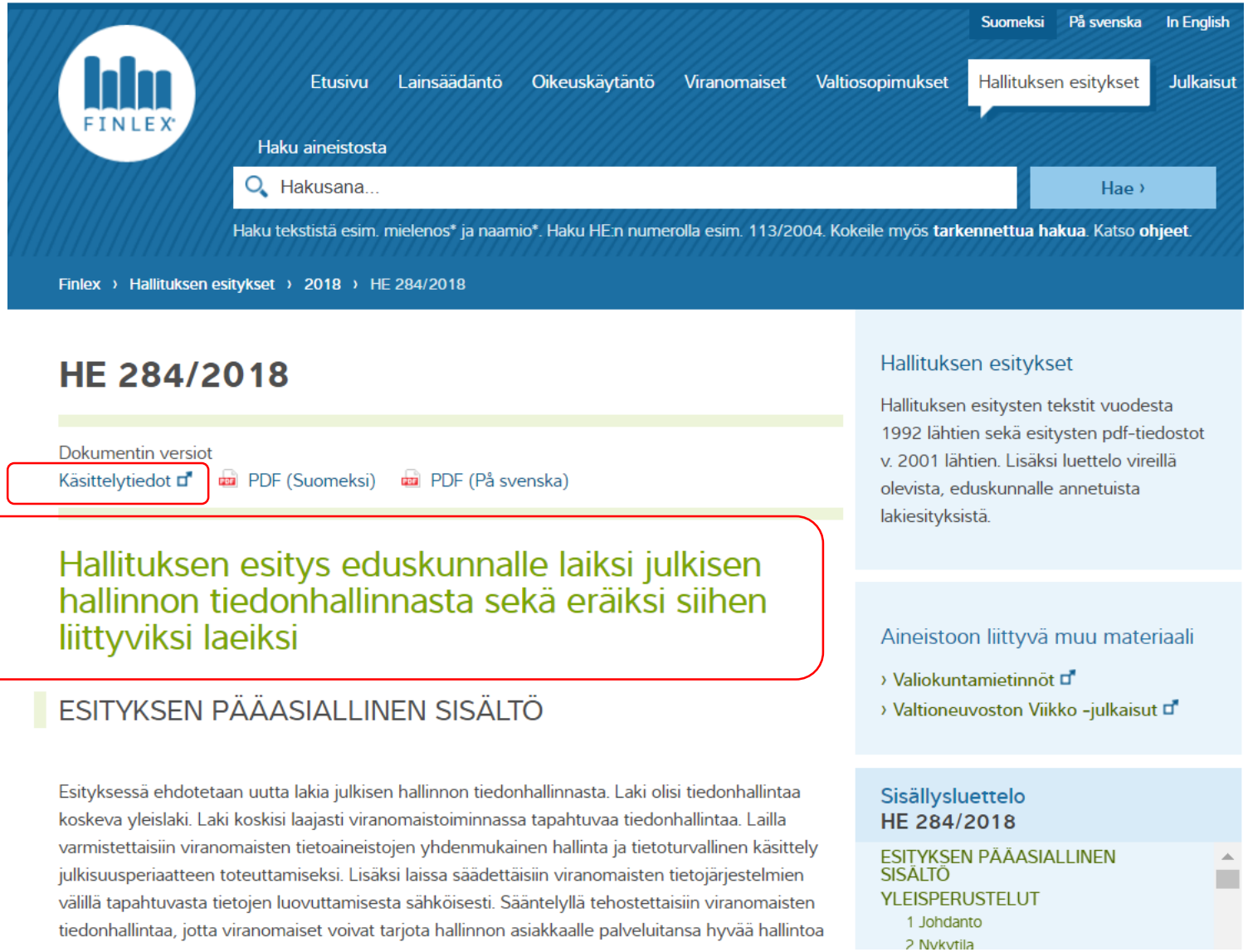
Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta. Henkilöturvallisuusselvityksen laatimisen edellytyksistä säädetään turvallisuusselvityslaissa (726/2014). Työnantajan oikeudesta 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.

www.finlex.fi



Tutustutaan seuraavaksi keskeisiin pykäliin.

Pohdinnat on merkitty näin 

Jos kohdasta löytyy suositus tai sen luonnos, se on merkitty näin ★

4.2 § Tiedonhallintayksikön johdon velvoitteita huolehtia

- tiedonhallinnan toteuttamiseen liittyvien vastuiden määrittämisestä,
- ajantasaisista ohjeista,
- koulutuksesta,
- työvälineistä ja
- valvonnasta.

Miten nämä toteutetaan tietoturvallisuuden näkökulmasta?

Löytyykö yhteinen kieli johdon ja tietoturvavastaavien välillä?

Luvussa 4 Tietoturvallisuus on 12 – 18 §:t

- 12 § Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen
- 13 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus
- 14 § Tietojen siirtäminen tietoverkoissa
- 15 § Tietoaineistojen turvallisuuden varmistaminen
- 16 § Tietojärjestelmien käyttöoikeuksien hallinta
- 17 § Lokitietojen kerääminen
- 18 § Turvallisuusluokiteltavat asiakirjat valtionhallinnossa

12 § Tehtävät, joiden suorittaminen edellyttää henkilöiltä erityistä luotettavuutta on tunnistettu

- Sellaisten työtehtävien ja roolien tunnistaminen, jossa edellytetään luotettavuutta sekä sen varmistamista.
- Henkilöturvallisuusselvityksen edellytyksistä säädetään turvallisuusselvityslaissa (726/2014).
- Työnantajan oikeudesta selvittää luottotiedot ja käsitellä huumausainetestejä koskevia tietoja säädetään laissa yksityisyyden suojasta työelämässä (759/2004)

Kannattaisiko erityistä luotettavuutta edellyttävät tehtävät ja roolit luetteloida? Olisiko luettelolla käyttöä käyttöoikeushallinnassa ja lokienhallinnassa?

13 § 1 mom. Toimintaympäristön tietoturvallisuuden tilaa seurataan

- Tiedonhallintayksikön tulee seurata toimintaympäristön tietoturvallisuuden tilaa ja selvittää tietojenkäsittelyyn kohdistuvat riskit.

Miten varmistetaan, että tietoturvallisuuden tilaa pystytään seuraamaan myös ulkoa hankituissa palveluissa? 

13 § 1 mom. Tietoturvallisuus varmistetaan tiedon ja järjestelmien elinkaaren ajan

- Tietoturvallisuus huomioidaan tiedon elinkaaressa luomisesta hävittämiseen
- Tietoturvallisuudesta huolehditaan järjestelmien vaatimusmäärittelystä käytöstä poistoon

Miten käsitellään sellaisia tietoja, joihin kohdistuu erityisiä vaatimuksia? 

Miten huolehditaan siitä, että tiedonhallintaympäristössä tapahtuvat muutokset eivät vaaranna tietoturvaa? 

13 § 1 mom. Tietoriskien hallinta ja siihen perustuvat tietoturvatoimet on järjestetty

- Tietoriskien hallinta on järjestettyä ja järjestelmällistä toimintaa.
- Riskiarviointi ohjaa tietoturvatoimien mitoittamista.

Millainen riskienhallintaprosessi toimii parhaiten monimutkaisessa ja jatkuvasti muuttuvassa ympäristössä? 

Tekeekö johto viimekädessä päätöksiä keskeisistä riskeistä? 

13 § 2 mom. Vikasietoisuus ja toiminnallinen käytettävyys on varmistettu

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

Onko viranomaisen tehtävien kannalta olennaiset tietojärjestelmät tunnistettu? 

Ymmärretäänkö tietojärjestelmien ja toimintojen riippuvuuksia?

Miten em. tietoja ylläpidetään?

13 § 3 mom. Julkisuus ja salassapitorakenne on huomioitu tietovarantojen tietorakenteissa

- Suunnittelussa ja toteutuksessa huomioidaan, että tietoturvatoimet eivät turhaan haittaa asiakirjojen julkisuuden toteuttamista.

Miten varmistetaan, että tiedot on tarvittaessa luovutettavissa? Löytyykö tiedot riittävän helposti? 

13 § 4 mom. Hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet,

- Viranomainen huolehtii tietoturvallisuudesta hankinnoissa.
- Tietoturvallisuus huomioidaan hankintaprosessissa (vaatimusmäärittely, hankinta, sopimus, toimittajayhteistyö..)

Miten varmistetaan, että tietoturvavaatimukset saadaan riittävällä tavalla mukaan palvelusopimukseen ja yhteistyöhön? 

14 § 1 mom. Salassa pidettävät tiedot on suojattu yleisessä tietoverkossa tietoja siirrettäessä

- Viranomaisen tietojensiirto on salattu tai muuten suojattu, jos tiedot ovat salassa pidettäviä.
- Lisäksi vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin tämä pääsee käsittelemään siirrettyjä salassa pidettyjä tietoja.

Mikä on riittävän turvallinen tapa? 

15 § Tietoaineistojen turvallisuus on varmistettu

- Muuttumattomuus
- Suojaus teknisiltä ja fyysisiltä vahingoilta
- Alkuperäisyys, ajantasaisuus ja virheettömyys
- Saatavuus ja käyttökelpoisuus
- Saatavuutta rajoitetaan vain, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu
- Tietoaineistot voidaan tarvittavilta osin arkistoida

Miten nämä toteutetaan? 

15.2 § Tietoaineistoja käsitellään riittävän turvallisissa tiloissa

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

Miten toteutetaan? 

16 § Käyttöoikeudet on määritelty ja hallittu tietojärjestelmissä

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

Miten varmistetaan, että tiedot pysyvät ajantasaisina? 

17 § Tarpeelliset lokitiedot on kerätty

- Viranomainen huolehtii, että tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista.

Miten pitkään tietoja tulee säilyttää? Miten helposti ne tulee olla saatavilla ja kenen toimesta? 

18 § 1 mom. Turvallisuusluokiteltavista asiakirjoista ja niiden käsittelystä on huolehdittu

- 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.

Mitä käytännössä tarkoittaa?

https://www.finlex.fi/fi/laki/alkup/2019/20191101

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa

1 § – Soveltamisala

2 § – Määritelmät

3 § – Turvallisuusluokittelu ja turvallisuusluokan merkitseminen

4 § – Turvallisuusluokituksen vastaavuus kansainvälisiä tietoturvallisuusvelvoitteita toteutettaessa

5 § – Turvallisuusluokkaa koskevan merkinnän poistaminen tai muuttaminen

6 § – Turvallisuusluokitellun asiakirjan antamisen edellytykset

7 § – Monitasoinen suojaus

8 § – Käsittelyoikeudet ja niiden luettelointi

9 § – Turvallisuusalueet

10 § – Asiakirjan käsittelyn ja tietojärjestelmien suojaaminen turvallisuusalueiden avulla

11 § – Tietojärjestelmiä ja tietoliikennejärjestelyjä koskevat vaatimukset

12 § – Asiakirjan siirtäminen tietoverkon kautta

13 § – Asiakirjan kuljettaminen

14 § – Asiakirjan käsittelyn seuraaminen

15 § – Asiakirjan tuhoaminen

16 § – Voimaantulo ja siirtymäsäännökset

Turvallisuusluokitusasetuksesta 1101/2019

3 §
Turvallisuusluokittelu ja turvallisuusluokan merkitseminen

Tiedonhallintalain 18 §:n 1 momentissa tarkoitetut 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 tarkoitetulle 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 tarkoitetulle 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 tarkoitetulle 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 tarkoitetulle suojattavalle edulle.

Edellä 1 momentissa tarkoitetut 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”.

Tukea toimeenpanoon antaa jatkossa tiedonhallintalautakunta. Suosituksia on kuitenkin jo luonnosteltu.

Tiedonhallintaa avaavat soveltamiskortit (ollut kommenteilla joulukuussa 2019)

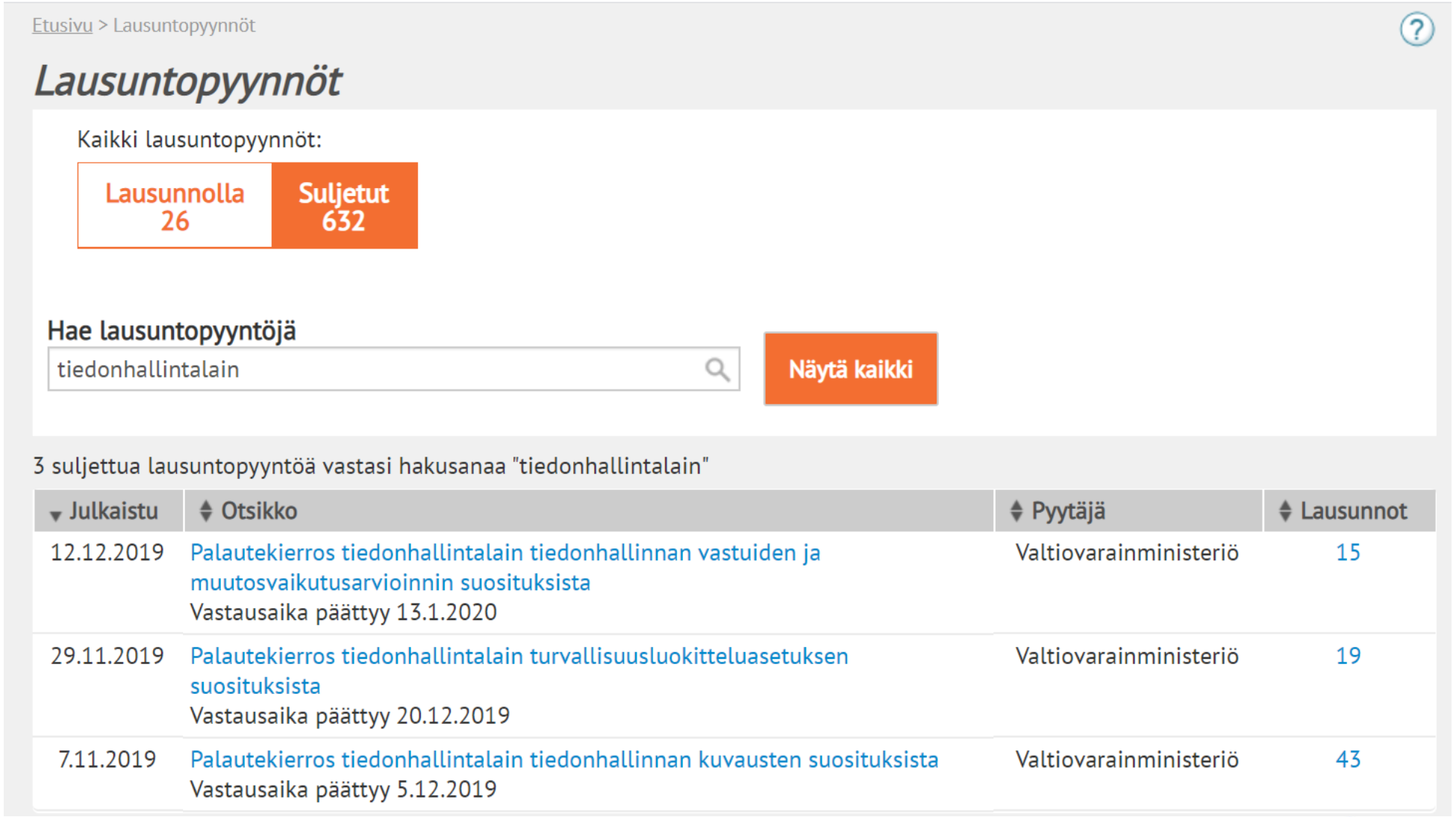
- Kortti 13 § Elinkaaren huomioiminen tietojen käsittelyssä
- Kortti 13 § Elinkaaren huomioiminen tietojärjestelmissä
- Kortti 13 § Riskienhallinta
- Kortti 13 § Tietoturvallisuus hankinnoissa
- Kortti 15 § Vahingoilta suojaaminen
- Kortti 17 § Lokitietojen kerääminen
- Suositus teknisistä rajapinnoista ja katseluyhteyksistä
- https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=2ca7718d-f53f-4efb-9619-f7ce5ac39057

Muut joulukuussa kommenteilla olleet soveltamiskortit

- Kortti JulkL Asiakirja merkinnät
- Kortti TLasetus 10 § Asiakirjan käsittely ja suojaaminen
- Kortti TLasetus 11 § Salausratkaisut
- Kortti TLasetus 11 § Tietojärjestelmien erottelu
- Kortti TLasetus 3 § Turvallisuusluokan merkitseminen
- Kortti TLasetus 9 § Hallinnolliset alueet
- Kortti TLasetus 9 § Turva-alueet

- https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=55acfba0-0e0a-4495-b63d-2851665c03b2

Suositusluonnokset löytyvät lausuntopalvelu.fi -sivustolta



Etusivu > Lausuntopyynnöt

Lausuntopyynnöt

Kaikki lausuntopyynnöt:

Lausunnolla 26 | Suljetut 632

Hae lausuntopyyntöjä

tiedonhallintalain

Näytä kaikki

3 suljettua lausuntopyyntöä vastasi hakusanaa "tiedonhallintalain"

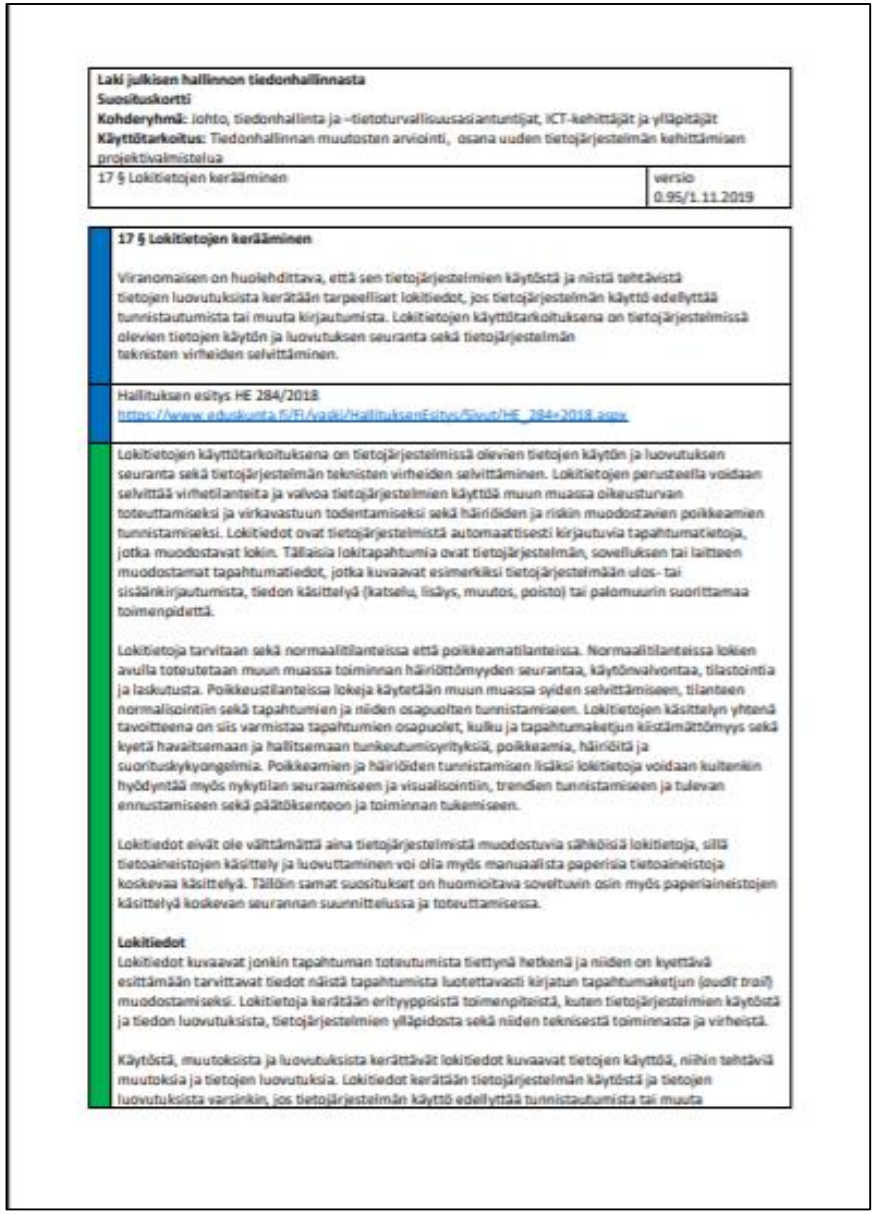
Julkaistu	Otsikko	Pyytäjä	Lausunnot
12.12.2019	Palautekierros tiedonhallintalain tiedonhallinnan vastuiden ja muutosvaikutusarvioinnin suosituksista Vastausaika päättyy 13.1.2020	Valtiovarainministeriö	15
29.11.2019	Palautekierros tiedonhallintalain turvallisuusluokitteluasetuksen suosituksista Vastausaika päättyy 20.12.2019	Valtiovarainministeriö	19
7.11.2019	Palautekierros tiedonhallintalain tiedonhallinnan kuvausten suosituksista Vastausaika päättyy 5.12.2019	Valtiovarainministeriö	43

Soveltamiskortti

Otsikkotiedot

Säännös/säännökset

Soveltamisesimerkki
(Ei velvoittava)



Laki julkisen hallinnon tiedonhallinnasta
Suosituskortti
Kohderyhmä: Johto, tiedonhallinta ja –tietoturvallisuusasiantuntijat, ICT-kehittäjät ja ylläpitäjät
Käyttötarkoitus: Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua

17 § Lokitietojen kerääminen	versio 0.95/1.11.2019

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.

Hallituksen esitys HE 284/2018
https://www.edustakunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_284+2018.aspx

Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen. Lokitietojen perusteella voidaan selvittää virhetilanteita ja vahvoa tietojärjestelmien käyttöä muun muassa oikeusturvan toteuttamiseksi ja virkavastuun todentamiseksi sekä häiriöiden ja riskin muodostavien poikkeamien tunnistamiseksi. Lokitiedot ovat tietojärjestelmistä automaattisesti kirjautuvia tapahtumatietoja, jotka muodostavat lokin. Tällaisia lokitapahtumia ovat tietojärjestelmän, sovelluksen tai laitteen muodostamat tapahtumatiedot, jotka kuvaavat esimerkiksi tietojärjestelmään ulos- tai sisäänkirjautumista, tiedon käsittelyä (katselu, lisäys, muutos, poisto) tai palomuurin suorittamaa toimenpidettä.

Lokitietoja tarvitaan sekä normaalitilanteissa että poikkeamatilanteissa. Normaalitilanteissa lokien avulla toteutetaan muun muassa toiminnan häiriöttömyyden seurantaa, käytönvalvontaa, tilastointia ja laskutusta. Poikkeustilanteissa lokeja käytetään muun muassa syiden selvittämiseen, tilanteen normalisointiin sekä tapahtumien ja niiden osapuolten tunnistamiseen. Lokitietojen käsittelyn yhtenä tavoitteena on siis varmistaa tapahtumien osapuolet, kulku ja tapahtumaketjun kiistämättömyys sekä kyetä havaitsemaan ja hallitsemaan tunkeutumisyrityksiä, poikkeamia, häiriöitä ja suorituskykyongelmia. Poikkeamien ja häiriöiden tunnistamisen lisäksi lokitietoja voidaan kuitenkin hyödyntää myös nykytilan seuraamiseen ja visualisointiin, trendien tunnistamiseen ja tulevan ennustamiseen sekä päätöksentoon ja toiminnan tukemiseen.

Lokitiedot eivät ole välttämättä aina tietojärjestelmistä muodostuvia sähköisiä lokitietoja, sillä tietoaineistojen käsittely ja luovuttaminen voi olla myös manuaalista paperisia tietoaineistoja koskevaa käsittelyä. Tällöin samat suositukset on huomioitava soveltuvin osin myös paperiaineistojen käsittelyä koskevan seurannan suunnittelussa ja toteuttamisessa.

Lokitiedot
Lokitiedot kuvaavat jonkin tapahtuman toteutumista tiettynä hetkenä ja niiden on kyettävä esittämään tarvittavat tiedot näistä tapahtumista luotettavasti kirjatun tapahtumaketjun (audit trail) muodostamiseksi. Lokitietoja kerätään erityyppisistä toimenpiteistä, kuten tietojärjestelmien käytöstä ja tiedon luovutuksista, tietojärjestelmien ylläpidosta sekä niiden teknisestä toiminnasta ja virheistä.

Käytöstä, muutoksista ja luovutuksista kerättävät lokitiedot kuvaavat tietojen käyttöä, niihin tehtäviä muutoksia ja tietojen luovutuksia. Lokitiedot kerätään tietojärjestelmän käytöstä ja tietojen luovutuksista varsinkin, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta

Esimerkki soveltamissuunnitelmasta yksinkertaistettuna

Vaatimus	Mitä vaatimus käytännössä tarkoittaa organisaation kannalta	Annettu määräaika	Vaatimuksen tilanne	Toimenpiteet, vastuut

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Kiitos!

Kirsi.janhunen@vm.fi
Puhelin 029 553 0428
Twitter @KirsiJanhunen