Tiedonhallintalautakunta
Informationshanteringsnämnden

Tiedonhallintalain vaatimusten toteuttaminen I

20.3.2025
Tiedonhallintalain vaatimusten toteuttaminen I - webinaari

Tilaisuuden ohjelma

klo 13.00 – 13.05 **Tilaisuuden avaus**

Tiedonhallintalautakunnan pääsihteeri Tommi Oikarinen

klo 13.05 – 13.15 **Tiedonhallintalaki – viranomaisten tiedonhallintaa sääntelevä yleislaki**

Tiedonhallintalautakunnan sihteeri Sami Aalto

klo 13.15 – 14.05 **Tiedonhallinnan järjestämistä koskevat vaatimukset – tiedonhallintalain 2 luku**

Tiedonhallintalautakunnan pääsihteeri Tommi Oikarinen

klo 14.05 – 14.55 **Tietoturvallisuus – tiedonhallintalain 4 luku**

Tiedonhallintalautakunnan sihteeri Sami Aalto

klo 14.55 – 15.00 **Tilaisuuden päätössanat**

Tiedonhallintalautakunnan pääsihteeri Tommi Oikarinen

Laki julkisen hallinnon tiedonhallinnasta (906/2019)

Tiedonhallintalaki (906/2019)

- Tiedonhallinnan järjestäminen (2 luku)
- Tiedonhallinnan yleinen ohjaus (3 luku)
- Tietoturvallisuus (4 luku)
- Kyberturvallisuusvelvollisuudet (uusi 4 a luku)
- Tietoaineistojen muodostaminen ja sähköinen luovutustapa (5 luku)
- Asianhallinta (6 luku)
- Automaattinen ratkaisumenettely (6 a luku)

- Viranomaisten tiedonhallintaa sääntelevä yleislaki
- varmistaa viranomaisten tietoaineistojen yhdenmukaisen ja laadukkaan hallinnan sekä tietoturvallisen käsittelyn julkisuusperiaatteen toteuttamiseksi
- mahdollistaa viranomaisten tietoaineistojen turvallisen ja tehokkaan hyödyntämisen, jotta viranomainen voi hoitaa tehtävänsä ja tarjota palvelunsa hallinnon asiakkaille hyvää hallintoa noudattaen tuloksellisesti ja laadukkaasti;
- edistää tietojärjestelmien ja tietovarantojen yhteentoimivuutta

Soveltamisala (3 §)

- Sovelletaan tiedonhallintaan ja tietojärjestelmien käyttöön, kun *viranomaiset* käsittelevät tietoaineistoja, jollei muualla laissa toisin säädetä. Lain 6 a lukua sovelletaan automaattisen ratkaisumenettelyn käyttöönottoon ja käyttöön.
- Julkisen hallinnon tiedonhallinnon ohjausta koskevaa sääntelyä (3 luku) ei sovelleta:
  - ylimpien laillisuusvalvojien, tuomioistuimien eikä valitusasioita käsittelemään perustettujen lautakuntien toimintaan
  - tasavallan presidentin kansliaan
  - eduskunnan virastoihin
  - Kansaneläkelaitokseen, Suomen Pankkiin, muihin itsenäisiin julkisoikeudellisiin laitoksiin
  - yliopistolaissa tarkoitettuihin yliopistoihin eikä ammattikorkeakoululaissa tarkoitettuihin ammattikorkeakouluihin

Soveltamisala (3 §)

- Julkista hallintotehtävää hoitaviin yksityisiin henkilöihin tai yhteisöihin taikka muihin kuin viranomaisena toimiviin julkisoikeudellisiin yhteisöihin sovelletaan sääntelyä
  - tietoturvallisuudesta (4 lukua)
  - sähköisestä luovutustavasta (22–24 §)
  - asiakirjarekisteristä ja tietoaineistojen hallinnasta palvelua tuotettaessa sekä
  - automaattisesta ratkaisumenettelystä (6 a luku)
- Lisäksi tiettyjä säännöksiä (tiedonhallinnan järjestäminen, tietojen saatavuus, asiakirjajulkisuuskuvaus) sovelletaan yksityisiin ja yhteisöihin näiden käyttäessä julkista valtaa.
- Lakia ei sovelleta Ahvenanmaan maakunnassa toimiviin valtion viranomaisiin.
  - Lain 13 a §:ää ja 6 a lukua sovelletaan kuitenkin Ahvenanmaalla toimiviin valtion viranomaisiin niiden hoitaessa sellaisia valtakunnan lainsäädäntövaltaan kuuluvia viranomaistehtäviä, joissa tehdään hallintolain 53 e §:ssä tarkoitettuja asian automaattisia ratkaisuja.

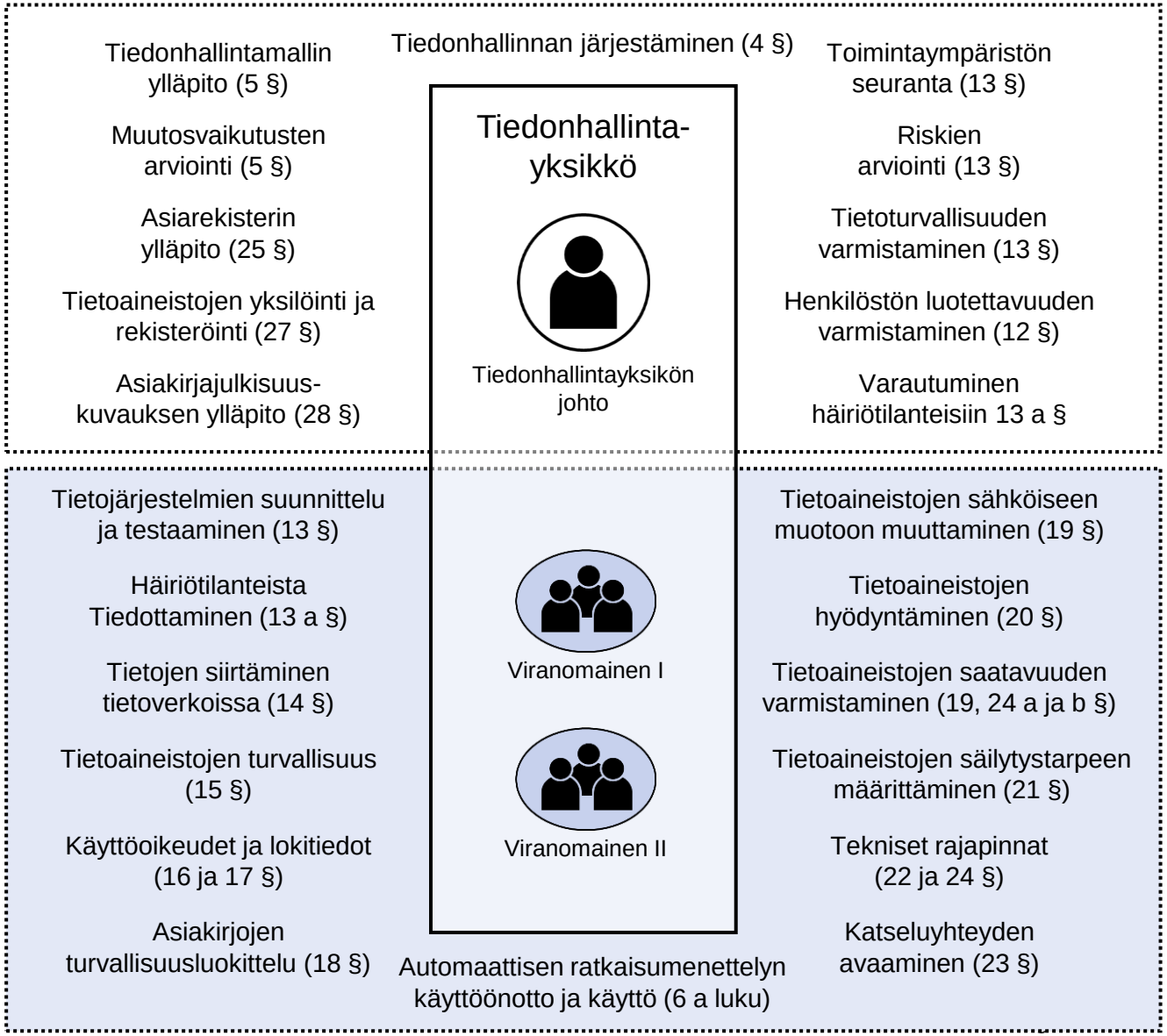
Tiedonhallinnan järjestäminen tiedonhallintayksiköissä (TiHL 2 luku)

Tiedonhallintayksikkö (4.1 §)

- Tiedonhallintalaissa tarkoitettuja tiedonhallintayksiköitä ovat:
  1) valtion virastot ja laitokset
  2) tuomioistuimet ja valitusasioita käsittelemään perustetut lautakunnat
  3) eduskunnan virastot
  4) valtion liikelaitokset
  5) hyvinvointialueet
  6) hyvinvointiyhtymät
  7) kunnat
  8) kuntayhtymät
  9) itsenäiset julkisoikeudelliset laitokset
  10) yliopistolaissa tarkoitetut yliopistot sekä ammattikorkeakoululaissa tarkoitetut ammattikorkeakoulut
- Tiedonhallintalaissa viranomainen kuuluu tiedonhallintayksikköön
- Tiedonhallintalain 4.1 §:ssä säädetään tyhjentävästi, mitkä viranomaiset ovat tiedonhallintayksiköitä

Tiedonhallintayksikkö ja viranomainen

- Tiedonhallintalaissa osa velvollisuuksista on säädetty koskemaan **tiedonhallintayksikköä** (organisaatio, joka koostuu yhdestä tai useammasta viranomaisesta)
  - ➔ tosiasiassa tiedonhallinnan järjestäminen on yleensä järjestetty organisaatiotasolla, vaikka organisaatio koostuisi useammasta viranomaisesta.
    - Kunta koostuu useista viranomaisista
    - Valtionhallinnossa työnantajavastuut kohdistuvat useasta viranomaisesta koostuvaan työnantajavirastoon
- Osa velvollisuuksista kohdistuu **julkisuuslaissa tarkoitettuihin viranomaisiin**, jotka ovat toimivaltaisia käsittelemään tietoaineistoja ja päättämään niiden käytöstä ja luovuttamisesta



Tiedonhallinnan järjestäminen (4.2 §)

- Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on:
  1) **määritelty** tiedonhallintalaissa 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.
- Tiedonhallintalaissa tiedonhallintayksikön johdolla tarkoitetaan sitä viranomaista tai virkamiestä, joka vastaa tiedonhallintayksikön, kuten valtion viraston tai kunnan, yleisjohdosta.
- **Suositus johdon vastuiden toteuttamisesta tiedonhallinnassa** (VM 2020:18)

Tiedonhallintayksikön johto (esimerkki)

Tiedonhallintayksikkö	Tiedonhallintayksikön johto
valtion virasto tai laitos	Virastopäällikkö, kuten pääjohtaja, ylijohtaja tai kansliapäällikkö (ministeriöt)
Kunta	Kunnanhallitus yhdessä kunnanjohtajan kanssa
Kuntayhtymä	Yhtymähallitus yhdessä kuntayhtymän johtajan kanssa (yhden toimielimen kuntayhtymässä ko. toimielin)
Hyvinvointialue	Aluehallitus yhdessä hyvinvointialuejohtajan kanssa
Hyvinvointiyhtymä	Yhtymähallitus yhdessä toimitusjohtajan kanssa
Tuomioistuimet	Tuomioistuimen päällikkötuomari
Valitusasioiden lautakunnat	Puheenjohtaja
Eduskunnan virastot	Virastopäällikkö
Valtion liikelaitokset	Liikelaitoksen hallitus yhdessä toimitusjohtajan kanssa
Itsenäiset julkisoikeudelliset laitokset	Laitoksen hallitus yhdessä johtajan kanssa
Yliopistot	Yliopiston hallitus yhdessä rehtorin kanssa
Ammattikorkeakoulut	Hallitus yhdessä rehtorin (toimitusjohtaja) kanssa

Tiedonhallinnan vastuiden määrittely (4.2 § 1 k)

- Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on määritelty tiedonhallinnan toteuttamiseen liittyvien tehtävien vastuut:
  - Tiedonhallintalaissa säädetyt vastuut
  - Muussa laissa säädetyt vastuut
- Konkreettisten vastuiden määrittäminen siitä, miten ja kenen vastuulla on toteuttaa lain mukaiset tiedonhallinnan velvoitteet ja palvelut
- Johdon tehtävänä määrittää myös, miten vastuut ja niihin liittyvät tehtävät jakautuvat tiedonhallintayksikössä

Tiedonhallinnan vastuiden määrittelyssä on huomioitava, että tiedonhallintalaissa vastuut ja velvollisuudet on säädetty jonkin viranomaisen tehtäviksi. Vastuita voidaan ulkoistaa vain perustuslain 124 §:n edellytysten täyttyessä.

Tiedonhallintalaki ei mahdollista tiedonhallinnan vastuiden delegointia yksityisoikeudellisille yhteisöille, ellei muualla ole toisin säädetty

Tiedonhallinnasta yleislainsäädännössä säädettyjä vastuita

Tiedonhallintayksikkö (organisaatiotasoiset vastuut)

Tiedonhallintayksikön johto (TiHL 4.2 §)	**Tiedonhallintamallin ylläpidosta vastaava** (TiHL 5.1 §)	**Tietosuojavastaava** (tietosuoja-asetus)	**Tietoturvallisuuden varmistamisesta vastaava** (TiHL 13.1 §)
Säännösten toteutumisen valvonnasta vastaava (TiHL 4.2 §)	**Muutosvaikutusten arvioinnista vastaava** (TiHL 5.3 §)	**Asianhallinnasta vastaava** (TiHL 25 ja 26 §)	**Riskien arvioinnista vastaava** (TiHL 13 §)
	Asiakirjajulkisuuskuvauksen ylläpidosta vastaava (TiHL 28 §)	**Arkistotoimesta vastaava** (Arkistolaki)	**Häiriötilanteisiin varautumisesta vastaava** (TiHL 13 a §)

Viranomainen

Tehtävät	Prosessit	Tietovarannot	Tietojärjestelmät
Säilytysaikojen määrittelystä vastaava (TiHL 21 §)	**Toimintaprosessista vastaava** (TiHL 5.2 §)	**Tietovarannosta vastaava** (TiHL 5.2 §)	**Tietojärjestelmästä vastaava** (TiHL 5.2 §)
Käyttöönottopäätöksen tekijä (TiHL 28 d §)	**Käsittelysääntöjen hyväksyjä** (TiHL 28 a §)		
	Laadunvarmistamisesta vastaava (TiHL 28 b §)	**Rekisterinpitäjä** (tietosuoja-asetus)	
	Laadunvalvonnasta vastaava (TiHL 28 c §)	**Tietojen laadunvalvonnasta vastaava** (TiHL 28 f §)	
	Virhetilanteiden käsittelystä vastaava (TiHL 28 c §)		

Tietoturvallisuustoimenpiteistä vastaavat (TiHL 4 luku)

Asiakirjan antamisesta vastaavat (Julkisuuslaki)	**Häiriötilanteista tiedottamisesta vastaava** (TiHL 13 a §)	

Tiedonhallinnan vastuiden määrittelystä

- Vastuut määritellään käytännössä tiedonhallintayksiköstä riippuen työjärjestyksessä, hallintosäännössä, työnjohtomääräyksissä tai vastaavassa
- Tiedonhallinnan vastuista päättää viranomainen tai virkamies, jolla on toimivalta:
  - tehdä hallintoon ja organisointiin liittyviä päätöksiä
  - päättää työjärjestyksen, hallintosäännön, johtosäännön tai muun vastaavan säännöstön sisällöstä.
- Käytännössä vastuita voi olla myös kirjattuna erilaisiin hanke- ja projektisuunnitelmiin ➔ suosituksena, että tällöin vastuiden määrittelyt kootaan yhteen erilliseen dokumentaation, joka on helposti hallittavissa
- Vastuut tulee kuvata myös tiedonhallintayksikön tiedonhallintamallissa (lisää myöhemmin esityksessä) ➔ suositeltavaa käyttää sekä tiedonhallintamallissa että työjärjestyksissä/hallintosäännöissä tai vastaavissa samoja käsitteitä

Vastuiden määrittely viranomaisten yhteistyössä

- **Useat viranomaiset käyttävät samaa tietojärjestelmää tietoaineistojensa käsittelyyn**
  - Tiedonhallintayksikön johdon vastuulla tiedonhallinnan järjestäminen myös käytettäessä yhteisiä tietojärjestelmäpalveluja
  - Yhteistä palvelua käyttävä viranomainen ei yleensä vastaa käytettävästä tietojärjestelmästä ➔ varmistettava kuitenkin, että viranomaisen vastuulla olevat vaatimukset toteutuvat myös yhteisessä palvelussa
  - Suositeltavaa varmistaa hankintasopimuksissa, että palveluntuottajat toteuttavat vaatimuksia ja pystyvät myös esittämään niiden toteuttamisen esim. sopimuksiin sisältyvissä palvelukuvauksissa
- **Viranomaiset valmistelevat asioita yhteistyössä (esim. yhteiset kehittämisprojektit, yhteiset hankinnat, yhteiset työtilat asioiden valmisteluun)**
  - Jos vastuu ovat epäselviä on syytä määrittää, kenen tai keiden viranomaisten hallinnassa ja määräysvallassa asiakirjat ovat ja minkä viranomaisen tiedonhallintaa ne kuuluvat (asiakirjat voidaan katsoa kuuluvan myös kaikkien osallistuvien tiedonhallintaan)
  - Tarvittaessa asiasta kannattaa sopia tarkemmin ja sellaisella tasolla, joka mahdollistaa tiedonhallinnasta säädettyjen vastuiden kohdentamisen käsiteltäviin tietoaineistoihin ja asiakirjoihin

Tiedonhallinnan ohjeiden ylläpito (4.2 § 2 k)

- **Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on ajantasaiset ohjeet:**
  - Tietoaineistojen käsittelystä
  - Tietojärjestelmien käytöstä
  - Tietojenkäsittelyoikeuksista
  - Tiedonhallinnan vastuiden toteuttamisesta
  - Tiedonsaantioikeuksien toteuttamisesta
  - Tietoturvallisuustoimenpiteistä
  - Poikkeusoloihin varautumisesta

Tiedonhallinnan ohjeiden ylläpidosta

- Ohjeiden osalta on huomioitava myös ne ohjeet, joilla tiedonhallintayksikkö ohjaa sen lukuun toimivia (mm. henkilötietojen käsittelyä koskevat ohjeet ja sopimukset, ohjeet palvelutuottajalle tietojen käsittelystä)
- Ohjeiden ajantasaisuuden varmistamiselle on suositeltavaa asettaa tarkistuspisteet siten, että tiedonhallintamallia päivitettäessä kunkin ohjeen ajantasaisuudesta vastuussa oleva raportoi johdolle, **miten tiedonhallintamallin muutokset ovat vaikuttaneet käytössä oleviin ohjeisiin**
  - Tiedonhallintaa ja tietojen käsittelyä koskevat lainsäädäntömuutokset
  - Tiedonhallintayksikössä toimivien viranomaisten organisoinnissa tapahtuvat muutokset
  - Tietoturvallisuuden tilassa tapahtuneet muutokset

Koulutuksen tarjoaminen osaamisen varmistamiseksi (4.2 § 3 k)

- Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on tarjolla koulutusta, jolla varmistetaan, että:

  1 henkilöstöllä ja

  2 tiedonhallintayksikön lukuun toimivilla

  on riittävä tuntemus voimassa olevista tiedonhallintaa, tietojenkäsittelyä sekä asiakirjojen julkisuutta ja salassapitoa koskevista säädöksistä, määräyksistä ja tiedonhallintayksikön ohjeista

- Johdon velvollisuus huolehtia, että tiedonhallintayksikön **koulutussuunnitelmissa** ja **uusien henkilöiden perehdytyksessä** on otettu huomioon, miten yksikössä varmistetaan riittävä osaaminen

- Jokaisen virkamiehen virkavelvollisuuksiin kuuluu ottaa selvää keskeisestä, virkatehtäviin liittyvästä lainsäädännöstä

Asianmukaisten työvälineiden järjestäminen (4.2 § 4 k)

- Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on asianmukaiset työvälineet tiedonhallintaa koskevien velvollisuuksien toteuttamiseksi
- Työvälineiden asianmukaisuuden varmistamiseen kuuluu, hankinnoissa on varmistettu mm.:
  - tietojärjestelmissä ja tietojenkäsittelyissä on toteutettu tietoturvallisuusvaatimukset
  - tietojärjestelmissä on asianhallinnan tai palvelujen tiedonhallinnan vaatimukset täyttävät toiminnallisuudet
  - tietojärjestelmät on riittävästi testattuja sekä tietojärjestelmät ovat toiminnallisesta käytettäviä (käytettävyystestaukset tai muut vastaavat arvioinnit on tehty)
  - tietojärjestelmien ja tietovarantojen yhteentoimivuus voidaan toteuttaa ja että tekniset rajapinnat voidaan avata ainakin niissä tilanteissa, joissa tiedonhallintalaki edellyttää;
  - teknisten rajapintojen tietorakenteet on määritelty ja rajapintakuvaukset on tiedonhallintayksikön sekä tietoja saavien toimijoiden käytettävissä
  - laitteistojen ja tietojärjestelmien elinkaaren hallinta
- ➔ Laillisuusvalvojien arvioinnit: tietojärjestelmiin liittyvillä syillä ei voida perustella poikkeamista hyvän hallinnon ja oikeusturvan viranomaismenettelyille asettamista vaatimuksista

Valvontavelvollisuus (4.2 § 5 k)

- Tiedonhallintayksikön johdon on huolehdittava siitä, että tiedonhallintayksikössä on järjestetty **riittävä valvonta tiedonhallintaan liittyvien säädösten, määräysten ja ohjeiden noudattamisesta**
- Valvonnan järjestämisen tavasta päättää tiedonhallintayksikkö
- Järjestämisessä hyvä huomioida muun valvonnan rooli osana tiedonhallintaa koskevien vaatimusten valvontaa:
  - Tietosuojavastaava
  - Sisäinen valvonta
- Valvonnan toteuttamiseksi suositeltavaa laatia **valvontasuunnitelma**, jonka perusteella valvonta toteutetaan
- Tiedonhallintayksikössä tulisi olla riittävät kontrollit, joilla varmistetaan, että viranomaiset noudattavat tiedonhallintaa koskevia vaatimuksia
- Yksi keskeisimmistä kontrolleista: henkilöstöllä on riittävä osaaminen tietoturvallisuuden ja muun tiedonhallinnan toteuttamisesta

Esimerkki valvonnan kohteet ja vastuut (4.2 §)

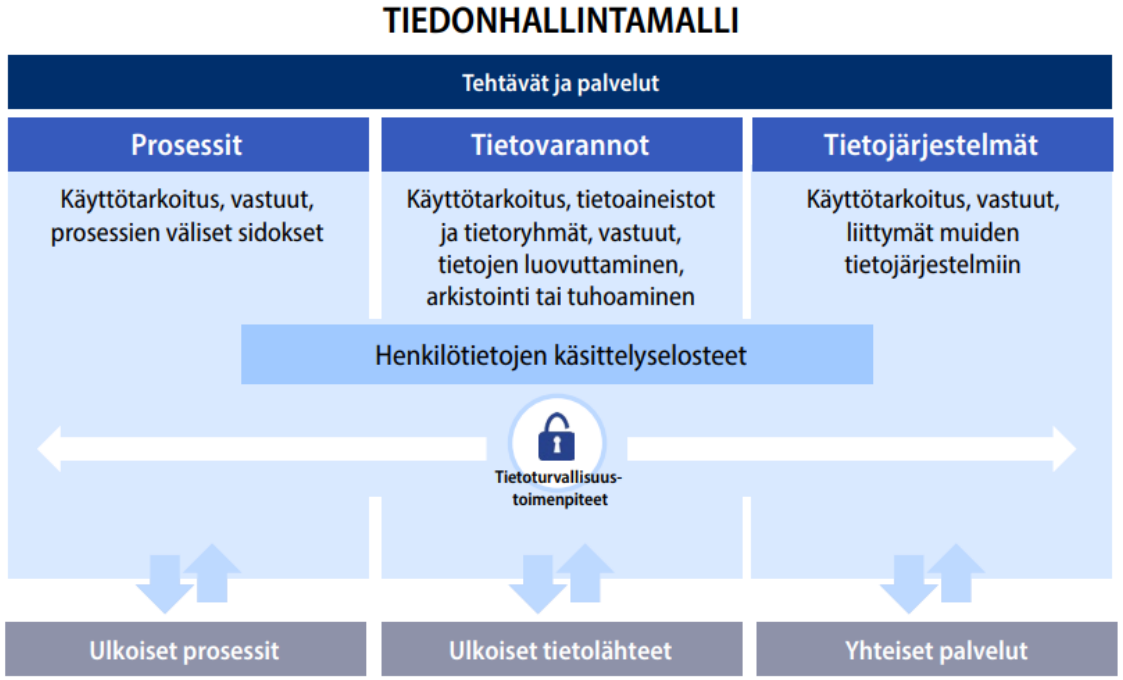
	Tiedonhallintayksikön tiedonhallinta				Tiedonhallintayksilön lukuun toimivat
	Valvontavastuut			Säännökset, määräykset ja ohjeet	Säännökset, määräykset ja ohjeet
Tietovarantojen ylläpito	 Toimiala/ yksikkö	 Tietovarannosta vastaava	 Sisäinen valvonta	• Tiedonhallintalaki, tietovarantoa koskevat erityissääntely • Tietovarannossa ylläpidettävien tietojen käsittelyohjeet • Tiedonhallintamalli	• Tiedonhallintalaki, tietovarantoa koskevat erityissääntely • Tietovarannossa ylläpidettävien tietojen käsittelyohjeet
Henkilötietojen käsittely	 Toimiala/ yksikkö	 Rekisterin-pitäjä	 Tietosuoja-vastaava	• Tietosuojalainsäädäntö • Henkilötietojen käsittelyselosteet • Rekisterinpitäjän ohjeet	• Sopimus henkilötietojen käsittelystä • Rekisterinpitäjän ohjeet • Tietosuojaliite (hankintasopimus)
Tieto-järjestelmien käyttö	 Toimiala/ yksikkö	 Järjestelmästä vastaava	 Pääkäyttäjä	• Tiedonhallintalaki, tietojärjestelmän käyttöä koskeva erityissääntely • Tiedonhallintamalli • Tietojärjestelmän käyttöohjeet	• Tiedonhallintalaki, tietojärjestelmän käyttöä koskeva erityissääntely • Tietojärjestelmässä käsiteltävien tietojen käsittelyvaatimukset (hankintasopimus)
Asianhallinta ja arkistointi	 Toimiala/ yksikkö	 Arkistotoimen järjestäjä	 Sisäinen valvonta	• Julkisuuslaki, tiedonhallintalaki, arkistolaki • Tietojen luovuttamista koskeva ohjeet • Arkistonmuodostussuunnitelma, tiedonohjaussuunnitelma	• Julkisuuslaki, tiedonhallintalaki, arkistolaki • Palvelussa muodostuvien tietojen käsittelyvaatimukset (hankintasopimus)
Tieto-turvallisuus	 Toimiala/ yksikkö	 Tietoturva-päällikkö	 Sisäinen valvonta	• Tiedonhallintalaki, julkisuuslaki, tietoturvallisuutta koskeva erityissääntely • Tietoturvallisuusohjeet	• Tiedonhallintalaki, julkisuuslaki, tietoturvallisuutta koskeva erityissääntely • Tietoturvallisuusliite (hankintasopimus)
Jatkuvuuden varmistaminen	 Toimiala/ yksikkö	 Valmius-päällikkö	 Sisäinen valvonta	• Valmiuslaki, tiedonhallintalaki • Valmiussuunnitelma • Valmiusharjoitusohjeet	• Valmiuslaki, tiedonhallintalaki • Varautumistoimenpiteet ja vastuut (palvelusopimus) • Palvelutasot (palvelusopimus)

Tiedonhallintamallin ylläpito ja muutosvaikutusten arviointi

Tiedonhallintamallin ylläpito (5.1 §)

- 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
  - tietoturvallisuuden ylläpitämiseksi
- ➔ Käyttötarkoitus määrittää tarkemmin mallissa esitettävien tietojen kuvaustapaa tai tarkkuustasoa (taso, jolla viranomainen pystyy velvollisuutensa toteuttamaan)

Tiedonhallintamallin sisältö ja käyttötarkoitus



Tiedonhallintamallin on sisällettävä vähintään tiedot:

1) Toimintaprosesseista
2) Tietovarannoista
3) Tietoaineistojen arkistoon siirtämisestä, arkistointitavasta ja arkistopaikasta tai tuhoamisesta
4) Tietojärjestelmistä
5) Tietoturvallisuustoimenpiteistä (joille turvataan tiedonhallintamallissa esitetty tietojen käsittely)

➔ Tiedonhallintamalliin on koottu aikaisemmin muualla laissa säädettyjä kuvausvelvollisuuksia

- Tiedonhallintalaissa toimintaympäristöllä tarkoitetaan tiedonhallintayksikön **oman toiminnan kuvausta** sekä **tiedonhallintayksikön toiminnan kannalta keskeisten sidosryhmien** tunnistamista suhteessa tiedonhallintayksikön toimintaan
- Sidosryhmät voivat muodostua tiedonhallintayksikön asiakkaiden, toimintaan osallistuvien muiden tiedonhallintayksiköiden tai tiedonhallintayksikön palvelutoimintaan liittyvien palvelun tuottajien kautta.

Tietovarannoista kuvattavat tiedot

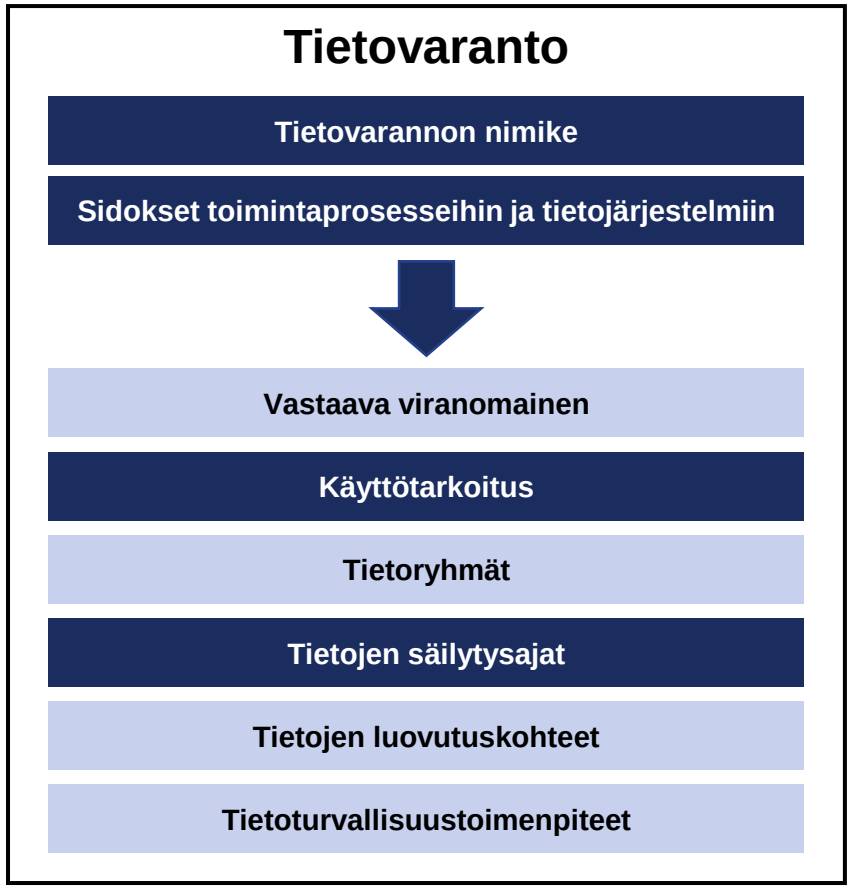
- Tiedonhallintamallissa esitettävien tietovarannon määrittely jää viranomaisen harkintaan (ellei tietovarannosta ole säädetty erikseen)
- **Tiedonhallintalautakunta on suositellut laissa säädettyjen tietovarantojen esittämistä laissa säädetyssä muodossa, joka auttaa viranomaista kohdentamaan tiedot niiden sääntelyperustaan**

- **Tietosuoja-asetuksen henkilötietojen käsittelytoimia koskevaan selosteeseen sisältyvät asiat ovat osa tiedonhallintamallia**
- Käsittelyselosteen sisältöä voi olla perusteltua rakenteellisesti yhdenmukaistaa muita tietovarantoja kuvaavien tietojen kanssa, jotta tietoja voidaan ylläpitää kokonaisuutena

Tiedonhallintamallin käyttötarkoitus / paikkatietoesimerkki

Tiedonhallinnan kohde: kriittistä infrastruktuuriin liittyvän paikkatiedon ja tiedon jakamisen hallinta

Tiedonhallintamallin käyttötarkoitus (5.1 §): A tietoaineistojen hallinnan suunnittelu ja toteuttaminen, B tiedonsaantia koskevien oikeuksien ja rajoitusten toteuttaminen sekä C tietoturvallisuuden ylläpitäminen



1. Viranomainen, joka vastaa tietovarannon paikkatietoja sisältävien tietoaineistojen ylläpidosta ja tietojen luovuttamisesta (esim. kunnassa tehtävästä vastaava lautakunta)

2. Tietovarannossa ylläpidettävät paikkatietoja sisältävät tietoaineistot sekä rajoitukset niiden sisältämien tietojen julkisuudelle tai luovuttamiselle
- salassa pidettävät tiedot ja salassapidon peruste (julkisuuslaki)
- Henkilötietoryhmät, erityisen henkilötietoryhmät (GDPR)

3. Paikkatietojen luovutuskohteet ja tietojen luovutukseen liittyvät rajoitukset
- Säännöllinen luovuttaminen muilla viranomaisille (esim. rakennetun ympäristön tietovaranto ja tietovarannon tietojen käsittelyä koskevat rajoitukset)
- Tietopyyntö (esim. arvokkaat tietoaineistot)
- Tietoverkko (esim. yleiskäyttöinen paikkatietoaineisto)

4. Tietoturvallisuustoimenpiteet, joilla varmistetaan paikkatietojen luovuttamisen säännöstenmukaisuus
- Käyttöoikeuksien hallinta (16 §)
- Lokitietojen kerääminen (17 §)
- Tiedonsaantioikeuden varmistaminen (19, 22, 24, 24 a ja b §)
- Tekniset kontrollit luovutuksen välttämättömyyden varmistamiseksi (22 §)

Tiedonhallintamallin ylläpito

- Tiedonhallintamallin on tarkoitus kuvata tiedonhallintayksikön tiedonhallintaa ajantasaisesti (ylläpidosta säädetty tiedonhallintalain 5.1 §:ssä)
- Ylläpidon käytännöistä ei ole säädetty, vaan sen toteuttaminen jää tiedonhallintayksikön harkittavaksi.
- Huomioitava, että tiedonhallintamalliin tehdyt muutokset tulee dokumentoida (versionhallinta)
- Suosituksia ja hyviä käytäntöjä ylläpitomenetelmistä:
  - muutosvaikutusten arviointi (TiHL 5.3 §)
  - sovittu aikataulu- tai vuosisykli
  - tiedonhallintayksikön oma kehittäminen
  - tiedonhallintayksikön toimintaympäristössä tapahtuvat muutokset

Viranomaiset voivat hyödyntää kokonaisarkkitehtuurimenetelmää myös tiedonhallintamallin ylläpidossa (esim. Digi- ja väestötietoviraston ylläpitämä kehys: https://kehittajille.suomi.fi/oppaat/kokonaisarkkitehtuuri)

Tiedonhallintamallin ylläpitoa koskevien vaatimusten toteuttaminen

- Tiedonhallintamalli on viranomaisen asiakirja, joita tulee käsitellä tiedonhallintalaissa tai muualla laissa säädetyn mukaisesti
  - Julkisuuslain 5 §:n 2 momentin mukaan viranomaisen asiakirjalla tarkoitetaan viranomaisen laatimaa asiakirjaa ➔ on tullut laatia 1.1.2021 mennessä (hyvinvointialueet 1.7.2021 alkaen)
- Myös päivitysversion hyväksyminen muodostaa asiakirjan
- Tiedonhallintamalliin sovelletaan julkisuuslaissa säädettyjä asiakirjan julkisuutta ja salassapitoa koskevia säännöksiä
- **Suositus tiedonhallintamallista** (VM 2022:22)

Tiedonhallintamalli on viranomaisen oma työväline tiedonhallintaan ➔ mallissa esitettävien tietojen rajaaminen mallin ulkopuolelle heikentää sen käyttöä tarkoitukseen (ks. TiHL 5.1 §)

Tiedonhallintalaissa ei ole säädetty perusteista, joilla tiedonhallintayksikkö voisi rajata tiedonhallintamallin tietosisältöä

Tiedonhallinnan muutosvaikutusten arviointi (5.3 §)

- Suunniteltaessa tiedonhallintamallin sisältöön vaikuttavia olennaisia hallinnollisia uudistuksia ja tietojärjestelmien käyttöönottoa tiedonhallintayksikössä on arvioitava näihin kohdistuvat muutokset ja niiden vaikutukset suhteessa:
  - Tiedonhallinnan vastuisiin
  - Tietoturvallisuusvaatimuksiin ja –toimenpiteisiin (TiHL 4 luku)
  - Tietoaineistojen muodostamiseen ja luovutustapaan (TiHL 5 luku)
  - Asianhallintaan ja palvelujen tiedonhallintaan (TiHL 6 luku)
  - Asiakirjojen julkisuuteen, salassapitoon ja suojaan
  - Tiedonsaantioikeuksiin
- Lisäksi arvioinnissa otettava huomioon tietovarantojen hyödyntäminen ja yhteentoimivuus

Muutosvaikutusten arvioinnin hyödyt

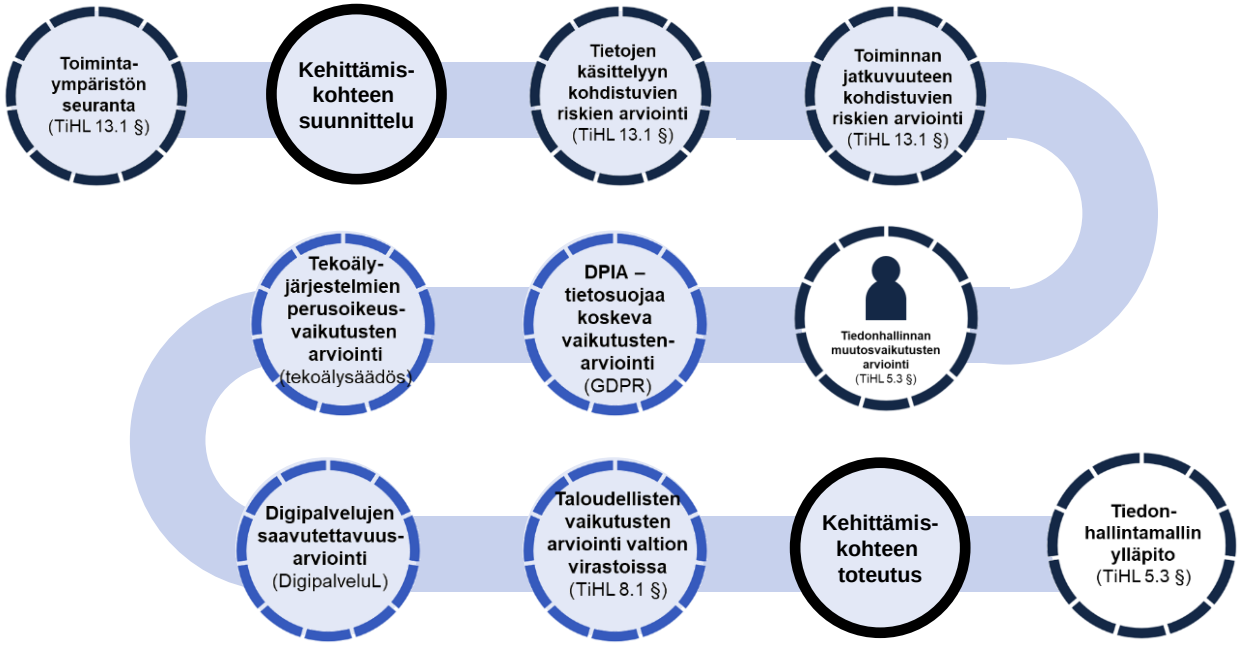
- Auttaa tiedonhallintayksikköä **arvioimaan etukäteen toimenpiteiden vaikutuksia**, joilla se aikoo toimintaansa muuttaa
- Auttaa **valitsemaan muutoksen toteuttamisen erilaisista vaihtoehdoista ne, jotka takaavat parhaiten ja mahdollisimman taloudellisesti** tiedonhallinnasta säädettyjen vaatimusten sekä julkisuusperiaatteen toteutumisen
- Mahdollistaa **ennakoimaan paremmin toimintaympäristössä tapahtuvia muutoksia**
- Tukee **tietosuoja-asetuksen** 35 artiklan vaikutusten arvioinnin toteuttamista
- **Varmistaa tiedon elinkaaren hallinnan** vaatimusten toteuttamisen muutoksen jälkeen
- Auttaa arvioimaan, **hyödynnetäänkö muiden toimijoiden hallinnassa olevia tietoaineistoja** tiedonhallintayksikön toiminnassa tehokkaasti
- Auttaa **arvioimaan sääntelyehdotusten vaikutuksia** tiedonhallintayksikön toimintaan ja tiedonhallintaan

Arviointivelvollisuuden toteuttamiseksi ja arvioinnilla saatavien hyötyjen varmistamiseksi useat viranomaiset ovat määritelleet muutosvaikutusten arvioinnin osaksi omaa kehittämisen hallinnan ja kehittämisen ohjauksen menettelyä

Muutoksen olennaisuuden arviointi

- Olennaisuutta määritteleviä kriteerejä esimerkiksi (viranomaisten käytäntöjä):
  - Muutoksen kohdentuminen viranomaisen keskeisten lakisääteisten tehtävien toteuttamiseen
  - Muutoksella on vaikutuksia useisiin toimijoihin (pienelläkin muutoksella voi olla suuret vaikutukset)
  - Muutokset viranomaisen velvollisuuksissa ja menettelyissä luovuttaa tietoja toisille viranomaisille
  - Tietosuoja-asetuksen 35 artiklan mukaisen vaikutusten arvioinnin toteuttaminen
  - Muutokseen arvioidaan liittyvän merkittävä taloudellinen tai toiminnallinen riski
  - Kehittämisen ja siihen liittyvien hankintojen suuruus

Tiedonhallintaan kohdistuvia arviointivelvollisuuksia



- Käytännössä viranomaiset ovat linkittäneet muutosvaikutusten arvioinnin osaksi:
  - Kehittämisenhallintaa (hanke-/projektinhallinta, hankittavien palvelujen / ratkaisujen vaikutukset tiedonhallintaan)
  - Tietosuojaa koskeva vaikutusten arviointi (DPIA)
  - Digitaalisten palvelujen saavutettavuusarviointi (digipalvelulaissa (306/2019)
  - Riskienarviointivelvollisuudet (toimintaa ja taloutta koskevien riskienhallinta)

- Tiedonhallintayksikkö päättää muutosvaikutusten arvioinnin järjestäminen (miten ja milloin arviointi toteutetaan)
- Suositusta, että tiedonhallintaan kohdistuvien vaikutusten arviointi liitetään osaksi muuta viranomaisen toimintaa ja tiedonhallintaa koskevaa vaikutusten- ja riskienarviointikokonaisuutta

Muutosvaikutusten arviointi / paikkatietoesimerkki

Tiedonhallinnan kohde: kriittistä infrastruktuuriin liittyvän paikkatiedon ja tiedon jakamisen hallinta

Muutosvaikutuksen arvioinnin käyttötarkoitus: muutokseen liittyvien riskien etukäteisarviointi, jotta voidaan valita oikeat toimenpiteet muutoksen toteuttamiseksi sekä yksilöiden oikeuksien toteuttamiseksi (HE 284/2018 vp)

Esimerkki: muutoksen vaikutusten arviointi suhteessa:

- **tiedonhallinnan vastuisiin** (muutokset paikkatiedon ylläpidosta ja luovuttamisessa vastaavissa viranomaisissa)
- **tietoturvallisuuteen** (riskiarvioon perustuvat muutokset vaatimuksissa ja toimenpiteissä, jos osa paikkatiedoista määritellään salassa pidettäväksi)
- **tietojen saatavuuteen** (paikkatietojen avoimuutta rajoittavat toimenpiteet)
- **tietojen luovutustapaan** (toimenpiteet luovutettavien paikkatietojen tarpeen ja välttämättömyyden varmistamiseksi)
- **tietojen yksilöintiin ja rekisteröintiin** (tietojen julkisuuteen liittyvien rajoitusten huomioiminen paikkatietoaineistojen rekisteröinnissä)
- **asiakirjajulkisuuteen ja tietojen saantioikeuksiin** (vaikutukset, kun paikkatieto muuttuu avoimesta julkisuuden tai luovuttamisen osalta rajoitetuksi)
- **tietovarantojen hyödyntämiseen** (vaikutus viranomaisen paikkatietoaineistoja hyödyntävään)

Yleisesti tietoturvallisuuteen liittyvästä sääntelystä

Tiedonhallintalain tietoturvallisuusvaatimusten (4 luku) soveltamisessa huomioitavaa muuta sääntelyä

- Julkisuuslain asiakirjojen julkisuutta ja salassa pitoa koskeva sääntely
- Tietosuojalainsäädännössä henkilötietojen käsittelyn turvaavat vaatimukset ja toimenpiteet
- Arkistolaki (pysyvästi säilytettävien asiakirjojen ja tietoaineistojen käsittely)
- Valmiuslaki (viranomaisten varautumisvelvollisuudet)
- Tietoturvallisuutta, kyberturvallisuutta ja kriittisen infrastruktuurin suojaamista koskeva muu sääntely, mm.:
  - Kyberturvallisuutta koskevat velvollisuudet ja niiden noudattamisen valvonta julkishallinnossa - tiedonhallintalain uusi 4 a luku (hyväksytty eduskunnassa 11.3.2025)
  - Kyberturvallisuuslaki (hyväksytty eduskunnassa 11.3.2025)
  - Laki kriittisen intrastruktuurin suojaamisesta (HE 205/2024 vp)
- Viranomaisen tehtävää koskeva erityissääntely (tiedonhallintalain vaatimuksia toteutetaan tehtävän edellyttämättä tietoaineistojen käsittelyssä ja tietojärjestelmien käytössä)

➔ Erityisesti tietoturvallisuutta, kyberturvallisuutta ja kriittisen infrastruktuurin suojaamista koskevat säännökset muodostavat samoille viranomaisille samansuuntaisia velvollisuuksia, joita toteutetaan käytännössä samoilla toimenpiteillä

Tietoturvallisuus, kyberturvallisuus ja kriittinen infrastruktuuri

Sääntelyn organisatorinen soveltamisala pääpiirteittäin (HUOM! webinaarin ajankohta)

	Tiedonhallintalaki 4 luku (tietoturvallisuus)	Tiedonhallintalaki 4 a luku (kyberturvallisuusvelvollisuudet julkishallinnossa)	Kyber-turvallisuuslaki (kyberturvallisuusvelvollisuudet)	Laki kriittisen infrastruktuurin suojaamisesta (HE 205/2024)	Valmiuslaki (varautumis-Velvollisuus 12 §)
Valtion virastot ja laitokset	**Kyllä**	Kyllä (ei turvallisuus-viranomaiset, tuomioistuimet)	Jos harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on liitteissä tarkoitettu toimija	Kyllä (julkishallinnon toimiala)	Kyllä
Hyvinvointialueet ja hyvinvointiyhtymät	**Kyllä**	Kyllä	Kyllä (terveyspalvelujen tuottaja)	Kyllä (jos kriittinen toimija terveyden toimiala)	Kyllä
Kunnat ja kuntayhtymät	**Kyllä**	Ei	Vain lain liitteessä I tai II tarkoitetun toiminnan osalta	Jos kriittinen toimija CER-direktiivin liitteen toimialojen toimijaluokkien piiristä	Kyllä
Yliopistot ja ammattikorkeakoulut	**Kyllä**	Ei	Ei	Jos kriittinen toimija CER-direktiivin liitteen toimialojen toimijaluokkien piiristä	Ei
Itsenäiset julkisoikeudelliset laitokset	**Kyllä**	Kyllä (ei Suomen Pankki)	Jos harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on liitteissä tarkoitettu toimija	Jos kriittinen toimija CER-direktiivin liitteen toimialojen toimijaluokkien piiristä	Kyllä
Julkista hallintotehtävää hoitavat yksityiset	**Kyllä**	Ei	Jos harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on liitteissä tarkoitettu toimija	Jos kriittinen toimija CER-direktiivin liitteen toimialojen toimijaluokkien piiristä	Ei

Tietoturvallisuus, kyberturvallisuus ja kriittinen infrastruktuuri

Vaatimukset / toimenpiteet	**Tiedonhallintalaki 4 luku** (tietoturvallisuus)	Tiedonhallintalaki 4 a luku (kyberturvallisuusvelvollisuudet julkishallinnossa)	Kyberturvallisuuslaki (kyberturvallisuusvelvollisuudet)	Laki kriittisen infrastruktuurin suojaamisesta (HE 205/2024)
Vastuu tietoturvallisuustoimenpiteiden toteuttamisesta	• Toimiva johto • Tietovarannosta ja tietojärjestelmistä vastaavat viranomaiset	• Toimiva johto	• Toimijan johto	
Tietoturvallisuustoimenpiteiden kuvaaminen	• Prosesseihin, tietovarantoihin ja tietojärjestelmiin kohdistuvat toimenpiteet (tiedon-hallintamalli)	• Kyberturvallisuutta koskeva riskienhallinnan toimintamalli (tavoitteet, menettelyt ja vastuut)	• Kyberturvallisuutta koskeva riskienhallinnan toimintamalli (tavoitteet, menettelyt ja vastuut)	• Suunnitelma häiriönsietokyvyn varmistamiseksi
Toimintaympäristön seuranta	• Toimintaympäristön määrittäminen (tiedonhallintamalli) • Toimintaympäristön tietoturvallisuuden seuranta			
Riskienhallinta	• Tietojen käsittelyyn kohdistuvat riskit • Toiminnan jatkuvuuteen kohdistuvat riskit	• Viestintäverkkoihin ja tietojärjestelmiin kohdistuvat kyberriskit	• viestintäverkkojen ja tietojärjestelmien turvallisuuteen. Kohdistuvat riskit	• Poikkeamaan johtavien riskien arviointi
Tietojärjestelmien tietoturvallisuustoimenpiteet	• Tietojärjestelmien tietoturvallisuustoimenpiteiden toteuttaminen (suunnittelu, hankinta, käyttöoikeudet ja lokitietojen kerääminen)	• Toimintaperiaatteet ja käytännöt tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden varmistamiseksi • Viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuustoimenpiteet	• Toimintaperiaatteet ja käytännöt tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden varmistamiseksi • Viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuustoimenpiteet	• Tilojen ja niissä sijaitsevan infrastruktuurin suojaaminen
Tietoaineistojen turvallisuustoimenpiteet	• Muuttumattomuuden, alkuperäisyyden, ajantasaisuuden ja virheettömyyden varmistaminen • Saatavuuden ja käyttökelpoisuuden varmistaminen	• Toimintaperiaatteet ja käytännöt tietoaineistoturvallisuuden varmistamiseksi	• Toimintaperiaatteet ja käytännöt tietoaineistoturvallisuuden varmistamiseksi	
Jatkuvuuden varmistavat toimenpiteet	• Valmiussuunnitelmat • Muut toimenpiteet	• Poikkeamien havainnointi ja käsittely • Varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muut toiminnan jatkuvuuden hallinta	• Toimitusketjun häiriönsietokyvyn hallintatoimenpiteet • Poikkeamien havainnointi ja käsittely • Varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muut toiminnan jatkuvuuden hallinta	• Toimenpiteet poikkeamien syntymisen estämiseksi • Toimenpiteet poikkeamien seurauksiin ja häiriötilanteisiin vastaamiseksi, torjumiseksi ja lieventämiseksi
Valvonta	• Tiedonhallintaa koskevien säännösten, määräysten ja ohjeiden noudattaminen	• Kyberturvallisuutta koskevan riskienhallinnan toteuttamisen valvonta	• Kyberturvallisuutta koskevan riskienhallinnan toteuttamisen valvonta	

Tietoturvallisuus (TiHL 4 luku)

Luotettavuutta edellyttävien tehtävien tunnistaminen ja luotettavuudesta varmistuminen (12 §)

Tiedonhallintayksikön on tunnistettava ne tehtävät, joiden suorittaminen edellyttää sen palveluksessa olevilta tai sen lukuun toimivilta henkilöiltä erityistä luotettavuutta.

- Erityistä luotettavuutta voivat edellyttää mm. varoihin, terveydenhuoltoon tai yleiseen turvallisuuteen liittyvät tehtävät
- 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).

Organisaatiot voivat toteuttaa seuraavia toimenpiteitä erityistä luotettavuutta edellyttävien tehtävien tunnistamiseksi:

- laatia kuvaukset tehtävistä, jotka edellyttävät erityistä luotettavuutta,
- dokumentoida perustelut, miksi tehtävässä edellytetään erityistä luotettavuutta sekä
- hakea turvallisuusselvitykset sekä selvittää työntekijän luottotiedot tai vaatia huumaisainetestejä, mikäli niihin on laissa säädetyt perusteet

Yleinen riskienhallintavelvoite (13 § 1 mom)

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.

- Asettaa vaatimuksen tiedonhallintayksiköllе riskienhallinnan toteuttamiseen
- Riskien hallinnassa on suositeltavaa hyödyntää olemassa olevaa riskienhallintamenetelmää
- Esimerkki riskienhallinnan menetelmästä löytyy Riskienhallinnan käsikirjasta
- Riskien arviointi kirjallisena ja hyväksyttynä

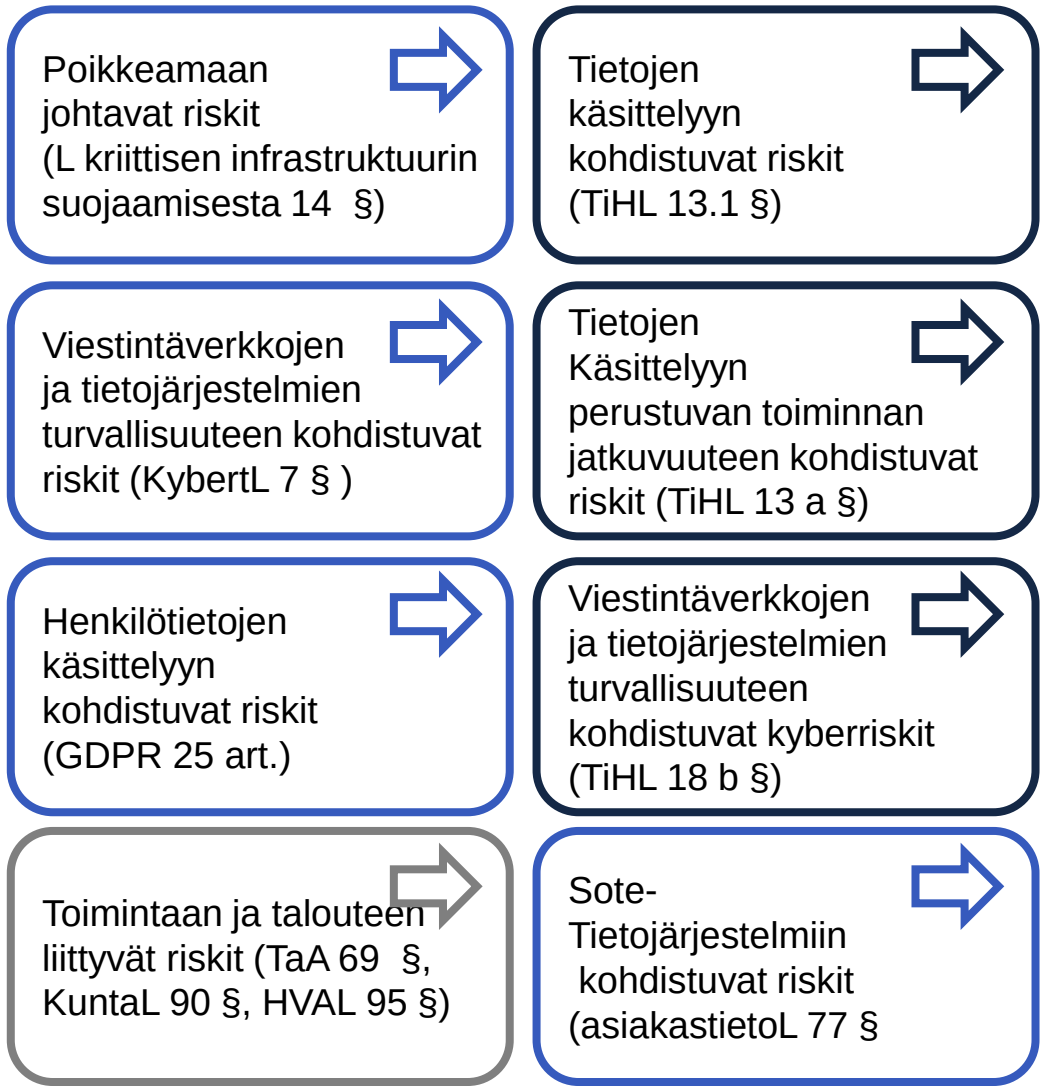
Häiriötilanteisiin liittyvä varautuminen ja riskienhallinta (13 a §:n 2 mom

Tiedonhallintayksikön on selvitettävä sen tietoaineistojen käsittelyn, tietojärjestelmien hyödyntämisen sekä niihin perustuvan toiminnan jatkuvuuteen kohdistuvat olennaiset riskit.

- Riskejä ovat tietojärjestelmän vikaantumisen lisäksi esimerkiksi
  - riippuvuudet muiden hallinnassa olevista tietoaineistoista ja –järjestelmistä,
  - häiriöt sähkönsyötössä tai viestintäverkkojen ja -palvelujen toiminnassa, sekä
  - toimitusketjujen kriittisyys ja niiden varautumisen taso.

Tiedonhallintayksikön on riskiarvioinnin perusteella valmiussuunnitelmin ja häiriötilanteissa tapahtuvan toiminnan etukäteisvalmisteluin sekä muilla toimenpiteillä huolehdittava, että sen tietoaineistojen käsittely, tietojärjestelmien hyödyntäminen ja niihin perustuva toiminta jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä valmiuslaissa (1552/2011) tarkoitetuissa poikkeusoloissa.

Riskienhallintavelvollisuudet ja -toimenpiteet



- Lainsäädäntö muodostaa viranomaisille useita riskienhallintaan kohdistuvia velvollisuuksia
- ➔ uhat ja riskit, joihin varaudutaan usein samoja tai ainakin samansuuntaisia (tietojärjestelmien käytettävyys, tietojen saatavuus, sähkön saatavuus)
- ➔ myös käytännön toimenpiteet, joilla riskejä hallitaan ovat usein samoja tai samansuuntaisia (varajärjestelyt, tietoaineistojen suojaaminen, tietojen käsittelyn valvonta)
- Käytännössä useat viranomaiset ovat linkittäneet tiedonhallintalain arviointivaatimukset osaksi laajempaa kokonaisuutta, jossa eri laeissa säädetyt näkökulmat huomioidaan kokonaisuutena

Riskiarvio ja tietoaineistot

- Tiedonhallintayksikön on otettava huomioon riskien hallinnassa käsiteltävien eri tietoaineistojen luonne
  - Riskien arviointi ja hallintakeinot voivat vaihdella tietoaineistoittain
  - Esimerkiksi paikkatietoihin liittyvässä riskien hallinnassa on otettava huomioon paikkatietoihin liittyvät ominaispiirteet
    - Arvioitava tarkkaan edellytykset tiedon avaamiselle (laista tuleva edellytys tiedon avaamiselle (INSPIRE) vs. tietoaineiston salassa pidettävyys (julkisuuslaki)
    - Paikkatiedon kansallisen riskiarvion työryhmän muistio julkaistu viime vuonna

Testausvelvoite (13 §:n 2 mom)

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

- Testaus on tarpeellista toiminnan jatkuvuuden varmistamiseksi ja tietoturvallisuustoimenpiteiden ajan tasalla pitämiseksi.

Keinoja vikasietoisuuden ja toiminnallisen käytettävyyden varmistamiseksi:

- Tietojärjestelmien luokittelu niiden toiminnallisen kriittisyyden mukaan,
- vikasietoisuuden ja toiminnallisen käytettävyyden säännöllinen testaus,
- Vikasietoisuuden parantaminen esim. kahdentamalla, hajauttamalla tai varajärjestelmillä,
- Varmistusten ottaminen tiedoista riittävän usein,
- Virheentarkastusmenettelyiden suunnittelu ja toteutus.

Asiakirjajulkisuuden toteuttamisen suunniteluvelvoite (13 §:n 3 mom)

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

Suunnittelussa huomioon otettavia seikkoja

- Viranomaiseen kohdistuvat tiedonantovaatimukset
- Viranomaisen julkiset ja salassa pidettävät tiedot
- tietojärjestelmien hakutoiminnot ottaen huomioon salassapitovaatimukset
- tietojärjestelmien ja tietovarantojen dokumentointi siten, että tiedonhallintalain 28 §:ssä edellytetty kuvaus asiakirjajulkisuuden toteuttamiseksi voidaan laatia.

Tietoturvallisuustoimenpiteiden varmistus hankinnoissa (13 § 4 mom)

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

- tarkoituksena on tunnistaa ja dokumentoida hankittavaan tietojärjestelmään ja sen toimittajaan kohdistuvat tietoturvallisuutta koskevat vaatimukset.
- Vaatimukset tulee määritellä riippumatta siitä, hankitaanko tietojärjestelmä palveluna vai asennetaanko se tilaajan ympäristöön

Vaatimusten määrittelyssä huomioitavia seikkoja

- Yleisesti käytettyjen vaatimusluetteloiden hyödyntäminen
- Vaatimusten osoittaminen auditoinnilla
- Vaatimukset tulee ulottaa koko alihankintaketjuun ja niiden tulee täyttyä koko elinkaaren ajan
- mahdollinen palvelun tuottamisen kansainvälinen ulottuvuus

Häiriötilanteista tiedottaminen (13 a 1 mom §)

Viranomaisen on viipymättä tiedotettava sen tietoaineistoja hyödyntäville, jos sen tiedonhallintaan kohdistuu häiriö, joka estää tai uhkaa estää viranomaisen tietoaineistojen saatavuuden.

Viranomaisen on tiedotettava häiriön tai sen uhkan

- arvioidusta kestosta
- mahdollisuuksien mukaan korvaavista tavoista hyödyntää viranomaisen tietoaineistoja sekä
- häiriön tai uhkan päättymisestä.

Edellyttää viranomaista:

- suunnittelemaan etukäteen, miten ja kenelle häiriötilanteissa tiedotetaan,
- määrittelemään tiedottamisen vastuut sekä
- varmistamaan tiedon nopea perillemeno ja ymmärrettävyys.

Tietojen siirtäminen tietoverkossa (14 §)

Viranomaisen on toteutettava tietojensiirto yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä, jos siirrettävät tiedot ovat salassa pidettäviä.

Tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja

- Yhteys voi olla suojattu esimerkiksi salauksella tai
- Tiedot voidaan siirtää ilman tietoliikenneyhteyden suojaustakin, jos tiedot ovat salattuna siirrettävässä tiedostossa ja salaus voidaan purkaa vain riittävän vahvalla salausavaimella

Tietoaineistojen tietoturvallisuuden varmistaminen (15 § 1 mom)

Viranomaisen on varmistettava tarpeellisin tietoturvallisuustoimenpitein, että sen:	
1) tietoaineistojen muuttumattomuus on riittävästi varmistettu;	•Tietoaineistojen muuttumattomuuden varmistaminen digitaalisilla varmenteilla,
2) tietoaineistot on suojattu teknisiltä ja fyysisiltä vahingoilta;	•Laitteistojen sijoittaminen fyysisen turvallisuuden standardit täyttäviin auditoituihin konesaleihin,
3) tietoaineistojen alkuperäisyys, ajantasaisuus ja virheettömyys on varmistettu;	•Dokumenttien alkuperäisyyden varmistaminen sähköisin allekirjoituksin,
4) tietoaineistojen saatavuus ja käyttökelpoisuus on varmistettu;	•Tietojen kirjauskäytännöt, tietojärjestelmän suorittama tietojen syöttömuodon tarkistaminen tietojen tallentamisen yhteydessä, vastaanotettujen tietojen muodon tarkistaminen, tietojen laadun testaaminen
5) tietoaineistojen saatavuutta rajoitetaan vain, jos tiedonsaantia tai käsittelyoikeuksia on laissa erikseen rajoitettu;	•Tietojen saatavuuden rajoittamista koskevien perusteiden dokumentointi
6) tietoaineistot voidaan tarvittavilta osin arkistoida.	•tietojen arkistointivaatimusten huomioon ottaminen tietojen elinkaaren alusta alkaen.

Toimitilaturvallisuuden varmistaminen (15 §:n 2 mom)

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

Toimitilaturvallisuuden varmistamiseksi organisaatio voi toteuttaa esimerkiksi seuraavia toimenpiteitä:

- huolehtia tilojen lukituksista sekä pääsyoikeuksien ja avainten hallinnasta,
- edellyttää henkilöstöltä kuvallisten henkilökorttien käyttöä,
- ottaa käyttöön kulunvalvontajärjestelmä,
- jakaa toimitilat tarvittaessa erillisiin turvallisuusalueisiin ja toteuttaa ylimääräisiä tietoturvallisuustoimenpiteitä alueilla, joissa käsitellään tietoja, joihin kohdistuu korkeampia turvallisuusvaatimuksia,
- sijoittaa työpisteet siten, että salakatselu tai -kuuntelu ei ole mahdollista sekä hankkia salakatselun estäviä suojia,
- huolehtia, että vierailijoilla on saattajat.

Tietojärjestelmien käyttöoikeuksien hallinta (16 §)

Tietojärjestelmästä vastuussa olevan viranomaisen on määriteltävä tietojärjestelmän käyttöoikeudet.

- tulee määritellä osana tiedonhallintamallia
- Tietojärjestelmästä vastuussa oleva viranomainen ei välttämättä ylläpidä käyttöoikeuksia, vaan tietojärjestelmää käyttävä viranomainen voi olla vastuussa käyttöoikeuksien ajan tasalla pitämisestä.

Käyttöoikeudet on määriteltävä käyttäjän tehtäviin liittyvien käyttötarpeiden mukaan, ja ne on pidettävä ajantasaisina.

Käyttöoikeudet on määriteltävä ennalta kullekin tietojärjestelmän käyttäjälle käyttäjän tyypillisten työtehtävien mukaisesti.

Käyttöoikeuksien oikeellisuuden ja ajantasaisuuden varmistamiskeinot:

- Käyttöoikeuksien hyväksyntään ja ylläpitoon liittyvien prosessien määrittely
- Tietojen luokittelusta ja sopimuksista johtuvien vaatimusten huomioiminen
- Käyttöoikeuksien hallinnan vastuiden määrittely
- Käyttöoikeuksien päivitys työntekijöiden tehtävämuutosten yhteydessä
- Käyttöoikeuksien poistaminen työsuhteiden ja palvelusopimusten päättyessä
- Käyttöoikeuksien ajantasaisuuden varmistaminen määräajoin tehtävillä tarkastuksilla
- Yhteiskäyttötunnuksien käytön välttäminen ilman pakottavaa perusteltua syytä
- Kertakirjautumisen käyttäminen mahdollisimman laajasti
- Monivaiheisen tunnistautumisen käyttö erityisesti kirjauduttaessa palveluihin suojatun ympäristön ulkopuolelta

Lokitietojen kerääminen (17 §)

Viranomaisen on huolehdittava, että sen tietojärjestelmien käytöstä ja niistä tehtävistä tietojen luovutuksista kerätään tarpeelliset lokitiedot, jos tietojärjestelmän käyttö edellyttää tunnistautumista tai muuta kirjautumista.

- Lokitietojen keräämisen tarpeen määrittelee se viranomainen, joka on vastuussa tietojärjestelmästä.

Lokitietojen käyttötarkoituksena on tietojärjestelmissä olevien tietojen käytön ja luovutuksen seuranta sekä tietojärjestelmän teknisten virheiden selvittäminen.

- Lokitiedot tulee kerätä oletusarvoisesti, kun tietojärjestelmässä käsitellään salassa pidettäviä tietoja tai tietoja, joilla voisi olla merkitystä yksilön oikeusturvan toteuttamisen näkökulmasta

Turvallisuusluokiteltavat asiakirjat (18 §)

- Valtion viranomaisilla velvoite turvallisuusluokitella asiakirjat, kun
  - 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 em. 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 (1101/2019)

Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa 28.11.2019/1101

- Tarkempaa sääntelyä muun muassa:
  - Turvallisuusmerkinnän tekemisestä ja poistamisesta
  - Turvallisuusluokitellun materiaalin käsittelyä koskevista vaatimuksista
  - Asiakirjan tuhoamisesta

Lautakunnan kannanotto hyvinvointialueen oikeuteen turvallisuusluokitella asiakirjojaan

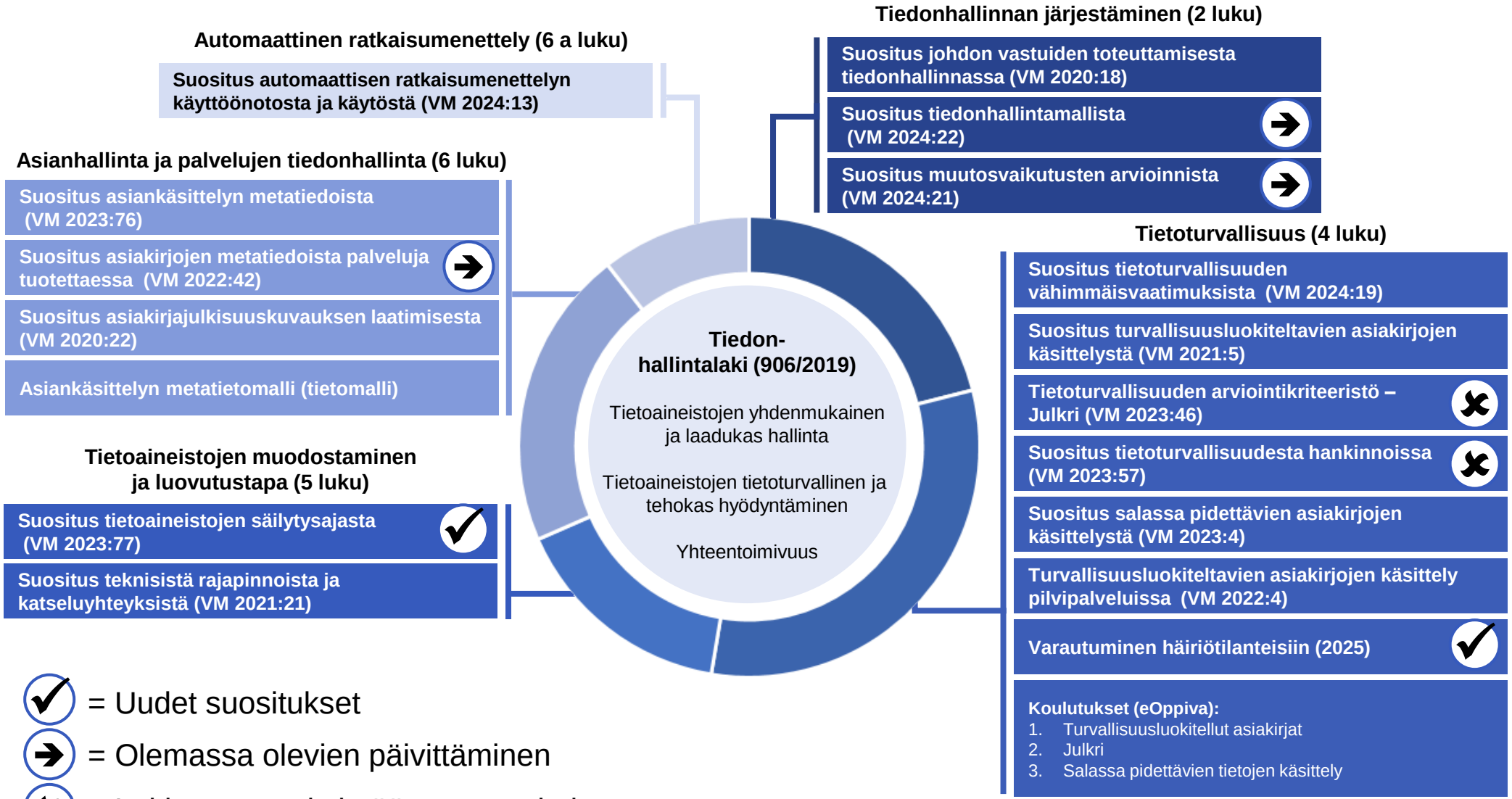
Kainuun hyvinvointialue pyysi tiedonhallintalautakunnalta kannanottoa siihen, onko hyvinvointialueella velvollisuus tai oikeus turvallisuusluokitella asiakirjojaan tiedonhallintalaissa tarkoitetulla tavalla

Lautakunnan kannanotto 26.10.2023:

- Hyvinvointialueen ei tulisi käyttää turvallisuusluokkaa koskevaa turvallisuusluokittelumerkintää – ainakaan sellaisena kuin merkinnöistä on säädetty tiedonhallintalain 18 §:ssä ja tiedonhallintalain 18 §:n 4 momentin perusteella annetussa valtioneuvoston asetuksessa asiakirjojen turvallisuusluokittelusta valtionhallinnossa (1101/2019, turvallisuusluokitteluasetus).
- Tiedonhallintalautakunta ei kuitenkaan näe estettä sille, että hyvinvointialue riskienhallintaan perustuen (esimerkiksi tiedonhallintalain 13 §:n 1 momentin perusteella) päätyy luokittelemaan asiakirjojaan ja merkitsemään niitä sen osoittamiseksi, mitä tietoturvallisuustoimenpiteitä asiakirjan käsittelyssä tulee hyvinvointialueen oman näkemyksen mukaan noudattaa.

Päätössanat

Tiedonhallintalautakunnan ylläpitämät suositukset 2025



= Uudet suositukset

= Olemassa olevien päivittäminen

= Lakkautettavaksi päätetyt suositukset

Tiedonhallintalautakunta
Informationshanteringsnämnden

Tiedonhallintalautakunnan tilaisuudet / kevät 2025

- Webinaari: **Kyberturvallisuusvelvollisuuksien toimeenpano julkisessa hallinnossa**

  Kyberturvallisuusvelvollisuudet julkisessa hallinnossa, kyberturvallisuusvelvollisuuksien valvonta sekä tiedonhallintalain tietoturvallisuusvelvollisuudet ja kyberturvallisuus

  Tiistai 1.4.2025, klo 9.00 – 11.00

- Webinaari: **Arviointitulokset tiedonhallintalain vaatimusten toteuttamisesta 2020-2025**

  Keskeiset havainnot tiedonhallintalautakunnan toteuttamista arvioinneista sekä arviointien perusteella toteutetuista ja suunnitelluista toimenpiteistä

  Torstai 15.5.2025 klo 13.00-14.30

- Webinaari: **Tiedonhallintalain (906/2019) vaatimusten toteuttaminen II**

  Tiedonhallintalaissa säädetyt vaatimukset, toimenpiteet vaatimusten toteuttamiseksi sekä tiedonhallintalautakunnan kannanottoja laissa säädetyistä vaatimuksista – osittain jatkoa edelliselle seminaarille

  Torstai 5.6.2025, klo 9.00 – 11.00

- **Suunnitteilla** (päivämäärä ja sisältö vielä avoin)
  - Opetustoimen säilytysaikasuositukset (alustavasti kesäkuu)
  - Tiedonhallintamallin ylläpito
  - Tiedonhallinnan muutosvaikutusten arviointi

  https://vm.fi/tiedonhallintalautakunnan-ajankohtaista-ja-tapahtumat

Palautetta tilaisuudesta ja kehittämisehdotukset

1. **Miten hyvin tilaisuus vastasi tarpeitasi?**
   - Erittäin hyvin
   - Hyvin
   - Tyydyttävästi
   - Huonosti
   - Ei lainkaan
2. **Mitä jäit kaipaamaan tilausuudesta?**
3. **Mitkä tiedonhallintalain vaatimukset ovat olleet hankalia toteuttaa ja miksi?**
4. **Toiveita ja kehittämisehdotuksia tiedonhallintalautakunnalle?**

Palautekyselyn linkki webinaarin viestikentässä

Tiedonhallintalautakunta

- **Tiedonhallintalautakunta**: https://vm.fi/tiedonhallintalautakunta
- **Kysymyksiä, kannanottopyyntöjä ja kehittämisehdotuksia** tiedonhallintalautakunnalle: tiedonhallintalautakunta@gov.fi
  - Lautakunnan mahdollista ottaa kantaa tiedonhallintalaissa säädettyyn
  - Asiakirjojen säilytysaikaan tai arkistointiin ei lautakunta pysty ottamaan kantaa
- **Ajankohtaista ja tilaisuudet**: https://vm.fi/tiedonhallintalautakunnan-ajankohtaista-ja-tapahtumat
  - Pyritään tarkentamaan kevään tilaisuudet ja suunnitelmat mahdollisimman pikaisesti
- **HUOM!** Tiedonhallintalautakunnan postituslistan ylläpidossa on ollut haasteista, jonka vuoksi listaa ei ole voitu käyttää tai pitää ajantasaisena (lista ylläpitoa arvioidaan myöhemmin)

Tiedonhallintalautakunta
Informationshanteringsnämnden

Kehotus / Kiitos

etunimi.sukunimi@loremipsum.fi
Loremipsum dolores sitamet
loremipsumdolores.fi