Suositus salassa pidettävän tiedon käsittelystä

Erja Kinnunen
8.9.2021

DIGI- JA VÄESTÖTIETO-VIRASTO

Taustaa

- Laki viranomaisten toiminnan julkisuudesta (621/1999, Julkisuuslaki) tuli voimaan 1.12.1999
  - 24§ määrittelee salassapidon perusteet
  - 25§ Salassapitomerkintä tehdään merkitsemällä asiakirjaan "SALASSA PIDETTÄVÄ"
  - Ei kuitenkaan määrittele miten tieto **luokitellaan** ja miten sitä **käsitellään** erilaisissa ympäristöissä ja/tai palveluissa
- Laki julkisen hallinnon tiedonhallinnasta (906/2019, Tiedonhallintalaki) tuli voimaan 1.1.2020
  - 18§ Turvallisuusluokiteltavat asiakirjat valtionhallinnossa
    - Asiakirjoihin tehtävistä salassapitoa koskevista merkinnöistä säädetään viranomaisten toiminnan julkisuudesta annetun lain 25 §:ssä
  - Kumosi aiemman Valtioneuvoston asetustietoturvallisuudesta valtionhallinnossa (681/2010, Tietoturvallisuusasetus)
    - 9§ Suojaustasot
    - 11§ Turvallisuusluokitus
- Huomioitava myös sektorikohtainen erityislainsäädäntö

Ohjeet ja suositukset

- Aiemmin VAHTI 2/2010 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta
  - Yleiset tietoturvavaatimukset
  - Tietoaineistojen luokittelu
  - Luokiteltujen tietoaineistojen käsittelyvaatimuksia
  - Tietoturvatasot – kytketty luokitteluun
- Olemassa
  - Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä
  - Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta
- Tulossa
  - Suositus turvallisuusluokitellun tiedon käsittelystä pilvipalveluissa
  - Salassa pidettävät tiedot ja asiakirjat – suositus

Suosituksen tila

- Suositus on laadittu Tiedonhallintalautakunnan alaisessa tietoturvallisuussuositusten valmistelujaostossa
- Rakenne noudattelee suositusta turvallisuusluokiteltavien asiakirjojen käsittelystä
- Tiivis, noin 15 sivua
- Luonnos valmiina
- Tulossa kommentoitavaksi lausuntopalveluun

- HUOM: Kaikki seuraavilla sivuilla esitetty on luonnostekstiä!

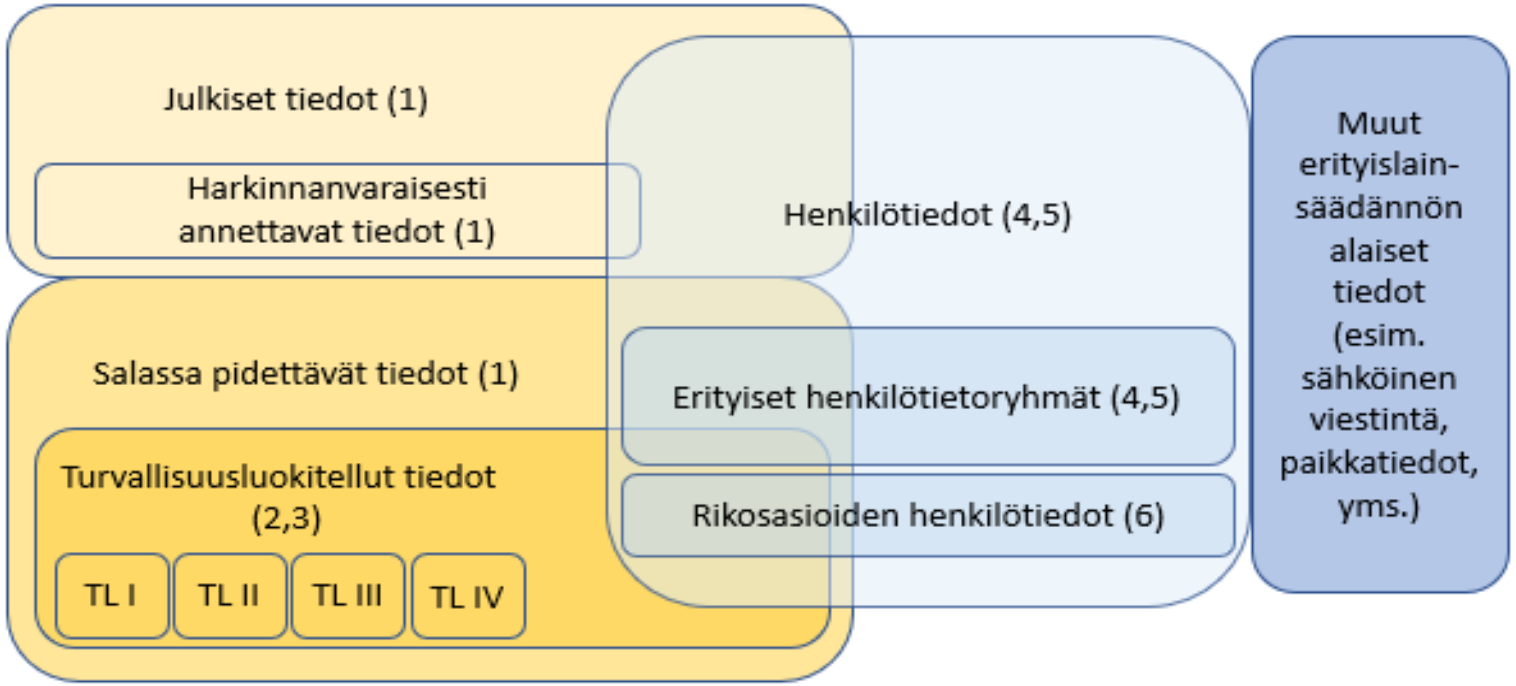
Suosituksen sisältö

1. Johdanto
2. Salassa pidettävä ja henkilötieto
3. Asiakirjojen ja tietojenkäsittelyn suojaamisen lähtökohdat
4. Salassa pidettävän tiedon käsittely
   - 4.1 Salassa pidettävän asiakirjan käsittelyn rekisteröinti ja seuraaminen
   - 4.2 Salassa pidettävän asiakirjan luovuttaminen ja vastaanottaminen
   - 4.3 Asiakirjan siirtäminen tietoverkon kautta
   - 4.4 Asiakirjan kuljettaminen
   - 4.5 Asiakirjan kopioiminen
   - 4.6 Tietojen säilyttäminen
   - 4.7 Asiakirjan tuhoaminen
5. Tietojärjestelmien ja tietoliikennejärjestelyjen suojaamisen vähimmäisvaatimukset
6. Säädökset ja lisätiedot

Johdanto

- Suositus on tarkoitettu kaikille salassa pidettäviä tietoja ja asiakirjoja käsitteleville – ensisijaisesti tiedonhallintayksiköille ja viranomaisille. Lisäksi suosituksen kuvaamia ohjeita voivat hyödyntää elinkeinoelämän toimijat ja kaikki muutkin, jotka käsittelevät viranomaisten salassa pidettäväksi määrittelemiä asioita ja asiakirjoja.
- Yleiset linjaukset salassa pidettävän tiedon käsittelyyn. Tiedonhallintayksiköiden tulee laatia tarkemmat ohjeet sisäiseen käyttöön.
- Tavoitteena on, että tietojärjestelmien turvallisuusratkaisut toteutetaan siten, että samoissa järjestelmissä voitaisiin tarvittaessa käsitellä sekä salassa pidettäviä että turvallisuusluokiteltuja TL IV tietoja. Toteutuksissa on tällöin huomioitava mm. tiedon fyysinen sijainti.
- Menettelyt koskevat kaikkea tietoa ja kaikkia välineitä, joilla salassa pidettävää tietoa käsitellään.

Tietoa voidaan luokitella monella tavoin



1) Julkisuuslaki 621/1999
2) Tiedonhallintalaki 906/2019
3) Turvallisuusluokitteluasetus 1011/2019
4) EU:n yleinen tietosuoja-asetus (EU) 2016/679
5) Tietosuojalaki 1050/2018
6) Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 1054/2018

Henkilötiedot

- Henkilötiedot voivat olla joko julkisia tai lain perusteella salassa pidettäviä.
- Lähtökohtaisesti viranomaisen asiakirjoissa olevat henkilötiedot ovat julkisia, ellei niiden julkisuutta ole rajoitettu salassapitosäännöksillä.
- Julkisuutta on voitu rajoittaa myös tiedon luovuttamista koskevilla rajoitussäännöksillä, mutta se liittyy tyypillisesti vain tietojen luovutustapaan eikä suoraan tietojen julkisuuteen.
- Henkilötietojen käsittelyedellytykset eivät suoraan ole sidoksissa asiakirjojen julkisuuteen.
- Tietosuojalainsäädännössä on säädetty edellytyksistä, joilla henkilötietoja voidaan käsitellä. Nämä edellytykset koskevat sekä julkisia että salassa pidettäviä henkilötietoja.
- Vaikka henkilötiedot olisivatkin julkisia, niin niitä pitää käsitellä tietosuojalainsäädännön mukaisesti.
- Henkilötietojen käsittelyyn liittyvät yleissäädökset ovat EU:n yleinen tietosuoja-asetus (EU) 2016/679 sekä tietosuojalaki (1050/2018).

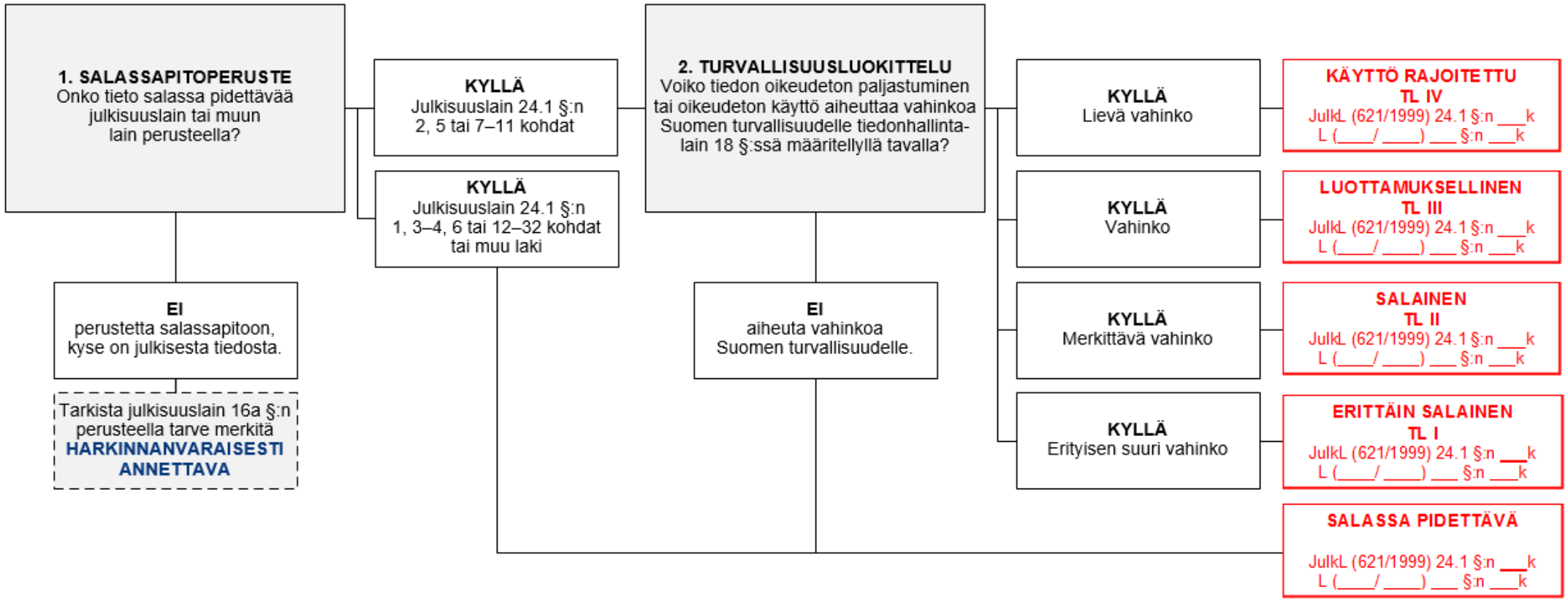
Salassa pidettävät tiedot, asiat ja asiakirjat

- Viranomaisen asiakirja on julkinen, ellei asiakirjan julkisuudesta tai salassapidosta tai muusta tietojen saantia koskevasta rajoituksesta ole laissa säädetty.
- Yleensä tiedon tai asiakirjan laatija määrittelee tiedon luokituksen. Luokitusmerkinnällä ei kuitenkaan ole sellaista merkitystä, ettei asiakirjaa pelkästään sen perusteella voitaisi antaa asiakirjan pyytäjälle.
- Asiakirjan julkisuus ja tiedon luovuttaminen asiakirjasta on ratkaistava viranomaisessa aina erikseen, jos tietoa asiakirjasta pyydetään.
- Salassapitomerkintä on informatiivinen eikä pelkästään sen perusteella voida ratkaista tiedonsaantiin liittyviä kysymyksiä. Salassapitomerkintä voi olla vanhentunut tai asiakirjan tietosisältö ei välttämättä ole enää tiedonantamisajankohtana salassa pidettävä. Lisäksi julkisuuslaissa säädetyt vahinkoedellytyslausekkeet voivat vaikuttaa asiakirjan tietosisällön salassapidon arviointiin.
- Viranomaisen salassa pidettävät asiakirjat määritellään yksityiskohtaisesti julkisuuslain 24 §:ssä tai erityislainsäädännössä.
- Salassa pidettävästä tiedosta, asiasta tai asiakirjasta tai asiakirjan sisällöstä voi saada tietoa vain julkisuuslaissa tai erityislainsäädännössä kuvatuin perustein.
- Asiakirjassa yleensä on sekä julkista että salassa pidettävää tietoa. Julkisuuslain 10 §:n mukaan, kun vain osa asiakirjasta on salassa pidettävä, tieto on annettava asiakirjan julkisesta osasta, jos se on mahdollista niin, ettei salassa pidettävä osa tule tietoon.
- Salassapitoa on arvioitava salassapitointressiin sekä tiedon antamista koskevaan mahdolliseen haittaan.

Salassa pitämisen perusteet

- Salassa pitämisen perusteena voi olla se, että asiakirja sisältää tietoja, joita koskee lailla säädetty vaitiolovelvollisuus.
- Salassa pitämisen perusteet kuvataan julkisuuslain 24 §:n 1 momentissa tai muussa säädöksessä.
- Usein erityislainsäädännössä otetaan kantaa salassa pitämiseen tai annetaan salassa pitämiseen liittyvistä menetelmistä ohjausta, mutta varsinainen salassa pitämisen peruste löytyy kuitenkin julkisuuslaista.
- Julkisuuslain 24 §:n 1 momentissa on erilaisia vahinkoedellytyksiä, jotka tulee ottaa huomioon salassapidon arvioinnissa:
  1. ehdoton salassapito (esim. kohta 29): – ei vahinkoedellytystä: säännöksessä lueteltuja tietoja sisältävät asiakirjat ovat ehdottomasti salassa pidettäviä (ellei esim. oikeudesta tiedonsaantiin ole erikseen säädetty),
  2. julkisuusolettamalla muotoillut (esim. kohdat 14, 15 ja 22) – vahinkoedellytys, jonka mukaan asiakirja on salassa pidettävä vain sillä edellytyksellä, että säännöksessä kuvatun tiedon antaminen vaarantaisi säännöksessä määriteltyä suojattavaa etua,
  3. salassapito-olettamalla muotoillut (esim. kohdat 7 ja 21) – vahinkoedellytys, jonka mukaan asiakirja on lähtökohtaisesti salassa pidettävä, ellei ole ilmeistä, ettei säännöksessä kuvatun tiedon antaminen vaaranna säännöksessä määriteltyä suojattavaa etua.

Salassa pitämisen perusteet



Salassapitomerkinnät

- ”Viranomaisen asiakirjaan, jonka viranomainen antaa asianosaiselle ja joka on salassa pidettävä toisen tai yleisen edun vuoksi, on tehtävä merkintä sen salassa pitämisestä. Asianosaiselle on annettava tieto hänen salassapitovelvollisuudestaan myös silloin, kun salassa pidettäviä tietoja annetaan suullisesti.” (JulkL 25 § 1 mom)
- Merkintä voidaan julkisuuslain 25 § 2 momentin mukaan tehdä muihinkin kuin 1 momentissa tarkoitettuihin asiakirjoihin.
- Merkinnän tekeminen on suositeltavaa muulloinkin tiedonhallintalain käsittelyvaatimusten kohdentamiseksi.
- Merkinnästä on käytävä ilmi, miltä osin asiakirja on salassa pidettävä sekä se, mihin salassa pitäminen perustuu.
- Salassa pitämisen perusteen päättymisen jälkeen merkinnän poistamisesta tai muuttamisesta on tehtävä merkintä samaan asiakirjaan, johon alkuperäinen merkintä on tehty (JulkL 25 § 2 mom).
- Salassa pitämistä koskevan merkinnän asianmukaisuus on tarkistettava aina viimeistään asiakirjaa ulkopuoliselle annettaessa luovutettaessa (JulkL 25 §).

Harkinnanvaraisesti annettavat asiakirjat

- Julkisuuslain 9 §:n 2 momentin mukaan: ”Tiedon antaminen asiakirjasta, joka 6 ja 7 §:n mukaan ei ole vielä julkinen, on viranomaisen harkinnassa. Harkinnassa on otettava huomioon, mitä 17 §:ssä säädetään.”
- ”Muuhun kuin lain mukaan salassa pidettävään asiakirjaan voidaan tehdä merkintä "HARKINNANVARAISESTI ANNETTAVA” (JulkL 16§)
- Asiakirjan merkitseminen voi olla tarpeellista
  - jos asiakirjan luovuttaminen on lain mukaan viranomaisen harkinnassa. Tämä viittaa tilanteisiin, joissa asiakirja ei ole vielä tullut 6 ja 7 §:n mukaisesti julkiseksi.
  - Asiakirjaan sisältyviä tietoja saa lain mukaan käyttää tai luovuttaa vain määrättyyn tarkoitukseen, kuten tietyt henkilötietoja sisältävät asiakirjat (HE 284/2018). Nämä asiakirjat eivät ole salassa pidettäviä, joten niihin eivät kohdistu salassa pidettäviä asiakirjoja koskevat käsittelyvaatimukset.
  - Suojatoimet on pääsääntöisesti arvioitava riskiperusteisesti ja lisäksi henkilötietojen käsittelyssä on otettava huomioon henkilötietoihin kohdistuvat käsittelyvaatimukset. erityisiä vaatimuksia. Laista ei tule käsittelyvaatimuksia, joten suojatoimet pitää arvioida riskiperusteisesti.
- Viranomainen on velvollinen huolehtimaan siitä, että tietojen saamista viranomaisen toiminnasta ei rajoiteta ilman asiallista ja laissa säädettyä perustetta eikä enempää kuin suojattavan edun vuoksi on tarpeellista ja että tiedon pyytäjiä kohdellaan tasapuolisesti.
- Lisäksi on otettava huomioon edellä mainitut erilaiset vahinkoedellytykset
- On pidettävä huolta siitä, että tiedonsaajalla on lain mukainen vaitiolovelvollisuus ja että tietoja annetaan muille kuin viranomaisille ja niissä toimiville vain, jos tiedon antamiselle on painava yleinen syy. (JulkL 17§)

Asiakirjojen ja tietojenkäsittelyn suojaamisen lähtökohdat

- Julkishallinnon hyvä hallinto ja tiedonhallintamalli
  - Tiedonhallintalain tarkoitus on varmistaa tietoaineistojen yhdenmukaisuus ja laadukas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi.
  - Tiedonhallintalain tarkoitus on myös mahdollistaa viranomaisten tietoaineistojen turvallinen ja tehokas hyödyntäminen sekä viranomaisten tehtävien hoito ja palvelut hallinnon asiakkaille hyvän hallinnon mukaisesti tuloksellisesti ja laadukkaasti.
  - Lisäksi lain tarkoituksena on edistää tietojärjestelmien ja tietovarantojen yhteentoimivuutta.
  - Tiedonhallinnan järjestämisessä olennaista on suunnitella keskeiset toimet ja tietoturvallisuustoimenpiteet. Suunnittelun tulisi perustua riskienhallintaan ja viranomaisen toiminnalle asetettuihin vaatimuksiin.
- Riskiperusteisuus toiminnassa ja vaatimuksissa
  - Tiedonhallintayksikön ja sen yhteydessä toimivan viranomaisen on huolehdittava toimintaympäristönsä tietoturvallisuudesta niin tietoaineistojen kuin tietojärjestelmien osalta.
  - Tietoturvallisuustoimenpiteitä on arvioitava riskiperusteisesti. Riskien arvioinnissa tulee huomioida käsiteltävien tietojen laatu ja määrä, esimerkiksi tietojen kasautumisvaikutus.
  - Tiedon paljastumiseen liittyvät riskit on aina arvioitava ja valittava tarvittavat lisäsuojaukset riskiarvioinnin perusteella.

Asiakirjojen ja tietojenkäsittelyn suojaamisen lähtökohdat

- Asioiden ja asiakirjojen hallinta
  - Tietoaineistojen tietoturvallisuudesta, tietojärjestelmien käyttöoikeuksien hallinnasta ja lokitietojen keräämisestä huolehtimisen lisäksi viranomaisen tulee huolehtia tietoaineistojen säilytystarpeiden määrittelystä sekä asioiden ja asiakirjojen merkinnästä asiarekisteriin
- Tietoturvallisuuden hallinta
  - Tiedonhallintalain 12-17 §:ssä on säädetty tietoturvallisuuteen liittyvät vähimmäisvaatimukset.
  - Vaatimusten toteutuminen varmistetaan siten, että tietoturvallisuuden hallinta on järjestelmällistä ja säännöllistä toimintaa. Tämä varmistetaan ottamalla käyttöön ja kuvaamalla organisaation tietoturvallisuuden hallintamalli.
- Palveluntarjoajille ja kumppaneille asetettavat vaatimukset
  - Tietoturvallisuus pitää huomioida myös kaikissa hankinnoissa ja yhteistyössä. Viranomaisen on varmistettava hankinnoissaan, että hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet. Käytännössä tietoturvavaatimukset on kuvattava hankinta-asiakirjoissa ja sopimuksissa sekä tarvittaessa varmistettava auditoinneilla.
  - Toimintaa ulkoistamalla ei voi ulkoistaa vastuuta tietoturvallisuudesta. Viranomainen vastaa siitä, että tietoturvallisuus on toteutettu myös ulkoistetuissa palveluissa. Myös tietosuojan toteutuminen on varmistettava samoin. Alihankkijoilla tai muilla sidosryhmillä ei ole viranomaisen tietoon liittyvää itsenäistä roolia, vaan tiedon salassapitoon ja julkisuuteen liittyvät päätökset tekee aina viranomainen. Toimeksiantotehtävää suoritettaessa toimeksiannon johdosta laadittuja asiakirjoja pidetään julkisuuslain 5 §:n mukaan lähtökohtaisesti tehtävän antaneen viranomaisen asiakirjoina. Niiden salassapitoon sovelletaan julkisuuslain (tai muita) salassapitosäännöksiä ja niiden antamisesta päättää julkisuuslain 14 §:n mukaan pääsääntöisesti tehtävän antanut viranomainen.
  - Salassa pidettävien asiakirjojen osalta on suositeltavaa, että salassapidosta sovitaan toimeksiantotilanteissa erikseen, jos salassa pidettäviä asiakirjoja tulee käsiteltäväksi. Näin voidaan myös katsoa, että viranomainen on tehnyt alun perin asiaan liittyvien tietojen luokittelua/salassapitoa koskevan päätöksen ja ohjeistaa sitten toimeksisaajaa noudattamaan sitä.
  - Kun muille kuin viranomaisille luovutetaan salassa pidettävää tietoa, heille tulee laatia ohjeistusta ja tarvittaessa järjestää koulutusta organisaation tietojen ja asiakirjojen turvallisesta käsittelystä.

Asiakirjojen ja tietojenkäsittelyn suojaamisen lähtökohdat

- Toimitilaturvallisuus
  - Kunkin viranomaisen on kuvattava omien toimitilojensa turvallisuusratkaisut ja määriteltävä missä tiloissa salassa pidettävää tietoa saa käsitellä ilman riskiperusteista arviointia ja suojausta.
  - On suositeltavaa, että salassa pidettävien asiakirjojen osalta noudatetaan lähtökohtaisesti samoja periaatteita kuin turvallisuusluokitteluasetuksessa (9 ja 10 §) on säädetty turvallisuusluokan IV asiakirjojen toimitila- ja käsittelyvaatimusten osalta.
  - Turvallisuusluokan IV asiakirjojen käsittely on sallittua asetuksessa kuvatuilla hallinnollisilla alueilla, eli alueilla, joilla on selkeästi määritetyt näkyvät rajat ja joihin vain valtionhallinnon viranomaisen valtuuttamilla henkilöillä on pääsy ilman saattajaa. Lisäksi tietojen käsittely on sallittua hallinnollisten alueiden ulkopuolella tietyin edellytyksin (asetuksen 10 §:n 4 mom).
  - Salassa pidettävien asiakirjojen osalta on esimerkiksi etätyön osalta vähintäänkin noudatettava tiedonhallintalain 14 §:n 1 momenttia, jonka mukaan: ”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.

Salassa pidettävän tiedon käsittely

- Tietoaineistojen käsittelylle asetettavat vaatimukset koskevat koko tiedon elinkaarta.
- Tiedon käsittelijä on erityisessä asemassa näiden vaatimusten toteuttamisessa. Hän vastaa kaikissa tietotyön tilanteissa siitä, että
  - henkilökohtainen tiedon käsittely tapahtuu oikein
  - työnantajan hänelle osoittamilla ja hyväksymillä työvälineillä
  - työnantajan antamien ohjeiden mukaisesti.

Salassa pidettävän asiakirjan käsittelyn rekisteröinti ja seuraaminen

- Tiedonhallintayksikön on ylläpidettävä viranomaisen käsittelyssä olevista ja olleista asioista asiarekisteriä, johon rekisteröidään asiaa, asiankäsittelyä ja asiakirjoja koskevat tiedot. (Tiedonhallintalaki 25 §)
- Lautakunta suosittelee, että käsittelyvaatimusten kohdentamiseksi salassa pidettävien asiakirjojen osalta tieto salassapidosta (ja salassapitoajasta) kirjataan myös asiarekisteriin asiakirjan metatietoihin.

Salassa pidettävän asiakirjan luovuttaminen

- Asiakirjojen luovuttajan on varmistettava, että tiedon luovutus tapahtuu turvallisesti. Esimerkiksi tietoliikenneyhteys tai luovutettava aineisto on salattava ja vastaanottaja tunnistettava riskiperusteisesti riittävän turvallisella tavalla (tiedonhallintalaki 14 §).
- Mikäli jollakin taholla on lakisääteinen oikeus saada tietoa, niin luovuttaja vastaa luovutuksen turvallisuudesta.
- Henkilötietojen luovuttamisessa on noudatettava yleistä tietosuoja-asetusta, julkisuuslakia sekä mahdollista henkilötietojen käsittelyn erityislainsäädäntöä.
- Lautakunta suosittelee että viranomainen ylläpitää turvallisia menettelyjä, joiden avulla vain tietoon oikeutetut pääsevät käsittelemään salassa pidettävää tietoa. Viranomaisen tulee todentaa riittävän vahvalla menettelyllä, esimerkiksi edellyttämällä henkilöiden tai palvelua pyytävien tahojen vahvaa tunnistamista, tarjotessaan käsittelymahdollisuuden salassa pidettävään tietoon.
- Asiakirjan antamisesta päättää julkisuuslain 14 §:n mukaan se viranomainen, jonka hallussa asiakirja on, jollei laissa toisin säädetä.
- Jos viranomaiselta pyydetään asiakirjaa, jonka toinen viranomainen on laatinut tai joka kuuluu toisen viranomaisen käsiteltävänä olevaan asiaan, viranomainen voi siirtää tiedonsaantipyynnön sille viranomaiselle, joka on laatinut asiakirjan tai jonka käsiteltävään asiaan se kuuluu (julkisuuslaki 15 § 1 mom). Jos on kyse turvallisuusluokiteltavasta asiakirjasta, jonka toinen viranomainen on laatinut, viranomaisen on siirrettävä tiedonsaantipyyntö asiakirjan laatineelle viranomaiselle (julkisuuslaki 15 § 3 mom).
- Asiakirjan luokittelumerkintä ei vaikuta viranomaisen velvollisuuteen arvioida asiakirjan julkisuutta tapaus- ja asiakirjakohtaisesti silloin, kun joku pyytää asiakirjasta tiedon julkisuuslain nojalla.
- Tiedonsaantipyyntöä ratkaistaessa on selvitettävä, ovatko perusteet salassapidolle edelleen olemassa. Salassapitomerkinnän asianmukaisuus on tarkistettava viimeistään asiakirjaa ulkopuoliselle annettaessa.

Asiakirjan vastaanottaminen

- Viranomaisten on tiedonhallintalain 25 §:n mukaisesti rekisteröitävä viipymättä sille saapunut tai sen laatima asiakirja asiakirjarekisteriin.
- Vastaanottajan on suositeltavaa myös arvioida, onko asiakirja salassa pidettävä ja tarvittaessa lisättävä asiakirjaan ja metatietoihin merkintä salassapidosta.
- Asiakirjan vastaanottaja, esimerkiksi kirjaamo, tarkistaa kenellä virkamiehellä on virkatehtäviensä puolesta oikeus käsitellä asiakirjaa. Välittäessään asiakirjaa kyseiselle virkamiehelle on huomioitava asiakirjan kuljettamiseen tai sähköiseen siirtoon liittyvät menettelytavat.

Asiakirjan siirtäminen tietoverkon kautta

- Salassa pidettäviä asiakirjoja saa siirtää yleisessä tietoverkossa salattua tai muuten suojattua tiedonsiirtoyhteyttä tai -tapaa käyttämällä (TihL 14 §). Salauksen riittävyys on arvioitava riskiperusteisesti.
- Lisäksi tietojensiirto on järjestettävä siten, että vastaanottaja varmistetaan tai tunnistetaan riittävän tietoturvallisella tavalla ennen kuin vastaanottaja pääsee käsittelemään siirrettyjä salassa pidettäviä tietoja. Salausratkaisujen turvallisuutta on käsitelty tarkemmin suosituksen Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä luvussa Salausratkaisut.
- Tiedonhallintalain 14 § koskee sekä viranomaisten välistä tiedonsiirtoa että tiedonsiirtoa hallinnon asiakkaille.
- Digitaalisen palvelun käyttäjän tunnistamisesta säädetään Digitaalisten palveluiden tarjoamisesta annetun lain 6 §.
- Esimerkiksi ilmaiset, verkosta saatavat pikaviestinpalvelut eivät pääsääntöisesti sovellu salassa pidettävän tiedon käsittelyyn tai henkilötietojen käsittelyyn asiakastyössä.

Asiakirjan kuljettaminen

- Kuljetukseen liittyvät riskit on arvioitava sekä tarvittavat tietoturvallisuustoimenpiteet on suunniteltava ja toteutettava riskilähtöisesti tunnistettujen riskien perusteella.
- Salassa pidettävien asiakirjojen kuljettaminen viranomaisen fyysisesti suojattujen suoja-alueiden ulkopuolella on toteutettava turvallisesti.
- Kuljettamisesta ei ole erityisiä vaatimuksia, vaan salassa pidettävä asiakirja voidaan antaa esimerkiksi postin kuljettaviksi tavanomaisesti pakattuina, mikäli se on riskiarvion perusteella mahdollista. Lähetyksestä ei kuitenkaan saa ulkoisesti käydä ilmi, että se sisältää salassa pidettävää tietoa.

Asiakirjan kopioiminen

- Salassa pidettävistä asiakirjoista voidaan ottaa sekä sähköisiä että paperimuotoisia kopioita.
- Kopioita tulee käsitellä samoin kuin alkuperäisiä asiakirjoja.
- Paperiasiakirjojen kopiointiin käytettyjen laitteiden turvallisuudesta pitää huolehtia riskiperusteisesti.

Tietojen säilyttäminen

- Salassa pidettäviä tietoja ja asiakirjoja sisältävät tietovarannot ja tietojärjestelmät on sijoitettava viranomaisen tähän tarkoitukseen määrittelemälle suoja-alueelle, jollainen on esimerkiksi turvallisuusluokitteluasetuksessa kuvattu hallinnollinen alue tai tieto pitää suojata riskiperusteisesti muilla turvakontrolleilla.
- Salassa pidettävät paperiasiakirjat on vastaavasti säilytettävä suoja-alueella tai soveltuvaksi arvioidussa lukitussa säilytyspaikassa.
- Tilanteissa, joissa salassa pidettävää tietoa käsitellään ja säilytetään päätelaitteessa suoja-alueiden ulkopuolella, on suositeltavaa että päätelaitteessa olevat tiedot olla on suojattu riittävän turvallisella salausratkaisulla. Erityisesti tulee varmistua päätelaitteen riittävästä eheydestä, jotta tiedon luottamuksellisuus ei vaarannu päätelaitteeseen kohdistuneen luvattoman pääsyn seurauksena.
- Tietojärjestelmien ja tietoliikennejärjestelyjen suojaamista on käsitelty tarkemmin Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä luvussa 7.

Asiakirjan tuhoaminen

- Tiedon suojaamisesta tulee huolehtia tiedon elinkaaren päättymiseen asti.
- Tarpeettomaksi käynyt, salassa pidettävä asiakirja on tuhottava tavalla, jolla riittävän luotettavasti estetään tietojen palauttaminen ja kokoaminen uudelleen kokonaan tai osittain.
- Organisaation tulee järjestää ja ohjeistaa henkilöstölle yksiselitteinen tapa salassa pidettävien tietojen tuhoamiseen; esimerkiksi keräysastioita, paperisilppureita ja henkilöstön turvallisuustietoisuuden varmistamista.
- Jos käytetään kolmannen osapuolen palvelua tiedon tuhoamiseen, palvelutoimittajan suorittaman tiedon turvallinen tuhoaminen tulee varmistaa sopimuksellisesti ja huolehtia toiminnan riittävästä valvonnasta.
- Erityisesti sähköisten aineistojen luotettavan tuhoamisen menettelyiden tulisi kattaa kaikki laitteistot, joihin on elinkaarensa aikana tallennettu salassa pidettävää tietoa. Menettelyiden tulee olla palvelutuottajien kanssa yhteisesti sovittuja.
- Salassa pidettävän tiedon luotettavasta tuhoamisesta on huolehdittava erityisesti laitteistojen käytöstä poiston, huoltoon lähetyksen tai uusiokäyttöön siirron yhteydessä. Mikäli luotettava tyhjennys ei ole mahdollista, salassa pidettävää tietoa sisältävää osaa ei tule luovuttaa kolmansille osapuolille.
- Jos laitteen muistia ei voida tyhjentää ennen huoltotoimenpiteitä, tulee kolmannen osapuolen suorittamia huoltotoimenpiteitä valvoa.
- Tietoaineiston tuhoamista koskevista teknisistä toteutuksista löytyy lisätietoa suosituksesta Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä

Tietojärjestelmien ja tietoliikennejärjestelyjen suojaamisen vähimmäisvaatimukset

- Viranomaisen 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.
- Tiedonhallintalain tietoturvallisuusvaatimusten (12-17 §) toteuttaminen: Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta.
- Tietojen ja tietojärjestelmien suojaamisessa pitää huomioida tietojärjestelmien tekninen toteutustapa ja niiden sijainti.
- Viranomaisen on ennakolta varmistuttava siitä, että salassa pidettävän asiakirjan suojaamisesta huolehditaan asianmukaisesti, jos se antaa salassa pidettävän asiakirjan ulkopuoliselle, kuten palvelutoimittajalle.
- Salassa pidettävien tietojen suojaamisessa tulee huomioida myös lainsäädäntöjohdannaiset riskit; eri maiden lainsäädännössä voidaan mahdollisesti velvoittaa palveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy palvelun asiakkaiden salassa pidettäviin tietoihin. Nämä riskit voivat ulottua sekä salassa pidettävän tiedon fyysiseen sijaintiin että muun muassa toisesta maasta käsin hallintayhteyksien kautta toteutettavaan tietojen luovutukseen.
- Salassa pidettävien tietojen käsittely tulisi rajata sellaisiin tietojenkäsittely-ympäristöihin ja tietojärjestelmiin, joiden riskeihin nähden riittävästä tietoturvallisuudesta viranomainen voi varmistua.

Salassa pidettävän tiedon käsittelyvälineet

- Salassa pidettävän tiedon sähköinen käsittely (myös etäyhteyden kautta) on mahdollista työnantajan tähän tarkoitukseen ohjeistamilla työvälineillä ja järjestelmillä.
- Ensisijaisesti käytetään työnantajan työntekijän käyttöön luovuttamia työvälineitä, muiden työvälineiden käyttö on mahdollista työnantajan suorittaman riskiarvioinnin ja antaman ohjeistuksen mukaisesti.
- Asiakirjan saa tulostaa verkkoon liitetyllä yhteiskäyttöisellä monitoimilaitteella edellyttäen, että kyseinen verkko ja monitoimilaite on arvioitu riittävän turvalliseksi riskiarvioinnin perusteella.

Muita huomioitavia seikkoja

- Tietojen ja tietojärjestelmien suojaamisesta tulee huolehtia riittävien fyysisten, teknisten ja hallinnollisten turvallisuusjärjestelyiden avulla. Näitä ovat mm.
  - Tietojärjestelmien erottelu
  - Ohjelmistohaavoittuvuuksien hallinta
  - Järjestelmäkovennusmenettelyt (turhien toiminnallisuuksien karsiminen)
  - Turvalliset muutoshallintamenettelyt
  - Varmuuskopiointimenettelyt
  - Käyttövaltuuksien hallinta ja vähimpien oikeuksien periaate
  - Käyttäjien ja laitteistojen tunnistaminen
  - Turvallinen ohjelmistokehitys ja käyttöönottomenettelyt
  - Lokitiedot ja jäljitettävyys
  - Poikkeamien havainnointi ja hallinta
  - Salausratkaisut
- Tarkempia tietoja
  - Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta
  - Suositus turvallisuusluokiteltavien asiakirjojen käsittelystä.

Suosituksen sisältö

- Johdanto
- Salassa pidettävä ja henkilötieto
- Asiakirjojen ja tietojenkäsittelyn suojaamisen lähtökohdat
- Salassa pidettävän tiedon käsittely
  - 4.1 Salassa pidettävän asiakirjan käsittelyn rekisteröinti ja seuraaminen
  - 4.2 Salassa pidettävän asiakirjan luovuttaminen ja vastaanottaminen
  - 4.3 Asiakirjan siirtäminen tietoverkon kautta
  - 4.4 Asiakirjan kuljettaminen
  - 4.5 Asiakirjan kopioiminen
  - 4.6 Tietojen säilyttäminen
  - 4.7 Asiakirjan tuhoaminen
- Tietojärjestelmien ja tietoliikennejärjestelyjen suojaamisen vähimmäisvaatimukset
- Säädökset ja lisätiedot

Lisätietoja

- Tiedonhallintalautakunta
- Tiedonhallintalautakunnan suositukset