Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua	
13 § Elinkaaren huomioiminen tietojen käsittelyssä	versio 0.9/01.11.2019

13.1 § Tietoaineistojen ja tietojärjestelmien tietoturvallisuus

Tiedonhallintayksikön on seurattava toimintaympäristönsä tietoturvallisuuden tilaa ja varmistettava tietoaineistojen ja tietojärjestelmien tietoturvallisuus koko niiden elinkaaren ajan.

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

Tiedon elinkaari alkaa sen käsittelyn käynnistyessä tiedon luonti tai vastaanottovaiheessa ja päättyy sen pysyvään säilyttämiseen arkistoinnin muodossa tai tiedon tuhoamiseen. Tiedon elinkaari kattaa siis kaikki tiedon käsittelyn vaiheet, jotka ovat **tiedon luonti** tai **vastaanotto**, **säilytys**, **käyttö**, **jakaminen** ja **siirto** sekä **arkistointi** tai **tuhoaminen**. Tiedon elinkaariajattelun lähtökohtana on tiedon suunnitelmallinen ja riskilähtöinen käsittely ja hallinta osana tiedonhallintayksikön toimintaa.

Tiedonhallintayksikkö varmistaa tietoaineistojen tietoturvallisuuden koko niiden elinkaaren ajan tunnistamalla tietoaineistojen käsittelyyn kohdistuvat riskit ja mitoitettava tietoturvallisuustoimenpiteet tämän riskiarvioinnin mukaisesti. Tietoaineistojen tietoturvallisuuden on täytettävä tiedonhallintalain asettamat vähimmäisvaatimukset, jotka on lueteltu kortissa Suositukset tietoturvallisuudesta.

Tiedon elinkaaren osalta on tärkeää huomioida, että tietoaineistoja käsitellään useassa eri sijainnissa ja tietojärjestelmässä tai laitteistossa, joissa tiedolla voi olla oma elinkaarensa ja tiedon elinkaari on yleensä pidempi kuin yksittäisen tietojärjestelmän elinkaari.

Tietoturvallisuus läpi tiedon elinkaaren
Tietoturvallisuus tietoaineistojen elinkaaressa muodostaa kokonaisuuden, johon kuuluvat **tiedon luokittelu, riskien arviointi**, **tietoturvallisuustoimenpiteiden suunnittelu** tunnistettujen riskien perusteella sekä **tietoturvallisuustoimenpiteiden toteuttaminen**. Tiedonhallintayksikön tulee arvioida tietoaineistoihin liittyviä riskejä säännöllisesti niiden koko elinkaaren ajan sekä huomioivat muuttuneiden riskien edellyttämät toimenpiteet tietoturvaa koskevissa suunnitelmissa ja toteutuksessa.

Tiedon osalta tunnistetaan ja määritetään, mihin sen käsittely perustuu ja mikä on tiedon käsittelyn tarkoitus varmistaen myös suunnitellun käsittelytarkoituksen toteutuminen läpi tiedon elinkaaren. Kaikissa tiedon elinkaaren vaiheissa varmistetaan, että tietoa käsitellään käsittelyperusteen muodostamien vaatimusten, tietoon kohdistuvien riskien ja tiedolle asetettujen tietoturvavaatimusten mukaisesti kaikissa käsittely-ympäristöissä. Tietoturvallisuus on alusta alkaen osa tietoaineistojen käsittelyyn liittyvien käytäntöjen ja käsittely-ympäristöjen suunnittelua ja toteutusta läpi koko tiedon elinkaaren.

Tiedon käsittelyyn liittyvät käytännöt ja käsittely-ympäristöt sekä muut käsittelyyn liittyvät tekijät ovat tiedonhallintayksikön tiedossa asianmukaisen tiedonhallinnan toteuttamiseksi ja tiedon käsittelyyn liittyvien riskien arvioimiseksi. Tietoa käsitellään tehtyjen suunnitelmien mukaisesti kaikissa elinkaaren vaiheissa. Lisätietoja turvallisuusluokitellun tiedon käsittelystä löytyy mm. Vahti-ohjeen 2/2010 Liitteestä 4.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua	
13 § Elinkaaren huomioiminen tietojen käsittelyssä	versio 0.9/01.11.2019

Keskeisiä tietoaineistojen elinkaareen liittyviä kysymyksiä:

- Onko tietoaineistojen käsittelyn peruste ja käyttötarkoitus tunnistettu ja määritetty?
- Onko tiedon käsittelyperusteen, kuten henkilötietojen muodostamat vaatimukset tunnistettu?
- Onko tietoaineistoihin liittyvät riskit arvioitu koko tiedon elinkaaren ajalta? Seurataanko riskejä säännöllisesti?
- Ovatko tiedon käsittelyyn liittyvät käytännöt ja käsittely-ympäristöt sekä muut käsittelyyn liittyvät tekijät tiedonhallintayksikön tiedossa (Tiedonhallintamalli & ministeriöillä lisäksi tiedonhallintakartta)

Tiedon luonti ja vastaanotto

Tietoaineistojen luonnilla tarkoitetaan käsittelyvaihetta, jossa luodaan uutta tietoa tai tehdään tietoaineistoon päivityksiä. Tietoaineistojen vastaanotolla tarkoitetaan käsittelyvaihetta, jossa tiedonhallintayksikkö vastaanottaa muualla tuotettuja tietoaineistoja.

Tiedon luonnin tai vastaanoton yhteydessä tunnistetaan ja kuvataan tiedon käsittelyn perusteet ja tarkoitus. Luotavan ja vastaanotettavan tiedon kohdalla tunnistetaan niiden käsittelyä koskevat erityisvaatimukset, jotka voivat muodostua esimerkiksi lainsäädännöstä tai toisen organisaation tiedon käsittelylle asettamista vaateista. Tällaisia erityisvaatimuksia muodostaa esimerkiksi henkilötietoja koskeva tietosuojalainsäädäntö.

Keskeisiä tiedon luontiin ja vastaanottoon liittyviä kysymyksiä:

- Onko tietoaineistojen käsittelyn peruste ja käyttötarkoitus tunnistettu ja määritetty?
- Onko käsiteltävää tietoaineistoa koskevat erityisvaatimukset, kuten henkilötietoihin liittyvät vaatimukset tunnistettu?

Tiedon säilytys

Säilytyksen osalta määritellään ja toteutetaan tiedon riittävä suojaus sille muodostettujen vaatimusten ja hallintakeinojen sekä riskitason mukaisesti. Tiedon suojauksen avulla turvataan tiedon luottamuksellisuuden ja eheyden säilymistä ja varmistetaan sen saatavuus. Suojaus kattaa tekniset ja hallinnolliset suojakeinot. Ohjeistuksia tiedon asianmukaiseen säilytykseen

Säilytyksessä varmistetaan tiedon saatavuus ja säilyminen sekä sen säilytysajan mittainen käytettävyys esimerkiksi datan kohdalla teknologioiden muuttuessa. Tiedon säilytyksen suunnittelussa ja toteutuksessa varaudutaan riskiarvioissa tunnistettuihin uhkatilanteisiin riskien edellyttämällä tasolla muun muassa asianmukaisen salauksen ja jatkuvuuden hallinnan avulla. Tietoaineistoille on määritetty säilytysajat, joiden päättyessä tietoaineistot joko arkistoidaan tai tuhotaan. Lisätietoja salauskäytännöistä löytyy mm. Vahti-ohjeesta 2/2015.

Tietoaineistojen säilytykseen käytetään ainoastaan siihen hyväksyttyjä ja asetettujen vaatimusten mukaisia säilytysympäristöjä, jotka noudattavat kortin 13 § Elinkaaren huomioiminen tietojärjestelmissä periaatteita.

Keskeisiä tiedon säilytykseen liittyviä kysymyksiä:

- Onko säilytettävä tieto suojaustasoluokiteltua (turvallisuusluokiteltua)? Jos on, onko tämän säilytykseen liittyvät vaatimukset tunnistettu ja täytetäänkö ne?
- Säilytetäänkö tietoa siten, että vain ne tahot joilla on oikeutettu pääsy tietoon pääsevät siihen käsiksi?
- Onko tiedon säilytys suunniteltu siten, että sen käytettävyys ja saatavuus on taattu myös poikkeusoloissa, mikäli riskiarvio näin edellyttää?
- Onko säilytettävälle tiedolle määritetty säilytysaika, jonka päättyessä se joko arkistoidaan tai tuhotaan asianmukaisesti?

Tiedon käyttö

Tietoaineistojen luvallinen käyttö mahdollistetaan ja luvaton käyttö estetään henkilöiden työtehtäviin perustuvalla roolipohjaisella fyysisten ja loogisten käyttöoikeuksien ja –valtuuksien määrittämisellä ja hallinnalla. Tietoaineistojen käyttäjän identiteetti todennetaan riskeihin ja käytettävään tietoon nähden riittävällä tavalla.

Tietoaineistojen käyttöä seurataan ja valvotaan tehdyn riskiarvioinnin mukaisesti asianmukaisella tavalla. Tietojärjestelmien kohdalla vähintään sisään ja uloskirjautumisista sekä näiden yrityksistä tulee tuottaa lokia, mutta useissa tapauksissa myös järjestelmän sisällä toimimisesta tulee kerätä käyttölokia. Tietoaineistojen käytön lokitus ja valvonta toteutetaan tarpeellisuusarvioinnin perusteella tiedon käyttötarkoituksen ja siihen liittyvien riskien edellyttämällä tavalla huomioiden kortin 17 § lokitietojen kerääminen periaatteet.

Tietoaineistoja käyttö tapahtuu siihen hyväksytyissä ja asetettujen vaatimusten mukaisissa tietojärjestelmissä, laitteissa ja käsittely-ympäristöissä. Keskeisiä tiedon käyttöön liittyviä kysymyksiä:

- Ovatko tietoaineiston käyttöoikeudet ja –valtuudet määritetty perustuen henkilön työtehtäviin?
- Valvotaanko tietoaineiston käyttöä riskiarvion mukaisesti?
- Voidaanko olla varmoja siitä, että tietoaineistoa käsitellään vain siihen hyväksytyissä ja asetettujen vaatimusten mukaisissa tietojärjestelmissä, laitteissa ja käsittely-ympäristöissä?

Tiedon jakaminen, siirtäminen ja luovuttaminen

Tietoaineistojen jakamisella tarkoitetaan toimia, joiden avulla päätetään tietoaineiston vastaanottajat, varmistetaan vastaanottajien tiedontarve ja oikeus sekä kyky käsitellä jaettavaa tietoaineistoa. Tietoaineistojen siirrolla tarkoitetaan niitä toimenpiteitä, joilla tietoaineistot siirretään määritetyille tahoille tai toisiin tietojärjestelmiin. Siirto voi tapahtua esimerkiksi postin, sähköpostin, sähköisen muistivälineen, tietojärjestelmien välisen tiedonsiirron tai käsittelyoikeuksien myöntämisen avulla. Ei-julkista tai suojaustaso- tai turvallisuusluokiteltua tietoa jakaessa ja siirtäessä tulee muistaa, että tavallinen sähköposti ei lähtökohtaisesti oli salattu, turvallinen tiedonvälityskanava. Tällaista tietoa siirrettäessä tulee olla erityisen varma, että tiedonsiirrossa käytettävä menetelmä on salattu ja riittävän turvallinen. Lisätietoja turvallisesta tiedon siirrosta Kyberturvallisuuskeskuksen ohjeessa yhdyskäytäväratkaisuista.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua	
13 § Elinkaaren huomioiminen tietojen käsittelyssä	versio 0.9/01.11.2019

Tietoa jaettaessa, siirrettäessä ja luovutettaessa varmistutaan aina riittävän luotettavasti mahdollisen vastaanottajan identiteetistä sekä toteutetaan tiedon siirto tunnistettuihin riskeihin nähden asianmukaista salausta ja suojausta käyttäen. Näin varmistetaan, etteivät tietoon pääse käsiksi siihen oikeudettomat henkilöt ja tietoaineisto jaetaan tai luovutetaan vain henkilöille, joilla on siihen työtehtäviinsä liittyvä oikeus. Lisätietoja turvallisista salausratkaisuista Kyberturvallisuuskeskuksen hyväksymissä salausratkaisuissa.

Kun tietoaineistoja jaetaan tai luovutetaan viranomaisten välillä, huomioidaan suositukset teknisistä rajapinnoista ja katseluyhteyksistä. Keskeisiä tiedon jakamiseen, siirtämiseen ja luovuttamiseen liittyviä kysymyksiä:

- Voidaanko tietoaineistoa jakaessa, siirtäessä ja luovuttaessa varmistua riittävällä tasolla vastaanottajan identiteetistä?
- Käytetäänkö tiedon siirrossa asianmukaista salausta?
- Onko tietoja luovutettaessa varmistuttu siitä, että tiedon luovuttaminen on lain mukaista ja vastaanottajalla on oikeus tietoaineiston käsittelyyn sekä kyky käsitellä sitä vaatimusten mukaisesti?

Tiedon arkistointi

Tietoaineistojen arkistoinnilla tarkoitetaan niitä menettelyjä, joilla varmistetaan tiedon säilyminen asetetun elinjakson ajan.

Arkistoinnissa huomioidaan tiedon säilytysaika, -paikka ja -tapa sekä varmistetaan tiedon käyttökelpoisuus ja luettavuus koko säilytysajaksi. Arkistointi perustuu sitä koskevaan sääntelyyn ja näiden pohjalta laadittuihin suunnitelmiin. Lisätietoja arkistoinnin vaatimuksista löytyy Kansallisarkiston ohjaussivulla.

Keskeisiä tiedon arkistointiin liittyviä kysymyksiä:

- Onko arkistoinnissa huomioitu tiedon säilytysaika, -paikka ja tapa?
- Onko tiedon käyttökelpoisuudesta ja luettavuudesta varmistuttu koko tiedon säilytysajan?
- Perustuuko arkistointi sitä koskevaan sääntelyyn ja näiden pohjalta laadittuihin suunnitelmiin?

Avoin data

Viranomainen voi laissa säädettyjen tiedonsaantioikeuksien perusteella julkaista tai luovuttaa tietoja avoimeksi dataksi. Viranomaisen on huomattava, että julkinen tieto ei tarkoita samaa asiaa kuin avoin data. Myös joukko henkilötietoja voidaan avata, kun niistä on tehty mahdottomaksi tunnistaa tietojen kohde, eli tieto on anonymisoitu. Anonymisoinnissa on pyrittävä arvioiman teknologioiden kehittyminen, ja mahdollisuudet siihen, että henkilöitä on tulevaisuudessa mahdollista tunnistaa tietoja yhdistelemällä tai purkamalla tehtyä anonymisointia. Avoimen datan luovuttamiseen anonymisoitunakin saattaa liittyä riskejä esimerkiksi mainehaitasta, mikäli tiedon luovuttamista saatettaisiin pitää sopimattomana. Esimerkkinä tällaisesta voisi toimia esimerkiksi anonymisoitujen, yksityiskohtaisten terveystietojen luovuttaminen.

Tiedon luovuttamiseen liittyvä hyöty- ja riskisuhde tulee arvioida huolellisesti, ennen päätöstä tietojen luovuttamisesta. Julkaistavan datan osalta tulee myös tunnistaa sen käsittelyyn liittyvät kustannukset,

kuten anonymisointi ja ylläpito. Suuri osa avoimen datan julkaisemisen kustannuksiin liittyy anonymisointiin käyttävään henkilöstöresurssiin.

Tiedon tuhoaminen
Tietoaineistojen tuhoamisella tarkoitetaan niitä toimenpiteitä, joiden avulla tietoaineistot tuhotaan tarkoituksella niiden säilytysajan ja käyttötarpeen päättyessä tai niitä sisältävän laitteiston käytöstä poiston, huoltoon lähetyksen tai uusiokäyttöön siirron yhteydessä.

Tiedon tuhoaminen tapahtuu määritellyn säilytysajan tai käyttötarpeen päättyessä tunnistettuihin riskeihin nähden riittävän luotettavalla tavalla. Tietoaineistoille määritetyt säilytysajat huomioidaan tiedon tuhoamisen suunnittelussa. Tietoaineistoista muodostetut kopiot ja luonnokset sekä väliaikaistiedostot tuhotaan niiden käyttötarpeen päätyttyä.

Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen joutuminen oikeudettomien henkilöiden haltuun esimerkiksi kokoamalla tietoaineistoja kokonaan tai osittain uudelleen. Salassa pidettävän tietoaineiston tuhoamiseen voidaan käyttää useita eri menetelmiä ja työvälineitä riippuen muun muassa tiedon olomuodosta ja saatavilla olevista erilaisista ratkaisuista. Esimerkiksi tiedon silppuamisen tai kovalevyn ylikirjoituksen sijaan tai lisäksi silppu voidaan polttaa ja kiintolevy sulattaa.

Erityisesti sähköisten aineistojen luotettavan tuhoamisen menettelyjen tulisi kattaa kaikki laitteistot, joihin on elinkaarensa aikana tallennettu salassa pidettävää tietoa. Laitteistojen osien (kiintolevyt, muistit, muistikortit, jne.) sisältämän salassa pidettävän tiedon luotettavasta tuhoamisesta on huolehdittava erityisesti käytöstä poiston, huoltoon lähetyksen tai uusiokäyttöön siirron yhteydessä. Mikäli luotettava tyhjennys (esimerkiksi viranomaisen hyväksymä ylikirjoitusmenettely) ei ole mahdollista, salassa pidettävää tietoa sisältävää osaa ei tule luovuttaa kolmansille osapuolille. Tilanteissa, joissa laitteen muistia tai vastaavaa ei voida luotettavasti tyhjentää ennen huoltotoimenpiteitä, tulisi kolmannen osapuolen suorittamia huoltotoimenpiteitä valvoa, ja pyrkiä varmistumaan siitä, että salassa pidettävää tietoa ei viedä huoltotoimenpiteen yhteydessä.

Keskeisiä tiedon tuhoamiseen liityviä kysymyksiä:

- Tapahtuuko tiedon tuhoaminen määritellyn säilytysajan tai käyttötarpeen päättyessä riittävän luotettavalla tavalla? Käytetäänkö tässä menetelmää, jolla estetään tietojen kokoaminen uudestaan tai osittain?
- Kattavatko luotettavan tuhoamisen menettelyt kaikki laitteistot joihin on elinkaarensa aikana tallennettu salassa pidettävää tietoa?

EU:n yleinen tietosuoja-asetus
Arkistolaki
Kortti Suositukset tietoturvallisuudesta
Kortti 13 § Elinkaaren huomioiminen tietojärjestelmissä
Kyberturvallisuuskeskuksen hyväksymät salausratkaisut
Kyberturvallisuuskeskuksen hyväksymä ylikirjoitusmenettely
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/Yhdyskaytavaratkaisuohje.pdf

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua	
13 § Elinkaaren huomioiminen tietojen käsittelyssä	versio 0.9/01.11.2019

https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje-kryptografiset-vahvuusvaatimukset-kansalliset-suojaustasot.pdf

Koko elinkaari	Tietoaineistoihin liittyvät riskit arvioidaan säännöllisesti
	Tunnistetaan ja määritetään tietoaineistojen käsittelyn peruste ja käyttötarkoitus
	Varmistetaan, että tiedon käsittelyperusteen muodostamat vaatimukset, tietoon kohdistuvat riskit ja tiedolle asetetut tietoturvavaatimukset huomioidaan tiedon käsittelyn kaikissa vaiheissa
	Tiedon käsittelyyn liittyvät käytännöt ja käsittely-ympäristöt sekä muut käsittelyyn liittyvät tekijät tulee olla tiedonhallintayksikön tiedossa (Tiedonhallintamalli & ministeriöillä lisäksi tiedonhallintakartta)
Tiedon luonti ja vastaanotto	Tunnistetaan ja kuvataan tiedon käsittelyn perusteet ja käsittelytarkoitus
	Tunnistetaan tiedon käsittelyä koskevat erityisvaatimukset (esim. lainsäädännöstä tai toisen organisaation vaatimuksista muodostuvat)
Tiedon säilytys	Säilytettävää tietoa suojataan sille muodostettujen vaatimusten ja hallintakeinojen sekä riskitason mukaisesti
	Säilytettävän tiedon säilyminen ja saatavuus on turvattu
	Säilytettävän tiedon käytettävyys on varmistettu koko säilytysajan
	Tietoaineistolle on määritetty säilytysaika ja sen päättyessä tieto joko arkistoidaan tai tuhotaan
	Tietoaineistojen säilytykseen käytetään ainoastaan siihen hyväksyttyjä ja asetettujen vaatimusten mukaisia säilytysympäristöjä.
Tiedon käyttö	Käyttöoikeudet ja –valtuudet tietoaineistoihin perustuvat henkilöiden työtehtäviin
	Tietoaineistojen käyttöä lokitetaan riskiperustaisesti
	Tietoaineistoja käyttö tapahtuu ainoastaan siihen hyväksytyissä ja asetettujen vaatimusten mukaisissa tietojärjestelmissä, laitteissa ja käsittely-ympäristöissä.
Tiedon jakaminen, siirtäminen ja luovuttaminen	Tietoa jaettaessa, siirrettäessä ja luovuttaessa varmistutaan riittävällä tasolla vastaanottajan identiteetistä
	Tiedon siirrossa käytetään asianmukaista salausta
	Tietoa luovutettaessa varmistetaan, että tiedon luovuttaminen on lain mukaista ja vastaanottajalla on oikeus tietoaineiston käsittelyyn sekä kyky käsitellä sitä vaatimusten mukaisesti
Tiedon arkistointi	Arkistoinnissa huomioidaan tiedon säilytysaika, -paikka ja –tapa.

Laki julkisen hallinnon tiedonhallinnasta **Suosituskortti** **Kohderyhmä:** Johto, tiedonhallinta ja tietoturvallisuusasiantuntijat, ICT-kehittäjät, tiedonkäsittelijät **Käyttötarkoitus:** Tiedonhallinnan muutosten arviointi, osana uuden tietojärjestelmän kehittämisen projektivalmistelua	
13 § Elinkaaren huomioiminen tietojen käsittelyssä	versio 0.9/01.11.2019

	Arkistoinnissa on varmistettu tiedon käyttökelpoisuus ja luettavuus koko säilytysajaksi.
	Arkistointi perustuu sitä koskevaan sääntelyyn ja näiden pohjalta laadittuihin suunnitelmiin.
Tiedon tuhoaminen	Tiedon tuhoaminen tapahtuu määritellyn säilytysajan tai käyttötarpeen päättyessä riittävän luotettavalla tavalla.
	Tuhoamisessa käytetään menetelmiä, joilla estetään tietojen kokoaminen uudelleen kokonaan tai osittain.
	Sähköisten aineistojen luotettavan tuhoamisen menettelyt kattavat kaikki laitteistot, joihin on elinkaarensa aikana tallennettu salassa pidettävää tietoa.