Tietotilinpäätös – osoitusvelvollisuuden toteuttamisessa

Esitys perustuu Kati Suojasen ja Minna Järvisen kehittämistyöhön ”Tietotilinpäätös – sen prosessit, toimijat ja rakenne” vuodelta 2018

Juhta/VAHTI työpaja 22.8.2018
Tuula Seppo, Kuntaliitto

DOKUMENTIN EI TULISI OLLA VAIN SELOSTAVA SAAVUTUSTEN LUETTELO!

(erään haastatellun henkilön huomio)

Kehittämistyö ja malli

- Kati Suojanen ja Minna Järvinen kävivät läpi 6 organisaation tietotilinpäätöksen (THL, Trafi, HALTIK, Viestintävirasto, Tietoarkisto, VRK)ja haastattelivat 3 (Tampere, Espoo, Forssa) tietosuojavastaavaa
- He vertasivat tietotilinpäätöksiä tietosuojavaltuutetun toimiston v. 2012 olevaan ohjeistukseen

Yleisiä havaintoja:

- Tietotilinpäätös ei ole vielä vakiintunut johdon työkaluna
- Laadinta on usein tietosuojavastaavan harteilla
- Eivät ole kuntasektorilla kovin yleisiä
  - » 2017 tietotilinpäätös oli vain 8 % kaikista kunnista (suurimmilla 17%) (PG Seppo 2017)
  - » Julkisuus/salassapito, ovatko vain organisaation sisäisiä dokumentteja

Yleisiä havaintoja tietotilinpäätöksestä:

- Ei ole asemaa virallisena dokumenttina
- On usein yleisluonteisia ja selostavia
- Tarve saada yhteismitallisia ja todellisia tietosuojan ja tietoturvan tilaa koskevia mittaristoja
- Miten huomioidaan esim. palvelusetelitoimittajat
- Tietotilinpäätöksellä tärkeä rooli osoitusvelvollisuuden toteuttajana sekä läpinäkyvyyden ja avoimuuden osoittajana

Tietotilinpäätös

- Tulee antaa kokonaiskuva tietojenkäsittelyn tilasta ja koko henkilötietojen käsittelyn elinkaarta kuvaava arviointi
- Arvioi tietojenkäsittelyn nykytilaa, tietosuojaa, tietoturvaa
- Vapaaehtoinen kerran vuodessa tehtävä sisäisen tietojohtamisen raportti

- Osa riskienhallintaa ja sisäistä valvontaa

- Hyvää hallintotapaa ja luottamuksen rakentamista
- Miten yksilön ja organisaation oikeudet ja velvollisuudet toteutuvat
- Miten tietosuojaperiaatteita noudatetaan ja miten ne toteutuvat?
-

Tietotilinpäätös

- Tietojenkäsittelyllä on merkitystä kilpailukykyyn, vaikuttavuuteen, tehokkuuteen
- Tärkeää tietoa myös sidosryhmille

- Rekisterinpitäjien välinen yhteistyö

- Apuväline kehittämistoimenpiteiden seurantaan

- Lainsäädännön toteutuminen
  - » osoitusvelvollisuus, avoimuus, läpinäkyvyys

Tietotilinpäätösmalli

1. Tietotilinpäätöksen tarkoitus
2. Tietoturvallisuuden ja –suojan toteuttaminen organisaatiossa
3. Tiedonhallinta, tietovarannot ja tietovirrat
4. Tietojenkäsittelyyn vaikuttava lainsäädäntö ja muu ohjeistus
5. Rekisteröidyn oikeudet ja niiden toteuttaminen
6. Seuranta ja mittaaminen
7. Arviointi ja kehittäminen

1. Tietotilinpäätöksen tarkoitus

- Johdanto-osio
- Mikä merkitys tällä dokumentilla on
- Kenelle se on tarkoitettu
- Miten tiedot on koottu
- Onko osa strategiatyötä
- Onko kyseessä tiivistelmä, onko erikseen julkinen ja salassapidettävä osio
- Keskeiset käsitteet, lait ja tietosuojaperiaatteet
- Keskeiset havainnot ja tärkeimmät tapahtuneet asiat
- **Tiivistelmä**

2. Tietoturvallisuuden ja –suojan toteuttaminen organisaatiossa

- Tietosuojaperiaatteina (5 art.) eheys, luottamuksellisuus
- Miten tietoturva ja -suojatyö on organisoitu
- Miten on toteutettu tekniset ja organisatoriset toimenpiteet (esim. henkilöstön koulutus, sisäiset ohjeet ja määräykset, salassapitosopimukset, tilavalvontaa, käytönvalvontaa, tietojen salaus, anonymisointi, pseudonymisointi, etäkäyttöyhteydet, auditoinnit, käytetyt sertifikaatit)
- Sovellusten ja tietokoneiden hankinta, käyttöönotto, kehittäminen ja ylläpito
- Riskianalyysit, vaikutustenarvioinnit, ennakkokuulemiset, jatkuvuuden hallinta, varautuminen
- Tietoturvapoikkeamiin varautuminen ja niiden määrä

3. Tiedonhallinta, tietovarannot ja tietovirrat

- Tietosuojaperiaatteina (5 art.) tietojen minimointi, käyttötarkoitussidonnaisuus, säilytyksen rajoittaminen
- Tiedonhallinnan, tietovarantojen ja tietovirtojen kokonaistilan kuvaus
- Kokonaisarkkitehtuuri, tiedonohjaussuunnitelmat, sopimusmallit
- Keneltä tietoa saadaan ja kenelle sitä luovutetaan?
- Miten asioita laitetaan vireille?
- Miten hallitaan tiedon koko elinkaari, säilytysajat, hävittäminen, arkistointi

4. Tietojenkäsittelyyn vaikuttava lainsäädäntö ja muu ohjeistus

- Tietosuojaperiaatteina (5 art.) lainmukaisuus, kohtuullisuus, läpinäkyvyys
- Lainsäädännöllinen tausta esim. mihin lainsäädäntöön henkilötietojen käsittely perustuu
- Käytännesäännöt, sertifioinnit, auditoinnit
- Laaditut tietosuojaselosteet ja niiden ajantasaisuus
- Toimintapolitiikat, ohjeet, koulutukset ja perehdytykset ja seloste henkilötietojen käsittelytoimista
- Tiedon laatu ja käytettyvyys

5. Rekisteröidyn oikeudet ja niiden toteuttaminen

- Tietosuojaperiaatteina (5 art.) läpinäkyvyys ja kohtuullisuus
- Miten rekisteröidyn oikeudet toteutuvat omassa organisaatiossa käytännössä
- Kuinka paljon näitä oikeuksia on käytetty
  - » Mittareina esim. tarkastusoikeuksien ja virheenkorjauspyyntöjen määrä
- Tietosuojaselosteiden ajantasaisuus
- Informoinnin läpinäkyvyys

6. Seuranta ja mittaaminen

- Kokoaa yhteen organisaation tietosuojatyöhön liittyvät keskeiset seurannan menetelmät ja tulokset
- Tietosuojamittarit, mitä seurataan ja kuinka
- Tietoturvaloukkausten määrä
- Tehdyt riski-ja vaikutustenarvioinnit
- Rekisteröidyn oikeuksiin liittyvät mittarit
  - » Mittareina esim. tarkastusoikeuksien ja virheenkorjauspyyntöjen määrä, tietoturvaloukkausilmoitukset
- Yhteistyö valvontaviranomaisen kanssa
- Asiakastyytyväisyys ja palvelujen saatavuus

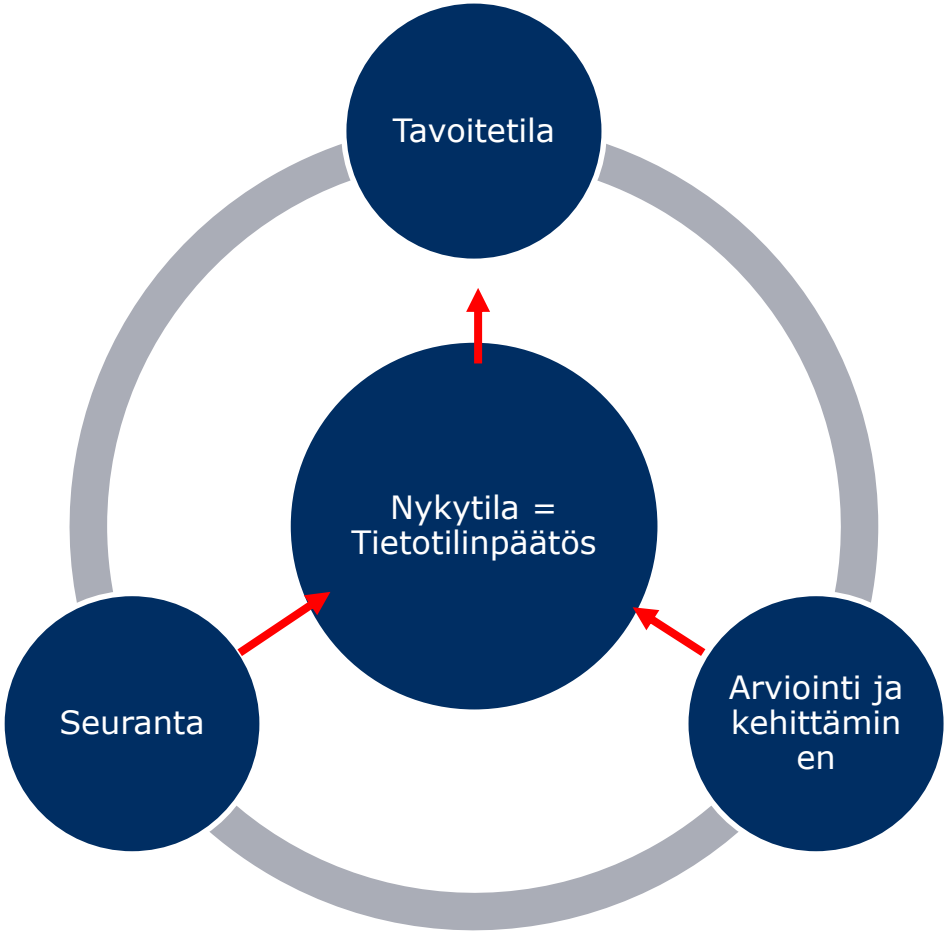
Mittareita esim. (Andreasson, Riikonen, Ylipartanen, 2017)

- Henkilötietojen tarkastusoikeuden, poisto- ja korjauspyyntöjen määrä
- Valvontaviranomaisten selvitys- ja tietopyynnöt
- Tarpeelliset ilmoitukset valvontaviranomaiselle
- Käyttö- ja luovutuslokipyynnöt
- Käytönvalvonnan toteuttaminen kuukausitasolla
- Vakavat tietoturvapoikkeamat
- Esille tulleet tietosuojarikkomukset ja niiden epäillyt
- Tietojärjestelmien käyttökatkot ja niiden laajuudet
- Tietojärjestelmien määrä
- Auditoinnit
- Käyttötukipyynnöt
- Koulutusmäärät

7. Arviointi ja kehittäminen

- Tilannearvio ja kehittämistavoitteet
- Apuna mm. kokonaisarkkitehtuurikuvaukset
- Työntekijöiden tarpeet (millaista koulutusta, ohjeistusta, prosessien kehittämistä tarvitaan?)
- Miten jo tehdyt kehittämistoimenpiteet ovat toteutuneet

Tietotilinpäätös prosessin vaiheet.



Yhteistyössä tehtävä jatkuva prosessi!

Läpinäkyvyys ja avoimuus!

Visuaalinen ja selkeä!

Helppolukuinen!

Luottamuksen rakentaja!

Yksi osoitusvelvollisuuden osoittamisen dokumenteista!