

TIETOTILINPÄÄTÖS

Ylitarkastaja Arto Ylipartanen/
Tietosuojavaltuutetun toimisto

Terveydenhuollon ATK-päivät 20.5.2014;
Jyväskylä

LUENNON AIHEET

- 1. MIKÄ ON TIETOTILINPÄÄTÖS ?**
- 2. MIKSI TIETOTILINPÄÄTÖS KANNATTAÄ TEHDÄ ?**
- 3. MITEN TIETOTILINPÄÄTÖS TEHDÄÄN ?**
- 4. ARVIOINTI JA KEHITTÄMISKOHTEET**
- 5. HAASTEET**

1. MIKÄ ON TIETOTILINPÄÄTÖS ?

- Tilinpäätöksellä pitkä historia organisaatioiden taloudellisen aseman raportoijana
- Täydentävinä: yhteiskunta- ja ympäristövastuuraportit sekä henkilöstötilinpäätös
- Tietotilinpäätös: dynaaminen työkalu, joka tukee organisaation tehokkuutta, vaikuttavuutta ja kilpailukykyä
- Tietotilinpäätöksen sisältö voi vaihdella organisaation toimialasta ja toiminnan laadusta riippuen.

Tietotilinpäätös on organisaation sisäisen tarkastelun tuloksena syntyvä raportti, joka esimerkiksi:

- antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta
- kuvaa mitä tietovarantoja organisaation hallussa on
- kuvaa organisaation toimintaan liittyvät tietovirrat
- kuvaa organisaation tietovirtojen yhteentoimivuuden tietojenkäsittelyn kanssa
- kuvaa miten tietosuoja ja -turva toteutuvat organisaation toiminnassa
- kuvaa miten tietojenkäsittelyyn liittyvä riskienhallinta on toteutettu

- toimii suunnittelun ja toiminnan ohjauksen tukena organisaatiossa
- toimii raportoinnin ja johtamisen tukena organisaatiossa
- toimii kehittämistoimenpiteiden seurannan apuvälineenä
- toimii organisaatiosta ulospäin tapahtuvan sidosryhmäraportoinnin välineenä
- varmistaa sovellettavan lainsäädännön noudattamisen

- Tietotilin päätös toteuttaa myös ns. accountability- eli ”tilintekovelvollisuus”-periaatetta. Tämän periaatteen mukaan organisaatio itse näyttää, että se noudattaa lakia, hyvää tietojenkäsittelytapaa ja hyvää tiedonhallintatapaa.
- Lähitulevaisuudessa EU:n tietosuoja-asetus edellyttänee ”tilintekovelvollisuus” -periaatteen mukaisten menettelyjen käyttöön ottamista.
- Tietotilin päätöksessä tapahtuva dokumentointi ohjaa myös systemaattisesti läpikäymään asioita ja tarkastelemaan niitä kriittisemmin.

2. MIKSI TIETOTILINPÄÄTÖS KANNATTAA TEHDÄ ?

- 2.1. Tietotilinpäätös luottamuksen rakentajana
- 2.2. Tietotilinpäätös johdon työvälineenä
- 2.3. Tietotilinpäätös sisäisen ja ulkoisen valvonnan apuvälineenä

Yleistä

- Tietojen korkea laatu ja toimivat menettelytavat tietojen käsittelyssä vaikuttavat positiivisesti kaikkiin organisaation toiminnan osa-alueisiin.
- Tieto on arvokas ja ainoa voimakkaasti kasvava tuotannontekijä.
- Tietojen käsittely vaikuttaa myös olennaisesti kilpailukykyyn, vaikuttavuuteen ja organisaation tehokkuuteen.
- Nykyisin on olemassa selkeä tarve kokonaisvaltaiseen näkökulmaan tietovarantojen hallinnassa, ratkaisu tällaisiin tarpeisiin on tietotilinpäätöksen laatiminen.

2.1. Tietotilinpäätös luottamuksen rakentajana

- Riskien minimointi, hyvän maineen rakentaminen, kansalaisten ja kuluttajien luottamuksen säilyttäminen ovat ratkaisevan tärkeitä asioita kaikkien sektoreiden toiminnan menestymiselle.
- Erityisesti verkkoympäristössä tietosuojaan liittyvät puutteet koetaan ongelmana asioinnin luotettavuuden ja käytettävyyden kannalta.
- Vääriin käsiin joutuneet henkilötiedot ovat uhka tietojen kohteen eli rekisteröidyn oikeuksille ja tietojen suojauksen laiminlyönnistä vastuullisen organisaation toiminnalle.
- Tietotilinpäätös kertoo eri sidosryhmille, että organisaatio näkee tärkeäksi panostaa tietojen käsittelyssä noudatettaviin menettelytapoihin ja hyvän tietojenkäsittelytavan sekä tiedonhallintatavan noudattamiseen.

2.2. Tietotilinpäättös johdon työvälineenä

- Tietotilinpäättös on osa tietojohdantamista sekä siihen kuuluvaa riskienhallintaa ja sisäistä valvontaa.
- Tietoturvallisuuden ja tietosuojan säännöllinen arviointi on osa organisaation tietojohdantamista.
- Arvioinnin tavoitteena on varmistaa tarjottavien palvelujen toimintakyky ja käytettävyys, tietoaineistojen laatu ja käytössä olevan tietotekniikan turvallisuus.

2.3. Tietotilinpäättös sisäisen ja ulkoisen valvonnan apuvälineenä

- Organisaation on huolehdittava siitä, että sisäinen valvonta on asianmukaisesti järjestetty.
- Sisäisen valvonnan asianmukaisuudesta ja riittävydestä vastaa organisaation johto.
- Organisaation oma etu on tehokkaasti valvoa sekä tarkastaa sisäisen ja ulkoisen tarkastuksen keinoin myös tietojenkäsittelyjärjestelmiään; toisaalta asiaan liittyy voimakas yleinen lainvalvontaintressi.
- Tietotilinpäättöksellä voidaan toteuttaa nämä molemmat tarpeet. Tietotilinpäättös palvelee myös lainvalvontaviranomaisten tiedonsaantitarpeita.

3. MITEN TIETOTILINPÄÄTÖS TEHDÄÄN ?

Esimerkiksi:

- 3.1. Tietotilinpäätökseen sisällytettävät tiedot
- 3.2. Organisaation hallussa olevat tietovarannot
- 3.3. Tietojen käsittelyssä noudatettavat menettelytavat ja periaatteet
- 3.4. Tietojen suojaus
- 3.5. Tietojen käsittelyn seuranta ja valvonta
- 3.6. Rekisteröityjen oikeuksien toteutuminen

Yleistä

- Tietotilinpäättöksen tavoitteena on antaa kuvaus tietojen käsittelyn nykytilasta sekä arvio tietosuojan ja tietoturvan toteutumisesta.
- Tietotilinpäättöksessä kartoitetaan myös tietojen käsittelyyn liittyviä kehittämistarpeita ja niiden edellyttämiä toimenpiteitä.

3.1. Tietotilinpäätökseen sisällytettävät tiedot

- Tietotilinpäätökseen sisällytettävät tiedot voivat vaihdella organisaation toimialasta ja toiminnan laadusta riippuen.
- Seuraavassa esimerkkejä asioista, joita voidaan sisällyttää tietotilinpäätökseen.

3.2. Organisaation hallussa olevat tietovarannot

- Organisaatiossa tietoja kerätään ja käsitellään monissa tietojärjestelmissä ja sovelluksissa.
- Organisaation johdolla ei aina ole käsitystä siitä, mitä tietoja organisaation hallussa on.
- Irrallisten tietojen käsittely erillään olevissa tietojärjestelmissä vaatii runsaasti resursseja ja muodostaa uhan tietosuojan ja tietoturvan toteutumiselle.
- Henkilötietojen käsittelyn näkökulmasta on tärkeää arvioida eri käyttötarkoituksiin muodostetut henkilörekisterit, niiden tietosisältö ja perusteet rekisterien pitämiseen. Hyvän tiedonhallintavan näkökulmasta organisaatiolla tulee olla selkeä kuva tietojärjestelmistään ja sen tulee huolehtia tietojen laadusta ja saatavuudesta.

3.3. Tietojen käsittelyssä noudatettavat menettelytavat ja periaatteet

Menettelytapojen osalta voidaan kuvata esimerkiksi:

- tietojen käsittelyyn vaikuttava keskeinen lainsäädäntö
- toimintaperiaatteet
- tietoturva- ja jatkuvuussuunnitelmat
- muu tietojen käsittelyä koskeva ohjeistus
- tietojen käsittelyn ulkoistamiseen liittyvät menettelytavat ja sopimukset
- tietojärjestelmien ylläpitoon ja hankintaan liittyvät menettelyt ja sopimukset

Tietojen käsittelyn toimintaperiaatteiden osalta voidaan arvioida esimerkiksi:

- tietojen saamiseen ja luovuttamiseen liittyvät menettelytavat
- käyttöoikeushallinta
- erityisesti sähköiseen tiedonsiirtoon liittyvät tietosuoja- ja tietoturvavaatimukset

Tietotilinpäätöksessä arvioidaan esimerkiksi:

- Miten tietojen käsittelyyn liittyvä henkilöstölle annettava ohjaus ja koulutus on järjestetty sekä millä tavoin ohjeet ja koulutus pidetään ajan tasalla.

3.4. Tietojen suojaus

Tietotilinpäätyöksessä voidaan arvioida:

- tietojen suojaamiseen liittyvät periaatteet ja menettelytavat
- tietoturvallisuuteen liittyvät keskeiset tavoitteet ja toteutuskeinot
- riskienhallinnan menettelytavat
- tietoturvallisuuden organisointi
- vastuut ja kehittämisprouessi, menettelytavat

3.5. Tietojen käsittelyn seuranta ja valvonta

Tietotilinpäätöksessä voidaan kuvata muun muassa:

- tietojen käsittelyyn kohdistuvaa riskien arviointia ja hallintaa
- tietovarantojen ja tietovirtojen laadun valvomiseksi tehtyjä toimenpiteitä
- tietojen käsittelyprosessien valvomiseksi tehtyjä toimenpiteitä
- valvonnan ja seurannan perusteella tehtyjä toimenpiteitä ja kehittämistoimia
- Lisäksi voidaan arvioida tietojen käsittelyn valvonnan ja seurannan riittävyttä ja kehittämistarvetta.

3.6. Rekisteröityjen oikeuksien toteutuminen

Esimerkiksi:

- Rekisteröityjen oikeuksien toteutumista voidaan arvioida henkilötietolain mukaisen tarkastusoikeus- ja tiedonkorjauspyyntöjen lukumäärän ja pyyntöihin annettujen vastausten perusteella.

4. ARVIOINTI JA KEHITTÄMISKOHTEET

- Tilinpäätöksessä tunnistetaan nykytilanteen analysoinnin kautta ilmeneviä kehittämis- ja mittaamistarpeita sekä niihin liittyvää seurantaa ja raportointia.
- Kehittämistoimet voivat liittyä esimerkiksi itse tiedon laatuun tai tietojen käsittelyyn liittyvään prosessiin.
- Kehittämistoimet voivat liittyä myös uuden teknologian menestykselliseen käyttöönottoon ja muutenkin valmiuteen ottaa käyttöön uusia tietotyön välineitä.

Tietotilinpäättöksen perusteella tehdään johtopäätöksiä, esimerkiksi:

- ”toiminta ja tietojen käsittely on ollut hyvän tietojenkäsittelytavan ja hyvän tiedonhallintatavan mukaista.”
- ”tietojen käsittelyn seuranta ja valvonta on onnistunut lainsäädännön, määräysten ja sisäisen ohjeistuksen mukaisesti.”
- ”tietojen käsittelyn seurannassa ja valvonnassa on havaittu kehittämiskohteita tai poikkeamia, joiden johdosta on ryhdytty erikseen lueteltuihin toimenpiteisiin”

Tietotilinpäätöksessä todetaan esimerkiksi:

- ne tietojen käsittelyn osa-alueet, joissa on kehittämiskohteita.
- määrittellään kehittämiskohteet ja arvioidaan mitä ratkaisuja niihin on tarjolla.
- arvioidaan edellisellä seurantakaudella toteutettujen kehittämistoimenpiteiden onnistumista.

- Tietotilinpäätös voi olla luonteeltaan dynaaminen asiakirja, jonka sisältö voidaan muokata kohderyhmäkohtaisesti.
- Esimerkiksi tietojen suojauksesta ja valvonnasta voidaan raportoida johdolle yksityiskohtaisesti, kun taas muille sidosryhmille kohdistetussa tietotilinpäätöksessä voidaan samoja asioita kuvata yhteenvetona tai kokonaisarviona.

5. HAASTEET

- Laatumiseen pitää varata aikaa ja henkilöresursseja
- Poimittavat asiat pitää rajata/priorisoida
- Isoissa organisaatioissa kerättävät tiedot ylittävät toiminnan rajoja, joten olisi hyvä vastuuttaa eri yksiköistä henkilöt jo etukäteen, jotta tietotilinpäätökseen toimitettavien tietojen luovuttaminen varsinaiselle laatijalle olisi suunnitelmallista
- Mittaristo pitää olla luotuna, jotta vuoden aikana syntyvät halutut tunnuslukutiedot syntyvät taustalla ja ne on helpompi kerätä eri raporteilta/tietokannoista tietotilinpäätökseen
- jos mittareita/tunnuslukuja ei ole etukäteen suunniteltu ja varmistettu niiden luotettavuutta – ei myöskään tietotilinpäätös anna oikeaa vertailukelpoista kuvaa asioista vuosien edetessä.
- Tietotilinpäätöksen tausta ja tavoitteet pitää olla johdon tiedossa - tietotilinpäätös on johdon apuväline.

- **KIITOS,**
mielenkiinnostanne!