TIETOTILINPÄÄTÖS 2022

Kempeleen kunta

Julkinen versio

Tietotilinpäätöksen tiivistelmä

Tietotilinpäätöksen tehtävänä on organisaation tietoturvan, tietosuojan ja tiedonhallinnan tilannekuvan tarjoaminen. Tietotilinpäätös osoittaa osaltaan, että organisaatiossa noudatetaan tiedonhallintaan, tietosuojaan ja tietoturvaan liittyviä lakeja ja määräyksiä. Kempeleen kunnan tietotilinpäätöksen 2022 on laatinut kunnan uusi tietosuojavastaava ja tietohallintopäällikkö.

Kempeleen tietoturvan ja tietosuojan toteutusta ohjataan erityisesti kunnan tietoturvapolitiikan avulla. Tietoturva- ja tietosuojatyötä tarkastellaan toistuvammin kunnan tietoturvaryhmässä. Tietoturvan asiantuntijana toimii tietoturvavastaava ja tietosuojan asiantuntijana tietosuojavastaava. Tietosuojavastaavan toimesta on kirjattu 9 ja tietohallinnon henkilöstön toimesta 30 tietoturvapoikkeamaa vuoden 2022 aikana. Tämä on 21 poikkeamaa enemmän kuin edellisvuonna.

Kunnalla oli vuonna 2022 hallussaan 55 erilaista palvelualueisiin liittyvää, henkilötietoja sisältävää rekisteriä. Rekisteröityjen oikeudet toteutuvat kunnan toiminnassa ja rekisteröidyillä on mahdollisuus jättää henkilötietojensa tarkastus- ja korjauspyyntö kunnan kirjaamon kautta www-sivuilta löytyvien lomakkeiden avulla tai suoraan palvelun yhteydessä.

Henkilötietojen käsittely tehdään suurimmalta osin sähköisten järjestelmien avulla. Kunnan merkittävimpiä tiedonhallintaan liittyviä järjestelmiä ovat terveyspalveluiden, sosiaalipalveluiden ja varhaiskasvatuksen asiakastietojärjestelmät, asianhallintajärjestelmä sekä oppilastietojärjestelmä. Vuoden 2023 alusta sosiaali- ja terveyspalveluiden rekistereiden rekisterinpitäjyys siirtyy tietyin osin hyvinvointialue Pohteelle.

Kunta osallistuu 19 kunnan yhteiseen Digityy - Digiturvallinen työkulttuuri ja -ympäristö -hankkeeseen, joka jatkuu vuoteen 2023 asti. Hankkeen tavoitteena on kehittää digiturvallisuuden prosesseja ja hallintamalleja osallistujien yhteisten tarpeiden pohjalta. Hanketta rahoittaa valtiovarainministeriö.

1. Tausta ja tarkoitus

Tietotilinpäätöksen tarkoituksena on kuvata:

- miten tietosuoja ja -turva toteutuvat organisaation toiminnassa
- miten tietojenkäsittelyyn liittyvä riskienhallinta on toteutettu
- organisaation hallussa olevat tietovarannot
- organisaation toimintaan liittyvät tietovirrat
- organisaation tietovirtojen ja tietojenkäsittelyn yhteen toimivuus

Tietotilinpäätös toimii lisäksi suunnittelun ja toiminnan ohjauksen tukena organisaatiossa sekä apuvälineenä kehittämistoimenpiteiden seurannassa. Sitä voidaan käyttää organisaatiosta ulospäin tapahtuvan sidosryhmäraportoinnin välineenä ja varmistamaan sovellettavan lainsäädännön noudattaminen.

2. Johdanto

Tietotilinpäätös tarjoaa ajantasaisen tilannekuvan Kempeleen kunnan henkilötietojen käsittelyn nykytilasta sekä arvion tietosuojan toteutumisesta. Tietotilinpäätöksessä kartoitetaan henkilötietojen käsittelyyn liittyviä kehittämistarpeita ja niiden edellyttämiä toimenpiteitä. Tavoitteena on tukea tietosuojatyön tekemistä ja lisätä tekemisen vaikuttavuutta.

Tietotilinpäätös toimii yhtenä osoitusvelvollisuuden osoittamisen välineenä. Osoitusvelvollisuus tarkoittaa, että tietosuojalainsäädännön asettamien velvoitteiden mukaisen toiminnan lisäksi organisaation on kyettävä osoittamaan velvoitteiden mukainen toiminta. Osoitusvelvollisuuteen vastataan teknisten ja organisatoristen toimenpiteiden avulla. Osoitusvelvollisuus tarkoittaa vahvasti mm. dokumentointivelvollisuutta.

EU:n yleisessä tietosuoja-asetuksessa määritellyt tietosuojaperiaatteet ovat 1. lainmukaisuuden, kohtuullisen ja läpinäkyvyyden periaate, 2. käyttötarkoitussidonnaisuuden periaate, 3. tietojen minimoinnin periaate, 4. täsmällisyyden periaate, 5. säilytyksen rajoittamisen periaate ja 6. eheyden ja luottamuksellisuuden periaate. Tietotilinpäätöksellä voidaan lisätä luottamusta siihen, että organisaatiossa noudatetaan edellä mainittuja tietosuojaperiaatteita ja käsitellään henkilötietoja sen mukaisesti.

Tietotilinpäätös on koottu tietosuojavastaavan työssä luodun dokumentaation pohjalta. Tietotilinpäätös 2022 keskittyy tietosuoja- ja tietoturvakysymyksiin.

3. Nykytila Kempeleen kunnassa

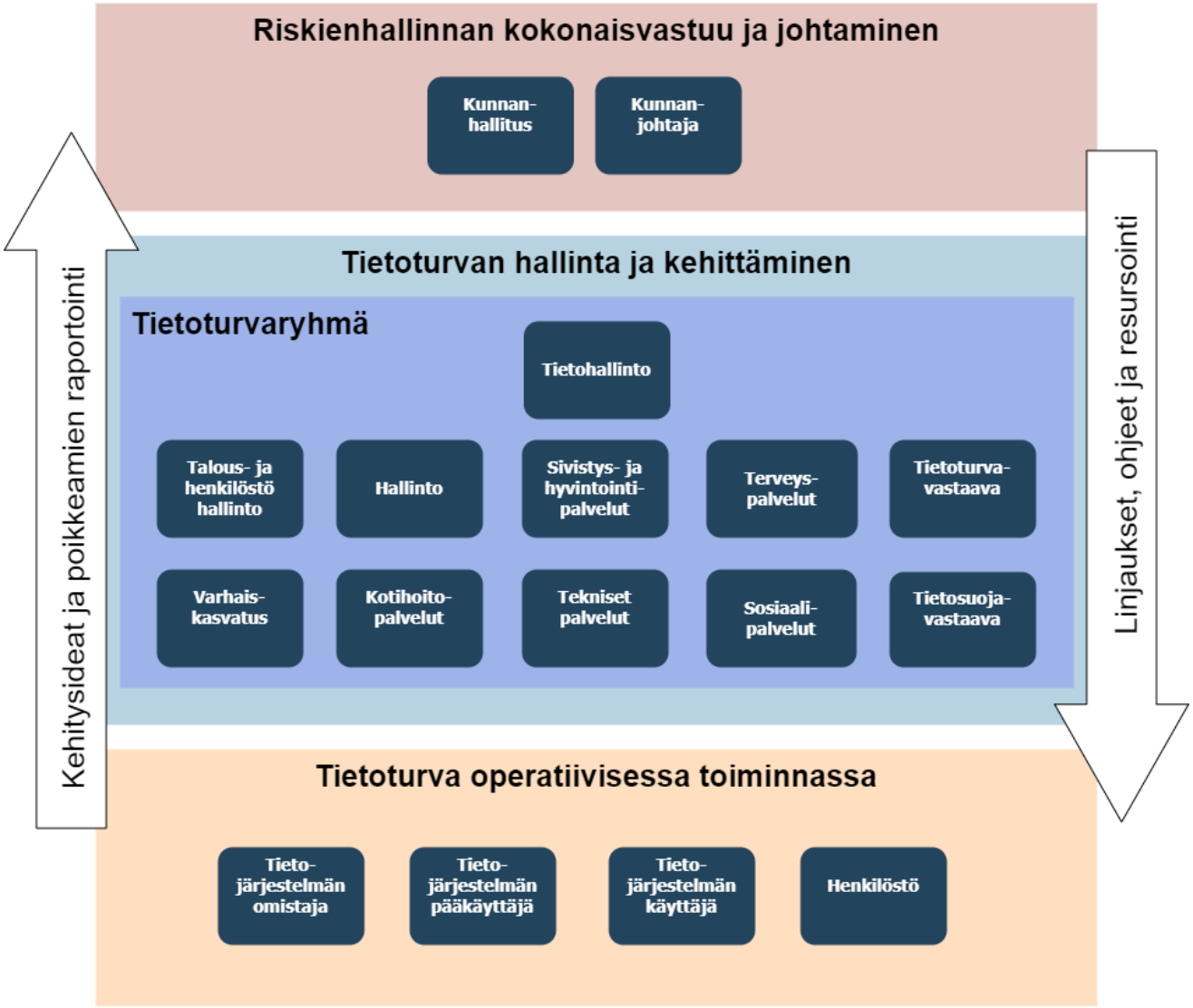
3.1 Tietosuoja, tietoturva ja riskienhallinta

Tietosuoja-asetuksen (artikla 24) mukaan rekisterinpitäjä on vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi henkilöstön koulutuksia, sisäisiä ohjeistuksia ja määräyksiä, salassapitosopimuksia ja -sitoumuksia, käytönvalvontaa, pääsynhallintaa, päivitysten ja muutosten hallintaa, fyysistä turvallisuutta, henkilöstöturvallisuutta, toimittajien ja sopimusten hallintaa, tietoturvallisuuden hallintaa, tietojen salausta, tietojen anonymisointia ja pseudonymisointia, tietojärjestelmien ja rekistereiden auditointeja, etäkäyttöyhteyksiä, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, käytännesääntöjen sekä sertifikaattien käyttöä.

Kempeleen kunnan ohjeistuksen mukaan sisäisen valvonnan ja riskienhallinnan asianmukainen järjestäminen koskee kaikkia kunnan ja kuntakonsernin toimielimiä ja tilivelvollista johtoa.

Sisäinen valvonta on osa kuntakonsernin johtamisjärjestelmää sekä kunnan poliittisen johdon, viranhaltijajohdon ja hallinnon työväline, jonka avulla arvioidaan asetettujen tavoitteiden toteutumista, toimintaprosesseja ja riskienhallinnan tuloksellisuutta sekä vaikuttavuutta. Valvonnan tarkoituksena on edistää organisaation tehokasta johtamista, riskien hallintaa ja toiminnan tuloksellisuuden arviointia sekä vahvistaa hyvää johtamis- ja hallintotapaa.

Kempeleen kunnassa on käytössä tietoturvapolitiikka, joka on hyväksytty kunnanhallituksessa 10.5.2021. Tietoturvapolitiikassa määritellään tietoturvatyön tavoitteet ja strategiset painopisteet, tietoturvaviestinnän periaatteet, organisointi ja vastuut, tietoturvan ja tietosuojan varmistaminen hankinnoissa sekä arviointi- ja seurantamenetelmät. Kunnanhallituksen ja -kunnanjohtajan vastuulla on riskienhallinnan kokonaisvastuu ja poikkeus-, erityis- ja kriisitilanteissa toimimisen edellytysten varmistaminen (kuva 1).



Kuva 1. Riskienhallinnan kokonaisvastuu ja tietoturva.

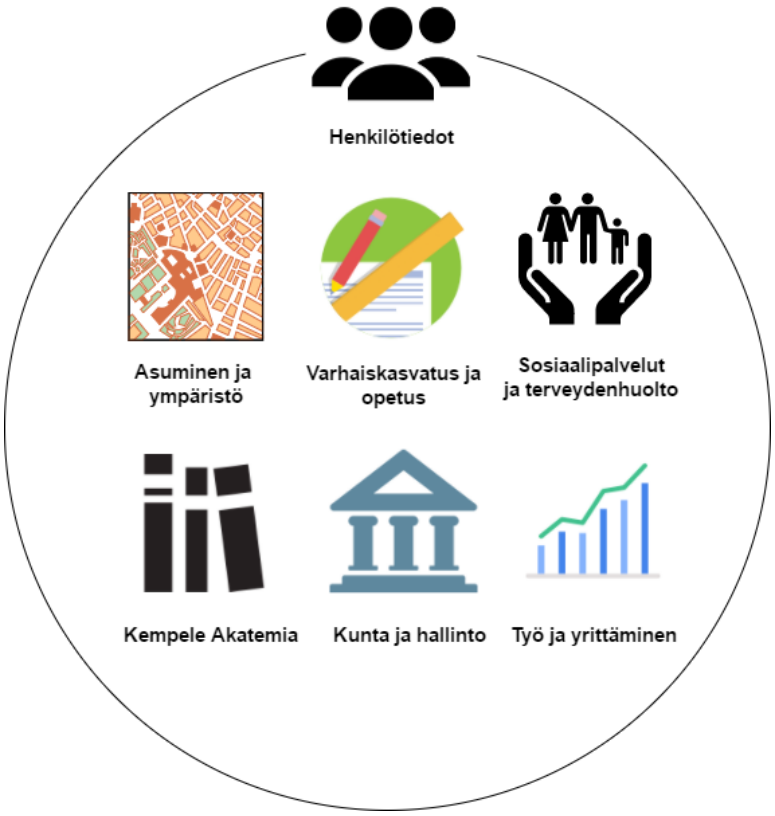
Tietoturvaryhmän tarkoituksena on käsitellä tietoturvan linjaukset ja ohjeet ennen kuin ne esitetään johdolle hyväksyttäväksi. Ryhmä arvioi myös tietoturvatason ja toteutuksen sekä käsittelee esiin tulleet poikkeamat. Tietoturvatyöryhmä kokoontui vuoden 2022 aikana neljä kertaa. Operatiivisella tasolla tietoturvaa toteuttavat tietojärjestelmien omistajat, pääkäyttäjät ja käyttäjät, jotka ovat toimintansa osalta tekemisissä henkilötietojen kanssa ja huolehtivat tietoturvasta omassa toiminnassaan. Tietohallintopäällikkö vastaa tietojärjestelmäkokonaisuudesta sekä tietoturvaan liittyvästä viestinnästä kunnassa. Tietohallinto vastaa poikkeamatilanteisiin ja pyrkii palauttamaan toiminnan normaaliksi poikkeamatilanteissa. Tämän lisäksi tietohallinto ehkäisee poikkeavien tilanteiden syntymistä tietoverkon ja laitteiston seurannan avulla.

Kempeleen kunnassa tehtiin vuoden 2022 aikana päätös ostaa tietosuojavastaavan palvelut Joki ICT Oy:ltä. Tietosuojavastaavan tehtävänä on valvoa tietosuojan toteutumista kunnan toiminnassa. Tietosuojavastaava tekee yhteistyötä palvelualueiden kanssa henkilötietojen käsittelytoimien suunnittelussa sekä tietohallinnon kanssa tietosuojan huomioimiseksi tietoteknisissä toimissa. Palvelualueet vastaavat hyvin itsenäisesti henkilötietojen tarkastus- ja korjauspyyntöihin kunnassa ja tietosuojavastaava antaa neuvoja haastavimmissa kysymyksissä.

Kuntaan nimetyn tietoturvavastaavan tehtävänä on kehittää tietoturvaa, valvoa sen toteutusta sekä edistää tietoturvatietoutta tietohallintopäälliköltä saamiensa resurssien ja toimintavaltuuksien puitteissa. Tietoturvavastaava osallistuu yhdessä tietosuojavastaavan kanssa kunnan turvallisuus-, tietoturva- ja tietosuoja-asioiden kokonaisuuden koordinointiin. Tietoturvavastaavan tehtävää suorittava henkilö vaihtui keväällä 2022 henkilöstömuutosten vuoksi.

3.2 Henkilötietorekisterit

Kempeleen kunnan henkilötietojen tietopääoma koostuu kunnan lakisääteiseen toimintaympäristöön liittyvistä rekistereistä. Kempeleen kunnan henkilörekisterien tietoja tarvitaan julkisten palveluiden tuottamiseksi ja lakisääteisten tehtävien hoitamiseksi kunnan eri palvelualueilla (kuva 2).



Kuva 2. Kempeleen kunnan henkilötietoja käsittelevät palvelualueet

Kempeleen kunnalla on hallussaan 55 erilaista palvelualueisiin liittyvää, henkilötietoja sisältävää rekisteriä. Kempeleen kunta ylläpitää edellä mainittujen rekistereiden tietosuojaselosteita verkkosivuillaan, josta ne ovat kuntalaisten ja muiden rekisteröityjen nähtävissä. Näin kunta toteuttaa informointivelvoitettaan rekisteröidyille. Rekisteröity voi halutessaan olla yhteydessä rekisterin yhteyshenkilöön, vastuuhenkilöön tai tietosuojavastaavaan. Rekisteröidyillä on mahdollisuus jättää henkilötietojensa tarkastus- ja korjauspyyntö kunnan kirjaamon kautta www-sivuilta löytyvien lomakkeiden avulla tai suoraan palvelun yhteydessä.

3.3 Tietovirrat

Kempeleen kunnan toiminta perustuu pääosin lainsäädäntöön, jossa kuntaa velvoitetaan tuottamaan palveluita kuntalaisille. Palvelun tuottamiseksi kunta käyttää hyväkseen erilaisia sidosryhmien, kuten viranomaisten, rekistereitä ja luovuttaa myös itse tilastotietoja viranomaisten käyttöön. Henkilötietojen lähteitä Kempeleen kunnalle ovat seuraavat tahot:

- Rekisteröidyt itse: Kuntalainen, kuntalaisen huoltaja, omainen tai edunvalvoja, työnhakija, yrittäjä
- Väestörekisterikeskus
- Asemakaava
- Eläketurvakeskus
- Eläkeyhtiöt
- Hoitavat yksiköt
- Kameravalvonta
- Kansaneläkelaitos
- Kiinteistörekisteri
- Lastensuojeluilmoitukset
- Lääkärintodistukset
- Opetushallitus
- Ostopalveluiden tuottajat
- Poliisi
- Sijoittajakuntien sosiaalitoimet
- Sijoitusvanhemmat
- Työnantajat
- Työtoimintapaikat
- Työvoimatoimisto
- Ulkopuoliset sosiaalihuollon järjestäjät
- Veroviranomainen

Kempeleen Kunta luovuttaa tietoja säännönmukaisesti seuraaville tahoille:

- Kansaneläkelaitokselle
- KEHA-keskukselle
- Lääkelaitokselle
- Opetushallitukselle
- Pankeille (maksatustietoja)
- Perintätoimistoille
- Rakennuslupahankkeiden sidosryhmille
- Sosiaalihuollon valtakunnallisille rekisterinpitäjille
- Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskukselle
- Terveyden ja hyvinvoinnin laitokselle
- Tilastokeskukselle
- Ylioppilastutkintolautakunnalle

3.4 Tiedonhallintalaki

Tiedonhallintalain mukainen asiakirjajulkisuuskuvaus on julkaistu kuntalaisille kunnan internet-sivulle. Tiedonhallintalain mukaista tiedonhallintamallia joka kuvaa kunnan digitaalista toimintaympäristöä, on ylläpidetty aktiivisesti. Tiedonhallintalain vaatimukset on huomioitu tietojärjestelmien hankinnassa ja palveluiden tarjoamisessa. Tiedonhallintalain asianhallintaan ja palveluiden tiedonhallintaan liittyviin vaatimuksiin on vastattu esimerkiksi kunnan arkistojärjestelmän kilpailutuksen yhteydessä.

4. Kehittämiskohteet

4.1 Valmistuneet kehittämiskohteet

Arkistointijärjestelmä ja sähköinen allekirjoituspalvelu on otettu käyttöön.

Kunnan omilla pohjilla on tuotettu hankintojen tueksi tietosuojaan liittyvät sopimusliitteet.