Hämeenkyrön kunnan tietotilinpäätös 2020

Sisällys

1. Tietotilinpäätöksen tarkoitus Hämeenkyrön kunnassa

Kunnan tietotilinpäätös laaditaan vuosittain osana tilinpäätöstä. Sen tarkoitus on kuvata ja arvioida tietosuojan ja tietoturvan tilannetta kunnassa. Se toimii sisäisen ja ulkoisen valvonnan raporttina, johdon työvälineenä sekä vahvistaa rekisteröityjen ja sidosryhmien luottamusta. Hyvin hoidettu tietosuoja mahdollistaa kertyvän tiedon aikaisempaa tehokkaamman hyödyntämisen, ja näin ollen tietotilinpäätös on työkalu myös tiedolla johtamiseen.

Tietotilinpäätöksellä vastataan EU:n Yleisen tietosuoja-asetuksen osoitusvelvollisuuteen (artikla 24, Rekisterinpitäjän vastuu). Rekisterinpitäjä on vastuussa siitä, että se toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan ja osoitetaan, että henkilötietojen käsittelyssä noudatetaan tietosuoja-asetuksen vaatimuksia. Tämä pitää myös osoittaa oma-aloitteisesti ja aktiivisesti. Hämeenkyrön kunnassa rekisterinpitäjä on kunnanhallitus.

Tietotilinpäätöksellä halutaan lisätä niin henkilöstön kuin suuren yleisön tietoisuutta tietosuojasta ja tietoturvasta sekä tehdä näkyväksi näiden eteen tehtävää työtä. Lisäksi tietotilinpäätöksessä kartoitetaan tietojen käsittelyyn liittyviä kehittämistarpeita.

Tietotilinpäätöksen laatimisesta vastaa kunnan tietosuojavastaava. Sitä on käsitelty kunnan tietosuojatyöryhmässä 16.4.2021.

2. Tietoturvallisuuden ja -suojan toteuttaminen organisaatiossa

Tietosuojalla tarkoitetaan yksilön tietojen käsittelyä ja oikeutta yksityisyyteen omien henkilötietojen käsittelyssä. Tietosuoja kattaa henkilötietojen käsittelyn koko elinkaaren. Se toteuttaa rekisteröidyn perustuslaillista oikeutta yksityiselämän suojaan. Siihen sisältyy oikeudet tarkastaa ja korjata sekä vaatia poistettavaksi tarpeeton tieto.

Tietoturva tarkoittaa niitä hallinnollisia ja teknisiä toimenpiteitä, joilla tietosuojaa käytännössä

toteutetaan. Tietoturvallisuuden tarkoitus on suojata sekä digitaalinen että paperinen tietoaineisto ja tietojärjestelmät. Tietoturvallisuuden tavoitteena on varmistaa, että tiedot ovat vain niiden käytössä, joilla on siihen oikeus (luottamuksellisuus), silloin kun he niitä tarvitsevat (käytettävyys) ja tieto on oikeassa muodossa eikä ole muuttunut hallitsemattomasti (eheys). Tiedon luotettavuus vaarantuu, jos ulkopuoliset tahot pääsevät käsiksi tietoon, johon heillä ei tulisi olla pääsyä. Tiedon eheys vaarantuu, jos tieto voi muuttua joko teknisen virheen takia tai ihmisen aiheuttamana, eikä paikkansa pitävyyteen voida luottaa. Tiedon saatavuus vaarantuu, jos tieto ei ole tarvitsijoiden saatavilla tarvittavana aikana.

Tietosuoja on tärkeää mitoittaa oikein, niin että rekisteröidyn oikeudet säilytetään, mutta tietoa voidaan käyttää toiminnan kannalta tarkoituksenmukaisesti eikä tietosuojasäädöksien soveltaminen estä tarpeellisia toimenpiteitä ja päätöksiä. Velvoitteet ja suojatoimet on suhteutettava tietokäsittelyjen aiheuttamaan riskiin (artikla 32). Korkeamman riskin henkilötietojen käsittely edellyttää enemmän panostamista teknisiin ja hallinnollisiin toimenpiteisiin, kun taas vähäisen riskin toiminta ei aiheuta merkittävää uhkaa rekisteröidyn yksityisyyden suojalle.

Kunnassa toimii kunnanjohtajan nimeämä tietosuojatyöryhmä, jossa on edustajat jokaiselta palvelualueelta. Tietosuojavastaava on ryhmän puheenjohtaja. Tietosuojatyöryhmä kokoontui vuonna 2020 kaksi kertaa. Kunnan tietosuojavastaavana on kirjastotoimenjohtaja Liisa Neronen. Terveys- ja sosiaalipalveluissa tietosuojavastaavan tehtävä on ollut pakollinen jo vuodesta 2007. Terveys- ja sosiaalipalvelujen tietosuojavastaavana toimi sosiaali- ja terveysjohtaja Tarja Soukko 30.4.2020 asti ja sosiaalityön päällikkö Taija Jokimaa-Frusti 3.8. alkaen. Hämeenkyrö on mukana seudullisessa ja valtakunnallisessa tietosuojavastaavien verkostossa. Suomen kansallisena valvontaviranomaisena toimii toiminnassaan itsenäinen ja riippumaton tietosuojavaltuutettu, joka on Euroopan tietosuojaneuvoston jäsen.

Hämeenkyrön kunnanhallitus on hyväksynyt 14.5.2018 § 77 tietosuojaohjeistukset henkilöstölle ja kunnan luottamushenkilöille. Oletusarvoisesti kaikkea kunnassa tapahtuvaa henkilötietojen käsittelyä ohjaa sisäänrakennetun tietosuojan periaate. Oletusarvoisen tietosuojan periaate merkitsee, että rekisterinpitäjä oletusarvoisesti käsittelee vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Velvollisuus koskee kerättyjen henkilötietojen

määrää, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa. Henkilötietojen käsittelylle on aina laissa säädetty käsittelyn oikeusperuste. Henkilöstö on tietoinen siitä, missä kaikkialla henkilötietoja sijaitsee ja miten niitä käytetään. Tietosuojaosio kuuluu uusien työntekijöiden perehdytysohjelmaan.

Toukokuussa 2018 alettiin soveltaa EU:n tietosuoja-asetusta, joka on lisännyt sekä henkilöstön että kuntalaisten tietoisuutta tietosuoja-asioista. Asetuksen voimaantuloa seurannut koulutus ja ohjeistus on lisännyt osaamista ja vastuullista suhtautumista henkilötietoihin. Tietoturvaa ja tietosuojaa voidaan kehittää oikeaan suuntaan jo oikealla asenteella, myönteisellä kulttuurilla ja tietoisuutta kasvattamalla. Työntekijän päivittäisillä valinnoilla ja henkilökohtaisella riskienhallinnalla on merkitystä.

Koko henkilöstö on osallistunut seudullisen tietoturvakoulutuksen oppimisympäristö Kyberopissa järjestettävään koulutukseen. Vuonna 2020 käsiteltiin seuraavat kuusi osiota: Laitteiden huollattaminen, tuntemattomat henkilöt toimitiloissa, salassa pidettävän tiedon käsittely, kultaiset säännöt, salassa pidettävän tiedon jakaminen, GPDR - EU:n tietosuoja-asetus. Kyberopissa on mahdollista seurata tietoturvakoulutukseen osallistuvien määrää ja muistuttaa henkilökohtaisesti suorittamisesta. Koko vuoden osion suoritti kokonaisuudessaan 34 % henkilöstöstä (vuonna 2019 18%).

Vuoden 2020 seudullinen tietohallinto varoitti useaan otteeseen kalastelu- ja urkintaviesteistä, joita tuli muun muassa kunnan sähköpostiosoitteisiin. Tietohallinto varoitti myös Populuksen tiettyyn toimintoon kohdistuneesta tietoturvaloukkauksesta 13.11.2020.

Hämeenkyrön kunta antoi Etätyöohjeistuksen 29.6.2020. Ohjeissa otettiin huomioon myös tietoturva. Kotona tehtävä työ sisältää erilaisia sekä teknisen että inhimillisen toiminnan aiheuttamia riskejä. Koronan ansiosta lisääntynyt työnteon digitalisuus lisäsi teknistä tietoturvaa Pulse-yhteyden käyttöönoton myötä.

Psykoterapiakeskus Vastaamoon tehty tietomurto ei suoraan koskettanut Hämeenkyrön kunnan palvelujen asiakkaita. Tapaus antoi kuitenkin kunnille muistutuksen siitä, miten tärkeää on huolehtia myös ostopalveluissa tietoturvan toteutumisesta. Kunnan sopimusohjeessa tämä on otettu huomioon.

Kunnan monitoimilaitteilla käytetään turvatulostusta. Avainturvallisuus on keskitetty kiinteistötoimelle, lisävalvontaa tehdään yksiköissä.

Kunta osallistui syksyllä pidettyyn tietoturva- ja tietosuojaloukkausten hallinnan harjoitukseen. TAISTO20 -harjoitukseen järjestettiin 19.11.2020 ja siihen osallistuttiin osaksi etäyhteyksien avulla. Simuloidussa harjoituksessa tehtiin tietoturvahyökkäyksistä Traficomin Kyberturvallisuuskeskukseen viisi ilmoitusta, poliisille kaksi rikosilmoitusta sekä yksi ilmoitus Tietosuojavaltuutetulle. Harjoituksen saatiin onnistuneesti yhteys myös muihin tarvittaviin tahoihin (Tietoon ja kunnan johtoryhmään. Harjoitukseen kuului ennen ja jälkeen harjoituspäivän tehty oman toiminnan arviointi, jossa kirjattiin havaitut puutteet ja aikataulutettiin niiden korjaustoimet.

Tiedonhallintalaki tuli voimaan 1.1.2020. Se on yleislaki, joka säätelee julkisuusperiaatteen ja hyvän hallinnon vaatimusten toteuttamisesta viranomaisten tiedonhallinnassa digitaalisessa toimintaympäristössä. Lain voimaantuloon liittyy useita siirtymäaikoja. Näihin valmistautuminen kehittää myös kunnan tietoturvaa ja siihen liittyviä toimintoja. Vuoden 2020 aikana kunta on tehnyt tiedonhallintalakiin liittyen tiedonhallintamallia ja asiakirjajulkisuuskuvausta. Tiedonhallintamalli on kuvaus tiedonhallintayksikössä toimivien viranomaisen tehtävien hoidossa toteutettavasta tiedonhallinnasta ja se sisältää tiedot mm. tietovarantojen, tietojärjestelmien ja tietoturvallisuuden osalta. Asiakirjajulkisuuskuvaus on kunnan ylläpitämä kuvaus mm. hallinnoimistaan tietovarannoista, asiakirjoista ja tiedon antamisesta.”

Tietojen hävittäminen on ohjeistettu tietosuoja-asetuksen mukaisesti. Kunta käyttää Encore Ympäristöpalvelut Oy:n palveluita henkilötietoja sisältävien paperisten asiakirjojen hävittämiseen. Asianhallintaohjelma CaseM mahdollistaa asetuksenmukaisen henkilötietojen käsittelyn myös tietojenkäsittelyn elinkaaren loppuvaiheessa. Vuonna 2020 alettiin käyttää Kuusankoski Oy:n suljettuja rullakoita 3-StepIt:n kautta tulevien laitteiden hävitykseen.

Kunnanhallitus hyväksyi sopimusohjeen 15.6.2020 § 117. Ohjeeseen sisältyy määräykset tietosuoja-asioiden huomioon ottamiseksi ja Kuntaliiton tietosuojaohjeistuksien mukainen tietosuojaliite.

3. Tiedonhallinta, tietovarannot ja tietovirrat

Henkilötietona voidaan pitää merkintää, jonka perusteella henkilö voidaan tunnistaa. Henkilö voidaan tunnistaa suoraan tai epäsuorasti eli myös tietoja yhdistämällä. Henkilötietojen käsittelynä pidetään kaikkia toimenpiteitä, jotka kohdistuvat henkilötietoihin, kuten henkilötietojen kerääminen, tallentaminen, käyttäminen, muuttaminen ja poistaminen. Henkilörekisteri on henkilötietoja sisältävä tietojoukko, esimerkiksi paperinen nimilista tai asiakastietojen hallintaan käytettävä ohjelmisto. Hämeenkyrön kunnalla on myös yhteisrekistereitä, jolloin samaa rekisteriä käyttävät palvelun tarjoaja ja palvelun tuottaja.

Tietosuoja-asetuksessa on määritelty erityiset henkilötiedot, joiden käsittely saattaa aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja -vapauksille. Perusturvassa lähes kaikki henkilötieto on sensitiivistä henkilötietoa. Kunnassa erityisiä tietoja käsitellään etenkin perusturvapalveluissa. Sivistyspalveluissa erityisten henkilötietoryhmien käsittelyä sisältyy esimerkiksi opiskeluhuoltoasioihin, kuljetuspäätöksiin ja tietoihin erityisruokavalioista.

Tietosuoja-asetuksen informointivelvoite edellyttävät organisaatiota informoimaan läpinäkyvästi sen toteuttamasta henkilötietojen käsittelystä. Kunnan henkilötietojen käsittelytoimet kuvataan tietosuojaselosteissa, joihin on kirjattu tietojen käyttötarkoitus, oikeusperusteet, tietosisältö, tietojen luovutus ja rekisteröityjen oikeudet. Tietosuojaselosteita on tallennettu kunnan nettisivuille, jossa ne toimivat asiakkaiden informaatioasiakirjoina. Henkilötietojen käsittelyn kartoitus on nyt tehty keskeisten henkilötietoa sisältävien tietojärjestelmien osalta ja kuvattu lähinnä järjestelmäkohtaisesti.

Hämeenkyrön kunnan henkilötietoja sisältävät tietovarannot koostuvat noin 60 rekisteristä. Tietosuojaselosteet löytyvät kunnan verkkosivuilta ja ne on laadittu tietosuojavaltuutetun ohjeiden mukaan.

Tietosuojaselosteet ovat osa kunnan tiedottamisvelvollisuutta ja tietosuojaselosteesta käyvät ilmi henkilötietojen käsittelyn tarkoitus, rekisterin tietosisältö, tietolähteet, tietojen

säilyttäminen ja rekisteröidyn oikeudet. Tietosuojaselosteiden päivittäminen on rekisterinpitäjän vastuulla.

4. Tietosuojan toteuttaminen seudullisesti

Tampereen seudullisesta tietohallintoyhteistyöstä on sovittu ensimmäisen kerran 2008 ja sopimus on uudistettu 2014. Yhteistyön sisältö on sopimuksessa määritelty seuraavasti:

• Seudullisen tietohallinnon strateginen koordinointi ja ohjaus, sekä hallintopalvelut

• Tietoturva ja -suoja

• Kehittämishankkeiden johtaminen ja hallinta sekä kehittämistyö tietohallinnon seudullisessa johtoryhmässä sovitussa laajuudessa

• Pääkäyttäjäpalvelut

• Tietoteknisten laitteiden ja palvelusten hankinta

• Järjestelmätoimittajien kanssa tehtyjen seudullisten toimitussopimusten hallinta ja valvonta

Tietoturva - ja tietosuojayhteistyö on seudullisesti hyvin vahvasti kuntien yhdessä hallinnoimaa ja tuottamaa. Seudulliset yhteiset toimintapolitiikat ja tietosuojaohjeet sitovat kaikkia toimijoita. Seudulliset ohjeistukset ovat olemassa mm. seuraavista aiheista:

- Seudullinen tietoturvapolitiikka- ja ohjeistus: 9.12.2016
- Tampereen ympäristökuntien tietosuojapolitiikka 28.5.2018
- Tampereen seudun sähköisten viestintävälineiden käyttösäännöt 9.5.2015
- Tampereen seudun mobiilipolitiikka
- Tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus 28.5.2018
- Tietojenkäsittely pilvipalveluissa 26.5.2020

5. Tietojenkäsittelyyn vaikuttava lainsäädäntö ja muu ohjeistus

Henkilötietojen käsittelyn taustalla oleva lainsäädäntö on laaja alkaen Suomen perustuslain 10 § (Yksityiselämän suoja) tai EU:n perusoikeuskirjan 8 artiklasta (Henkilötietojen suoja). Toisaalta Julkisuuslain 1 § mukaan viranomaisten asiakirjat ovat julkisia, jollei tässä tai muussa laissa erikseen toisin säädetä. Myös julkisissa asiakirjoissa on henkilötietoja, ja on usein haasteellista ratkaista, onko julkisuusperiaate vai tietosuoja ratkaisevampi tekijä.

EU:n Yleistä tietosuoja-asetusta alettiin soveltaa 25.5.2018. Sitä on täydennetty ja täsmennetty kansallisella Tietosuojalailla (voimaan 1.1.2019). Eroa on esimerkiksi siinä, että Suomessa kunnallinen viranomainen ei voi saada hallinnollista sakkoa tietosuojaan liittyvissä asioissa.

Kuntalain 29 §:n mukaan kunnan on huolehdittava, että asioiden valmistelusta annetaan riittävästi tietoja yleisessä tietoverkossa. Verkossa tiedottaminen tuo haasteita asiakirjahallintoon, sillä henkilötietoja tulee viedä verkkoon harkitusti eikä niitä saa pitää siellä tarpeettomasti.

Hämeenkyrön kunnanhallitus on hyväksynyt 14.5.2018 § 77 tietosuojaohjeistukset henkilöstölle ja kunnan luottamushenkilöille. Päätöksessä on seuraavat 11 liitettä:

1. Rekisteröidyn oikeudet
2. Tietosuojavastaavan tehtävänkuvan vahvistaminen
3. Kuntalaisen informointi organisaation henkilötietojen käsittelytavoista ja eri rekistereistä
4. Seudullisen tietosuojapolitiikan vahvistaminen
5. Pikaopas henkilötietojen käsittelijöille ja käsittelyä koskevat vaatimukset
6. Tietosuojan toteuttamiseen liittyvien roolien vahvistaminen
7. Rekisterinpitäjän seloste henkilötietojen käsittelytoimista
8. Tietosuojaa koskevan vaikutustenarvioinnin (DPIA) toteuttaminen
9. Ohje henkilötietojen käsittelystä

10. Käyttövaltuuspolitiikka

11. Tietosuojapoikkeaminen hallintaohje

6. Rekisteröidyn oikeudet ja niiden toteutuminen

Kunta noudattaa henkilötietojen käsittelyssä läpinäkyvyyttä ja tietojen täsmällisyyttä asetuksen mukaisesti (artikla 5). Informointivelvoitteen täyttämiseksi käytetään toistaiseksi tietosuojaselosteita. Hyväksytyt ja ajantasaiset tietosuojaselosteet löytyvät kunnan nettisivuilta.

Tietosuoja-sivulta löytyy myös muun muassa lomakkeet henkilötietojen tarkastukseen, niiden korjaamiseen ja käyttölokirekisterin selvityspyyntö. Kuntaan tuli vuoden 2019 aikana 5 tietopyyntöä henkilötietojen käsittelystä, joista yksi oli poistopyyntö, kolme olivat korjauspyyntöjä ja yksi pyyntö koski lokitietoja. Sosiaali- ja terveyspalveluissa tehdään lokitarkastuksia pistokokeilla kahden kuukauden välein. Tietosuojavastaava on antanut Aluehallintovirastolle pyynnöstä selvityksen lokitietojen luovuttamiseen liittyvästä asiasta 22.11.2019.

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa 72 tunnin kuluessa tietosuojavastaavalle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Henkilötietoihin kohdistuvasta tietoturvaloukkauksesta on ilmoitettava rekisteröidylle ilman aiheetonta viivytystä silloin, kun loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Tietoturvaloukkauksista ilmoittaminen (artikla 33) tapahtuu tietosuojavastaavan harkinnan mukaan.

7. Seuranta ja mittaaminen

Ohjelmien pääkäyttäjät huolehtivat, että henkilöstön käyttövaltuudet ohjelmissa pidetään ajan tasalla. Tietosuojavastaava pitää kirjaa tietopyynnöistä ja tietosuojapoikkeamista. Tietojen kalasteluviestejä tulee aika ajoin sähköpostiin ja niistä on varoitettu henkilökuntaa ja annettu ohjeita, miten toimia, jos on antanut niihin tietojaan. Tietosuojaselosteita päivitetään tarpeen mukaan ja ajantasaiset tietosuojaselosteet julkaistaan kunnan verkkosivulla.

8. Arviointi ja kehittäminen

EU:n tietosuoja-asetuksen (GDPR) on jo tuttu henkilöstölle ja uusien työntekijöiden perehdytys sisältää aina tietoturvaosion. Henkilötietojen käsittelytoimien vaikutustenarviointia (DPIA) ei ole vielä toteutettu. Kunnan tiedonhallinnan, tietovarantojen sekä niihin liittyvien tietovirtojen kokonaistilanteen kuvausta ei ole toistaiseksi laadittu.

Tiedonhallintalaki tuli voimaan 1.1.2020. Se on yleislaki, joka säätelee julkisuusperiaatteen ja hyvän hallinnon vaatimusten toteuttamisesta viranomaisten tiedonhallinnassa digitaalisessa toimintaympäristössä. Lain voimaantuloon liittyy useita siirtymäaikoja. Näihin valmistautuminen kehittää myös kunnan tietoturvaa ja siihen liittyviä toimintoja.

Vuoden 2020 aikana kunta on tehnyt tiedonhallintalakiin liittyen tiedonhallintamallia ja asiakirjajulkisuuskuvausta. Tiedonhallintamalli on kuvaus tiedonhallintayksikössä toimivien viranomaisen tehtävien hoidossa toteutettavasta tiedonhallinnasta ja se sisältää tiedot mm. tietovarantojen, tietojärjestelmien ja tietoturvallisuuden osalta. Asiakirjajulkisuuskuvaus on kunnan ylläpitämä kuvaus mm. hallinnoimistaan tietovarannoista, asiakirjoista ja tiedon antamisesta.

Syksyllä Tietohallinto valmisteli SPF:n perustuvaa sähköpostin lähettäjän tunnistusta, joka tulee karsimaan roskapostia ja lisäämään sähköpostiviestinnän turvallisuutta.

9. Lähteet ja lyhenteet

1 Andreasson et al Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus

2 Ministeriöiden ja kunnallishallinnon yhteisen julkisen tietohallinnon neuvottelukunnan (JUHTA) ja julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) tuottamaa materiaalia

Tietosuojaan liittyviä lyhenteitä

GDPR	EU:n 25.5.2018 voimaan astunut tietosuoja-asetus (General Data Protection Regulation)
DPIA	tietosuojaa koskeva vaikutustenarviointi (Data Protection Impact Assessment)
JUDO -hanke	Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma
JUHTA	Ministeriöiden ja kunnallishallinnon yhteisen julkisen tietohallinnon neuvottelukunta
SPF	Sender Policy Framework. Tekniikka, jolla tunnistetaan sähköpostin lähettäjä
TAISTO	vuosittain pidettävä tietoturva- ja tietosuojaloukkausten hallinnan harjoitus
VAHTI	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä
VALTORI	Valtion tieto-ja viestintätekniikkakeskus