

Hämeenkyrön kunnan tietotilinpäätös 2019



Sisällylys

1. Tietotilinpäättöksen tarkoitus Hämeenkyrön kunnassa	2
2. Tietoturvallisuuden ja -suojan toteuttaminen organisaatiossa	2
3. Tiedonhallinta, tietovarannot ja tietovirrat	5
4. Tietosuojan toteuttaminen seudullisesti	6
5. Tietojenkäsittelyyn vaikuttava lainsäädäntö ja muu ohjeistus	7
6. Rekisteröidyn oikeudet ja niiden toteutuminen	8
7. Seuranta ja mittaaminen	9
8. Arviointi ja kehittäminen	10
9. Lähteet ja lyhenteet	10

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 ja se on käsitelty kunnan tietosuojatyöryhmässä 14.5.2020.

2. Tietoturvallisuuden ja -suojaan 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 tietosuoja 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 tietosuojasäädöksiä 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. Kunnan tietosuojavastaavana oli 1.1. - 30.9.2019 arkistosihteeri Tiina -Riitta Rinne ja 1.10 alkaen ma. hallintopäällikkö Liisa Neronen. Terveys- ja sosiaalipalveluissa tietosuojavastaavan tehtävä on ollut pakollinen jo vuodesta 2007. Terveys- ja sosiaalipalvelujen tietosuojavastaavana toimi johtava hoitaja Tarja Soukko. 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. Koko henkilöstö on osallistunut seudullisen tietoturvakoulutuksen oppimisympäristö Kyberopissa järjestettävään koulutukseen. Vuonna 2019 käsiteltiin seuraavat kuusi osiota: henkilötietojen käsittely, tallennusvälineet, tietojen urkinta, etätyöskentely, laitteen suojaaminen ja työhön liittyvien tietojen käsittely. Kyberopissa on mahdollista seurata tietoturvakoulutukseen osallistuvien määrää ja muistuttaa henkilökohtaisesti suorittamisesta. Koko vuoden osion suoritti kokonaisuudessaan 18 % henkilöstöstä. Osioden suorituksesta muistutetaan henkilökohtaisesti.

Tietosuojavastaava osallistui tietosuojavastaavan koulutusohjelmaan kuuluviin koulutuspäiviin 4. - 5.9. ja 10.10.2019 Kunnan Tietohallintoyksikkö osallistui Kuntien ja maakuntien kyberturvallisuuspäiville 25. - 26.9.2019. Aiheena olivat mm. tietoturvaloukkaukset, pilvitietoturva, ja IoT-laitteiden turvallisuus.

Tietoturvaa ja tietosuojaajaa voidaan kehittää oikeaan suuntaan jo oikealla asenteella, myönteisellä kulttuurilla ja tietoisuutta kasvattamalla. Työntekijän päivittäisillä valinnoilla ja henkilökohtaisella riskienhallinnalla on merkitystä.

Kunnan monitoimilaitteilla otettiin vuoden 2019 aikana käyttöön turvatulostus. Tulostetut asiakirjat saa noudettua tulostimelta henkilökortin tai tunnisteoletin avulla kirjautumalla. Näin estetään, ettei asiakirjoja jää monitoimilaitteille lojumaan esim. henkilötietoja sisältäviä dokumentteja ilman valvontaa. Kunnanviraston yhteiset postilokerikot siirrettiin lukittuun huoneeseen. Koneiden ja tilojen lukitsemiseen kiinnitettiin entistä enemmän huomiota. Avainturvallisuus on keskitetty kiinteistötoimelle, lisävalvontaa tehdään yksiköissä.

Kunta osallistui syksyllä pidettyyn tietoturva- ja tietosuojaloukkausten hallinnan harjoitukseen. Harjoitusta varten laadittiin ennakolta selvityksiä kunnan tietosuojasta ja valmistauduttiin 7.11.2019 pidettyyn harjoituspäivään. Taisto19 -harjoitukseen kuului ennen ja jälkeen harjoituspäivän tehty oman toiminnan arviointi, jossa kirjattiin havaitut puutteet ja aikataulutettiin niiden korjaustoimet. Kunnan johtoryhmä tutustui 5.11. harjoitukseen. Myös varsinaisena harjoituspäivänä johtoryhmään otettiin yhteyttä. Taisto-harjoituksen vaatimien kokoontumisten lisäksi tietosuojatyöryhmä kokoontui kolme kertaa.

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.

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 käsittelyä 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. Tietosuoja 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 tietoturvapoliittikka- ja ohjeistus: 9.12.2016
- Tampereen ympäristökuntien tietosuojapolitiikka 28.5.2018
- Tampereen seudun sähköisten viestintävälineiden käyttösäännöt 9.5.2015
- Tampereen seudun mobiilipoliittikka
- Tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus 28.5.2018

Tietosuoja-asioiden vauhdittamiseksi aloitettiin kehyskuntien toimesta yhteinen Tietosuoja-hanke seudullisesti syksyllä 2017, vetäjänä toimi Tieto Oyj. Tietosuojavastaavat kokoontuivat Tietosuoja-hankkeen aikana yhteensä 11 kertaa ja lisäksi he osallistuivat myös alueellisten työpajojen järjestelyihin ja niissä ryhmätöiden ohjaamiseen. Tietosuojatyöpajoja pidettiin ajalla 1.11.2017-30.5.2018 yhteensä 23 kpl. Seudun kunnat jakoivat hankkeen 80 000 euron kustannukset keskenään. Seudullisella projektilla varmistettiin, että seudun kunnat soveltavat tietosuojaan kattavasti ja yhtenäisesti.

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 Tietosujalalla (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. Tietosuojavaikuttavan tehtäväkuvan 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. Tietosuoja koskevan vaikutustenvaikutustenarvioinnin (DPIA) toteuttaminen
9. Ohje henkilötietojen käsittelystä
10. Käyttövaltuuspolitiikka
11. Tietosuojajoikkeaminen hallinta-ohje

6. Rekisteröidyn oikeudet ja niiden toteutuminen

Kunta noudattaa henkilötietojen käsittelyssä läpinäkyvyyttä ja tietojen täsmällisyyttä asetuksen mukaisesti (artikla 5). Informointivelvoitteen täyttämiseksi käytetään toistaiseksi tietosuoja selosteita. Hyväksytyt ja ajantasaiset tietosuoja selosteet 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 terveystietopalveluissa 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.

Vuonna 2019 tapahtui yksi tietosuojaloukkaus, josta tehtiin tietosuojavaltuutetulle ilmoitus ja tiedotettiin asianomaisia rekisteröityjä. Tietosuojavaltuutetun lausunnon 18.11.2019 mukaan loukkaus oli vaikutukseltaan vähäinen eikä koskenut erityisiä henkilötietoja.

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.

Hämeenkyrön kunnan johtoryhmä vastasi Digi- ja väestötietoviraston JUDO-hankkeen Digitaalisen toimintaympäristön turvallisuustilanteen muutos ja vaadittavat varautumistoimet -nimiseen julkisen hallinnon organisaatioille suunnattuun kyselyyn. Kyselystä saadaan arviointituloksen lisäksi kartoitettua korjaustarpeita ja kehittämiskohteita.

Tietosuoja ja –turvaohjeiden noudattaminen oli yksi vuoden 2019 sisäisen tarkastuksen kohde.

8. Arviointi ja kehittäminen

EU:n tietosuoja-asetuksen (GDPR) soveltamisessa on vielä tehtävää. 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.

Kunnan sopimusohjetta valmisteltiin vuoden aikana. Ohje hyväksytään kesällä 2020. Ohjeeseen sisältyy määräykset tietosuoja-asioiden huomioon ottamisesta sekä tietosuojaliitemalli.

9. Lähteet ja lyhenteet

- 1 Andreasson et al Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus
- 2 Korpisaari Päivi et al Tietosuojalainsäädäntö
- 3 Lakimylläkkä tiedon ympärillä. Kuntalehti 1/2020
- 4 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

TAISTO vuosittain pidettävä tietoturva- ja tietosuojaloukkausten hallinnan harjoitus

VAHTI Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

VALTORI Valtion tieto- ja viestintätekniikkakeskus