2020

Tietotilinpäätös

ORIVESI

Sisällys

1 Tietotilinpäätöksen tarkoitus

Tietotilinpäätöksen tarkoitus on kuvata ja arvioida tietosuojan ja tietoturvan tilannetta Oriveden kaupungissa. Se toimii sisäisen ja ulkoisen valvonnan raporttina, johdon työvälineenä sekä luottamuksen osoituksena rekisteröityjen ja sidosryhmien suuntaan. Tietotilinpäätöksellä vastataan EU Yleinen tietosuoja-asetuksen osoitusvelvollisuuteen (artikla 24, Rekisterinpitäjän vastuu). Organisaation tulee osoittaa noudattavansa asetusta ja tietosuojaperiaatteita henkilötietojen käsittelyssä sekä toimivansa niin myös käytännössä. Rekisterinpitäjä vastaa osoitusvelvollisuuden toteuttamisesta.

Tietosuoja ja tietoturva ovat kaupungin yhteinen asia, joka vaatii johdon, henkilöstön, luottamushenkilöiden ja tytäryhtiöiden sitoutumista tietoturva- ja tietosuojatyöhön. Tässä tietotilinpäätöksessä kuvataan keskeisiä toimenpiteitä, kuinka Oriveden kaupunki huolehtii asiakkaiden, henkilöstön ja sidosryhmien henkilötiedoista ja yksityisyydestä.

Oriveden kaupungin organisaatiossa noudatetaan Tampereen seudun yhteistä tietoturvapolitiikkaa, joka sisältää myös tietosuojaan liittyvät ohjeet.

Tietotilinpäätöksen laatimisesta on vastannut tietosuojavastaava ja tietohallintopäällikkö. Tietotilinpäätös laaditaan kerran vuodessa keväällä.

2 Tietoturvallisuuden ja tietosuojan toteuttaminen

2.1 Tietosuojavastaava

Oriveden kaupungille on nimetty tietosuojavastaava. Tietosuojavastaava on organisaation sisäinen riippumaton asiantuntija. Tietosuojavastaavan tehtävänä on toimia yhteyshenkilönä sekä rekisteröidyille, että tietosuojavaltuutetulle. Hän seuraa tietosuojasääntöjen noudattamista organisaatiossa ja tuo esiin mahdolliset puutteet. Tietosuojasäännösten noudattaminen on rekisterinpitäjän vastuulla, eikä tietosuojavastaava ole henkilökohtaisessa vastuussa asetuksen ja lain rikkomisesta. Tietoturva ja tietosuojatyön toteuttamisen kokonaisvastuu on kaupungin johdolla.

2.2 Tietoturvavastaava

Oriveden kaupungin tietohallintopäällikön tehtäviin kuuluu vastata kaupungin tietoturvaratkaisuista. Tietoturvaa kehitetään yhdessä Tampereen seudun kuntien kanssa ja tietohallintopäällikkö edustaa Oriveden kaupunkia yhteisessä Tampereen seudun tietoturvaryhmässä. Seudun tietoturvaryhmässä käsitellään kuukausittain mm. tietoturvaan liittyviä poikkeamia, linjauksia, ohjeita sekä muita ajankohtaisia asioita.

2.3 Tietoturva- ja tietosuojaopas

Oriveden kaupungin tietosuojaa ja tietoturvaa ohjaa Tampereen seudun kuntien ja kaupunkien yhteinen tietoturva- ja tietosuojaopas. Opas on tarkoitettu Tampereen seudun kuntien ja kaupunkien (Hämeenkyrö, Kangasala, Lempäälä, Nokia, Orivesi, Pirkkala, Tampere, Vesilahti ja Ylöjärvi) henkilöstölle sekä niiden tietoja ja tietojärjestelmiä tai toimitiloja käyttäville henkilöille kuten ulkopuoliset palveluntuottajat, opiskelijat, työharjoittelijat, siviilipalvelusmiehet ja tiedelainaajat. Oppaan tarkoitus on nostaa henkilöstön tietoturva- ja tietosuojatietoisuutta ja täten edesauttaa jokaista huolehtimaan omalta osaltaan sen toteuttamisesta. Opas löytyy jokaisen työaseman työpöydältä PDF-muodossa.

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 oltava laissa säädetty käsittelyn oikeusperuste ja henkilöstön tulee olla tietoisia siitä missä kaikkialla henkilötietoja sijaitsee ja miten niitä käytetään. Tietosuoja-asetuksen informointivelvoite (artiklat 13 ja 14) edellyttävät organisaatiota informoimaan läpinäkyvästi sen toteuttamasta henkilötietojen käsittelystä.

2.4 Tietosuojasta tiedottaminen

Tietosuojasivusto on avattu henkilöstön intranettiin, Lipastoon, josta löytyvät materiaalit, linkit ja ohjeet. Oriveden kaupungin henkilötietojen käsittelytoimet kuvataan tietosuojaselosteissa, joihin on kirjattu tietojen käyttötarkoitus, oikeusperusteet, tietosisältö, tietojen luovutus ja rekisteröityjen oikeudet. Tietosuojaselosteet ovat toimialoittain kaupungin verkkosivuilla, jossa ne toimivat asiakkaiden informaatioasiakirjoina. Tietosuojaselosteita on päivitetty ja lisätty verkkosivuille v. 2020 aikana.

2.5 Tietosuojan hallintamalli

Oriveden kaupungissa on käytössä tietosuojan hallintamalli (Digiturvamalli). Digiturvamalliin on tallennettu mm. tietojärjestelmät, joissa käsitellään henkilötietoja, järjestelmätoimittajat, integraatiot, tietolähteet, henkilörekisterit. Digiturvamallista saa erilaisia raportteja, joilla voidaan toteuttaa tietosuojalainsäädännön noudattamisen osoitusvelvollisuutta.

2.6 TAISTO-harjoitus

Oriveden kaupungin tietosuojaryhmä ja johtoryhmän jäseniä osallistui marraskuussa 2020 puolen päivän pituiseen Digi- ja väestötietoviraston järjestämään TAISTO2020-harjoitukseen. TAISTO-harjoituksessa harjoitellaan organisaation toimintakykyä erilaisissa tietoturva- ja tietosuojaloukkaustilanteissa.
Harjoituksessa mukana ollut tarkkailija sekä tietosuojaryhmä tunnistivat seuraavia kehittämiskohteita:

- tilannejohtaminen
- tilannekuvan ylläpito koko harjoituksen ajan
- selkeämmät roolit ja vastuut
- sisäinen viestintä
- selkeämpi toimintaohje
- käyttöoikeusprosessien turvaaminen
- kriittiset järjestelmät ja palvelut (esim. riippuvuuksien tunnistaminen)

2.7 Tietoturvan kehitystoimet

Koronaepidemian puhkeaminen keväällä 2020 muutti työskentelytapoja ja lisäsi huomattavasti etätyöskentelyä. Tietoturvalliseen etätyöskentelyyn kiinnitettiin entistä enemmän huomiota ja oheistuksia sekä tietoturvaprosesseja päivitettiin. Työasemien käyttöjärjestelmän päivitysaikataulua nopeutettiin, jotta työasemien tietoturvataso saatiin nostettua paremmalle tasolle etätyöskentelyä varten. Tietoliikennekapasiteettia nostettiin sekä mahdollistettiin tietoturvallinen vpn-yhteyden käyttö entistä useammalle lisääntyneen etätyöskentelyn mahdollistamiseksi. Vuoden 2020 aikana Office 365 palveluiden käyttö laajentui merkittävästi etäkokousten myötä. Tässä yhteydessä kiinnitettiin huomiota myös Office 365 palveluiden tietoturva asioihin mm. ottamalla käyttöön ns. kaksivaiheinen tunnistautuminen Office 365 palveluihin.

3 Tiedonhallinta, tietovarannot ja tietovirrat

3.1 Tiedonhallintalaki

Vuoden 2020 alussa tuli voimaan tiedonhallintalaki (Laki julkisen hallinnon tiedonhallinnasta 906/2019

Lain tarkoituksena on

- varmistaa viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely julkisuusperiaatteen toteuttamiseksi;
- mahdollistaa viranomaisten tietoaineistojen turvallinen ja tehokas hyödyntäminen, jotta viranomainen voi hoitaa tehtävänsä ja tarjota palvelunsa hallinnon asiakkaille hyvää hallintoa noudattaen tuloksellisesti ja laadukkaasti;
- edistää tietojärjestelmien ja tietovarantojen yhteen toimivuutta

Laki määrittelee merkittäviä kuvaus- ja dokumentointivelvoitteita kunnille mm. tiedonhallintamalli ja asiakirjajulkisuuskuvaus.

3.2 Tiedonhallintamalli

Tiedonhallintalain edellyttämän tiedonhallintamallin laadinta aloitettiin 2020.
Tiedonhallintamalli on ylätason kuvaus organisaatiossa tehtävästä tietojen käsittelystä sekä tietoturvallisuuden varmistamiseksi tehtävistä toimenpiteistä.
Mallissa tulee kuvata myös sitä minkälaisia tietojärjestelmiin ja tietovarantoihin liittyviä kytköksiä kunnalla on muihin toimijoihin, esimerkiksi väestörekisterikeskukseen.
Mallissa kuvataan minimissään:

- toimintaprosessit
- tietovarannot
- tietoaineistot
- tietojärjestelmät sekä
- tietoturvajärjestelyt

Oriveden kaupungin tiedonhallintamalli rakentuu Digiturvamalli-työkaluun tallennettavien tietojen pohjalta.

3.3 Asiakirjajulkisuuskuvaus

Asiakirjajulkisuuskuvauksen avulla kerrotaan missä laajuudessa asioiden käsittelyssä ja kunnan palveluja käytettäessä kerätään tietoja kuntalaisista, palvelujen käyttäjistä ja henkilöstöstä.
Asiakirjajulkisuuskuvauksen on tarkoitus palvella kuntalaisia helpottamalla asiakirja- ja tietopyyntöjen tekemistä.
Oriveden kaupungin asiakirjajulkisuuskuvaus on julkaistu kaupungin verkkosivuilla.

4 Rekisteröidyn oikeudet ja niiden toteutuminen

Tietosuojavaltuutetun toimiston mukaan rekisteröidyllä on oikeus mm.:

- saada tietoa henkilötietojensa käsittelystä
- saada pääsy tietoihin
- oikaista tietoja
- poistaa tiedot tai tulla unohdetuksi
- rajoittaa tietojen käsittelyä
- siirtää tiedot järjestelmästä toiseen
- vastustaa tietojen käsittelyä
- olla joutumatta automaattisen päätöksenteon kohteeksi.

Rekisteröity ei voi käyttää kaikkia oikeuksia kaikissa tilanteissa. Tilanteeseen vaikuttaa esim. henkilötietojen käsittelyperuste.

Oriveden kaupunki pyrkii noudattamaan henkilötietojen käsittelyssä läpinäkyvyyttä ja tietojen täsmällisyyttä asetuksen mukaisesti (artikla 5). Informointivelvoitteen täyttämiseksi käytetään toistaiseksi tietosuojaselosteita. Hyväksytyt ja ajantasaiset tietosuojaselosteet löytyvät kaupungin verkkosivuilta (artiklat 13 ja 14).
Verkkosivuilta löytyvät myös rekisteröityjen oikeuksiin perustuvat tarkastuspyyntö- ja oikaisupyyntölomakkeet (artiklat 15, 16). Ko. lomakkeita voi lähettää myös sähköisenä Suomi.fi-viestit palvelun kautta.

Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle 72 tunnin kuluessa, 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, talous- ja hallintojohtajan ja tietohallintopäällikön harkinnan mukaan.

5 Seuranta ja mittaaminen

5.1 Dokumentointi

Tietoturva- ja tietosuoja-asioiden hallintajärjestelmän, Digiturvamallin avulla Oriveden kaupunki dokumentoi tietosuoja-asetuksessa vaaditut asiat.

Järjestelmään on tallennettu mm. seuraavat tiedot:

- tietojärjestelmät (mitkä yksiköt järjestelmää käyttävät, kenen tietoja käsitellään, mitä henkilötietoryhmiä järjestelmä sisältää, kuka järjestelmää ylläpitää, miten tieto virtaa järjestelmään ja sieltä eteenpäin jne.)
- järjestelmätoimittajat (mm. tiedot henkilötietojen käsittelysopimuksista)
- henkilörekisterit (mikä yksikkö rekisteristä vastaa, tietovarannot, joista rekisteri muodostuu, käsittelytarkoitukset, tietojen luovutus muuhun käyttöön jne.)
- tietolähteet
- tietoturvaloukkaukset
- tietopyyntöjen määrä

5.2 Tietopyynnöt

Saapuneet tietopyynnöt kirjataan asianhallintajärjestelmään. Vuonna 2020 Oriveden kaupungille on tullut 39 kpl henkilörekistereihin kohdistuvaa tietopyyntöä. Suurin osa pyynnöistä koski potilasasiakirjoja. Potilasasiakirjapyyntöjä tuli 16 kpl. Em. pyynnöt ovat tulleet pääasiassa sosiaali- tai terveydenhuollon toimijoilta.
Potilasasiakirjapyyntöihin pyritään vastaamaan viipymättä ja pääsääntöisesti vastaus on lähetetty pyynnön saapumispäivänä. Jos kyseessä on rekisteröidyn lähettämä hyvin laaja tietopyyntö, vastausaika on enintään kuukausi pyynnön vastaanottamisesta. Määräaikaa voidaan myös jatkaa.

5.3 Tietosuoja-/tietoturvapoikkeamat

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu tai niihin pääsee käsiksi ulkopuolinen taho, jolla ei ole oikeutta käsitellä tietoja. Tietoturvaloukkaus voi tapahtua vahingossa tai tahallisesti. Henkilötietojen tietoturvaloukkauksia ovat esimerkiksi tietojen lähettäminen väärälle henkilölle, kadonnut henkilötietoja sisältävä paperi, omaan työhön kuulumattomien henkilötietojen katselu, kadonnut muistitikku, varastettu tietokone tai murtautuminen henkilötietoja sisältävään järjestelmään.

Vuonna 2020 havaittiin yksi tietosuojapoikkeama, josta tehtiin ilmoitus tietosuojaviranomaiselle. Lisäksi oli 2 lievempää tietosuojapoikkeamaa, joista ei tarvinnut tehdä tietosuojaviranomaisille ilmoitusta. Tietoturvapoikkeamia havaittiin 2 kpl:ta, jotka liittyivät tietojärjestelmissä olevien tietojen saatavuuteen.

6 Arviointi ja kehittäminen

Henkilötietojen käsittelyssä Oriveden kaupunki tulee noudattamaan hyvää tiedonhallintatapaa ja kehittää edelleen toimintatapojaan siten, että ne vastaavat EU:n yleisessä tietosuoja-asetuksessa annettuja vaatimuksia. Keskeisenä ohjaavana dokumenttina toimii henkilöstön tietoturva- ja tietosuojaopas.

6.1 Tiedonohjaussuunnitelma

Tiedonhallintaan ja tiedonhallintaympäristöön merkittävästi vaikuttava projekti vuonna 2021 asianhallintajärjestelmän version päivitys. Tiedonohjaussuunnitelmat täytyy olla valmiit tätä ennen, jotta asianhallintajärjestelmään integroitava tiedonohjausjärjestelmä välittää metatietoarvoja, ohjaustietoja ja käsittelysääntöjä asianhallintajärjestelmään, jossa asiakirjatietoa syntyy tai käsitellään. Tiedonohjaussuunnitelma on edellytys sähköisten asiakirjatietojen hallinnalle.
Oriveden kaupungin tiedonohjaussuunnitelma noudattaa SÄHKE2 -normia (Sähköisten asiakirjallisten tietojen käsittely, hallinta ja säilyttäminen).
Palvelukeskusten arkistovastaavat ovat jatkaneet tiedonohjaussuunnitelmien laatimista. Tiedonohjaussuunnitelmat tulee olla valmiit syksyyn 2021 mennessä, jolloin uusi asianhallintajärjestelmän versio otetaan käyttöön.

6.2 Tietoturvakoulutus

Henkilöstön koulutukseen on edelleen saatavilla videopohjaisia 21 osiosta koostuva Kyberoppikoulutus. Henkilöstön perehdyttämisessä on käytössä sähköinen käyttö- ja salassapitositoumus kaikille tietokoneiden käyttäjille sekä henkilöstön tietoturva- ja tietosuojaopas, joka löytyy kaikkien hallintoverkon tietokoneiden työpöydältä.

6.3 Tietosuojakoulutus

Keskeinen osa tietosuoja-asetuksen edellyttämää organisaation osoittamisvelvollisuutta on, että henkilöstö tietää ja ymmärtää, miten henkilötietoja käsitellään. Tämä edellyttää säännöllisiä tietosuojakoulutuksia. Tavoitteena on, että tietosuojakoulutukset ovat mahdollisimman käytännön läheisiä ja niitä järjestetään säännöllisesti.
Kaupungin henkilöstöllä on velvollisuus allekirjoittaa vaitiolo- ja salassapitositoumus sekä suorittaa hyväksytysti voimassa oleva tietoturva- ja tietosuojan verkkokoulutus. Tietosuojan ABC julkishallinnon henkilöstölle - verkkokoulutukseen ja nettitestiin pääsee kaupungin intranetissä, tietosuoja-sivustolla olevan linkin kautta. Testin hyväksytystä suorittamisesta saa todistuksen, joka lähetetään tietosuojavastaavalle tietosuojakoulutuksen dokumentointia varten.

7 Tietojenkäsittelyyn vaikuttava lainsäädäntö ja muu ohjeistus

Keskeiset kaupungin tietojen käsittelyä koskevat lait ja ohjeet:

- Kuntalaki 410/2015
- Hallintolaki 434/2003
- Tiedonhallintalaki (Laki julkisen hallinnon tiedonhallinnasta 906/2019)
- Laki sähköisestä asioinnista viranomaistoiminnassa 13/2003
- Laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista 571/2016
- Arkistolaki 831/1994
- EU:n yleinen tietosuoja-asetus (GDPR) 679/2016
- Tietosuojalaki 1050/2018
- Julkisuuslaki (Laki viranomaisen toiminnan julkisuudesta 621/1999
- Toimialakohtaiset erityislait
- Kaupungin ohjeistus
- Henkilöstön tietoturva- ja tietosuojaopas
- Henkilötietojen käsittelyopas
- Sähköisten viestintävälineiden käyttösäännöt
- Käyttövaltuusperiaatteet