2019

Tietotilinpäätös

Joutsan kunta

Kunnanhallitus xx.x.2020

Sisällysluettelo

1 JOHDANTO

Kunnallisella puolella tietosuojalainsäädännön kokonaisuuden muodostavat kansallinen tietosuojalaki, EU:n tietosuoja-asetus sekä sektorikohtaiset erityislainsäädännöt yhdessä julkisuuslain kanssa.

EU:n tietosuoja-asetus (GDPR) soveltaminen astui voimaan 25.5.2018 kaikissa EU-maissa. Kansallinen tietosuojalaki hyväksyttiin eduskunnassa syksyllä 2018 ja se astui voimaan Suomessa 1.1.2019. Kansallisessa tietosuojalaissa on määritelty mm. lapsen ikä, kansallinen valvontaviranomainen ja kansalliset rangaistukset. Henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta kumoutuivat tietosuojalain tullessa voimaan.

Tietosuojalain mukaan kansallisena valvontaviranomaisena Suomessa toimii tietosuojavaltuutetun toimisto. Ns. hallinnollisia sakkoja eli seuraamusmaksuja ei Suomessa voida määrätä valtion tai kunnan viranmaiselle, mutta muita seuraamuksia, kuten varoituksia, huomautuksia ja määräyksiä voidaan määrätä viranomaisille kuten muillekin toimijoille. Lapsen iäksi tietosuojalaissa Suomessa on määritelty 13 vuotta.

1.1 Tietotilinpäätöksen tarkoitus

Vuosittain laadittava Joutsan kunnan tietotilinpäätös kuvaa tietojen käsittelyn nykytilaa, arvioi tietosuojan ja tietoturvan toteutumista, tarkastelee tietosuojan valvontaa ja esittelee kehityskohteita. Tietotilinpäätös on kunnan johdolle tarkoitettu tietosuojan seurannan ja kehittämisen työkalu ja sitä voidaan käyttää sisäisen ja ulkoisen valvonnan apuvälineenä.

Tietotilinpäätöksen koonnista vastaa tietosuojavastaava yhdessä tietosuojatyöryhmän kanssa. Tietotilinpäätöstä laadittaessa on huomioitu tietosuojavaltuutetun toimiston ohjeistus sekä kunnan tietosuojavastaavan saama koulutus. Tietotilinpäätöksen hyväksyy kunnanhallitus.

Joutsan kunnan ensimmäinen tietotilinpäätös tehtiin vuodesta 2017. Silloin tietotilinpäätös keskittyi pääasiassa kehittämiskohteisiin. Vuoden 2018 tietotilinpäätöksessä päästiin tarkastelemaan enemmän toimenpiteitä, joita tietosuoja-asetuksen eteen on tehty. Vuonna 2019 tietosuojan parissa on keskitytty tietosuojakäytäntöjen jalkauttamiseen kunnassa.

1.2 Organisaation kuvaus

Joutsan kunnassa oli vuoden 2019 lopussa 277 työntekijää, joista vakituisessa työsuhteessa oli 239 työntekijää.

Joutsan kunnan työntekijät joutuvat käsittelemään henkilötietoja työssään useissa tietojärjestelmissä ja henkilörekistereissä. Suurin osa henkilötietojen käsittelystä kunnassa perustuu lakiin sekä yleistä etua koskevaan etuun tai julkiseen valtaan.

Viimekädessä vastuu lainmukaisuudesta sekä tietosuojan ja tietoturvan toteutumisesta on organisaation johdolla. Joutsan kuntaan on nimetty tietosuojatyöryhmä, joka omalta osaltaan valvoo tietosuojan toteutumista sekä kehittää tietosuojatyötä.

Tietosuojavastaavan rooli korostuu tietosuojatyössä. Hän toimii mm. yhdyshenkilönä henkilötietojen käsittelijöille (kunnan työntekijät), rekisteröidyille (kuntalaiset) ja valvontaviranomaiselle (tietosuojavaltuutetun toimisto). Tietosuojavastaavan tehtäviin kuuluu myös asiantuntijana ja tiedottajana toimiminen, tietosuoja-asetuksen ja –lain noudattamisen valvominen sekä kouluttajana ja neuvonantaja toimiminen. Tietosuojavastaava raportoi säännöllisesti kunnan johdolle tietosuojan toteutumista kunnassa.

2 TIETOVARANNOT

2.1 Tietosuojaselosteet

Joutsan kunnan tietovarannot koostuvat useista rekistereistä. Kunnassa päivitettiin vanhat rekisteriselosteet tietosuojaselosteiksi vuonna 2018. Tietosuojaselosteiden laatiminen henkilötietoja sisältävistä rekistereistä on jatkunut vuoden 2019 aikana. Tietosuoja-asetuksen 12 artiklan mukaan henkilötietojen käsittelijän tulee esittää käsittelyä koskevat tiedot tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Tietosuojaselosteet on tallennettu kunnan verkkolevylle ja ne voi pyytää nähtäväksi kunnan asiointipisteeltä (Länsitie 5). Tietosuojaselosteet on laadittu tietosuojavaltuutetun ohjeiden mukaan.

Tietosuojaselosteet ovat osa kunnan informointivelvollisuutta. Rekisteröidyillä on oikeus tietää, mihin tarkoitukseen hänen henkilötietojaan kerätään sekä miten niitä käsitellään. Tietosuojaselosteesta käy ilmi mm. henkilötietojen käsittelyn tarkoitus, rekisterin tietosisältö, tietolähteet ja tietojen säilyttäminen, suojaukseen periaatteet sekä rekisteröidyn oikeudet. Tietosuojaselosteet ovat julkisia asiakirjoja. Työntekijöiden tulee pystyä vastaamaan rekisteröidyille rekisteriin liittyviin kysymyksiin, jolloin hän voi apuna käyttää tietosuojaselostetta.

Tietosuojavastaava on laatinut kunnalle pohjan tietosuojaselosteelle, jolloin uusista rekisteristä on helppo tehdä tietosuojaselosteet. Tietosuojavastaava yhdessä rekisterin pääkäyttäjän kanssa huolehtii tietosuojaselosteiden päivittämisestä.

2.2 Seloste käsittelytoimista

Seloste käsittelytoimista on kirjallinen kuvaus organisaation tekemästä henkilötietojen käsittelystä. Kunnassa on tietosuoja-asetuksen 30 artiklan määrittelemä velvollisuus laatia seloste käsittelytoimista. Asetuksen mukaan selosteen on sisällettävä mm. rekisterinpitäjän ja tietosuojavastaavan yhteystiedot, käsittelyn tarkoitukset, kuvaus rekisteröityjen ryhmistä ja kuvaus teknisistä ja organisatorisista turvatoimista.

Seloste käsittelytoimista on kunnan omaan käyttöön laadittu sisäinen asiakirja. Se edistää kunnan osoitusvelvollisuuden toteutumista. Selostetta voidaan käyttää rekisteröidyille suunnatun informaation tuottamiseen, vaikka sitä suoraan ei ole tarkoitettu rekisteröidyn informointiin. Joutsan kunnassa rekisteröidyn informointiin käytetään ensisijassa tietosuojaselosteita. Seloste käsittelytoimista voidaan tarvittaessa toimittaa valvontaviranomaiselle.

Tietosuojavastaava on laatinut Joutsan kunnalle selosteen käsittelytoimista. Seloste on tallennettu kunnan verkkolevylle sekä intranettiin työntekijöiden saataville. Tietosuojavastaava huolehtii selosteen päivittämisestä.

2.3 Henkilötietojen käsittely

2.3.1 Yleisiä käsitteitä

Tietosuoja-asetuksen 4 artiklassa on määritelty tietosuoja-asetuksessa käytettäviä käsitteitä. Asetuksen mukaan henkilötietona pidetään merkintää, jonka perusteella henkilö voidaan tunnistaa. Henkilö voidaan tunnistaa suoraan tai epäsuorasti eli myös tietoja yhdistelemällä. Henkilötunnus on tehty henkilön yksilöintiin eikä henkilötunnusta yksinään voida pitää henkilön tunnistamiseen riittävänä.

Henkilötietojen käsittelynä pidetään kaikkia toimenpiteitä, jotka kohdistuvat henkilötietoihin, kuten henkilötietojen kerääminen, tallettaminen, käyttäminen, muuttaminen ja poistaminen. Henkilörekisteri on henkilötietoja sisältävät tietojoukko, teknisesti esim. paperinen nimilista tai asiakastietojen hallintaan käytettävä ohjelmisto. Joutsan kunnalla on myös yhteisrekistereitä, jolloin samaa rekisteriä käyttää esim. palvelun tarjoaja ja palvelutuottaja. Kunnalla on yhteisrekisteri mm. Keski-kirjastojen kanssa sekä Joutsan seurakunnan kanssa yhtenäiskoulun iltapäiväkerhon asiakkaista.

Tietosuoja-asetuksessa on määritelty erityiset henkilötiedot, joiden käsittely saattaa aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja –vapauksille ja johtaa syrjintään. Kunnassa erityisiä henkilötietoja käsitellään etenkin perusturvaosastolla. Lisäksi tietosuoja-asetus antaa erityistä suojaa lasten henkilötiedoille. Tietosuojalain § 5:ssä on määritellyt Suomessa lapsen iäksi 13-vuotta, jolloin alle 13-vuotiaan henkilötietoja ei saa käsitellä ilman huoltajan suostumusta.

2.3.2 Käsittelyperuste

Henkilötietojen käsittelyperusteet on määritelty tietosuoja-asetuksen 6 artiklassa. Kunnassa henkilötietojen käsittely perustuu usein lakisääteisen velvoitteen noudattamiseen tai yleiseen etuun ja julkiseen valtaan. Kunnalla on monissa tapauksissa tehtävään perustuva oikeus henkilötietojen käsittelyyn eli laissa määrätyn tehtävän hoitaminen edellyttää henkilötietojen käsittelyä. Yleistä etua koskevaa käsittelyä kunnassa käytetään mm. tilastointiin. Yleistä etua koskeva tehtävä tai julkinen valta on täytynyt antaa lailla tai muulla oikeudellisella säännöksellä.

Työntekijöillä on oikeus käsitellä vain työssään välttämättömiä henkilötietoja. Esimiehet myöntävät työntekijöille käyttöoikeudet niihin tietojärjestelmiin, joita he työssään tarvitsevat. Kunnan henkilöstön koulutuksissa on painotettu sitä, että työntekijän tulee kiinnittää huomiota miten ja missä henkilötietoja käsittelevät, mitä tietoja käsittelevät sekä kenelle henkilötietoja luovuttavat.

Perusturvassa, mm. sosiaalitoimessa, vanhuspalveluissa ja kotihoidossa, työntekijät allekirjoittavat salassapito- ja vaitiololupauksen, koska he käsittelevät työssään paljon erityisiä henkilötietoja. Työntekijöiden tulee huomioida henkilötietoja käsitellessään laki viranomaisen toiminnan julkisuudesta (621/1999) ja sieltä etenkin salassapitoon liittyvät § 22-25. Työntekijöiden tulee huolehtia salassapito- ja vaitiolovelvollisuudesta käsitellessään erityisiä henkilötietoja tai muutoin salaisiksi määriteltyä tietoja.

3 TIETOJENKÄSITTELYN NYKYTILA KUNNASSA

Kunnalla on julkisena toimijana lakisääteinen velvollisuus nimetä tietosuojavastaava (tietosuoja-asetus 37 artikla). Kunnanhallituksen aiemman päätöksen mukaisesti (khall 29.1.2018 § 15) kunnan tietosuojavastaavana toimii toimistovirkailija Liisa Alfthan ja tietoturvavastaavana ICT-asiantuntija Jarkko Puhakka sekä johtoryhmän edustajana talous- ja hallintojohtaja (khall 13.8.2018 § 175). Vuonna 2019 henkilöstövaihdosten myötä kunnanhallitus (khall 25.11.2019 § 226) päätti nimetä perusturvaosaston tietosuojan vastuuhenkilöksi perusturvajohtajan, josta tuli samalla tietosuojatyöryhmän jäsen.

3.1 Kuntalaisille tiedottaminen

Tietosuoja-asetuksen voimaan tultua kunnan verkkosivuille lisättiin oma osionsa tietosuojasta http://www.joutsa.fi/asiointi-ja-neuvonta/tietosuoja/. Sivulla tiedotetaan kuntalaisia mm. heidän tarkastusoikeudestaan omiin tietoihin. Sivulta löytyy kunnan omat tarkastuspyyntö- ja korjaamisvaatimuslomakkeet.

Kunnan tietosuojavastaavan työpiste on kunnan asiointipisteellä, joten hän on helposti myös kuntalaisten tavoitettavissa. Kunnan verkkosivuilla on tietosuojavastaavan yhteystiedot.

3.2 Johdolle raportointi ja luottamushenkilöt

Tietosuojavastaava ja tietoturvavastaava olivat esittelemässä kunnanhallitukselle 25.3.2019 tietotilinpäätöksen 2018, päivitetyn tietoturvasuunnitelman ja riskianalyysin sekä hallinnon tietosuojaselosteet.

3.3 Koulutukset ja tiedottaminen henkilöstölle

Tietosuojavastaava koulutti kunnan henkilöstön osastoittain vuonna 2018. Vuonna 2019 järjestettiin keskitetty koulutus henkilöstölle 28.5.2019, jossa käytiin läpi käytännön ohjeet henkilötietojen käsittelyssä (liite 1.).

Osastoille pidettyjen koulutusten materiaalit on toimitettu osastoille, joissa ne ovat työntekijöiden luettavissa. Materiaali löytyy myös sähköisesti osastojen verkkolevyltä. Intrasta löytyy tietosuojaan ja –turvaan liittyvät ohjeistukset.

Työntekijöitä tiedotetaan tietosuojaan liittyvistä ajankohtaisista asioista sähköpostitse. Noin kerran vuodessa pyritään järjestämään koulutusta joko itse opiskeltavien materiaalien muodossa tai esim. luentotyyppisesti.

Kunnan työntekijät on koulutettu ja ohjeistettu henkilötietojen käsittelystä. Kuntaan on vuoden 2019 aikana laadittu rekrytointisuunnitelma (otetaan käyttöön vuoden 2020 alusta), johon on liitetty tietosuoja, tietoturva ja henkilötietojen käsittelyn ohjeistus uudelle työntekijälle.

3.3.1 Käytännön ohjeet henkilötietojen käsittelyssä Joutsan kunnassa

Julkisena toimijana kunnan tulee noudattaa myös lakia viranomaisen toiminnan julkisuudesta (1999/621). Kyseinen laki määrittelee mm. asiakirjojen julkisuudesta. Vaikka kuntaan tulleet ja lähtevät asiakirjat ovat pääsääntöisesti julkisia, ei niitä kaikkia kuitenkaan julkaista.

Kunta tiedottaa kuntalaisia laajasti mm. verkkosivuillaan, mutta samalla tulee kiinnittää huomiota siihen, että henkilötietojen sähköiseen luovuttamiseen tarvitaan aina asianomaisen suostumus.

Kunnan työntekijöillä on julkinen työrooli, joten heidän nimi, asema, työtehtävä ja työyhteystiedot ovat julkisia. Työntekijöiden kuvia tai yksityisiä henkilötietoja, kuten yhteystietoja, ei saa julkaista eikä työntekijöiden poissaolojen syitä saa ilmoittaa ulkopuolisille ilman työntekijän omaan suostumusta.

Joutsan kunnan käytännön ohjeet henkilötietojen käsittelyyn ovat tämän tietotilinpäätöksen liitteenä.

4 TIETOSUOJAN JA TIETOTURVAN TOTEUTUMINEN

4.1 Organisaatio ja vastuut

Tietoturvaa ja tietosuojaa johtaa ja valvoo kunnanhallitus. Kunnanhallitus nimeää tietoturvavastaavan, tietosuojavastaavan ja tietosuojatyöryhmän.

Tietoturvan kehittämisestä, toteutuksen valvonnasta, tietoturvatietouden edistämisestä ja tietoturvallisesta toimintatavasta kunnassa sekä raportoinnista vastaa kunnan johdolta saamiensa resurssien ja toimintavaltuuksien puitteissa tietoturvavastaava. Hän vastaa myös tietoturva-asioista tiedottamisesta kunnan ulkopuolelle ja kunnan sisällä yleisellä tasolla. Tietosuojavastaava seuraa henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet sekä toimii valvontaviranomaisen sekä rekisteröityjen yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä kysymyksissä.

Tietoturva- ja tietosuoja-asioiden ohjeistamisesta, tiedottamisesta ja valvonnasta omassa yksikössään vastaa yksikön esimies yhdessä tietoturvavastaavan ja tietosuojavastaavan avustuksella. Jokainen kunnan työntekijä, tietoja käsittelevä, tietojärjestelmien tai tietoverkkojen ylläpitäjä ja käyttäjä on omalta osaltaan vastuussa tietoturvan ja –suojan toteuttamisesta sekä niihin liittyvien ohjeiden noudattamisesta. Työntekijät ovat velvollisia ilmoittamaan tietoturvaan liittyvistä uhista ja poikkeamista esimiehelleen tai tietoturvavastaavalle.

Käyttöoikeudet järjestelmiin annetaan työtehtävän mukaan ja esimies määrittelee annetut oikeudet. Järjestelmien pääkäyttäjät huolehtivat, että työntekijällä on oikeudet työssään tarpeellisiin tietoihin. Työntekijän tulee huomata, että käyttöoikeus ei anna oikeutta käsitellä tietoa, jota ei työssään tarvitse vaikka tietoon pääsisikin käsiksi.

4.2 Tietosuojatyöryhmä

Tietosuojatyöryhmän tehtävänä on tietoturvan ja tietosuojan kehittämiseen liittyvät linjaukset ja ohjeistukset ennen kuin ne esitellään johdolle hyväksyttäväksi. Lisäksi tietosuojatyöryhmä käsittelee kokouksissaan mm. tietoturvaloukkaukset ja niihin liittyvät toimenpiteet sekä muut tietosuojaan ja –turvaan liittyvät ajankohtaiset asiat.

Tietosuojatyöryhmä on kokouksissaan käynyt läpi tietosuojan toteutumista kunnassa, koulutusten materiaalia sekä tietopyyntöihin ja tietosuojarikkomuksiin liittyviä tilanteita. Tietosuojavastaava kirjaa muistion kaikista tietosuojatyöryhmän kokoontumisista. Vuoden 2019 aikana tietosuojatyöryhmä kokoontui noin joka toinen kuukausi.

4.2.1 Tietosuojavastaava

Kunnanhallituksen kokouksessa 29.1.2018 § 15 tietosuojavastaavaksi nimitettiin toimistovirkailija Liisa Alfthan.

Tietosuojavastaava toimii kokoonkutsujana tietosuojatyöryhmän kokouksissa sekä kirjoittaa muistion niistä. Kunnan johto antaa tietosuojavastaavalle riittävät resurssit tehtävän hoitamiseen. Tietosuojavasta toimii kunnassa tietosuojan asiantuntijana, kouluttajana ja neuvonantajana, valvojana sekä yhdyshenkilönä niin henkilötietojen käsittelijöille, rekisteröidyille kuin valvontavirnaomaiselle.

Tietosuojavastaava osallistui kesällä perusturvan tietosuojakoulutukseen, mutta kyseinen koulutus oli lähinnä perustietoa tietosuojasta eikä antanut tietosuojavastaavalle erityisesti uutta ja toivottua tietoa nimenomaan perusturvan tietosuojasta.

4.3 Tietosuojan ja tietoturvan ohjeistus

Kuntaan on laadittu vuonna 2019 henkilöstöopas sekä perehdytyssuunnitelma. Näissä molemmissa on huomioitu tietosuoja ja tietoturva. Etenkin uusien työntekijöiden perehdytyksessä tullaan jatkossa selkeämmin käymään läpi myös tietosuoja ja henkilötietojen käsittelyyn liittyvä ohjeistus.

Aiemman vuoden ohjeistus ja materiaali tietosuojaan liittyen on löydettävissä verkkolevyltä sekä henkilöstölle suunnatut ohjeet ovat kunnan intrassa.

5 TIETOSUOJAN PROSESSIT JA VALVONTA

5.1 Tietojen tarkistaminen, korjaaminen ja poistaminen

Rekisteröidyillä on oikeus saada pääsy tietoihin sekä oikaista ja poistaa henkilötietojaan rekisteristä tietyissä tapauksissa. Rekisteröityä koskevat virheelliset ja epätarkat henkilötiedot on mahdollista korjata rekisteröidyn pyynnöstä. Lisäksi on mahdollista, että asiakkaan puuttuvia henkilötietoja lisätään tai virheellisiä tietoja poistetaan. Oikeus tulla unohdetuksi eli henkilötietojen poistaminen rekisteristä on joissakin tilanteissa mahdollista. Rekisteröidyllä ei kuitenkaan ole oikeutta saada tietojaan pois rekisteristä, jos tietojen käsittely perustuu esim. lakiin.

Tietosuojatyöryhmä on laatinut tietojen tarkastamiseen, korjaamiseen ja poistamiseen prosessikaavion. Kuntaan laadittiin myös omat lomakkeet tietopyyntöjä varten. Lomakkeet löytyvät kunnan verkkosivuilta sekä asiointipisteeltä. Kunnan verkkosivuilla on myös ohjeistettu

kuntalaisia kuinka tietopyyntö kuntaan tulee jättää. Tietopyyntö jätetään kunnan tietosuojavastaavalle osoitettuna. Tietopyynnön vastaanottajan tulee varmistaa tietopyynnön jättäjän henkilöllisyys.

Kunta vastaa rekisteröityjen tietopyyntöihin asetuksen määrittämässä ajassa eli kuukauden sisällä. Tietyissä tapauksissa kunnalla on mahdollisuus kieltäytyä tietojen antamisesta, jolloin kieltäytymisen tulee perustua lakiin ja siitä tulee antaa rekisteröidylle kirjallinen tieto. Mikäli rekisteröidyn tietopyyntö on vaativa ja monimutkainen, voi kunta ilmoittaa pyytäjälle perusteluineen käsittelyn kestävän pidempään kuin 30 pv, jatkoaika on kuitenkin enintään kaksi kuukautta.

Tietojen pyytäminen on pääsääntöisesti maksutonta, mutta kunnanhallituksen päätöksen (§ 113/2018) mukaan jatkuvista ja työllistävistä tietopyynnöistä kunta perii 100 € käsittelymaksun.

Tietosuojavastaava kirjaa kaikki tietopyynnöt ja niihin liittyvät toimet on Dynasty-asiakirjahallintaohjelmaan. Tietopyynnöissä sovelletaan tietosuoja-asetusta ja lakia sekä pyynnöstä riippuen myös muita lakeja, esim. hallintolakia (434/2003) ja lakia potilaan asemasta ja oikeuksista (785/1992). Vuoden 2019 aikana kuntaan ei tullut yhtään henkilötietoihin kohdistuvaa tietopyyntöä.

5.2 Tietosuojan toteutuminen

Jokainen kunnan työntekijä on vastuussa omalta osaltaan tietosuojan toteutumisesta ja noudattamisesta. Tietosuojavastaava ohjaa ja valvoo tietosuoja-asetuksen ja lain noudattamista. Tärkeä osa tietosuojan toteutumista on ollut henkilöstölle suunnatut koulutuksen henkilötietojen käsittelystä. Tietosuojan toteutumisessa korostuu käytännön ohjeet, joiden käyttöönotto osaksi arkityötä vaatii vielä aikaa.

5.3 Tietoturvaloukkaus

Tietosuojatyöryhmä on laatinut prosessikaavion tietoturvaloukkauksien hoitamiseen. Käyttäjien ja ylläpitäjien tulee ilmoittaa havaitsemastaan tietoturvan puutteesta, tietoturvaan liittyvästä väärinkäytöksestä tai epäilemästään tietoturvarikkomuksesta esimiehelleen tai tietoturvavastaavalle. Tietoturvavastaava yhdessä esimiehen ja tarvittaessa tietosuojavastaavan kanssa arvioi ja selvittää tilanteen sekä suorittaa tarvittavat toimenpiteet vahinkojen minimoimiseksi. Tarvittaessa tietoturvavastaava kutsuu tietosuojatyöryhmän sekä muut mahdolliset henkilöt koolle ja tehdään päätös tiedottamisen laajuudesta. Kaikki tietoturvaepäilyt ja niihin kohdistetut toimenpiteet kirjataan tiedostoon kunnan verkkolevylle.

Yksikön esimiehen tehtävänä on valvoa tietoturvan toteutumista omassa yksikössään. Tietoturvavastaavan tehtävänä on seurata ja valvoa Joutsan kunnan tietojärjestelmien tietoturvan toteutumista ja ryhtyä toimenpiteisiin havaittujen tietoturvan heikkouksien korjaamiseksi.

Vuoden 2019 aikana kunnan tietosuojatyöryhmällä oli tutkinnassa neljä (4) kappaletta tietoturvapoikkeus epäilyä. Kahdessa tapauksessa ei todettu tietosuojan vaarantuneen. Kahdessa tapauksessa informoitiin asianosaisia tietosuojatapahtumasta, näistä molemmat koskivat yksittäisen henkilön tietoja.

6 TIETOJENKÄSITTELYN KEHITTÄMISKOHTEET

Tietosuoja ei ole enää ns. uusi asia, josta keskustellaan jatkuvasti. Siksi on tärkeätä saada jatkossakin tietosuoja sisällytettyä kunnan työntekijöiden jokapäiväiseen työhön.

6.1 Henkilörekisterit ja tietojärjestelmät

Tietojärjestelmiin laaditaan tietosuojaselosteet ja ohjelmien käyttöoikeudet myönnetään työtehtävien ja tietosuojan mukaisesti. Uusista henkilötietoja sisältävistä ohjelmistoista tulee laatia tietosuojaselosteet, joiden tekemisestä vastaa tietosuojavastaava sekä ohjelmiston pääkäyttäjä.

6.2 Kouluttaminen ja tiedottaminen

Kunnan työntekijöitä tullaan ensisijaisesti tiedottamaan tietosuojaan liittyen uudistuneessa intrassa.

Vuosittain järjestetään vähintään yksi koulutustilaisuus henkilöstölle, jossa käydään läpi henkilötietojen käsittelyyn liittyvät käytännön ohjeet Joutsan kunnassa. Koulutukseen on mahdollista tulla paitsi uusien työntekijöiden myös vanhojen työntekijöiden kertaamaan ja kysymään tietosuojaan liittyviä kysymyksiä. Lisäksi perehdytyksessä tullaan entistä enemmän kiinnittämään huomiota tietosuojaan ja tietoturvaan.

6.3 Haasteita

Tietosuojavastaavalle tulee jatkossakin löytää aikaa ja mahdollisuus pitää asiantuntemustaan yllä. Lisäksi on tärkeätä, että tietosuojavastaava on paitsi rekisteröityjen, myös kunnan työntekijöiden käytettävissä. Tietosuojavastaavan tulee jatkossakin informoida kunnan työntekijöitä tietosuojaan liittyvistä asioista. Uusien työntekijöiden tulee saada riittävä perehdytys tietosuojaan ja henkilötietojen käsittelyyn liittyen, jolloin perehdyttäjän tulee itse olla hyvin tietoinen näistä asioista.

Henkilötietojen käsittely

EU:n tietosuoja-asetus

Liisa Alfthan

Tietosuojavastaava

Tietosuoja - Tietoturva

- EU:n tietosuoja-asetusta (GDPR) noudatettava 25.5.2018 alkaen
  - Rekisterinpitäjän **velvollisuudet** kasvavat
  - Rekisteröidyn **oikeudet** kasvavat
  - Henkilötietolaki korvataan **kansallisella tietosuojalailla** (syksy 2018?)
- Tietoturva on tietosuojan toteuttamisen keino
- Tietosuoja tarkoittaa pääasiassa **henkilön tekemiä** henkilötietojen suojaamiseen liittyviä toimia (yksityisyyden suoja)
- Tietoturva tarkoittaa pääasiassa tiedon suojaamista **teknisin ja organisatorisin keinoin**
- Tietosuoja ja tietoturva ovat kaksi eri asiaa, mutta menevät osittain päällekkäin

Käsitteitä

- **Henkilötieto** – merkintä, jonka perusteella henkilö voidaan tunnistaa (esim. nimi, osoite, sormenjälki, fyysinen piirre, IP-osoite)
- **Henkilötietojen käsittely** – henkilötietoihin kohdistuvat toimenpiteet (esim. kerääminen, käyttö, muuttaminen, poistaminen)
- **Henkilörekisteri** – henkilötietoja sisältävä tietojoukko. Teknisesti rekisteri voi olla esimerkiksi paperinen lista, Excel-tiedosto tai asiakastietojen hallintaan käytetty ohjelmisto.
- **Rekisterinpitäjä** – taho, jonka käyttöä varten rekisteri on perustettu (Joutsan kunta)
- **Rekisteröity** – ketä henkilötieto koskee (kuntalainen)
- **Käsittelijä** – käsittelee henkilötietoja rekisterinpitäjän lukuun (kunnan työntekijä)
- **Tietosuojaseloste** – asiakirja, josta ilmenee mm. rekisterinpitäjän tiedot sekä rekisterin käyttötarkoitus ja kuvaus (ent. rekisteriseloste)
- **Yhteisrekisteri** – samaa rekisteriä käyttää esim. palvelun tarjoaja ja palvelun tuottaja
  - Tilaaja/palvelun tarjoaja -> Joutsan kunta
  - Palveluntuottaja -> esim. seurakunta (iltapäiväkerho)

Tietosuojavastaava

- Kunnalla **lakisääteinen velvollisuus** nimetä tietosuojavastaava (julkinen sektori)
- Viimekädessä **vastuu** toiminnan lainmukaisuudesta sekä tietosuojan ja tietoturvan toteutumisesta on **organisaation johdolla**
- **Asiantuntija**
  - Mukaan henkilötietojen suojaa koskevien kysymysten käsittelyyn (tuotanto- ja palveluprosessit, hankinnat)
  - Osallistuu tietosuoja- ja tietoturvaohjeita koskevaan valmisteluun ja ylläpitoon (esim. tietotilinpäätös)
  - Yhteistyö tietoturvavastaavan kanssa
  - Tiedonantaja
- **Kouluttaja/neuvoja**
  - Ohjeistuksen laadinta
  - Koulutukset
- **Valvoja**
  - Seuraa ja valvoo henkilötietojen käsittelyä sekä niiden suojausmenetelmiä
  - Raportoi johdolle (johtoryhmä ja kunnanhallitus)
- **Yhdyshenkilö**
  - Henkilötietojen käsittelijöille
  - Rekisteröidyille (esim. tietopyynnöt)
  - Valvontaviranomaiselle (tietosuojavaltuutetun toimisto?)
- **Johdon antamien tehtävien hoitaminen**

Henkilötietojen käsittelijän vastuu

- Noudattaa **lakia** ja **tietosuoja-asetusta** sekä rekisterinpitäjän **ohjeita**
  - Ilmoittaa, mikäli rekisterinpitäjän ohjeistus on puutteellista, lainvastaista tms.
- Toteuttaa riittävät **suojatoimet** asianmukaisten teknisten ja organisatoristen toimien täytäntöön panemiseksi niin, että käsittely täyttää **lainsäädännön vaatimukset** ja sillä varmistetaan **rekisteröityjen oikeuksien** suojelu
- **Itsenäinen vastuu**, esim. vahingonkorvausvastuu

Henkilötietojen käsittely

- Mitä tietoja käsittelet?
- Miten ja missä käsittelet tietoja?
- Kenelle tietoja annat?
- TARKISTA!

Tietosuojaperiaatteet henkilötietojen käsittelyssä

- Käsittelyn **lainmukaisuus, kohtuullisuus ja läpinäkyvyys** (miten, miksi ja mihin)
- **Käyttötarkoitussidonnaisuus** (vain kerättyyn tarkoitukseen)
- Tietojen **minimointi** (vain tarpeellinen tieto kerätään)
- Tietojen **täsmällisyys** (virheelliset tiedot korjataan/ poistetaan)
- Tietojen **säilytyksen rajoittaminen** (säilytetään vain niin kauan kuin tarpeellista)
- Tietojen **turvallisuus, eheys ja luottamuksellisuus**

Tietosuojaperiaatteet henkilötietojen käsittelyssä

- Käsittelyn **lainmukaisuus, kohtuullisuus ja läpinäkyvyys** (miten, miksi ja mihin)
- **Käyttötarkoitussidonnaisuus** (vain kerättyyn tarkoitukseen)
- Tietojen **minimointi** (vain tarpeellinen tieto kerätään)
- Tietojen **täsmällisyys** (virheelliset tiedot korjataan/ poistetaan)
- Tietojen **säilytyksen rajoittaminen** (säilytetään vain niin kauan kuin tarpeellista)
- Tietojen **turvallisuus, eheys ja luottamuksellisuus**

Henkilötietojen käsittely

Käsittelyn on aina perustuttava:

- lakiin
- rekisteröidyn suostumukseen
- sopimukseen
- elintärkeiden etujen suojaamiseen
- yleistä etua koskevaan tehtävään tai julkiseen valtaan TAI
- rekisterinpitäjän tai kolmannen osapuolen oikeutettuun etuun

Käytännön ohjeita henkilötietojen käsittelyyn

- Käytä vain työssäsi **välttämättömiä** tietoja
  - Korjaa (pyydä rekisterin pääkäyttäjää korjaamaan) virheelliset tiedot
- **Älä pidä** henkilötietoja yleisesti **nähtävillä**
  - Henkilötietoja sisältävät tiedot vain omaan käyttöön
  - > Huomioi salassapitovelvollisuus
  - > Huomioi tietojen säilytyspaikka ja -tapa

Käytännön ohjeita henkilötietojen käsittelyyn

- Käytä aina **suojattua tulosta**
- Säilytä manuaaliset henkilötietoja sisältävät paperit aina **lukkojen takana**

- Huolehdi, että tietokoneella olevat tiedostot ja tietojärjestelmät ovat **salasanan takana**
  - Varmista, että salasanat ovat vain sinun tiedossa
  - Varmista salasanan ”turvallisuus”
- **Lukitse tietokoneesi** aina kun poistut työpöytäsi äärestä

Käytännön ohjeita henkilötietojen käsittelyyn

- **Hävitä** henkilötietoja sisältävät paperit ja tiedostot **asianmukaisesti**
  - silppuri, tietoturvaroskis
  - varmuuskopion poistaminen
- Mikäli sinulla on henkilötietoja sisältäviä rekistereitä/listoja/excel-taulukoita yms, muista **tietosuojaselosteet**

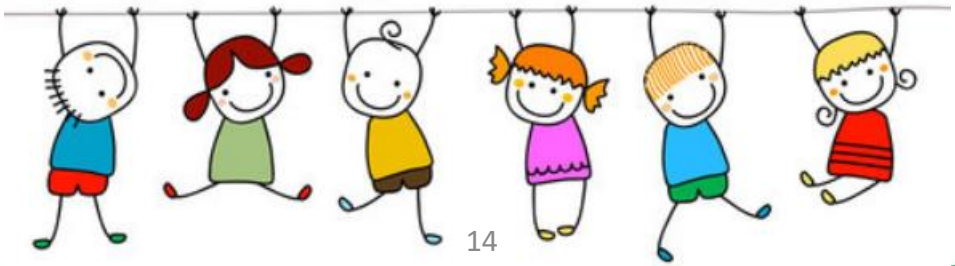
Käyttöoikeudet

- Käyttöoikeudet tietojärjestelmiin tullaan tarkistamaan
- Tietojärjestelmiin tarvittavat **käyttöoikeudet saadaan esimieheltä**

  - Oikeudet vain sellaisiin ohjelmiin/toimintoihin, joita **työsi vaatii**
  - Huomioi, että **käyttöoikeus ei anna lupaa käsitellä tietoja, joita et työssäsi tarvitse**
  - Pidä käyttäjätunnus ja salasana vain **omana tietonasi**

Erityiset henkilötiedot

- Erityisten (arkaluonteisten) henkilötietojen käsittely saattaa aiheuttaa huomattavia **riskejä henkilön perusoikeuksille ja –vapauksille** (-> syrjiminen)
- Erityisiä henkilötietoja ovat mm. rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen vakaumus, ammattiliiton jäsenyys, terveyttä koskevat tiedot ja seksuaalinen suuntautuminen
- **Erityisiä henkilötietoja voi käsitellä, jos** käsittely perustuu esim.
  - **Lakiin** (esim. erityislainsäädäntö)
  - Henkilön antamaan nimenomaiseen **suostumukseen** kyseisten henkilötietojen käsittelystä
  - Elintärkeiden etujen **suojaamiseen**
  - Tietyissä tapauksissa **yhteisön laillisen toiminnan** yhteydessä
  - Henkilö on nimenomaisesti **saattanut julkiseksi** kyseisen henkilötiedon (esim. somessa)
  - **Oikeusvaateen** laatimiseen, esittämiseen tai puolustamiseen
- HUOM! Tietosuoja-asetus antaa **erityistä suojaa lasten henkilötiedoille**. Se poikkeaa siten henkilötietolain määräyksistä. Lapsen henkilötietoja saa käsitellä vain huoltajan suostumuksella (kansallisen tietosuojalain *ehdotuksessa* Suomessa ikärajana olisi 13 v.).



Rekisterinpitäjän velvollisuudet

- **Osoitusvelvollisuus**
- Toteuttaa **tekniset ja organisatoriset toimenpiteet**, joilla varmistetaan ja osoitetaan tietosuoja-asetuksen noudattaminen
  - HUOM! Vastuuta ei voi ulkoistaa
- **Sisäänrakennettu** ja oletusarvoinen tietosuoja
  - Tietosuoja huomioidaan jo suunnitteluvaiheessa
  - Tietoja käsitellään tietoturvallisesti
- **Ilmoitusvelvollisuus**

Osoitusvelvollisuus – Joutsan kunta

- Tietosuojatyöryhmä
  - Tietosuojavastaava Liisa Alfthan
  - Tietoturvavastaava Jarkko Puhakka
  - Perusturvan tietosuojan vastuuhenkilö Anna-Maija Kääriäinen
  - Johtoryhmän edustaja talous- ja hallintojohtaja Antti-Pekka Hokkanen
- Tietosuojaselosteet, seloste käsittelytoimista
- Tietotilinpäätös
- Tarkastuspyyntö- ja korjaamisvaatimuslomakkeet
- Tietoturvapoikkeaman käsittely –prosessi
- Sopimukset yhteisrekistereistä
- Koulutukset ja tiedotteet henkilöstölle ja luottamushenkilöille
- Tietoturvapolitiikka, tietoturvauhkan riskianalyysi…

Huomioitavaa

- **Sanktiot, sakot, seuraamukset**
  - Varoitus, huomautus, määräykset, rajoitukset
  - Hallinnollinen sakko voidaan määrätä rekisterinpitäjälle ja/tai henkilötietojen käsittelijälle (max. 20 milj euroa tai 4 % liikevaihdosta) -> ei julkishallinnolle (?)
  - Rikosoikeudelliset seuraamukset
  - Vahingonkorvaus (lakiperusteinen, sopimusperusteinen)
  - Huomioi erityislait
- Kansallinen **tietosuojalaki** tulossa (syksy 2018?)
  - Kansallisella lainsäädännöllä voidaan ainoastaan täydentää ja joiltain osin täsmentää yleistä tietosuoja-asetusta
  - Korvaa nykyisen henkilötietolain
- **Tiedonhallintalaki** tulossa (2019?)
  - Henkilötietojen suoja vs. asiakirjojen julkisuus
  - Korvaa nykyisen arkistolain
- **Erityislainsäädäntö**
  - Laki viranomaisen toiminnan julkisuudesta

Rekisteröidyn oikeudet

- Saada tietoa henkilötietojen **käsittelystä**
- **Pääsy** omiin tietoihin
- Omien tietojen **oikaiseminen** (virheellisten korjaaminen, puuttuvien lisääminen)
- Tietojen **poistaminen** (oikeus tulla unohdetuksi)
- **Rajoittaa** tietojen käsittelyä
- **Siirtää** tiedot järjestelmästä toiseen
- **Vastustaa** tietojen käsittelyä
- Olla joutumatta **automaattisen päätöksenteon** kohteeksi

Tietojen tarkastus, oikaiseminen tai poistaminen

Kuntalainen (rekisteröity) pyytää tietojaan

Lomakkeen täyttäminen ja palautus asiointipisteelle tietosuojavastaavalle

Lomakkeita saa asiointipisteeltä ja kunnan verkkosivuilta

Tietosuojavastaava kirjaa kaikki tietopyynnöt, käsittelyn kulun ja niihin annetut vastaukset

Tietosuojavastaava laittaa pyynnön rekisterin pääkäyttäjälle

Jos tietoja ei voida lain mukaan antaa annetaan siitä kuntalaiselle kirjallinen selvitys

Rekisterin käyttäjä toimittaa pyydetyt tiedot tietosuojavastaavalle

Tietosuojavastaava toimittaa kuntalaiselle pyydetyt tiedot

Tietoturvaloukkaus

- Henkilötietojen tietoturvaloukkauksella tarkoitetaan sellaista tapahtumaa, jonka seurauksena siirrettyjä, tallennettuja tai muuten käsiteltyjä **henkilötietoja** vahingossa tai lainvastaisesti **tuhoutuu, häviää tai muuttuu**. Tietoturvaloukkaukseksi katsotaan myös **tietojen luvaton luovuttaminen** sekä luvaton pääsy tietoihin. Tietoturvaloukkaus on esim.
    - hävinnyt USB-tikku
    - varastettu tietokone/älypuhelin/tabletti
    - henkilötietoja sisältävän paperin joutuminen esim. roskiin tai vääriin käsiin
- Tietoturvaloukkauksesta (epäilystä) on **välittömästi ilmoitettava** tietoturvavastaavalla ja/tai tietosuojavastaavalle
- Tietosuojatyöryhmä kirjaa kaikki tietoturvaloukkaukset (ja epäilyt) ja niihin liittyvät toimenpiteet
- Kunnan tulee antaa **viranomaisille tieto tietoturvaloukkauksesta 72 h kuluessa**
- Tietoturvaloukkaus ilmoituksesta tulee ilmetä seuraavat tiedot:
    - kuvattava henkilötietojen tietosuojapoikkeama, mahdollisuuksien mukaan myös asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä henkilötietotyyppien ryhmät ja arvioidut lukumäärät
    - ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa
    - kuvattava henkilötietojen tietosuojapoikkeaman todennäköiset seuraukset
    - kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi

”Tärpit”

- (Lähes) jokainen meistä käsittelee työssään henkilötietoja – mitä tietoja sinä käsittelet?
- Mitä, miten ja missä?
- Tarkista ja varmista

Lisätietoa

- www.tietosuoja.fi

- www.arjentietosuoja.fi (videoita)
- www.yrittajat.fi -> yrittäjän tietosuojaopas

- **Joutsan kunta**
  - tietosuojavastaava Liisa Alfthan (Länsitie 5, asiointipiste)
    - puh. 040 358 0002
    - liisa.alfthan@joutsa.fi
  - Tietoturvavastaava Jarkko Puhakka (Länsitie 7)
    - puh. 040 640 2008
    - Jarkko.puhakka@joutsa.fi