Ruokolahden kunta

Tietosuojaohje

KH 5.11.2018 / § 262

Sisällysluettelo

1 Johdanto

Kunnallisten palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn. Tieto voi olla salassa pidettävää tai julkista. Lisäksi teknologian kehittyminen on lisännyt henkilötietojen käsittelyä, jolloin tietosuoja ja tietoturva ovat kasvattaneet merkitystään ja tulleet pysyväksi osaksi hyvää hallintotapaa. Puutteellinen tietoturvallisuus voi vaarantaa kunnan ja sen asiakkaiden etuja sekä aiheuttaa lisätyötä ja -kustannuksia. Organisaation menettämä luottamus ja maine on vaikea palauttaa.

Kuntien toimintaan vaikuttavat julkisuus- ja henkilötietolainsäädäntö, jotka säätelevät toiminnan avoimuutta. Julkisuuslaki koskee lähinnä asiakirjatietoja ja niiden käsittelyä, henkilötietolaki henkilötietojen ja -rekistereiden käsittelyä. Vuonna 2018 toukokuusta sovellettava EU:n tietosuoja-asetus (General Data Protection Regulation, GDPR 679/2016) korvaa nykyisen henkilötietolain siltä osin, kun henkilötietolaki on ristiriidassa tietosuoja-asetuksen kanssa. Uusi kansallinen tietosuojalaki ei ole vielä voimassa. Se tulee korvaamaan henkilötietolain.

Lainsäädäntöuudistusten tavoitteena on varmistaa, että ihmisten oikeus henkilötietojen suojaan ja sitä kautta yksityisyyteen toteutuu myös digitaaliaikana. Sääntely pyrkii vastaamaan teknologian nopean kehityksen haasteisiin ja vahvistamaan ihmisten oikeutta valvoa henkilötietojaan. Tietosuoja-asetus tuo sekä rekisterinpitäjille että henkilötietojen käsittelijöille uusia tehtäviä ja velvollisuuksia. Uutena asiana rekisterinpitäjälle on tullut osoitusvelvollisuus. Kun vanhan henkilötietolain aikana riitti, että säännöksiä noudatetaan, niin nyt rekisterinpitäjän on pystyttävä osoittamaan, että asetuksen tietosuojaperiaatteita ja vaatimuksia on noudatettu. Tämä tarkoittaa mm. henkilötietojen käsittelytoimien tarkempaa dokumentointia. Asetus pitää myös sisällään uusia oikeuksia rekisteröidyille.

Tämä asiakirja koskee koko kuntaorganisaatiota ja sen henkilöstöä mukaan lukien kuntakonserni sekä niitä kunnan sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Ruokolahden kunnan omistamaa tai hallinnoimaa tietoa.

2 Käsitteet

2.1 Henkilörekisteri

Henkilörekisteri on mikä tahansa jäsenneltyä henkilötietoa sisältävä tietojoukko, josta tiedot on saatavilla tietyin perustein. Henkilörekisteri sisältää samaa käyttötarkoitusta varten henkilötietoja. Tietomassa voi olla keskitetty, hajautettu tai jaettu eri perustein. Esimerkiksi jäsenrekisteri ja käyttäjärekisteri ovat henkilörekistereitä.

2.2 Henkilötieto

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tavanomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Henkilötieto voi määritelmään mukaan olla esim. paikkatieto, joka kertoo jotakin tietystä henkilöstä, esimerkiksi kuva yhdistettynä osoitetietoihin, tai IP-osoite, jos tämä voidaan liittää tiettyyn käyttäjään, tai käyttäjätunnus.

2.3 Henkilötiedon käsittelijä

Henkilötietojen käsittelijä on se henkilö, viranomainen, virasto tai muu taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

2.4 Henkilötiedon käsittely

Henkilötiedon käsittelyllä tarkoitetaan toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietojen kokoelmiin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, esim. tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen.

2.5 Rekisterinpitäjä

Rekisterinpitäjä on se taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjä on siis se henkilö tai organisaatio, jonka käyttöä varten rekisteri perustetaan ja jolla on oikeus määrätä rekisterin käytöstä.

2.6 Tietosuoja

Tietosuojalla tarkoitetaan kansalaisten yksityisyyden suojaamista sekä oikeuksien, etujen, vapauksien ja oikeusturvan turvaamista henkilötietoja käsiteltäessä.

2.7 Tietosuojavastaava

Henkilö, jonka tehtävänä on mm. seurata henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet. Asema on itsenäinen ja riippumaton. Vastaava raportoi suoraan rekisterinpitäjän ylimmälle johdolle, joka on päävastuussa henkilötietojen käsittelyn lainmukaisuudesta.

2.8 Tietoturva

Tietoturvalla tarkoitetaan niitä teknisiä ja hallinnollisia toimenpiteitä, joilla pyritään tietosuojan toteuttamiseen.

3 Tietosuojapolitiikka

3.1 Tietosuojan tavoitteet

Yksityisyydensuoja ja henkilötietojen suoja on jokaisen perusoikeus. Ruokolahden kunnan tavoitteena on edistää hyvää tietojenkäsittelytapaa sekä varmistaa tietojenkäsittelyn turvallisuus sekä tehtävien sujuva ja häiriötön toiminta kunnassa. Tietoja käsitellään niin, että kaikki osapuolet voivat luottaa käsittelyn asianmukaisuuteen.

Ruokolahden kunta määrittää tarvittavat suojatoimet ottamalla huomioon mm. käytettävissä olevan tekniikan, toteuttamiskustannukset, käsittelyn luonteen ja laajuuden, asiayhteyden ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvan riskin.

Hyvän tietosuojan tason saavuttamiseksi jokaisen tietoa käsittelevän henkilön tulee ymmärtää tietojen käsittelyn periaatteet:

- mitä tietoa saa käsitellä,
- missä tarkoituksessa ja milloin tietoa saa käsitellä sekä
- mitkä ovat rekisteröidyn oikeudet.

3.2 Organisaatio ja vastuut

Henkilötietojen käsittelyn lainmukaisuudesta vastaa ensisijaisesti Ruokolahden kunnanhallitus sekä lautakunnat. Vastuu ei riipu siitä, onko joitakin organisaation toimintoja ulkoistettu vai ei. Johdolla on vastuu huolehtia mm. tietoturvatyön riittävästä resursoinnista ja siitä, että tietosuoja otetaan huomioon suunnitelmissa.

Kunkin tulosalueen esimies vastaa omalla tulosalueellaan tietosuojan lainmukaisuudesta. Lisäksi yksiköiden esimiehet valvovat tietosuojan toteutumista omissa yksiköissään. Jokaisen esimiehen tulee huolehtia, että tietosuoja- ja tietoturvaohjeet sekä tietoverkon käyttösäännöt perehdytetään henkilöstölle.

Tietosuojavastaava toimii tietosuoja-asioissa asiantuntijana ja yhteyshenkilönä. Tietosuojavastaavan tehtävänä on auttaa rekisterinpitäjää saavuttamaan hyvän henkilötietojen käsittelytavan ja tietosuojan taso.

TVT-päällikkö vastaa yhdessä yhteistyötahojen kanssa teknisen tietoturvan kehittämisestä, tietojärjestelmien toiminnasta, hoidosta ja turvallisuudesta saamiensa resurssien ja toimintavaltuuksien puitteissa.

Jokaisella, joka käsittelee Ruokolahden kunnan omistamaa tietoa, on omalta osaltaan henkilökohtainen vastuu kokonaisturvallisuudesta. Jokainen tietoja ja tietojärjestelmiä käyttävä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista ohjeistetulla tavalla.

3.3 Tietosuojan toteuttaminen

Hyvän tietosuojan tason toteuttaminen vaatii organisaation kaikille tasoilla ulottuvia jatkuvia toimia, jolloin taataan organisaation häiriötön toiminta sekä normaali- että poikkeusoloissa. Toteuttaminen tapahtuu erilaisten hallinnollisten ja teknisten toimenpiteiden avulla. Tietosuoja tulee huomioida kaikessa toiminnassa niin manuaalisessa kuin sähköisessä henkilötietojen käsittelyssä sekä puhutussa ja kirjoitetussa tiedossa.

Henkilötietojen käsittelyssä noudatetaan seuraavia tietosuoja-asetuksessa annettuja tietosuojaperiaatteita:

- Henkilötietoja käsitellään lainmukaisesti, kohtuullisesti sekä rekisteröidyn kannalta läpinäkyvästi. Rekisteröidylle tulee olla läpinäkyvää, miten heitä koskeva tietoja kerätään ja käytetään sekä missä määrin henkilötietoja käsitellään tai aiotaan käsitellä.
- Henkilötietojen kerääminen tulee olla sidoksissa käyttötarkoitukseen ja tietojen kerääminen tulee tapahtua tiettyä, nimenomaista ja laillista tarkoitusta varten. Kerättyä tietoa ei saa käyttää myöhemmin sellaiseen käyttötarkoitukseen, johon sillä ei ole sidonnaisuutta.
- Henkilötietojen kerääminen tulee rajata ja minimoida tarpeelliseen tietoon suhteessa keräämisen tarkoitukseen ja henkilötietojen on oltava asianmukaisia sekä olennaisia.
- Henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä sekä rekisterinpitäjän on kohtuullisen toimenpitein varmistettava, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.
- Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin se on tarpeen tietojen käsittelyä varten. Tietoja voidaan säilyttää kauemmin, mikäli tietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia varten tai tietoja käytetään historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten.
- Henkilötietojen käsittelyssä on varmistettava tietojen asianmukainen turvallisuus ja siten tietojen eheys ja luottamuksellisuus. Tietoja tulee suojata luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Suojaamiseen on käytettävä asianmukaisia teknisiä tai organisatorisia toimia.

3.4 Lait ja asetukset

Ruokolahden kunnan tietosuojan ja tietoturvan käytänteet noudattavat voimassa olevia säädöksiä, määräyksiä, ohjeita ja suosituksia. Tietoturvaratkaisujen tulee noudattaa myös taloudellisia realiteetteja, eivätkä ne saa vaikeuttaa merkittävästi tietojärjestelmien hyötykäyttöä ja asiakaspalvelua. Organisaatiossa tehdyt omat päätökset, määräykset ja ohjeet eivät saa olla ristiriidassa Ruokolahden kunnan tietosuojapolitiikan kanssa.

Tietosuojaan liittyvä keskeinen lainsäädäntö:

- EU:n yleinen tietosuoja-asetus (679/2016)
- Suomen perustuslaki (731/1999)
- Laki viranomaisten toiminnan julkisuudesta (621/1999)
- Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
- Laki kunnallisesta viranhaltijasta (304/2003)
- Työsopimuslaki (55/2001)
- Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä, VAHTI 7/2009, Valtionvarainministeriö.
- Arkistolaki (831/1994): Asiakirjojen laatiminen, säilyttäminen ja käyttö
- Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
- Laki sähköisen viestinnän palveluista 917/2014.
- Rikoslaki (39/1889)
- Vahingonkorvauslaki (412/1974)

Lisäksi

- Hallituksen esitys eduskunnalle laeiksi Euroopan unionin verkko- ja tietoturvadirektiivin täytäntöönpanoon liittyvien lakien muuttamisesta, HE 192/2017 vp.
- Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (812/2000)
- Laki potilaan asemasta ja oikeuksista (785/1992)
- Laki terveydenhuollon ammattihenkilöistä (559/1994)

3.5 Rikkomukset ja seuraamukset

Jokainen Ruokolahden kunnan tietojärjestelmien käyttäjä on velvollinen noudattamaan Ruokolahden kunnan tietosuojapolitiikkaa, tietoverkon käyttösääntöjä sekä tietosuoja- ja tietoturvaohjeita. Tietojen käsittelijä on vastuussa mahdollisesta vahingosta, jos hän ei ole noudattanut tietosuoja-asetuksessa käsittelijälle nimenomaisesti asetettuja velvoitteita tai rekisterinpitäjän lainmukaista ohjeistusta. Havaitut rikkomukset raportoidaan johdolle ja tietosuojavastaavalle. Rikkomuksen tekijä saatetaan edesvastuuseen ja häntä vastaan ryhdytään rikkomuksen luonteen vaatimiin toimenpiteisiin. Vakaviin tietosuojarikkomuksiin liittyvä sisäinen ja julkinen tiedottaminen hoidetaan tapauskohtaisesti johdon tai johdon valtuuttaman henkilön toimesta.

4 Tietosuoja – tietojen käsitteleminen

4.1 Henkilötietojen käsittely

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja eli ei pelkästään nimeä ja henkilötunnusta vaan myös henkilön ominaisuuksia, ruokavaliota tai harrastuksia.

Henkilötietoja käsiteltäessä tulee toteuttaa kansalaisten yksityiselämän suojaa ja muita perusoikeuksia sekä edistää hyvää tiedonhallintatapaa. Tietoturvanäkökulmasta merkittäviä käsittelyvaiheita ovat tiedon luominen, käyttäminen, muuttaminen, tallettaminen, säilyttäminen, siirtäminen, jakelu, kopioiminen, arkistointi ja hävittäminen eli kaikki henkilötietoihin liittyvät aktiiviset ja passiiviset toimenpiteet.

4.1.1 Henkilötietojen kerääminen

Henkilötietojen käsittely alkaa niiden keräämisestä. Henkilötietoja saa kerätä ja käsitellä vain, jos jokin alla olevista perusteista täyttyy. Henkilötietoja ei saa kerätä ilman perustetta ja sitä varten, että tietoja voidaan joskus tarvita.

- Rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten.
- Käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä.
- Käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi.
- Käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi.
- Käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi.
- Käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.

Iso osa kunnan tietojen keräämisestä perustuu lakisääteisten velvoitteiden hoitamiseen. Jos käsittely ei perustu lakisääteisen velvoitteen hoitamiseen ja rekisteröitävältä kysytään suostumus henkilötietojen käsittelyyn, rekisteröitävälle on tiedotettava suostumuksen merkityksestä ennen suostumuksen antamista. Suostumus on pätevä vain, kun se on vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, joka on selkeästi ymmärrettävissä. Suostumus kysytään kirjallisena (suostumuslomakkeella), jolloin pystytään myöhemmin osoittamaan, kuka on suostumuksen antanut, kenelle suostumus on annettu ja mihin tarkoitukseen suostumus on annettu. Jos henkilötietojen käyttötarkoitus muuttuu, tulee pyytää uusi suostumus.

4.1.2 Arkaluonteinen henkilötieto eli erityisiin henkilötietoryhmiin kuuluva tieto

Erityisiä henkilötietoryhmiä koskevia tietoja eli arkaluonteisia henkilötietoja ei saa lähtökohtaisesti lainkaan käsitellä. Näitä tietoja ovat muun muassa rotu tai etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys. Lisäksi geneettisiä tai biometrisiä tietoja, joista henkilö voidaan yksiselitteisesti tunnistaa, terveyttä koskevia tietoja tai luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevia tietoja ei lähtökohtaisesti saa käsitellä.

Erityisiä henkilötietoryhmiä koskevia tietoja käsitellään

a) suostumuksen perusteella,

b) henkilön elintärkeiden etujen suojaamiseksi tai

c) jos käsittely on tarpeen yleistä etua koskevasta syystä lainsäädännön nojalla.

Alle 16-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman suostumusta. (Kansallisessa lainsäädännössä eli tulevassa tietosuojalaissa on vielä mahdollisuus soveltaa alempaa ikärajaa, joka voi alimmillaan olla 13 vuotta.)

4.1.3 Henkilörekisteri ja henkilötietojen elinkaari

Henkilötiedoista syntynyt henkilörekisteri on mikä tahansa henkilötietoluettelo, joka voi olla niin paperilla, taulukkolaskentaohjelmassa, tekstitiedostossa, tietojärjestelmässä, sähköpostissa tai arkistossa. Kunnan ja sen henkilöstön tulee tietää, mitä henkilörekistereitä heidän käytössään on, sillä tietosuoja-asetus määrää, että kaikki tietovarannot tulee kartoittaa ja kuvata. Henkilörekisterit tulee kuvata tietosuojaselosteissa.

Henkilörekisteriin tulee tallentaa vain rekisterin käyttötarkoituksen ja muun hallintotoiminnan kannalta tarpeellisia tietoja. Henkilötietoja saa käyttää ainoastaan siihen tarkoitukseen, mihin ne on kerätty. Tiedot tai koko henkilörekisteri on hävitettävä, jos se ei ole tarpeellinen. Henkilötietoja ei saa säilyttää varmuuden vuoksi eli sitä varten, että niitä saatetaan joskus tarvita. Poikkeuksen muodostavat lakisääteiset rekisterit. Henkilötietojen säilyttämisen ja käytön aikarajat määritellään arkistonmuodostussuunnitelmassa.

Henkilötietojen käsittelijän tulee käyttää luotettavia tietolähteitä eikä henkilörekisteriin saa tallettaa tarpeettomia, puutteellisia tai vanhentuneita henkilötietoja. Tällaiset tiedot on poistettava rekisteristä.

4.1.4 Käyttöoikeudet, vaitiolo- ja salassapitovelvollisuus

Henkilötietoja saavat käsitellä vain ne henkilöt, joilla on siihen tehtäviensä vuoksi oikeus. Yksiköiden esimiehet päättävät, kenelle tietojärjestelmien käyttöoikeuksia annetaan. Käyttöoikeudet tulee rajata henkilön työtehtävien mukaisesti. Käyttöoikeuksia myönnettäessä ja muutettaessa tulee jäädä merkintä (loki tai dokumentti), jotta käyttöoikeuksia voidaan tarvittaessa selvittää myös jälkikäteen.

Henkilötietoja käsittelevät kunnan palveluksessa olevat henkilöt tai ulkopuoliset työn suorittajat eivät saa ilmaista sivullisille tietoja toisen henkilön ominaisuuksista, henkilökohtaisista oloista tai taloudellisesta asemasta, joita he ovat saaneet tietoonsa henkilötietojen käsittelyyn liittyviä toimenpiteitä suorittaessaan tai muutoin.

Henkilötietoja käsittelevät henkilöt velvoitetaan vaitiolovelvollisuuteen työ- tai muilla sopimuksilla ja velvoituksen on oltava voimassa työ-, sopimus- tai toimeksiantosuhteen päätyttyäkin. Henkilötietojen oikeudeton käsittely on rangaistava teko.

4.1.5 Käsittelyn ohjeita

- Selvitä itsellesi tietojen ja asiakirjojen luokittelu ja siihen liittyvät käyttöä, luovutusta ja käsittelyä koskevat säännöt ja rajoitukset.
- Mikäli laadit salassa pidettävää asiakirjaa, vastaat tehtäviesi mukaisesti myös sen luokittelusta ja merkinnästä. Osa salassa pidettävästä aineistosta kuuluu turvaluokittelun piiriin.
- Käsittele tietoja huolellisesti käsittely- tai tallennusvälineestä riippumatta.
- Muista, että voit käyttää ja käsitellä käyttöösi saamiasi salassa pidettäviä ja arkaluonteisia tietoja vain työtehtäviesi hoitamisessa. Esimerkiksi henkilörekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista. Huomioi myös, että tietojärjestelmien käyttöä valvotaan.
- Varo antamasta viattomankin oloisten keskustelujen ja lomakkeiden yhteydessä tietoa salassa pidettävistä ja yksityisyyden suojan piiriin kuuluvista tiedoista.
- Kaikki ovat vaitiolovelvollisia toisten viesteistä, jotka on työtehtävissään vahingossa saanut tietoonsa.
- Tukahduta juorut.

4.2 Rekisteröidyn oikeudet

Rekisteröidyllä on oikeus pyytää hänen henkilötietojensa käsittelyä koskevat tiedot. Tiedot on pystyttävä esittämään mahdollisimman helposti ymmärrettävässä ja tiiviissä muodossa. Näitä tietoja ovat ainakin tieto-

suojaselosteet, tarkastusoikeuden kohteena olevat tiedot, tiedot henkilötietojen korjaamisesta, poistamisesta, rajoittamisesta, siirrosta, tiedot käsittelyn tai profiloinnin vastustamisesta ja ilmoitukset tietoturvaloukkauksista.

4.2.1 Tietosuojaseloste

Henkilörekistereistä tulee olla laadittuna tietosuojaseloste tai vastaava, joka kertoo mm. mitä henkilötietoja rekisteri sisältää, mitkä ovat käsittelyn tarkoitukset, mistä tiedot on saatu ja minne tietoja luovutetaan. Tietosuojaselostetta käytetään kansalaisten perusoikeuksien, yleisen tiedonsaantioikeuden toteuttamiseksi ja rekisteröidyn informoimiseksi.

Ennen henkilötietojen keräämistä rekisteröitävälle on ilmoitettava tietosuojaselosteessa seuraavat tiedot:

1) rekisterinpitäjän ja

2) tietosuojavastaavan yhteystiedot,

3) rekisterin yhteyshenkilö,

4) rekisterin nimi,

5) henkilötietojen käsittelyn tarkoitus ja oikeusperusta,

6) rekisterin tietosisältö,

7) säännönmukaiset tietolähteet,

8) säännönmukaiset tietojen luovutukset,

9) tietojen siirto EU:n ulkopuolelle,

10) rekisterin suojauksen periaatteet,

11) henkilötietojen säilytysaika tai säilytysajan määräytymisperusteet,

12) rekisteröidyn oikeudet ja miten rekisteröidyt voivat niitä käyttää,

13) oikeus peruuttaa suostumus milloin tahansa,

14) oikeus tehdä valitus valvontaviranomaiselle.

Tietosuojaseloste on pidettävä jokaisen nähtävänä asianosaisessa toimintayksikössä. Seloste on pidettävä jatkuvasti ajan tasalla. Tietosuojaselosteen jäljennös toimitetaan kunnan tietosuojavastaavalle, joka ylläpitää luetteloa Ruokolahden kunnan henkilötietoja sisältävistä rekistereistä.

4.2.2 Rekisteröidyn oikeus saada tietoja

Rekisteröidyllä on kohtuullisin väliajoin oikeus saada pääsy henkilötietoihin, joita hänestä on kerätty sekä tietoihin hänen henkilötietojen käsittelyyn liittyen. Kaikilla rekisteröidyillä on siis oikeus tietää ja saada ilmoitus erityisesti henkilötietojen käsittelyn tarkoituksista, käsittelyajasta, henkilötietojen vastaanottajista, käsiteltävien henkilötietojen automaattisen käsittelyn logiikasta sekä kyseisen käsittelyn mahdollisista seurauksista. Lisäksi rekisteröidyillä on oikeus saada tietoa omista oikeuksistaan suhteessa rekisterinpitäjään. Tietopyyntöjä tehdään lomakkeilla, joita voi pyytää mm. kunnan tietosuojavastaavalta.

Rekisteröidylle on annettava tiedot ilman aiheetonta viivytystä ja viimeistään yhden kuukauden (1 kk) kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan tietyin edellytyksin jatkaa. Tietoja antaessa on huomioitava, että jos tietopyyntö koskee lisäksi myös viranomaisen asiakirjaa, tulee noudatettavaksi julkisuuslain mukaiset lyhyemmät määräajat (14 pv).

Rekisteröidyn pyynnön perusteella toimitetut tiedot ja rekisterinpitäjän toimet rekisteröidyn oikeuksien toteuttamiseksi ovat pääsääntöisesti maksuttomia. Pyydetyt tiedot pitää ensisijaisesti luovuttaa sähköisessä muodossa. Ennen tietojen luovuttamista, rekisteröidyn henkilöllisyys tulee pystyä varmistamaan.

4.2.3 Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot. Ottaen huomioon tarkoitukset, joissa tietoja käsiteltiin, rekisteröidyllä on oikeus saada puutteelliset henkilötiedot täydennettyä, esim. toimittamalla rekisterinpitäjälle lisäselvitystä.

Rekisteröidyllä on myös oikeus vaatia, että rekisterinpitäjä poistaa rekisteröityä koskevat henkilötiedot, kun tietoja ei enää tarvita. On huomioitava, että tämä oikeus ei koske lakisääteistä rekisteriä. Tietojen poistaminen niistä ei ole mahdollista lakisääteisten tehtävien suorittamiseen liittyvän käsittelyn yhteydessä.

4.2.4 Oikeus käsittelyn rajoittamiseen ja vastustamisoikeus

Rekisteröidyllä on oikeus pyytää henkilötietojensa rajoittamista muun muassa, kun henkilötiedot eivät pidä enää paikkaansa tai henkilötietojen käsittely rikkoo lainsäädäntöä. Käsittelyn rajoittaminen tarkoittaa esim. tietojen siirtämistä toiseen käsittelyjärjestelmään tai käyttäjien pääsyn estämistä valittuihin henkilötietoihin.

Rekisteröidyllä on oikeus vastustaa käsittelyä suoramarkkinointitarkoituksissa ja eräissä muissa tietosuojaasetuksessa mainituissa tilanteissa, jolloin hänen henkilötietojaan ei saa enää käsitellä ko. tarkoituksissa. Vastustusoikeus ei koske lakisääteisiä rekistereitä.

4.2.5 Oikeus siirtää tiedot järjestelmästä toiseen

Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot yleisesti käytössä olevassa siirtomuodossa (esim. muistitikulla) ja hänellä on oikeus toimittaa tiedot toiselle rekisterinpitäjälle. Eri rekisterinpitäjien järjestelmät eivät tarvitse olla yhteensopivia. Siirto-oikeutta sovelletaan kunnassa niihin rekistereihin, jotka on kerätty vapaaehtoisten tehtävien hoitamiseen. Siirto-oikeutta ei ole, kun kyse on yleistä etua koskevan tehtävän suorittamisesta tai julkisen vallan käyttämisestä.

4.2.6 Tietoturvaloukkauksesta ilmoittaminen

Henkilötietojen tietoturvaloukkauksen sattuessa Ruokolahden kunnalla on velvollisuus ilmoittaa tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle. Tietoturvaloukkauksella tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin.

Henkilötietojen käsittelijän on ilmoitettava tietoturvaloukkauksista kunnan tietosuojavastaavalle ilman aiheetonta viivytystä loukkauksen tietoonsa saatuaan. Loukkausta koskeva ilmoitus tehdään valvontaviranomaiselle (tietosuojavaltuutetulle) mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta, riippumatta siitä, onko loukkaus tapahtunut omassa vai ulkopuolisen käsittelijän toiminnassa.

Rekisteröidylle henkilötietojen tietoturvaloukkauksesta ilmoitetaan ilman aiheetonta viivytystä. Rekisteröidylle suunnattavassa ilmoituksessa tulee kertoa vähintään seuraavassa listatut kohdat.

- Tietosuojavastaavan nimi ja yhteystiedot tai muu yhteystieto, josta rekisteröidyt voivat halutessaan kysyä lisätietoja.

- Selkeä ja yksinkertainen kuvaus tapahtuneesta.
- Tiedot siitä, millaisia vaikutuksia henkilötietojen tietoturvaloukkauksella voi todennäköisesti olla rekisteröidylle.
- Kuvaus niistä toimenpiteistä, joita rekisterinpitäjä aikoo toteuttaa tai jotka se on jo toteuttanut haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi riittävän yleisellä tasolla.

Ilmoitusta ei kuitenkaan tarvitse tehdä, jos tietoturvaloukkauksesta ei todennäköisesti aiheudu riskiä rekisteröidyn oikeuksille.

Ilmoita myös mahdollisesta vakavasta lähellä-piti -tilanteesta tietosuojavastaavalle, jolloin tiedot voidaan tilastoida ja tietoturvaa voidaan kehittää.

4.3 Sopimusvaatimukset, kun henkilötietojen käsittelyä ulkoistetaan

Toimeksiantosuhteissa annettaessa palveluita ulkopuolisen hoidettaviksi, laaditaan toimeksiannosta kirjallinen sopimus. Sopimuksessa vahvistetaan mm. käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät ja rekisterinpitäjän velvollisuudet ja oikeudet. Toimeksiantotehtävää suorittavaa koskevat huolellisuusvelvoite, kielto käyttää saatuja tietoja ulkopuolisiin tarkoituksiin ja velvollisuus suojata saadut tiedot.

Kuntaliitto, Hansel, KL-Kuntahankinnat Oy ja Julkisten hankintojen neuvontayksikkö ovat tehneet ohjeen ”Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja”. Ohjeessa on myös valmiita lausekkeita sopimusehtoihin.

4.4 Seuraamukset ja hallinnolliset sanktiot

Tietosuoja-asetuksen mukaan henkilöllä, jolle on aiheutunut tietosuoja-asetuksen rikkomisen vuoksi vahinkoa, on oikeus saada täysi korvaus vahingosta joko rekisterinpitäjältä tai henkilötietojen käsittelijältä. Rekisterinpitäjällä on lähtökohtaisesti päävastuu ja henkilötietojen käsittelijän vastuu toissijaista. Käsittelijä on vastuussa vahingosta vain, jos se ei ole noudattanut tietosuoja-asetuksessa käsittelijälle nimenomaisesti asetettuja velvoitteita tai jos se ei ole noudattanut rekisterinpitäjän ohjeistusta.

Lisäksi mikäli henkilötietoja ei käsitellä lainmukaisesti ja tietosuoja-asetusta rikotaan, rekisterinpitäjä voi saada huomautuksen, varoituksen, henkilötietojen käsittelykiellon tai muun sanktion.

Hallinnollisen sanktion määräämisestä päättää tietosuoja-asetuksen nojalla perustettu valvontaviranomainen.

4.4 Tietosuojavastaavan tehtävä

Tietosuojavastaava antaa tietoja ja neuvoja rekisterinpitäjälle ja työntekijöille henkilötietojen käsittelyyn liittyen. Hän seuraa asetuksen noudattamista omassa organisaatiossaan ja hänen vastuulleen kuuluu myös tietosuoja-asioiden kouluttaminen henkilöstölle. Tietosuojavastaava neuvoo vaikutustenarviointeihin liittyen ja toimii yhteyshenkilönä valvontaviranomaiseen päin.

Jokaisen viranomaisen ja julkishallinnon elimen, joka ei ole tuomioistuin, on nimitettävä tietosuojavastaava. Tietosuojavastaava voi olla organisaation henkilöstön jäsen tai hoitaa tehtäviään palvelusopimuksen perusteella. Konserni, samoin kuin useampi viranomainen tai julkishallinnon elin, voi nimittää yhteisen tietosuojavastaavan. Tietosuojavastaava voi tehtävänsä ohella suorittaa muita tehtäviä, mutta nämä tehtävät eivät saa aiheuttaa intressiristiriitoja.

Tietosuojavastaava on otettava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn. Hänelle on asetuksen mukaan annettava riittävät resurssit sekä pääsyn

henkilötietoihin ja käsittelytoimeen. Hänellä on myös oikeus asetuksen perusteella resursseihin asiantuntemuksen ylläpitämiseksi.

Rekisterinpitäjä tai henkilötietojen käsittelijä ei saa erottaa tai rangaista tietosuojavastaavaa sen vuoksi, että hän on hoitanut tehtäviään tietosuojavastaavana.

5 Tietoturva

5.1 Mitä tietoturva tarkoittaa

Tietoturvalla tarkoitetaan niitä käytännön toimenpiteitä, joilla pyritään tietosuojan toteuttamiseen. Tietoturvatoimilla estetään tietojen luvaton käyttö ja haltuunotto. Tietoturvajärjestelyillä varmistetaan, että poikkeuksellisissakin olosuhteissa tietoaineistojen, tietojärjestelmien ja palveluiden saatavuus, eheys ja luottamuksellisuus säilyvät. Tiedot eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan, haittaohjelmien, laitteisto- tai ohjelmistovikojen tai muidenkaan vahinkojen ja tapahtumien seurauksena. Tietojen, järjestelmien ja palveluiden on myös pysyttävä toiminnassa ja oltava saatavilla silloin, kun niitä tarvitaan.

Sähköpostin ja verkon kautta leviävät haittaohjelmat eli virukset ovat vakava uhka tietoturvallisuudelle, koska ne voivat tuhota, varastaa ja välittää tiedostoja, tunnuksia ja salasanoja sekä hidastaa tietoverkon toimintaa. Kuitenkin myös jokapäiväiset toimintatapamme ja asenteemme vaikuttavat tietoturvallisuuteen. Suurimmat tietoturvallisuuden ongelmat liittyvätkin yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen ja muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin.

Jokaisen työntekijän tulee omalla toiminnallaan varmistaa, ettei kukaan ulkopuolinen pääse tietoihin käsiksi.

5.2 Käyttöoikeudet

- Käyttöoikeuksia myöntäessä tulee siitä jäädä jälki (lokitieto tai dokumentti), milloin ja millä perusteella käyttäjälle on myönnetty käyttöoikeus ja kuka sen on myöntänyt.
- Myös käyttöoikeuksia muuttaessa tulee jäädä jälki, milloin ja millä perusteella käyttöoikeuksia on muutettu ja kuka muutokset on tehnyt.
- Käyttöoikeudet ja avaimet tulee antaa vain niitä tarvitseville ja ne tulee poistaa, kun niitä ei tarvita.

5.3 Salasanat

- Käyttäjätunnukset kirjoitetaan pienellä, ei ä:tä, ei ö:tä eikä erikoismerkkejä.
- Verkon salasana on pakotettu vaihtamaan 90 päivän välein, mutta sen voi vaihtaa useamminkin.
- Salasanan minimipituus on 10 merkkiä, salasana ei saa olla aikaisemmin käytetty ja sen pitää sisältää kolmesta merkkikategoriasta merkkejä, esim. pienet kirjaimet, isot kirjaimet, erikoismerkit ja numerot.
- Jokaisella käyttäjällä on oma, henkilökohtainen käyttäjätunnus ja salasana. Omaa tunnusta EI luovuteta missään tilanteessa kenellekään toiselle (ei siis esim. sijaiselle tai muille käyttäjille). Sijaisille tehdään omat tunnukset. Käyttäjätunnukset muodostuvat automaattisesti työsopimuksen teon yhteydessä PHR-järjestelmässä.
- Jokainen käyttäjä on vastuussa omasta tunnuksestaan ja salasanastaan. Mikäli väärinkäytöksiä esiintyy, käyttäjätunnuksen haltija on vastuussa vahingoista, vaikka ei itse olisi tunnusta käyttänytkään.
- Tunnukset poistetaan työntekijän palvelussuhteen päätyttyä automaattisesti.

5.4 Muut käyttäjätunnukset ja salasanat

- Vaikka ohjelma ei vaatisikaan salasanaa, laita aina omalle käyttäjätunnuksellesi salasana. Ota tavaksesi vaihtaa myös muiden ohjelmien salasanat samalla kun Windows vaihdattaa salasanan. ÄLÄ käytä ohjelmia niiden oletussalasanalla, vaan vaihda se ehdottomasti!

Omaa tunnusta EI luovuteta missään tilanteessa kenellekään toiselle (ei siis esim. sijaiselle tai muille käyttäjille).

5.5 Tietokoneen käyttö

- Koneita ei saa jättää auki omilla tunnuksilla. Aina kun poistut koneelta, lukitse tietokone. Jos kone on useamman käyttäjän käytössä, kirjaudu ulos poistuessasi koneelta.
- Ohjelmien käyttäjistä ja käyttöoikeuksista pidetään kirjaa. Osaston esimies ilmoittaa uusien käyttöoikeuksien tarpeesta pääkäyttäjälle. Tarpeettomat käyttäjätunnukset ilmoitetaan pääkäyttäjälle ja ne poistetaan.
- Tallennus: Jokaisella käyttäjällä on oma kansio verkossa, johon muilla käyttäjillä ei ole pääsyä. Tiedostot tallennetaan vain tänne, ei koskaan paikallisesti oman koneen levylle (C:). Verkkokansio varmistetaan automaattisesti joka yö. Tiedostot voidaan tarvittaessa palauttaa.
- Yhteiset kansiot: Verkkoasemaan voidaan tehdä myös osastokohtaisia käyttäjäkansioita, joihin myönnetään käyttöoikeus ko. osaston työntekijöille. Verkkokansio varmistetaan automaattisesti joka yö. Tiedostot voidaan tarvittaessa palauttaa.
- Virustorjunnasta huolehtii F-Secure-virustorjuntaohjelma, joka päivittyy jatkuvasti automaattisesti. Internet-liikenne tarkistetaan automaattisesti virusten ja haittaohjelmien varalta. Verkko on varustettu erillisellä palveluntarjoajan palomuurilaitteella.
- Kaikki saapuva ja lähtevä sähköposti tarkistetaan koneellisesti automaattisesti. Saapuvat roskapostit suodatetaan palvelimessa automaattisesti Saitan sähköpostisuotimella ja roskapostit poistetaan kokonaan.
- Kaikilla käyttäjillä on kunnan toimesta sähköpostiosoite. Henkilökunnan sähköpostiosoitteet ovat muodossa Etunimi.Sukunimi@ruokolahti.fi (ilman ääkkösiä).
- USB-muisteja saa käyttää omien työtiedostojen siirtoon, kun huolehtii virustorjunnasta ja tietoturvasta.

Erityisen varovainen täytyy olla internetissä olevien ohjelmien kanssa. Jos et tiedä, mitä teet, jätäthän sen tekemättä!

Ohjelma-asennukset suorittaa Saita Oy. Jos koneelle tarvitaan jokin uusi ohjelma, otetaan yhteys Saitan servicedeskiin.

Ovet suljetaan ja lukitaan huoneesta poistuttaessa.

Kunnan tieto- ja viestintätekniikkapäällikkönä toimii Matti Backman, puh 044 4491 203,

matti.backman@ruokolahti.fi.

Kunnan tietotekniikkayhteistyöyrityksenä toimii Saimaan talous ja tieto Oy, puh. 05 616 6281, servicedesk@saita.fi, vastuualueena työasemat, palvelimet ja verkkoyhteydet.

Ongelmatilanteessa ota pääsääntöisesti yhteys Saitaan numeroon 05 616 6281.

Kaikkein tärkein tietoturvaa edistävä tekijä on käyttäjä itse!

5.6 Tulostaminen ja kopiointi

- Vältetään ylimääräistä tulostamista ja kopiointia. Ylimääräiset kopiot (kustannus- ja ympäristövaikutusten ohella) lisäävät riskiä siihen, että tieto joutuu vääriin käsiin.
- Varmistetaan, mihin tulostimeen tulostetaan ja missä tulostin sijaitsee. Tulosteet haetaan heti tulostuksen jälkeen.
- Henkilötietoja sisältävät tiedot tuhotaan aina silppuamalla.

5.7 Sähköpostin käyttö

Sähköisten asiakirjojen käsittelyssä sovelletaan kunnassa kirjesalaisuuden, yksityisyyden suojan ja hyvän hallintomenettelyn periaatteita samalla tavalla kuin muussakin virallisten asioiden hoidossa. Käyttäjiä koskevat vaitiolovelvollisuudet ja hyväksikäyttökiellot on kuvattu myöhemmin tässä dokumentissa.

Ruokolahden kunnalla on oikeus määrätä, mihin sähköpostia ja tietoverkkoa käytetään ja käyttöoikeuksia voidaan rajoittaa.

5.7.1 Sähköpostiosoitteet

Järjestelmän ensisijainen tarkoitus on välittää ja tallentaa Ruokolahden kunnan ja sen henkilöstön ja toiminnoissaan ja työssään tarvitsemia sähköisessä muodossa olevia viestejä ja asiakirjoja. Tätä tarkoitusta varten järjestelmä sisältää sähköpostiosoitetietoja ja postitusluetteloita (esim. johtoryhmä, hallinto-osasto jne.) sekä järjestelmän palvelutason varmistamiseen, häiriötilanteiden selvittämiseen ja tilastointiin käytettäviä lokitietoja (eli tapahtumien valvontatietoja).

Viran tai toimen hoitoon liittyviä viestejä varten on avattu kunnan nimellä olevia yleisiä sähköpostiosoitteita (yleisosoite voi olla myös postituslista). TVT-päällikkö päättää organisaatiosähköpostiosoitteen perustamisesta ja poistamisesta.

Ruokolahti julkaisee kunnan yleiset sähköpostiosoitteet sekä henkilökuntansa yhteystiedot, joissa sähköpostiosoitteet ovat muotoa Etunimi.Sukunimi@ruokolahti.fi

5.7.2 Sähköpostiviestin käsittelyssä huomioitavaa

Ruokolahden kunta kohtelee sähköpostiosoitteella kuntaan toimitettua viestiä pääsääntöisesti vastaanottajalle osoitettuna henkilökohtaisena viestinä, koska vastaanottaja ei voi estää henkilökohtaisten viestien saapumista.

Sähköpostiviestejä käsitellään ja ne kirjataan ja arkistoidaan tarvittaessa arkistonmuodostussuunnitelmassa ilmenevällä tavalla. Sähköpostin kautta kulkevista pysyvästi säilytettävistä asiakirjoista on otettava arkistokelpoinen paperituloste, jollei arkistonmuodostussuunnitelmassa muuta todeta.

Virkatehtäviin liittyvissä sähköpostiviesteissä on lähettäjän liitettävä virka-asema ja yksikön nimi allekirjoitukseen.

Sähköpostin käyttö yksityisiin tarkoituksiin on vähäisessä määrin luvallista. Käyttö kaupalliseen tai poliittiseen tarkoitukseen, kuten yksityiseen yritystoimintaan tai vaalimainontaan on kuitenkin ehdottomasti kielletty. Myöskään ketjukirjeitä ei saa lähettää kunnan sähköpostipalvelimilla. Tietohallinto valvoo palvelinten käyttöä.

5.7.3 Roskapostiviestin käsittelyssä huomioitavaa

Roskapostilla tarkoitetaan häiritseviä sähköpostiviestejä, joita käyttäjä ei halua. Yleensä kyse on mainospostista. Roskapostiin ei pidä vastata, koska vastaamalla osoittaa osoitteensa toimivaksi, jolloin osoite lisätään roskapostituslistoille.

Käyttäjä voi ilmoittaa häiritsevästä roskapostista ylläpidolle (Saita Oy).

5.7.4 Perille menemättömän sähköpostiviestin käsittely

Sähköpostiviestin lähettäjällä on pääasiallinen vastuu viestin luettavuudesta, viestin perillemenosta, määräajan ylittymisestä ja muista näihin verrattavista seikoista. Mikäli saapuvan viestin osoite ei ole sähköpostijärjestelmän tiedossa, posti palautuu automaattisesti lähettäjälle virheilmoituksen kera.

5.7.5 Palvelussuhteen päättyminen

Sähköpostin käyttöoikeudet päättyvät palvelussuhteen päättyessä, ellei yksikön esimiehen kanssa ole toisin sovittu. Jos työntekijä lakkaa hoitamasta tehtäviään jo ennen palvelussuhteen päättymistä, tulee joko estää sähköpostin vastaanotto tai asettaa automaattinen vastaus "... Näitä asioita hoitaa jatkossa ..."

5.7.6 Menettelysäännöt työntekijän ollessa väliaikaisesti poissa

Kun kyse on ennakoidusta poissaolosta, työntekijän on huolehdittava sähköpostinsa asianmukaisesta hoidosta. Ensisijainen menettely on automaattinen poissaoloviesti, josta ilmenee sijaisten yhteystiedot ja mikäli mahdollista poissaolon pituus. Mikäli kunnan tehtävien hoito on vaarassa vaikeutua vakavasti poissaolon takia, voidaan joutua tilanteeseen, jossa yksittäisen poissaolevan työntekijän sähköposteihin on päästävä käsiksi. Tällöin voidaan työntekijän suostumuksella avata tähän liittyvät viestit yksikön esimiehen päätöksellä teknisen ylläpidon toimesta. Tällöin noudatetaan yksityisiä viestejä koskevaa vaitiolovelvollisuutta ja hyväksikäyttökieltoa. Mikäli suostumusta ei voida saada, hallintojohtaja päättää viestien aukaisemisesta yksikön esimiehen esittelystä.

5.7.7 Sähköpostiviestien ja niiden liitetiedostojen rajoittaminen

Kunnalla on oikeus asettaa rajoituksia sähköpostiviestien ja niiden liitetiedostojen suhteen. Käyttäjille tiedotetaan näistä rajoituksista.

Kunnalla on oikeus ohjelmallisesti tarkistaa viestit ja liitetiedostot mahdollisten virusten ja muiden haittaohjelmien osalta (jatkuva reaaliaikainen virustarkistus). Kunnalla on oikeus myös poistaa viruksia ja muita haittaohjelmia sisältävät viestit ja liitetiedostot. Viestin välittämisessä tehty liitetiedostojen poistaminen on tarvittaessa saatettava viestin vastaanottajan ja lähettäjän tietoon.

5.7.8 Sähköpostiviestin salaus ja todentaminen

Muita kuin julkisia tietoja ja julkisia henkilötietoja sisältäviä asiakirjoja ei tule siirtää sähköpostina tai muuna tietoverkon yli tapahtuvana tiedonsiirtona.

Sähköpostilla vastaanotetun asiakirjan oikeellisuus ja aitous on tarvittaessa varmistettava.

5.7.9 Sähköpostin ja tietoverkon käytön valvonta

Kunta ei valvo perusteettomasti sähköposteja, eikä loukkaa viestintäosapuolten eikä viestien käsittelemien henkilöiden yksityisyyttä. Myöskään muussa verkkokäytön valvonnassa ei perusteettomasti loukata yksityisyyttä. Joissain olosuhteissa yksityiskohtaisempi tutkinta voi olla välttämätöntä.

5.7.10 Kunnan oikeudet sähköpostiviestien lukemiseen

Kunta ei saa oikeudettomasti lukea käyttäjälle lähetettyjä tai hänen lähettämiään sähköpostiviestejä, yleensä siihen tarvitaan käyttäjän suostumus.

Tietojärjestelmän toimintaa tai palvelutasoa uhkaavissa häiriötilanteissa voivat järjestelmänvalvojat joutua avaamaan sähköpostilaatikon tai viestin sisältävän tiedoston.

5.7.11 Tukihenkilöt

Sähköpostijärjestelmistä vastaa kunnan tietotekniikkayhteistyöyritys (tällä hetkellä Saita Oy).

Postipalvelimet ovat tiukasti suojattuja ja niiden ylläpitäminen tapahtuu siten, että niin käytettävyys kuin myös luottamuksellisuus säilyvät.

5.7.12 Järjestelmän suojauksen periaatteet:

- Sähköpostien välityksellä leviäviä viruksia vastaan suojaudutaan keskitetyllä virustorjunnalla sekä työasemakohtaisilla torjuntaohjelmilla. Kaikki saapuneet ja lähtevät sähköpostit virustarkistetaan koneellisesti automaattisesti.
- Laitetekniikan häiriöihin varaudutaan mm. riittävällä varmistuskopioinnilla, RAID-tekniikoilla (kiintolevyjen ”kahdennus”), vikasietoisilla levyjärjestelmillä, palvelinlaitteistojen kahdennuksilla, varavirtalaitteilla sekä huoltosopimuksin.
- Inhimillisiin riskeihin varaudutaan ohjeistuksilla sekä koulutuksella. ICT-tukihenkilöt valvovat järjestelmän asianmukaista käyttöä, luovat ja poistavat sähköpostiosoitteet ja postituslistat.

5.8 Henkilöstön sosiaalisen median ohjeistus

- Kun mainitset profiilissasi tai keskusteluissa työnantajasi, esiinnyt työpaikkasi edustajana. Mieti, millaisen kuvan annat työnantajastasi.
- Muista, että sinulla on lojaliteettivelvoite työnantajaa kohtaan. Kirjoita asioista, joista ei ole haittaa työnantajan maineelle tai taloudelle. Jos työasiat vaivaavat mieltäsi, ota yhteyttä henkilöön, joka voi asiaan vaikuttaa.
- Harkitse, ennen kuin kirjoitat. Pohdi julkaistessasi kirjoituksia, kuvia tai videoita, voiko niitä tulkita väärin. Kirjoita ja julkaise työnantajastasi tai työstäsi sellaisia asioita, jotka voisit julkaista esim. lehdessä.
- Muista vaitiolovelvollisuuden piiriin kuuluvat asiat.
- Työaika on tarkoitettu työtehtävien hoitamiseen.
- Työsähköposti on tarkoitettu työasioiden hoitoon. Hanki vapaa-ajan käyttöön henkilökohtainen sähköpostiosoite.
- Sosiaalisen median käytöstä työtehtävissä on sovittava esimiehen kanssa erikseen.
- Huomioi, että vaikutat sosiaalisessa mediassa toimiessasi omaan ammattiuskottavuuteesi.
- Tiedosta, että jos toimit sosiaalisessa mediassa työnantajaa haittaavalla tavalla, sillä voi olla seurauksia palvelussuhteeseesi.

5.9 Toimitilojen turvallisuus

Toimitilojen turvallisuudella varmistetaan laitteiden ja asiakirjojen säilyminen turvallisissa tiloissa. Toimitilojen turvallisuuteen kuuluu kulunvalvonta, tekninen valvonta, vartiointi, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunta sekä tietoaineistoja sisältävien lähetysten turvallisuus.

- Mieti asiakaspalvelupisteessä ja –tilanteessa, saavatko tietokoneesi näytöllä näkyvät tiedot näkyä asioijille vai ei?
- Noudata kulunvalvonnasta annettuja ohjeita. Käytä tarvittaessa kuvallista henkilökorttiasi.
- Tarkista työpisteeseesi tullessasi, ettei mitään asiatonta ole tapahtunut poissaolosi aikana.
- Säilytä tieto ja laitteet turvassa, mahdollisuuksien mukaan lukitussa kaapissa ja huoneessa. Mitä arkaluonteisempaa tietoa sitä varmemmassa paikassa se tulee säilyttää.
- Älä jätä kannettavaa tietokonetta tai matkapuhelinta ilman valvontaa. Säilytä laitteita lukitussa tilassa. Huolehdi myös muistitikkujen, paperitulosteiden ja ym. asianmukaisesta säilyttämisestä.
- Noudata puhtaan pöydän periaatetta. Työpöydällä ei saa säilyttää salassa pidettävää tietoa.
- Älä jätä vierasta yksin tai ilman valvontaa työhuoneeseesi tai muihin toimitiloihin.
- Lukitse työhuoneesi ovi työpäivän päättyessä tai poistuessasi pidemmäksi aikaa työpisteestäsi.

- Ohjaa vieraat tai eksyneet henkilöt oikeisiin paikkoihin. Älä päästä asiattomia henkilöitä toimitiloihin esim. töistä lähtiessäsi.
- Älä jätä kulunvalvonnassa olevia tai muuten suljettuina pidettäväksi tarkoitettuja ovia auki.
- Henkilötietoja sisältävät asiakirjat hävitetään tavalla, joka estää niiden asiattoman käytön ja henkilörekisterien käyttämisen hävittämisen yhteydessä tai sen jälkeen.

5.10 Etätyö tai työmatka

Etätyössä ja matkoilla ympäristöt vaihtelevat eikä ympäristön turvallisuuteen voida juurikaan vaikuttaa. Etätyöntekijän omilla toimenpiteillä ja menettelytavoilla on tällöin suuri merkitys tietoturvallisuuden takaamisessa.

- Huolehdi, että etätyössä käyttämäsi laitteistot, ohjelmistot, tietoliikenneyhteydet ja paperiaineistot ovat ja pysyvät vain sinun käytössäsi.
- Säilytä tieto ja laitteet turvassa. Älä jätä kannettavaa tietokonetta tai matkapuhelinta ilman valvontaa. Säilytä laitetta lukitussa paikassa. Muista myös tietovälineiden, paperitulosteiden ym. asianmukainen säilyttäminen.
- Kuljeta mukanasi vain välttämättömimmät tietoaineistot ja varmistu aineiston suojauksesta.
- Vältä puhumasta luottamuksellisista työasioista julkisilla paikoilla ja kulkuvälineissä.
- Mikäli työskentelet julkisessa kulkuvälineessä, varmistu, etteivät kanssamatkustajat pysty näkemään käsittelemiäsi tietoja ja asiakirjoja. Varo myös aiheettomien langattomien yhteyksien aktivoitumista koneeseesi.
- Kannettavia tietokoneita ja matkapuhelimia ei saa jättää autoon näkyvälle paikalle, eikä niitä saa säilyttää autossa yön yli.
- Vältä julkisten päätteiden (esim. nettikahvilat, kirjastot) käyttöä työasioihin. Et voi vaikuttaa siihen, mitä tietoja käytöstäsi kerätään ja mitä tiedoilla tehdään. Yleensä sinulle ei myöskään tarjoudu mahdollisuutta poistaa näitä tietoja laitteelta.

5.11 Toimintaohjeet ongelmatilanteiden varalle

Ilmoitusvelvollisuus ja toiminta ongelmatilanteessa

- Henkilötietojen käsittelijän on ilmoitettava tietoturvaloukkauksista (esim. henkilötietojen vahingossa tapahtunut tai tahallinen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin) kunnan tietosuojavastaavalle ja esimiehelle ilman aiheetonta viivytystä loukkauksen tietoonsa saatuaan.
- Ilmoita myös vakavat läheltä-piti -tilanteet tietosuojavastaavalle ja/tai esimiehellesi. Läheltä-piti -tilanteet tilastoimalla voidaan kehittää tietoturvaa.
- Mikäli hallussasi oleva laite tms. katoaa tai varastetaan, ilmoita siitä välittömästi esimiehelle ja tietosuojavastaavalle sekä Saitan servicedeskiin.
- Ilmoita aina haittaohjelmista (esim. virukset, madot tai troijalaiset) ja muista tietoturvallisuuteen liittyvistä ongelmista välittömästi Saitan servicedeskiin.
- Ilmoita aina myös muista turvallisuuteen liittyvistä epäilyistä, suojauspuutteista tai ongelmista Saitan servicedeskiin.

Jos epäilet tietoturvaloukkausta tai haittaohjelmatartuntaa

- Älä hätiköi.
- Tietokonetta ei tarvitse sulkea, mutta irrota lähiverkkokaapeli työasemastasi.
- Kirjoita ylös, mitä mahdollisessa ilmoituksessa tai varoituksessa luki tai ota kännykkäkameralla kuva. Kirjoita muistiin tekemisesi.

- Ota yhteyttä Saitan servicedeskiin. Auta tutkinnassa. Kerro, mitä olit tekemässä, kun kone alkoi toimia odottamattomasti. Toimi saamiesi ohjeiden mukaisesti.

6 Soveltaminen

Tämä Ruokolahden kunnan tietosuojaohje annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmien käyttäjälle. Tietoturvapolitiikkaa ja ohjeita noudatetaan kaikessa toiminnassa ja ne koskevat kaikkia kunnan palveluksessa olevia henkilöitä, luottamushenkilöstöä sekä organisaation ulkopuolisia yhteistyökumppaneita.

Tämä tietosuojaohje on voimassa toistaiseksi ja voimassaolo jatkuu, ellei sitä nimenomaisesti kumota. Tietosuojaohje korvaa erilliset tietoturvaohjeet, sähköpostin tietoturvaohjeen sekä sosiaalisen median ohjeistuksen.

7 Lähteet

EU-tietosuojan kokonaisuudistus, VAHTI-raportti 1/2016, Julkisen hallinnon ICT, Valtionvarainministeriö 2016.

Henkilöstön tietoturvaohje, VAHTI 4/2013, Valtionhallinnon tietoturvallisuuden johtoryhmä, valtionvarainministeriö 2013.

Vahti Yhteishankkeiden materiaalit 2017-2018

Tietoturvaohje, Ruokolahden kunta 2017.

Tietoturvaohje sähköposti, Ruokolahden kunta 2017

Ruokolahden kunnan henkilöstön sosiaalisen median ohjeistus

Miten valmistautua EU:n tietosuoja-asetukseen? Selvityksiä ja ohjeita 4/2017, Tietosuojavaltuutetun toimisto, Oikeusministeriö 2017.