

# TIETOSUOJAOHJE

voimaantulo 23.4.2018 alkaen  
hyväksytty KHALL 16.04.2018 § 73



Isonkyrön kunta

# SISÄLLYSLUETTELO

|   |           |
|---|-----------|
| <b>JOHDANTO</b> .....   | <b>4</b>  |
| <b>KÄSITTEET</b> .....  | <b>5</b>  |
| HENKILÖREKISTERI.....   | 5         |
| HENKILÖTIETO .....  | 5         |
| HENKILÖTIEDON KÄSITTELIJÄ .....   | 5         |
| HENKILÖTIEDON KÄSITTELY .....   | 5         |
| REKISTERINPITÄJÄ .....  | 5         |
| TIETOSUOJA .....  | 5         |
| TIETOSUOJAVASTAAVA .....  | 6         |
| TIETOTURVA .....  | 6         |
| <b>OSA I: TIETOSUOJAPOLITIIKKA</b> .....  | <b>7</b>  |
| <b>1. TIETOSUOJAN TAVOITTEET</b> .....  | <b>7</b>  |
| <b>2. ORGANISAATIO JA VASTUUT</b> .....   | <b>7</b>  |
| <b>3. TIETOSUOJAN TOTEUTTAMINEN</b> .....   | <b>7</b>  |
| <b>4. LAIT JA ASETUKSET</b> .....   | <b>8</b>  |
| <b>5. RIKKOMUKSET JA SEURAAMUKSET</b> .....                                       | <b>9</b>  |
| <b>OSA II: TIETOSUOJA – TIETOJEN KÄSITTELEMINEN</b> .....                         | <b>10</b> |
| <b>6. HENKILÖTIETOJEN KÄSITTELY</b> .....   | <b>10</b> |
| HENKILÖTIETOJEN KERÄÄMINEN.....   | 10        |
| ARKALUONTEINEN HENKILÖTIETO ELI ERITYISIIN HENKILÖTIETORYHMIIN KUULUVA TIETO..... | 11        |
| HENKILÖREKISTERI JA HENKILÖTIETOJEN ELINKAARI .....                               | 11        |
| KÄYTTÖOIKEUDET, VAITIOLO- JA SALASSAPITOVELVOLLISUUS.....                         | 11        |
| <b>7. REKISTERÖIDYN OIKEUDET</b> .....  | <b>12</b> |
| TIETOSUOJASELOSTE .....   | 12        |
| REKISTERÖIDYN OIKEUS SAADA TIETOJA .....  | 13        |
| OIKEUS TIETOJEN OIKAISEMISEEN JA OIKEUS TULLA UNOHDETUksi.....                    | 13        |
| OIKEUS KÄSITTELYN RAJOITTAMISEEN JA VASTUSTAMISOIKEUS .....                       | 14        |
| OIKEUS SIIRTÄÄ TIEDOT JÄRJESTELMÄSTÄ TOISEEN .....                                | 14        |
| TIETOTURVALOUKKAUKSESTA ILMOITTAMINEN.....  | 14        |
| <b>8. SOPIMUSVAATIMUKSET, KUN HENKILÖTIETOJEN KÄSITTELYÄ ULKOISTETAAN</b> .....   | <b>15</b> |
| <b>9. SEURAAMUKSET JA HALLINNOLLISET SANKTIOT</b> .....                           | <b>15</b> |
| <b>10. TIETOSUOJAVASTAAVAN TEHTÄVÄ</b> .....                                      | <b>15</b> |
| <b>OSA III: TIETOTURVA</b> .....  | <b>17</b> |
| <b>11. MITÄ TIETOTURVA TARKOITTAÄ</b> .....                                       | <b>17</b> |
| <b>12. KÄYTTÖOIKEUDET</b> .....   | <b>17</b> |
| <b>13. SALASANAT</b> .....  | <b>17</b> |
| <b>14. TIETOKONEEN KÄYTTÖ</b> .....   | <b>18</b> |
| <b>15. TULOSTAMINEN JA KOPIOINTI</b> .....  | <b>18</b> |
| <b>16. SÄHKÖPOSTIN KÄYTTÖ</b> .....   | <b>18</b> |
| <b>17. INTERNET JA SOSIAALINEN MEDIA</b> .....                                    | <b>19</b> |

|  |    |
|--|----|
| 18. TOIMITILOJEN TURVALLISUUS.....                 | 20 |
| 19. ETÄTYÖ TAI TYÖMATKA .....                      | 20 |
| 20. TOIMINTAOHJEET ONGELMATILANTEIDEN VARALLE..... | 21 |
| SOVELTAMINEN.....                                  | 22 |
| LÄHTEET .....                                      | 23 |

## Johdanto

Kunnallisten palveluiden tuottaminen perustuu tietoon ja sen käsittelyyn. Tietoa on sekä salassa pidettävää että julkista tietoa. 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 toukokuussa sovellettava EU:n tietosuoja-asetus (General Data Protection Regulation, GDPR 679/2016) korvaa nykyisen 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 käsitteilytoimien tarkempaa dokumentointia. Asetus pitää myös sisällään uusia oikeuksia rekisteröidyille.

Tämä asiakirja koostuu kolmesta osasta: ensimmäisessä osassa esitellään Isonkyrön kunnan tietosuojaperiaatteet eli tietosuojapolitiikka, toisessa osassa annetaan ohjeistuksia henkilötietojen käsittelemiseen ja kolmannessa osassa on käytännön tietoturvatointia, joilla tietosuoja voidaan parantaa. Asiakirja koskee henkilötietojen käsittelyä, jossa Isonkyrön kunta toimii rekisterinpitäjänä.

Tietosuojapolitiikka sisältää ne henkilötietojen käsittelyyn liittyvät periaatteet, vastuut ja seuraamusjärjestelmän, joita noudatetaan Isonkyrön kunnan tietosuojan toteuttamisessa ja kehittämisessä. Tietosuojapolitiikka antaa pohjan ohjeiden ja määräysten soveltamiselle.

Toisen ja kolmannen osan ohjeiden tarkoituksena on selventää henkilötietojen käsittelyssä noudatettavia tietosuojaperiaatteita ja täsmentää EU:n tietosuoja-asetuksen edellyttämiä toimenpiteitä. Lisäksi ohjeeseen on koottu keskeisimmät tietoturvallisuuden perusasiat ja toimintaohjeet ongelmatilanteiden varalle.

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

Asiakirjan tekemisessä on käytetty hyväksi Lähteet-sivulla lueteltuja asiakirjoja.

## Käsitteet

### Henkilörekisteri

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

### 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, verkotunnistetietojen 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; kuva, joka yhdistettynä esim. osoitetietoihin, IP-osoite, jos tämä voidaan liittää tiettyyn käyttäjään tai käyttäjätunnus.

### Henkilötiedon käsittelijä

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

### 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.

### 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.

### Tietosuoja

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

## **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.

## **Tietoturva**

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

# OSA I: TIETOSUOJAPOLITIikka

## 1. Tietosuojan tavoitteet

Yksityisyydensuoja ja henkilötietojen suojaja on jokaisen perusoikeus. Isonkyrön 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.

Isonkyrön kunta määrittää tarvittavat suojatoimet ottamalla huomioon mm. käytettävissä oleva tekniikka, toteuttamiskustannukset, käsittelyn luonne ja laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuva riski.

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.

## 2. Organisaatio ja vastuut

Henkilötietojen käsittelyn lainmukaisuudesta vastaa ensisijaisesti Isonkyrön kunnan johto. Vastuu ei riipu siitä, onko joitakin organisaation toimintoja ulkoistettu vai ei. Johdolla on vastuu huolehtia mm. tietoturvatyön riittävästä resursoinnista ja että tietosuojaja otetaan huomioon suunnitelmissa.

Kukin palvelualueen johtaja vastaa omalla palvelualueellaan tietosuojan lainmukaisuudesta. Lisäksi yksiköiden esimiehet valvovat tietosuojan toteutumista omassa yksikössään. Jokaisen esimiehen tulee huolehtia, että tietosuojaja- ja tietoturvaohjeet sekä tietoverkon käyttöä säännöt perehdytetään henkilöstölle.

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

ICT-asiantuntija vastaa teknisen tietoturvan kehittämisestä, tietojärjestelmien toiminnasta, hoidosta ja turvallisuudesta saamiensa resurssien ja toimintavaltuuksien puitteissa.

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

## 3. Tietosuojan toteuttaminen

Hyvän tietosuojan tason toteuttaminen vaatii organisaation kaikilla tasoilla ulottuvia jatkuvia toimia, jolloin taataan organisaation häiriötön toiminta sekä normaali- että poikkeusoloissa. Toteuttaminen

tapahtuu erilaisten hallinnollisten ja teknisten toimenpiteiden avulla. Tietosuojaja tulee huomioida kaikessa toiminnassa niin manuaalisessa kuin sähköisessä henkilötietojen käsittelyssä sekä puhutussa ja kirjoitetussa tiedossa.

Henkilötietojen käsittelyssä noudatetaan seuraavia Yleisessä tietosuojasetuksessa 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 on aikeissa käsitellä.
- Henkilötietojen kerääminen tulee olla **sidonnainen käyttötarkoitukseen** ja tietojen kerääminen tulee tapahtua tiettyä, nimenomaista ja laillista tarkoitusta varten. Kerättyä tietoa ei saa käyttää myöhemmin tarkoitukseen, jolla ei ole sidonnaisuutta kerättyyn käyttötarkoitukseen.
- 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 virheettiset 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, jossa on käytettävä asianmukaisia teknisiä tai organisatorisia toimia.

## 4. Lait ja asetukset

Isonkyrön 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. Organisaation omat päätökset, määräykset ja ohjeet eivät saa olla ristiriidassa Isonkyrön kunnan tietosuojapolitiikan kanssa.

### Tietosuojaan liittyvä keskeinen lainsäädäntö:

- EU:n yleinen tietosuojasetus (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)

## **5. Rikkomukset ja seuraamukset**

Jokainen Isonkyrön kunnan tietojärjestelmien käyttäjä on velvollinen noudattamaan Isonkyrön kunnan tietosuojapolitiikkaa, tietoverkonkäyttösääntöjä sekä tietosuoja- ja tietoturvaohjeita. Tietojen käsittelijä on vastuussa mahdollisesta vahingosta, jos se 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.

## OSA II: TIETOSUOJA – tietojen käsitleminen

### 6. 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.

#### 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 saatetaan joku päivä 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 edellyttävä 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 rekisteröidyltä kysytään suostumus henkilötietojen käsittelyyn, on rekisteröityä tiedotettava suostumuksen merkityksestä ennen suostumuksen antamista. Suostumus on pätevä vain, kun se on vapaaehtoinen, yksilöity, tietoinen, 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 tähän kysyä uusi suostumus.

## **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 uudistettavassa henkilötietolaissa on vielä mahdollisuus soveltaa alemmaa ikärajaa, joka voi alimmillaan olla 13 vuotta.)

## **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 tietosuojasetus määrää, että kaikki tietovarannot tulee kartoittaa ja kuvata. Henkilörekisterit tulee kuvata tietosuojaselosteissa (kts. 7. Rekisteröidyn oikeudet).

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 joku päivä 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.

## **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 myöntäessä ja muuttaessa tulee jäädä merkintä (loki tai dokumentti), jolloin 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 veloitetaan vaitiolovelvollisuuteen työ- tai muilla sopimuksilla, ja veloituksen on oltava voimassa työ-, sopimus- tai toimeksiantosuhteen päätyttyäkin. Henkilötietojen oikeudeton käsittely on rangaistava teko.

#### 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 henkilökäytön 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.

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

### Tietosuojaseloste

Henkilörekistereistä tulee olla laadittuna rekisteriseloste eli tietosuojaseloste, 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 ja
- 9) tietojen siirto EU:n ulkopuolelle,
- 10) rekisterin suojauksen periaatteet,
- 11) henkilötietojen säilytysaika tai säilytysajan määräytymisperusteet sekä
- 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 luetteloja Isonkyrön kunnan henkilötietoja sisältävistä rekistereistä.

### **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 rekisteröiden oikeuksien toteuttamiseksi ovat pääsääntöisesti **maksuttomia**. Pyydetty tiedot pitää ensisijaisesti luovuttaa sähköisessä muodossa. Ennen tietojen luovuttamista, rekisteröidyn henkilöllisyys tulee pystyä varmistamaan.

### **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, joihin 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.

## 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 tietosujoa-asetuksessa mainituissa tilanteissa, jolloin hänen henkilötietojaan ei saa enää käsitellä ko. tarkoituksissa. Vastustusoikeus ei koske lakisääteisiä rekistereitä.

## 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.

## Tietoturvaloukkauksesta ilmoittaminen

Henkilötietojen tietoturvaloukkauksen sattuessa Isonkyrön 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. Ilmoituksen voi tehdä lomakkeella ”Tietoturvapoikkeamasta ilmoittaminen rekisteröidylle”. Rekisteröidylle suunnattavassa ilmoituksessa tulee kertoa vähintään seuraavassa listatut kohdat.

- Tietosuojavastaavan nimi ja yhteystiedot tai muu yhteystieto, josta rekisteröidyt voivat halutessaan kysellä 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 hättävien vaikutusten 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.

## **8. Sopimusvaatimukset, kun henkilötietojen käsittelyä ulkoistetaan**

Toimeksiantosuhteissa, annettaessa palveluita ulkopuolisen hoidettaviksi, laaditaan toimeksiantosta 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, kieltä käyttää saatuja tietoja ulkopuolisiin tarkoituksiin ja velvollisuus suojata saadut tiedot.

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

## **9. Seuraamukset ja hallinnolliset sanktiot**

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

Lisäksi mikäli henkilötietoja ei käsitellä lainmukaisesti ja tietosuojaa-asetusta rikotaan, voi rekisterinpitäjä saada huomautuksen, varoituksen, henkilötietojen käsittelykiellon tai muun sanktion. Hallinnollisen sanktion määräämisestä päättää tietosuojaa-asetuksen nojalla perustettu valvontaviranomainen.

## **10. Tietosuojavastaavan tehtävä**

Tietosuojavastaava antaa tietoja ja neuvoja rekisterinpitäjälle ja työntekijöille henkilötietojen käsittelyyn liittyen. Hän seuraa asetuksen noudattamista omassa organisaatiossaan ja hänen vastuulleen kuuluu myös tietosuojaa-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 suojaamista 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.



## OSA III: TIETOTURVA

### 11. 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.

### 12. Käyttöoikeudet

- Käyttöoikeudet eri järjestelmiin pystyy myöntämään vain siihen oikeutetut henkilöt kuten ICT-asiantuntija tai tietojärjestelmän pääkäyttäjä.
- **Käyttöoikeuksia myöntäessä tulee siitä jäädä jälki** (lokietieto 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.

### 13. Salasanat

- Käytä palveluissa vahvoja salasanoja ja älä luovuta salasanaasi kenellekään toiselle.
- **Vahva salasana on riittävän pitkä, vähintään kahdeksan merkkiä ja sen tulee sisältää isoja (A, B, C...) ja pieniä kirjaimia (a, b, c...), numeroita (0,1,2..) sekä mielellään erikoismerkkejä (näppäimistön symbolit). Erityisen vahva salasana sisältää 20–30 merkkiä, joka on joukko sanoja, joista muodostuu lause.**
- Salasana ei saa sisältää käyttäjänimeäsi, oikeaa nimeäsi tai yrityksen/kunnan/yhteisön nimeä.
- Älä käytä samaa salasanaa Isonkyrön kunnan ulkopuolisessa palvelussa.
- Vaihda salasanat riittävän usein ja heti, jos epäilet niiden paljastuneen.

## 14. Tietokoneen käyttö

- Vastaat käyttäjänä omasta koneestasi. Ole siis huolellinen.
- Kirjaudu koneelle aina omilla käyttöoikeuksillasi.
- Vain kunnan ICT-asiantuntija saa asentaa laitteita verkkoon ja asentaa tai päivittää koneisiin ohjelmia. Jos tietoturvaohjelmisto ilmoittaa uudesta päivityksestä, tulee ohjelmisto päivittää viivytyksettä.
- **Estä asiaton pääsy tietoverkkoon lukitsemalla työasemasi (Windows-työasemalla paina Windows näppäin + L) aina kun poistut työpisteestäsi.**
- Huolehdi, että myös matkapuhelimessasi on päällä automaattinen lukitus ja suojakoodikysely.
- Tallenna työsi käyttäen välitallennuksia. Älä jätä työtä tallentamatta, kun poistut työpisteestäsi.
- Tallenna kaikki tärkeä tieto sellaisen verkkopalvelimen levyille, josta otetaan säännöllisesti varmuuskopiot.
- Jos työaseman kiintolevy tai muu tallennusväline, kuten esimerkiksi muistitikku poistetaan käytöstä, ei sitä saa laittaa roskakoriin. Toimita tallennusväline hävitettäväksi.
- Varo toimisto-ohjelmilla (esim. tekstinkäsittely, esitysgrafiikka, taulukkolaskenta, PDF) tehtyjen tiedostojen piiloon jääviä tietoja (ns. meta-, jäännös- ja piilotiedot) erityisesti lähettäessäsi tiedostoja organisaation ulkopuolelle tai siirtäessäsi niitä tietovälineellä. Tiedosto voi sisältää siinä aiemmin ollutta tietoa tai muuta järjestelmässä olevaa tietoa, vaikka se ei näytöllä näkyisikään. Tarkista tiedot esim. painamalla hiiren oikealla tiedostoa > valitse Ominaisuudet > Tiedot-välilehti.
- Kirjaudu ulos sekä ohjelmistoista että koneeltasi ja sammuta tietokoneesi työpäivän päättyessä.

## 15. Tulostaminen ja kopiointi

- Vältä ylimääräistä tulostamista ja kopiointia. Ylimääräiset kopiot (kustannus- ja ympäristövaikutusten ohella) lisäävät riskiä siihen, että tieto joutuu väärin käsiin.
- Varmista, mihin tulostimeen tulostat ja missä tulostin sijaitsee. Hae tulosteesi heti tulostuksen jälkeen. PIN-koodin syöttämisen vaatiminen tulostimeen tulostetta noudettaessa pienentää väärälle tulostimelle tulostamisen sekä asiakirjan tulostimelle unohtamisen riskejä.
- **Kun hävität salassa pidettäviä tietoja, käytä aina hävittämispalveluun kuuluvia keräys-säiliöitä (tietosuojasäiliö).**

## 16. Sähköpostin käyttö

Sähköposti on hyvä työväline yhteydenpitoon. On kuitenkin muistettava, että sähköpostissa ei ole mitään suojausta, vaan tiedot liikkuvat salaamattomana julkisessa verkossa.

- Isonkyrön kunnan antama sähköpostiosoite on tarkoitettu käytettäväksi työasioissa. Sähköpostia voi käyttää henkilökohtaiseen käyttöön kohtuullisesti ja pienimuotoisesti. Yksityiset sähköpostit on pidettävä kuitenkin selkeästi erillään työsähköpostista sähköpostikansioilla (nimeä esim. ”yksityisviestit”)
- Huolehdi sähköpostin käsittelystä myös poissaolosi aikana velvollisuuksiesi mukaisesti ja käytä tarvittaessa automaattista poissaoloviestiä, jolla kerrot kuka hoitaa tehtäviäsi poissaolosi aikana.

- **Sähköpostiviestit liikkuvat verkossa yleensä salaamattomina ilman mitään suojausta, joten suojaamista edellyttäviä tietoja ja aineistoja ei saa lähettää sähköpostitse ilman suojausta.**
- **Asiakasta tulee informoida sähköpostin tietoturvallisuuden tasosta esimerkiksi, että sähköpostia ei ole suojattu.**
- Sähköpostiviestit voivat sisältää haittaohjelmia tai linkkejä, jotka vievät haittaohjelmia sisältävälle sivustolle. Älä avaa epäilyttäviä sähköpostiviestejä, joiden alkuperästä et ole varma. Tarkista linkin kohdeosoite ennen klikkaamista.
- Varo kalasteluviestejä, joissa pyydetään tunnuksiasi ja salasanojasi, luottokortin numeroa tai muita henkilötietojasi. Ylläpitäjät missään yhteisössä eivät koskaan kysy salasanaasi, pankkitunnuksia tai luottokortin tietoja.
- **Tarkista saamasi laskut huolella. Huijarit voivat yrittää hyödyntää esimerkiksi lomakautta, jolloin henkilöstöä yritetään saada maksamaan valheellisia maksuja kiireellisyteen vedoten.**
- Poista roskapostit, älä vastaa niihin. Roskapostia ovat mm. mainokset ja ketjukirjeet, jotka on lähetetty ilman vastaanottajan lupaa.
- Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostiosoite. Mikäli oikea osoite ei ole tiedossa, ilmoita virheellisestä lähetyksestä lähettäjälle. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä.
- Huolehdi, että lähettämäsi sähköpostiviesti on kohdistettu oikeille henkilöille ja oikeisiin osoitteisiin. Vältä turhien sähköpostien lähettämistä. Ennen viestin lähettämistä varmista, että vastaanottaja (To:) ja mahdollisissa kopio (Cc:) sekä piilokopio (Bcc:) –kentissä olevat vastaanottajat ovat juuri ne henkilöt, joille tarkoituksesi on viesti lähettää.
- Työhön liittyvä sähköposti vastaanotetaan ja ohjataan kunnan sähköpostijärjestelmään. Sitä ei saa ohjata tai jatkolähettää automaattisesti kunnan sähköpostijärjestelmän ulkopuolelle.
- Älä kirjaudu Isonkyrön kunnan sähköpostiosoitteella sosiaalisen median palveluihin. Käyttäessäsi kunnan sähköpostiosoitetta edustat aina myös kuntaa. Hanki yksityiseen käyttöösi toinen sähköpostiosoite.
- **Työsuhteen päättyessä sähköpostiosoite ja –laatikko poistetaan. Huolehdi postin käännöstä ja henkilökohtaisten sähköpostien poistamisesta.**

## 17. Internet ja sosiaalinen media

- **Lue Isonkyrön kunnan ohjeistus sosiaalisen median käyttämiseen.**
- **Jos mainitset sosiaalisen median palvelun henkilöprofiilissasi työnantajasi, esiinnyt tällöin organisaatiosi (epävirallisena) edustajana. Muista käyttäytyä sen mukaisesti!**
- Älä keskustele työasioista muissa kuin työtehtäviin hyväksytyissä sosiaalisissa medioissa. Ole erityisen huolellinen salassa pidettävän tiedon suhteen. Muista, että palvelun ylläpitäjät pääsevät teknisesti käsiksi kaikkeen palveluun talletettuun ja myös vain keskustelun osapuolten väliseksi tarkoitettuun tietoon.
- **On lainvastaista välittää internetin kautta salassa pidettävää tietoa ilman asianmukaista salausta.** Tällaiset viestit ja liitetiedostot on salattava organisaation hyväksymillä tuotteilla tai palveluilla.
- Opettele salaustuotteiden oikea käyttö, jotta tieto ei vahingossa siirry salaamattomana.

- Jos käytät julkisia päätelaitteita tai tilapäisesti toisen henkilön hallussa olevaa tietokonetta, muista tyhjentää Internet-selaimen välimuisti ja evästeet (cookies).

## 18. 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 kunnan toimitiloissa kuvallista henkilökorttiasi, mikäli sellainen on annettu.
- 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 muistitikojen, 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. Paperiset asiakirjat laitetaan lukittuun keräyssäiliöön, jonka sisältö menee asianmukaisesti tuhottavaksi, jotta tietoturvasäilyminen säilyy.

## 19. Etätyö tai työmatka

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

## 20. 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.
- Ilmoita aina haittaohjelmista (esim. virukset, madot tai troijalaiset) ja muista tietoturvallisuuden liittyvistä ongelmista välittömästi omalle esimiehellesi ja ICT-asiantuntijalle.
- Ilmoita aina myös muista turvallisuuteen liittyvistä epäilyistä, suojauspuutteista tai ongelmista turvallisuusvastaaville tai omalle esimiehellesi.

### 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 ICT-asiantuntijaan ja/tai tietoturvavastaavaan. Auta tutkinnassa. Kerro mitä olit tekemässä, kun kone alkoi toimia odottamattomasti. Toimi saamiesi ohjeiden mukaisesti.

## **SOVELTAMINEN**

Tämä Isonkyrön kunnan tietosuojaohje annetaan tiedoksi jokaiselle työntekijälle ja tietojärjestelmien käyttäjälle.

Tietoturvaliteikkaa ja ohjeita noudatetaan kaikessa toiminnassa ja ne koskevat kaikkia organisaation palveluksessa olevia henkilöitä, luottamushenkilöstöä sekä organisaation ulkopuolisia yhteistyökumppaneita.

Tämä tietosuojaohje on voimassa toistaiseksi ja voimassaolo jatkuu, ellei sitä nimenomaisesti kumota.

## Lähteet

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

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

Henkilöstön tietoturvaohjeet, Perusturvaosasto, Isonkyrön kunta 2011.

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

Tietoturvapoliittikka, malliesimerkki, Sosiaali- ja terveysministeriö 2010.

Yleinen tietosuoja-asetus, Yleiskirje 14/2017, Ida Sulin 29.5.2017, Kuntaliitto 2017.