Pyhäjoen kunnan Tietoturva- ja tietosuojapolitiikka

Kunnanhallitus 13.4.2026

Sisällysluettelo

1 Johdanto 1

2 Keskeiset käsitteet 1

3 Tietoturvan organisointi ja vastuut 2

3.1 Kunnanhallitus ja kunnan johto 2

3.2 Tietohallinnon vastuu 3

3.3 Toimialajohtajien vastuu 3

3.4 Tietosuojavastaavan vastuu 3

3.5 Työntekijän vastuu 4

4 Tietoturvatyön tavoitteet 4

5 Tietosuoja 4

5.1 Henkilötietojen kerääminen ja käsittely 4

5.2 Arkaluonteinen henkilötieto eli erityisiin henkilötietoihin kuuluva tieto 5

5.3 Henkilörekisteri ja sitä koskevat käyttöoikeudet, vaitiolo- ja salassapitovelvollisuus 6

5.4 Tietosuojaseloste 6

5.5 Rekisteröidyn oikeudet 6

5.6 Tietosuojan huomioiminen henkilötietojen käsittelyn ulkoistuksen yhteydessä 9

5.7 Seuraamukset ja hallinnolliset sanktiot 9

6 Tietoturva 10

6.1 Mitä tarkoittaa tietoturva 10

6.2 Tietoturvan osa-alueita 10

6.3 Tietoturvariskeihin varautuminen 12

6.4 Tietoturvariskien arviointi ja hallinta 12

1 Johdanto

Tämä tietoturvapolitikkaa kuvaa Pyhäjoen kunnan tietoturvallisuuden tavoitteet, vastuut ja toteuttamiskeinot, jotka kunnanhallitus on hyväksynyt. Organisaatio sitoutuu noudattamaan julkishallintoa koskevia tietoturvaan ja tietosuojaan liittyvää lainsäädäntöä sekä uusimpia viranomaisvaatimuksia ja ottaa tietoturvan huomioon toiminnassaan.

Tietoturva- ja tietosuojapolitiikan tavoitteena on suojata kunnan tietoja ja tietojärjestelmiä vahingoilta, luvattomalta pääsyltä, muutoksilta, paljastumiselta tai tuhoamiselta.

Tietoturvan tarkoitus on varmistaa tietojen asianmukainen ja luotettava käsittely. Päivittäisessä työssä tämä tarkoittaa pääasiassa sitä, että henkilöstöllä on käytössään ohjeistus, henkilöstö on saanut riittävän tietoturvakoulutuksen ja tietojen näkyvyys rajataan vain työssään niitä tarvitseville henkilöille. Järjestelmähankintoja ja käyttöönottoja suunniteltaessa otetaan huomioon järjestelmille asetettavat käytettävyys-, tietosuoja- ja tietoturvavaatimukset.

Poikkeamatilanteisiin varautumisen ensisijainen vastuu on kunnan ylimmällä johdolla, jonka on varmistettava tietoturvatyön riittävä resursointi ja seuranta. Panostaminen tietoturvaan sekä yleisellä että tekniikan tasolla ovat strategisia päätöksiä, joilla vaikutetaan myös kunnan toimintakykyyn. Myös lainsäädäntö edellyttää tietoturvan asianmukaista hoitamista. Edut ovat häiriötön toiminta, toiminnan laatu ja positiivisen julkisuuskuvan säilyminen.

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

2 Keskeiset käsitteet

Henkilötiedot ovat tiedot, jotka tunnistavat henkilön suoraan tai välillisesti, kuten nimi, osoite tai IP-osoite. Tietosuoja-asetus suojaa näitä tietoja riippumatta siitä, mitä tekniikkaa tietojenkäsittelyssä käytetään tai millä tavalla tiedot säilytetään.

Henkilörekisteri on jäsennelty tietojoukko, joka sisältää henkilötietoja. Se voi olla keskitetty, hajautettu tai jaettu eri tavoin. Henkilörekisteriä käytetään henkilötietojen keräämiseen, tallettamiseen ja käsittelyyn, ja se on suojattu tietosuoja-asetuksilla.
Henkilötietoja voidaan tallettaa esimerkiksi sähköisiin tiedostoihin, tietokantoihin, paperisina, mappeihin, kortistoihin tai ääni- ja kuvatallenteisiin.

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

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 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.

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

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

Tietoturvallisuus määritellään yleensä kolmen peruskäsitteen kautta:

1. **Tietojen saatavuus:** tieto on saatavissa ja käytettävissä silloin ja siinä muodossa, kuin sitä tarvitaan.
2. **Tietojen luottamuksellisuus:** tieto on vain niiden tahojen käytettävissä, joilla on siihen oikeus. Luottamuksellisuus turvaa tietojen julkaisun tai luovuttamisen vain ja ainoastaan suunniteltuja väyliä pitkin, suunnitellussa laajuudessa.
3. **Tietojen eheys:** tiedot on suojattu siten, ettei niitä voi muuttaa tahallisesti tai tahattomasti siten, että niiden luotettavuus vaarantuu, tai ainakin tällaiset muutokset voidaan havaita. Eheys turvaa tietojen hyödynnettävyyden ja arvon säilymisen.

Kolmea yllä mainittua tietoturvallisuuden peruskäsitettä täydentävät:

4. **Kiistämättömyys:** tietoon kohdistuvista toimenpiteistä jää jälki, jota muutoksen tekijä ei voi kiistää.
5. **Tunnistus:** tietojärjestelmän käyttäjä voidaan tarvittaessa liittää käyttäjätunnukseen.
6. **Todennus:** tietojärjestelmän käyttäjä voidaan luotettavasti tunnistaa luonnolliseksi henkilöksi tai oikeushenkilöksi

3 Tietoturvan organisointi ja vastuut

3.1 Kunnanhallitus ja kunnan johto

Kuntalain mukaisesti kokonaisvaltainen riskienhallinta ja sitä kautta tietoturvan ja tietosuojan toteuttamisen kokonaisvastuu on kunnanhallituksella ja kunnanjohtajalla. Ylimmän johdon

tehtävänä on valvoa kokonaisuutta sekä riskienhallinnan ja sisäisen valvonnan toteutusta. Kunnan johdon on sitouduttava tietoturvan ja tietosuojan jatkuvaan kehittämiseen ja huolehdittava resursoinnin riittävyydestä ja jatkuvuudesta. Kunnanhallitus vastaa teknisen ja hallinnollisen tietoturvan yleisestä järjestämisestä, kehittämisestä ja seurannasta.

3.2 Tietohallinnon vastuu

Tietohallinto huolehtii, että tietoturvasta huolehditaan asianmukaisesti. Tämä tarkoittaa tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu. Tietoturvatoimenpiteet koskevat sekä sähköistä että manuaalista tietojenkäsittelyä. Tietoturvalliseen toimintatapaan ohjeistetaan ja sen tulee olla jokapäiväistä niin työpaikalla kuin sen ulkopuolella.

Tietojärjestelmien teknisen ympäristön sekä laitteiden ylläpito on ICT-palveluiden omana työnä suoritettavaa. ICT-palvelut vastaa tietoturvan toteutumisesta lain ja asetusten sekä rekisterinpitäjän ohjeiden mukaisesti. Tiedonhallintamalliin nimetyt vastuulliset viranhaltijat vastaavat osaltaan käytettyjen sovellusten tietoturvallisuudesta sovelluksen elinkaaren ajan.

3.3 Toimialajohtajien vastuu

Toimialajohtajat vastaavat tietoturva- ja tietosuojapolitiikan ja ohjeiden noudattamisesta toiminnassaan sekä oman palvelun sisällä että sopimussuhteissa ostopalveluiden toimittajiin. Kukin palvelu vastaa omalla toimialallaan tietosuojan lainmukaisuudesta. Lisäksi yksiköiden esihenkilöt valvovat tietosuojan ja tietoturvan toteutumista omassa yksikössään. Jokaisen esihenkilön tulee huolehtia, että tietosuoja- ja tietoturvaohjeet sekä tietoverkon käyttösäännöt perehdytetään henkilöstölle.

Esihenkilöt ja tietojärjestelmien pääkäyttäjät vastaavat työntekijöiden käyttöoikeuksista tietojärjestelmiin ja niiden tietosisältöihin työtehtävien edellyttämässä laajuudessa.

Esihenkilöiden ja pääkäyttäjien tulee huolehtia, että työtehtävien muutokset huomioidaan järjestelmien käyttöoikeuksissa. Heidän on huolehdittava, että työsuhteen päättyessä työntekijät palauttavat kaiken työnantajalle kuuluvan omaisuuden sekä käyttöoikeudet tietojärjestelmistä poistetaan. Esihenkilöillä on raportointivelvollisuus tietoturvapoikkeamista ja kehittämistarpeista ICT-palveluille.

3.4 Tietosuojavastaavan vastuu

Tietosuojavastaavan työtä ohjaa EU:n yleinen tietosuoja-asetus. Tietosuojavastaava toimii tietosuoja-asioissa asiantuntijana ja yhteyshenkilönä. Tietosuojavastaavan tehtävänä on auttaa rekisterinpitäjää saavuttamaan hyvän henkilötietojen käsittelytavan ja tietosuojan tason. Tietosuojavastaava on otettava asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn ja kehittämiseen. Tietosuojavastaavan palvelu voidaan hankkia ulkopuolisena asiantuntijatyönä.

3.5 Työntekijän vastuu

Jokaisella, joka käsittelee kunnan omistamaa tietoa, on omalta osaltaan henkilökohtainen vastuu kokonaisturvallisuudesta. Työntekijällä on vastuu noudattaa hyväksyttyjä tietoturva- ja tietosuojaohjeita ja huolehtia päivittäisissä työtehtävissä hyvän tiedonhallintatavan käytänteistä. Työntekijän vastuulla on myös huolehtia käsittelemänsä tiedon oikeellisuudesta, saatavuudesta ja luokittelusta sekä huolehtia, että organisaation tiedot ovat asianmukaisesti käytettävissä. Tietojen säilytys- tai arkistointiajan päätyttyä ne on hävitettävä ohjeiden mukaisesti. Jokainen tietoja ja tietojärjestelmiä käyttävä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, ongelmista ja kehittämistarpeista esihenkilölleen.

4 Tietoturvatyön tavoitteet

Tietoturvatyö on osa kunnan yleistä turvallisuustoimintaa, riskien hallintaa ja sisäistä valvontaa. Tietoturva- ja tietosuojatyössä huomioidaan yleiset lait ja asetukset, joilla pyritään kokonaisvaltaiseen johtamiseen, riskien tunnistamiseen ja ennaltaehkäisyyn sekä tietojen suojaamiseen.

Tavoitteena on kehittää ja parantaa kunnan toiminnan luotettavuutta, jatkuvuutta, laatua, ICTriskien hallintaa ja riskeihin varautumista sekä edistää tietoturva- ja tietosuojatyön saattamista kiinteäksi osaksi kunnan johtamista. Työn tavoitteena on luoda yhdenmukaiset käytännöt ja toimintatavat.

Tietoturva- ja tietosuojaohjeita noudatetaan kaikissa tiedon elinkaaren vaiheissa. Tietosuojan toteuttamisessa tavoitteena on varmistaa tietosuojalainsäädännön ja toimialakohtaisen lainsäädännön vaatimusten toteutuminen käsiteltävien henkilötietojen elinkaaren ajan. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja tietojen käyttötarkoituksen mukaan. Tietosuoja tulee huomioida jo hankintojen suunnitteluvaiheessa silloin, kun hankinnan kohde sisältää henkilötietojen käsittelyä. Henkilötietojen käsittelyyn liittyvät vaatimusmäärittelyt tulee lisätä osaksi tarjouspyyntöä ja ottaa tietosuojavastaava mukaan vaatimusten määrittelyyn.

5 Tietosuoja

5.1 Henkilötietojen kerääminen ja käsittely

Tietosuoja on olennainen osa tietoturvaa. Tietosuojan lähtökohtana on suojata henkilöiden perusoikeudet ja -vapaudet sekä erityisesti henkilötiedot ja varmistaa yksityisyyden suoja. Tietosuojaa ja sen vaatimuksia määrittelee EU:n yleinen tietosuoja-asetus sekä kansallinen lainsäädäntö, joka velvoittaa rekisterinpitäjän suunnittelemaan ja osoittamaan henkilötietojen käsittelyn lainmukaisuuden.

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 käsittely alkaa niiden keräämisestä. Pyhäjoen kunnassa henkilötietoja kerätään ja käsitellään vain siinä laajuudessa kuin se on palvelun tai työtehtävien kannalta tarpeen. Henkilötietoja ei saa kerätä ilman perustetta tai sitä varten, että tietoja saatetaan joku päivä tarvita. Tietojen säilytys ja käyttö toteutetaan niin, että ettei ulkopuolisten ole mahdollista saada niitä tietoonsa.

Pyhäjoen kunta noudattaa EU:n tietosuoja-asetuksen tietosuojaperiaatteita, jonka mukaan henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Niitä saa kerätä ja käsitellä vain tiettyä, nimenomaista ja laillista tarkoitusta varten ja ainoastaan tarpeellinen määrä tarkoitukseen nähden. Henkilötiedot on aina tarvittaessa päivitettävä ja epätarkat ja virheelliset henkilötiedot on poistettava tai oikaistava viipymättä. Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Tietoja käsitellään luottamuksellisesti ja turvallisesti.

5.2 Arkaluonteinen henkilötieto eli erityisiin henkilötietoihin kuuluva tieto

Niin sanottuihin erityisiin henkilötietoryhmiin kuuluvien henkilötietojen käsittely on lähtökohtaisesti kiellettyä Pyhäjoen kunnassa. 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. Näitä tietoja on suojeltava erityisen tarkasti, koska niiden käsittely voi aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja -vapauksille. Erityisiin henkilötietoryhmiin kuuluvia henkilötietoja saa käsitellä, jos kieltoon on säädetty poikkeus EU:n tietosuoja-asetuksessa tai erikseen unionin oikeudessa tai kansallisessa lainsäädännössä.

Erityisiä henkilötietoryhmiä koskevia tietoja voi käsitellä suoraan tietosuoja-asetuksen perusteella seuraavissa tapauksissa:

a) nimenomaisen suostumuksen perusteella

b) henkilön elintärkeiden etujen suojaamiseksi tilanteessa, jossa rekisteröity on fyysisesti tai juridisesti estynyt antamasta suostumustaan tai

c) jos käsittely on tarpeen yleistä etua koskevasta syystä lainsäädännön nojalla. Alle 16-vuotiaaiden lasten henkilötietojen käsittely ei ole sallittua ilman huoltajan suostumusta.

5.3 Henkilörekisteri ja sitä koskevat käyttöoikeudet, vaitiolo- ja salassapitovelvollisuus

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 kuvataan tietosuojaselosteissa.

Henkilötietoja saa käsitellä vain kunnan palveluksessa olevat henkilöt tai ulkopuoliset palveluntuottajat, joiden kanssa on laadittu erillinen sopimus palvelun tuottamisesta. Toimialajohtajat ja yksiköiden esihenkilöt 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.

Henkilötietojen käsittelijät eivät saa ilmaista sivullisille tietoja toisen henkilön ominaisuuksista, henkilökohtaisista oloista tai taloudellisesta asemasta, joita ovat saaneet tietoonsa henkilötietojen käsittelyyn liittyviä toimenpiteitä suorittaessaan tai muutoin. Henkilötietoja käsittelevät henkilöt velvoitetaan vaitiolovelvollisuuteen työ- tai muilla sopimuksilla, ja velvoitus on voimassa työ-, sopimus- tai toimeksiantosuhteen päätyttyäkin. Henkilötietojen oikeudeton käsittely on rangaistava teko.

5.4 Tietosuojaseloste

EU:n yleinen tietosuoja-asetus velvoittaa kuntia tiedottamaan avoimesti tehdystä henkilötietojen käsittelystä ja tietosuojaseloste on yksi osa tätä. 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. Kunnan yleinen tietosuojaseloste on nähtävillä kunnan verkkosivuilla. Rekisterinpitäjän vastuulla on huolehtia, että tietosuojaseloste on ajan tasalla.

5.5 Rekisteröidyn oikeudet

5.5.1 Rekisteröidyn oikeus saada tietoa henkilötietojen käsittelystä

Rekisteröidyllä on kohtuullisin väliajoin oikeus saada tietoa hänen henkilötietojensa keräämisestä sekä käsittelystä. 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. Pyhäjoen kunta ottaa sähköiset tietopyynnöt keskitetysti kirjaamoon kunta@pyhajoki.fi.

Rekisteröidylle on annettava tiedot ilman aiheetonta viivytystä ja viimeistään kuukauden (1 kk) kuluessa pyynnön vastaanottamisesta. Määräaikaa voidaan tietyin edellytyksin jatkaa. Jos pyyntöjä

on monta tai ne ovat monimutkaisia, rekisterinpitäjä voi ilmoittaa vastauksessaan, että se tarvitsee niiden käsittelyyn enemmän aikaa. Tällöin määräaikaa voidaan jatkaa enintään kahdella kuukaudella. Määräajan jatkaminen on perusteltava. 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. Rekisterinpitäjä voi periä pyynnön toteuttamisesta kohtuullisen maksun silloin, jos rekisteröity pyytää tiedoista useampia jäljennöksiä tai jos rekisteröidyn pyyntö on ilmeisen perusteeton tai kohtuuton. Vaihtoehtoisesti rekisterinpitäjä voi kieltäytyä pyynnöstä. Pyyntöjä voidaan pitää ilmeisen perusteettomina tai kohtuuttomina erityisesti, jos niitä esitetään toistuvasti. Rekisterinpitäjän on osoitettava pyynnön ilmeinen perusteettomuus tai kohtuuttomuus. Useammin pyydetyistä rekisteritiedoista peritään kulloinkin voimassa oleva, asiakirjoista perittävä maksu.

Pyydetyt tiedot pitää ensisijaisesti luovuttaa sähköisessä muodossa. Ennen tietojen luovuttamista, rekisteröidyn henkilöllisyys tulee pystyä varmistamaan. Informaatio on annettava tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Informointia ei tarvitse tehdä, jos rekisteröity on jo saanut kyseessä olevan informaation, tai jos informoimatta jättäminen on välttämätöntä valtion turvallisuuden, puolustuksen tai yleisen järjestyksen ja turvallisuuden vuoksi, rikosten ehkäisemiseksi tai selvittämiseksi taikka verotukseen tai julkiseen talouteen liittyvän valvontatehtävän vuoksi. Informointia ei tarvitse tehdä myös silloin, kun tiedot on saatu muualta kuin rekisteröidyltä, ja informointi osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa.

5.5.2 Oikeus tietojen oikaisemiseen ja oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä häntä koskevat epätarkat ja virheelliset henkilötiedot. Ottaen huomioon tarkoitukset, joihin tietoja käsiteltiin, rekisteröidyllä on myös 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. Tämä oikeus ei kuitenkaan koske kunnan lakisääteisiä rekistereitä. Tietojen poistaminen niistä ei ole mahdollista lakisääteisten tehtävien suorittamiseen liittyvän käsittelyn yhteydessä.

Oikeuden käyttäminen on lähtökohtaisesti maksutonta. Jos poistopyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia, rekisterinpitäjä voi joko periä rekisteröidyltä kohtuullisen maksun tai kieltäytyä pyynnöstä.

5.5.3 Oikeus käsittelyn rajaamiseen 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 tietosuoja-asetuksessa mainituissa tilanteissa, jolloin hänen henkilötietojaan ei saa enää käsitellä ko. tarkoituksissa. Vastustusoikeus ei koske lakisääteisiä rekistereitä.

5.5.4 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. Tiedot on oikeus saada siirrettyä suoraan rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista. 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.

Oikeutta sovelletaan

- ainoastaan henkilötietojen automaattiseen käsittelyyn
- kun henkilötiedot koskevat rekisteröityä ja ovat hänen toimittamiaan
- kun henkilötietojen käsittely perustuu suostumukseen tai sopimukseen
- kun tietojen siirto ei vaikuta haitallisesti kolmansien osapuolten oikeuksiin ja vapauksiin.

5.5.5 Tietoturvaloukkauksesta ilmoittaminen

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta. Henkilötietojen tietoturvaloukkauksen sattuessa kunnalla on velvollisuus ilmoittaa tietoturvaloukkauksista tietosuojaviranomaiselle ja rekisteröidylle. Henkilötietojen tietoturvaloukkauksia voivat olla esimerkiksi kadonnut tiedonsiirtoväline (kuten USB-tikku), varastettu tietokone, hakkerointi, haittaohjelmatartunta tai kyberhyökkäys.

Henkilötietojen käsittelijän on ilmoitettava tietoturvaloukkauksista kunnan tietosuojavastaavalle ilman aiheetonta viivytystä loukkauksen tietoonsa saatuaan. Henkilötietojen tietoturvaloukkauksesta täytyy ilmoittaa valvontaviranomaiselle, jos loukkauksesta voi aiheutua riski luonnollisten henkilöiden oikeuksille ja vapauksille. Ilmoitus on tehtävä mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta, riippumatta siitä, onko loukkaus tapahtunut omassa vai ulkopuolisen käsittelijän toiminnassa. Suomessa valvontaviranomaisena toimii tietosuojavaltuutetun toimisto.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle ilman aiheetonta viivytystä, jos se todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille.
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 haittavaikutusten lieventämiseksi ja tilanteen ratkaisemiseksi riittävän yleisellä tasolla.

Ilmoitusta ei kuitenkaan tarvitse tehdä, jos tietoturvaloukkauksesta ei todennäköisesti aiheudu riskiä rekisteröidyn oikeuksille. Kunnan työntekijöiden tulee aina ilmoittaa mahdollisesta henkilötietoja koskevasta vakavasta lähellä-piti-tilanteesta tietosuojavastaavalle, jolloin tiedot voidaan tilastoida ja tietoturvaa voidaan kehittää.

5.6 Tietosuojan huomioiminen henkilötietojen käsittelyn ulkoistuksen yhteydessä

Kuntaa koskevissa toimeksiantosuhteissa, joissa palveluita annetaan ulkopuolisen toimijan hoidettaviksi, laaditaan toimeksiannosta aina kirjallinen sopimus. Sopimuksessa tulee varmistaa henkilötietojen käsittelyn lainmukaisuus tilanteissa, joissa ulkoinen sopimuskumppani tulee käsittelemään henkilötietoja hankintasopimuksen perusteella kunnan lukuun. Tällainen tilanne on esimerkiksi työterveyshuollon palveluiden tuottaminen kunnalle. Kun henkilötietojen käsittelyä koskevia tehtäviä annetaan sopimusperusteisesti palvelutuottajalle, on välttämätöntä huolehtia siitä, että henkilötietojen käsittelyä koskevat ehdot on sopimusvelvoittein saatettu käsittelijän tietoisuuteen.

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.

5.7 Seuraamukset ja hallinnolliset sanktiot

Tietosuoja-asetuksen mukaan henkilöllä, joka on kärsinyt tietosuoja-asetuksen rikkomisesta johtuvaa aineellista tai aineetonta vahinkoa, on oikeus saada rekisterinpitäjältä tai henkilötiedon käsittelijältä korvaus kärsittyyn vahinkoon liittyen. 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.

Rekisteröidyt henkilöt voivat kääntyä valvontaviranomaisen (tietosuojavaltuutettu) puoleen ja tehdä kantelun kuntaa vastaan, jos he katsovat, että kunta on käyttänyt henkilön tietoja tavalla, joka on ristiriidassa tietosuoja-asetuksen asettamien vaatimusten kanssa tai jos kunta laiminlyö rekisteröidyn oikeuksia.

Valvontaviranomainen voi määrätä kunnalle sanktioita, mikäli se havaitsee, että kunta laiminlyö tietosuojalain asettamia vaatimuksia. Hallinnolliset sanktiot eivät laukea automaattisesti, vaan sanktiot määrätään yksittäisten tapausten sekä olosuhteiden mukaisesti. Mikäli henkilötietoja ei käsitellä lainmukaisesti ja tietosuoja-asetusta rikotaan, voi rekisterinpitäjä saada huomautuksen, varoituksen, henkilötietojen käsittelykiellon tai muun sanktion.

6 Tietoturva

6.1 Mitä tarkoittaa tietoturva

Tietoturva tarkoittaa tietojen käsittelyn ja arkistoinnin turvaamista. 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.

Kyberturvallisuus on osa tietoturvaa. Kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.
Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä.

6.2 Tietoturvan osa-alueita

Tietoturvasta huolehtiminen tarkoittaa tietojen, tietojärjestelmien, tiedonvälityksen ja niitä käyttävien palveluiden turvaamista ja suojaamista siten, että tietojen olemassaolo, oikeellisuus, käytettävyys, luottamuksellisuus ja palveluiden jatkuvuus eivät vaarannu. Tietoturvatoimenpiteet koskevat sekä sähköistä että manuaalista tietojenkäsittelyä. Tietoturvalliseen toimintatapaan ohjeistetaan ja sen tulee olla jokapäiväistä niin työpaikalla kuin sen ulkopuolella. Tietoturva on kokonaisuus, jossa on monia eri osa-alueita. Ei riitä, että vain jotkin niistä ovat riittävällä tasolla suojattu, sillä tällöin riskit voivat toteutua heikommin suojatun osa-alueen kautta. Kunta huomioi ja varmistaa päivittäisessä toiminnassaan seuraavat tietoturvan näkökulmat.

Tietojärjestelmä on kokonaisuus, joka koostuu tietovarannoista, niitä käsittelevistä sovelluksista ja laitteista sekä tietoverkoista, tietojen käyttöä määrittävistä ohjeista, käyttäjistä sekä liittymistä toisiin tietojärjestelmiin. Tietojärjestelmään kuuluu oleellisena osana käsiteltävien tietojen turvallisuus ja tietoturvan yleinen hallinta ja valvonta.

Hallinnollinen tietoturva on tietoturvatoimintojen johtamista ja organisointia, ja sillä tarkoitetaan tietoturvatoimintojen, henkilöstön tehtävien ja vastuiden sekä ohjeistuksen, koulutuksen ja valvonnan muodostamaa kokonaisuutta. Hallinnollinen tietoturva pyrkii ennakoimaan riskit sekä arvioimaan ja hallitsemaan riskien mahdollisia vaikutuksia. Tavoitteena on sekä tietoturvan toteutuminen että johdon ja henkilöstön sitoutuminen sen suunnitelmalliseen hoitamiseen ja kehittämiseen.

Henkilöstöturvallisuus on henkilöiden toimista johtuvia ja heihin kohdistuvien tietoturvauhkien hallintaa. Tavoitteena on luotettava ja tehtäväänsä soveltuva henkilöstö, joka tuntee oman roolinsa mukaisesti hänelle asetetut tietoturvavaatimukset. Kunnan henkilöstön, opiskelijoiden, harjoittelijoiden ja kunnalle ostopalveluita tuottavien henkilöiden ja toimijoiden tulee noudattaa

tietoturvallisia toimintatapoja tehtävässään. Henkilöstöturvallisuuden toteutumiseksi kunnan vaaralliset työyhdistelmät tunnistetaan ja mahdollisuuksien mukaan eliminoidaan. Esihenkilö vastaa, että työntekijällä on työtehtävän mukainen käyttöoikeus järjestelmiin ja että uusi henkilöstö perehdytetään ja koulutetaan tehtäväänsä myös tietoturvan osalta.

Fyysisen tietoturvan keinoin pyritään suojaamaan kunnan hallussa olevia tietoja ja tietovarantoja fyysisten uhkien, kuten rakenteiden ja niiden vikojen aiheuttamilta vahingoilta ja luvattomien tai rikollisten toimien seurauksilta. Fyysisen tietoturvan suunnittelussa kartoitetaan ja huomioidaan tärkeimmät suojattavat kohteet ja varmistetaan teknisten järjestelmien toiminta. Kunnan fyysinen tietoturva sisältää mm. kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan.

Tietoaineiston turvallisuus perustuu tiedonhallintaa ohjaavaan lainsäädäntöön ja ohjeisiin. Keskeistä on tietojen käsittely ja luokittelu sekä säilyttäminen. Tietojen saatavuus ja käytettävyys varmistetaan teknisin toimin ja estetään tietojen tahaton tai tahallinen tuhoutuminen tai vääristyminen. Teknisillä toimilla pyritään varmistamaan toiminnan jatkuvuus häiriöttä ja varaudutaan mahdollisista häiriöistä toipumiseen. Samalla varmistetaan mahdollisen sähköisen asioinnin saatavuus, luotettavuus ja kiistämättömyys, joka tarkoittaa sähköisen asioinnin toimintaprosessin huolellista suunnittelua. Tietoturvatoimia sovelletaan tietoaineiston koko elinkaaren ajan, tiedon syntymisestä sen hävittämiseen.

Laitteistoturvallisuudella tarkoitetaan kunnan laitteistojen elinkaarta ja turvallista käyttöä. Siihen kuuluvat laitteiston asennuksen, suojauksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja sopimukset sekä laitteistojen turvallinen poisto niiden elinkaaren lopussa. Teknisin toimin pyritään varmistamaan tietojen keskeytyksetön käyttö ja toiminnan jatkuvuus sekä varaudutaan mahdollisista häiriöistä toipumiseen. Kriittisille laitteistoille taataan katkoton sähkönsyöttö ja ylläpidon korkea palvelutaso. Toimialajohtajat tai yksiköiden esihenkilöt hyväksyvät henkilöstönsä laitehankinnat. ICT-laitteiden hankinnasta, ohjelmistoasennuksista, suojauksesta ja ylläpidosta vastaa ICT-palvelut.

Ohjelmistoturvallisuus muodostuu tietojärjestelmissä käytettävien lisenssien ja ohjelmistojen hallinnasta. Pääsynhallinnalla ja sen suunnittelulla estetään tietoaineiston, ohjelmien ja järjestelmien luvaton käyttö. Ohjelmistojen tietoturvaan kiinnitetään huomiota jo niiden hankintavaiheessa toteutettavalla, tiedonhallintalain mukaisella vaikutustenarvioinnilla, jolloin varmistutaan ohjelmistojen tietoturvasta ja vaatimustenmukaisuudesta. Esihenkilö vastaa siitä, että hänen alaisuudessaan olevat käyttäjät perehdytetään ohjelmistojen käyttöön.

Tietoliikenneturvallisuus pyrkii varmistamaan viestinnän häiriöttömyyden, tiedonsiirtoyhteyksien käytettävyyden, tiedonsiirron suojaamisen ja salauksen sekä käyttäjien tunnistamisen. Tietoliikenneturvallisuus kattaa tietoverkon ja sen laitteiden kokoonpanon, ylläpidon ja muutosten hallinnan, jonka tuloksena ovat turvatut ja luotettavat tiedonsiirtoyhteydet. Kunnan tietoliikenneturvallisuuden ylläpito on keskitetty erillisellä sopimuksella ulkopuolisen toimijan hoidettavaksi palvelusopimuksen mukaisesti.

Käyttöturvallisuus tarkoittaa turvallisen käytön toimintaolosuhteita, tekniikan toimivuuden valvontaa, käytön ja lokien valvontaa, ohjelmistotukea, ylläpitoa ja huollon turvallisuustoimenpiteitä, varmuuskopiointia sekä häiriöraportointia. Tietoturva on suuressa

määrin käyttäjien toiminnasta riippuvaista. Käyttöturvallisuuden perustana on kunnan osaava ja sitoutunut henkilöstö sekä ajantasaiset ohjeistukset, joita toiminnassa noudatetaan. Tietojen oikeudeton käyttö estetään tietojen käsittelyn suunnittelulla ja käyttöoikeuksien hallinnalla. Esihenkilöt ja ohjelmien pääkäyttäjät opastavat ja kouluttavat henkilöstöä ohjelmistojen käyttöön ja tietoturvaan liittyvissä asioissa. Laitteiden ja ohjelmien käyttäjien on perehdyttävä annettuihin ohjeisiin ja noudatettava niitä. Käyttöturvallisuuden tekninen ylläpito ja tilannekeskustoiminta on keskitetty erillisellä sopimuksella ulkopuolisen toimijan hoidettavaksi palvelusopimuksen mukaisesti.

6.3 Tietoturvariskeihin varautuminen

Tietoturvariskejä arvioidaan ja niihin varaudutaan ennalta. Suurimmat tietoturvariskit sisällytetään kunnan riskienhallintasuunnitelmaan. Uhkia aiheuttavat mm. tietoisesti tehdyt väärinkäytökset, tietomurrot, virheellisesti toimivat ohjelmistot ja laitteet, virukset ja haittaohjelmat, palvelunestohyökkäykset sekä tekniset ongelmat. Tietoturvaan kohdistuvat uhat voivat aiheuttaa riskin tietojen, tietojärjestelmien tai tietoliikenteen luottamuksellisuudelle, eheydelle ja käytettävyydelle.

Sähköpostin ja verkon kautta leviävät haittaohjelmat ovat vakava uhka tietoturvallisuudelle, koska ne voivat tuhota, varastaa ja välittää tiedostoja, tunnuksia ja salasanoja sekä hidastaa tietoverkon toimintaa. Kuitenkin myös työntekijöiden jokapäiväiset toimintatavat ja asenteet vaikuttavat tietoturvallisuuteen. Suurimmat tietoturvallisuuden ongelmat liittyvätkin yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen ja muihin tietojärjestelmien toteutuksen ja käytön laadullisiin tekijöihin. Tämän vuoksi jokaisen kunnan työntekijän tulee omalla toiminnallaan varmistaa, ettei kukaan ulkopuolinen pääse tietoihin käsiksi.

Laitetason ratkaisuilla voidaan vaikuttaa tietoturvan toteutumiseen vain rajallisesti, henkilöstön osaaminen ja tietoisuus ovat suuressa roolissa tietoturvan toteutumisessa. Kouluttaminen sekä tietoisuuden lisääminen tietoturvasta ovat merkittävä tekijä uhkien pienentämisessä.

Esihenkilöiden vastuulla on huolehtia henkilöstön perehdyttämisestä.

Tietoturvariskien arviointi sisältyy kunnan sisäisen valvonnan ja riskienhallinnan ohjeeseen. Kunnan ICT -järjestelmien ylläpidon ja käytön tuen hoitaa ICT-palvelut. Käyttöoikeuksien myöntämisessä noudatetaan kunnan käyttövaltuushallinnan politiikkaa. Käyttöoikeudet perustaa joko ulkopuolinen toimija, ICT-asiantuntija tai ohjelmiston pääkäyttäjä ohjelmasta riippuen joko toistaiseksi tai määräajaksi.

6.4 Tietoturvariskien arviointi ja hallinta

Tietoturvariskien arviointi ja hallinta on oltava hallittua ja jatkuvaa, muuten tietoturvauhkien hallinta ei pysy uusien, koko ajan lisääntyvien uhkien tasolla. Tietoturvariskejä arvioitaessa on huomio kiinnitettävä erityisesti tietojen käsittelyn sisältämiin riskeihin. Riskejä syntyy aina kun tietoja käsitellään, erityisesti silloin, jos tietoja on tarpeen siirtää. Riskejä ovat myös tietojen

vahingossa tapahtuva tai tarkoituksellinen tuhoaminen, muuttaminen, luvaton luovuttaminen tai tietoihin oikeudettomasti pääseminen.

Kun erilaiset mahdolliset tietoturvauhkat on tunnistettu, tulee arvioida jokaisen uhkan osalta todennäköisyys uhkan toteutumiselle sekä mitä siitä seuraa, jos uhka toteutuu. Arvioimalla riskit pystytään keskittämään turvaamistoimet ja resurssit keskeisimpiin riskeihin, jotta riskien hallinta ei muodostu ylivoimaiseksi kustannuksiltaan tai resursoinniltaan. Järjestelmien luokittelu tapahtuu niiden kriittisyyden mukaan. Järjestelmien turvajärjestelyt tarkastetaan säännöllisesti ja tarvittaessa niiden toimivuus testataan. Tietoturvariskejä arvioidaan ja hallitaan riskienhallinnan ohjeistuksen mukaisesti. Riskienhallinnassa tunnistetaan riskit, suojataan tiedot, havaitaan rikkomukset, toimitaan tilanteen vaatimalla tavalla ja varmistetaan toiminnan vaikutukset.