KANGASNIEMEN KUNNAN

Tietoturva- ja tietosuojapolitiikka

hyväksytty

KH 24.10.2018 § 189

Versio	Tekijä	Sisältö
19.06.2018	**malli:**Tuomas Fjällström, Seija Romo ja Päivi Malinen **kuntasovellus:** Sari Kuusjärvi	Luonnos. Esitysjärjestys: kunnan johtoryhmä, YTR ja kunnanhallitus

Sisällysluettelo

Tietoturva- ja tietosuojapolitiikka

Tietoturva- ja tietosuojapolitiikka on Kangasniemen kunnan ylimmän johdon strateginen kannanotto tietoturvan ja tietosuojan kehittämiseen. Politiikka määrittelee kunnan tietoturva- ja tietosuojatyön vision, tavoitteet, toimintatavat, vastuut ja valvonnan. Tietoturva- ja tietosuojapolitiikan toteuttaminen on edellytys pitkäjänteiseen kehittämiseen. Työssä onnistuminen edellyttää kunnan johdon sitoutumisen tietoturva- ja tietosuojatyön tukemiseen.

Tietoturva- ja tietosuojapolitiikka koskee koko kuntakonsernia ja sen henkilöstöä. Samoin se koskee sidosryhmiä, jotka käsittelevät henkilötietoja rekisterinpitäjän lukuun ja ohjaamana. Politiikka kattaa kunnan omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.
Tämä politiikka koskee henkilötietojen käsittelyä silloin kun kunta toimii rekisterinpitäjänä.

Määritelmät

Tieto ja tietojenkäsittely on nykymuotoisen yhteiskunnan toiminnan perusta. Tämä edellyttää ICT-palveluiden tietoturvallista ja keskeytyksetöntä toimintaa. Digitalisaatio tuo laajentuessaan tämän vaatimuksen ja yksityisyyden suojan vaatimukset uusille alueille. Tietoturva- ja tietosuojaosaaminen voi nousta tulevaisuudessa organisaation toiminnan menestystekijäksi. Oikein toteutettuna tietoturva ja tietosuoja mahdollistavat kerätyn tiedon aikaisempaa tehokkaamman hyödyntämisen ja kustannussäästöt.

Tietoturvalla tarkoitetaan eri muodossa olevien tietojen - (esim. sähköisesti tallennettu tai välitetty tieto, puhuttu tai paperilla oleva tieto) suojaamista erilaisilta uhkatekijöiltä tavoitteena toiminnan jatkuvuuden varmistaminen ja toimintaan tai tietoihin, erityisesti henkilötietoihin, liittyvien riskien minimoiminen.

Tietoturvallisuus määritellään yleensä kolmen peruskäsitteen kautta:

1. Tietojen saatavuus: tieto on saatavissa ja käytettävissä silloin ja siinä muodossa, kuin sitä tarvitaan. Saatavuus turvaa tietojen hyödyntämisen ennalta suunnitellun aikaviiveen puitteissa.
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 yllämainittua 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.

Tietosuoja

Henkilötietojen suoja on jokaiselle kuuluva perusoikeus. Henkilötietojen käsittelyn on oltava asian- ja tarkoituksenmukaista. Henkilötietojen keräämiselle, tallentamiselle ja säilyttämiselle täytyy olla tietosuoja-asetuksen mukainen peruste.
Jokaisella henkilöllä on oikeus tutustua niihin tietoihin, joita hänestä on kunnan henkilörekisterissä. Henkilöllä on oikeus saada hänestä kerätyt tiedot muutetuiksi tai poistetuiksi, mikäli lainsäädäntö sen sallii.

Hyvä tietoturvan ja tietosuojan taso saavutetaan noudattamalla tietoturva- ja tietosuojapolitiikkaa ja sen pohjalta laadittuja ohjeita sekä ottamalla käyttöön erilaisia turvamekanismeja, joita hallitaan jatkuvan kehittämisen periaatteita noudattaen.

Kunnan roolin ja toimintaympäristön vaikutukset tietoturvaan ja tietosuojaan

Kunnan toiminnan perusta on asukkaiden tarvitsemat palvelut. Toimintaa ohjaavat strategiset päämäärät ovat:

- Yhteisöllisyys, kuntalaisten, vapaa-ajan asukkaiden ja sidosryhmien yhteisöllisyys ja aktiivinen osallistuminen
- Ympäristö, viihtyisän ja eläväisen kuntakeskuksen sekä maaseutumaisen asumisen kehittäminen
- Yritystoiminta, elinkeinotoiminnan ja työllisyyden edistäminen

Strategian tavoitteet antavat suuntaa jokaisen toimialan operatiiviselle kehittämiselle ja toimenpiteiden suunnittelulle. Tavoitteiden operatiivinen johtaminen ja vuosittaisten toimenpiteiden suunnittelu on kunnan johtoryhmän, toimialajohtajien ja lautakuntien vastuulla. Kehittämisestä ja suunnittelusta seuraa verkottunut, digitaalisuutta ja verkkopalveluja hyödyntävä toimintatapa, joka korostaa tietoturva- ja tietosuojatyön tarvetta ja merkitystä.

Kunnan palvelut kattavat laajan maantieteellisen ja toiminnallisen alueen. Toisaalta palveluiden toiminta perustuu pitkälti tietoteknisiin järjestelmiin (laitteisiin, verkkoihin ja sovelluksiin sekä niiden välisiin integraatioihin), jotka ovat tyypillisesti eri toimittajien hallussa ja siten organisatorisesti ja maantieteellisesti hajautettuja. Näin ollen Kunnan tietoturva- ja tietosuojatyön pitää ulottua Kunnan organisaation ja maantieteellisen alueen ulkopuolelle.

Kunnan tietoturvan, tietosuojan ja ICT-riskienhallinnan kehittäminen

Tiedon turvaaminen on merkittävä osa Kunnan toiminnan ja sen järjestämien palvelujen laatua, ICT-riskienhallintaa ja kokonaisturvallisuutta. Riskienhallinnan keskeisenä tavoitteena on tunnistaa

toimintaan kohdistuvat riskit, arvioida ne ja päättää tarvittavista toimenpiteistä. Tietoturva- ja tietosuojanäkökulmat:

1. Tietoteknisestä näkökulmasta hyvä toimintatapa edellyttää järjestelmäkokonaisuuden ja sen hallinnan pitkäjänteistä suunnittelua, jatkuvaa kehittämistä ja seurantaa.
2. Organisatorisesta näkökulmasta tietoturvan ja tietosuojan kehittämisen edellytys on koko henkilöstön ja luottamushenkilöstön tietoturva- ja tietosuojaosaamisen ja -tietoisuuden lisääminen kouluttamalla, ohjeistamalla ja viestimällä sekä yhteisesti sovittujen käytäntöjen noudattamisen valvomisella.
3. Tietosuojan toteutuminen ja kehittäminen edellyttää, että henkilötietojen käsittely arvioidaan ja suunnitellaan palvelukehityksessä alusta alkaen.

Tietoturva- tietosuojatyön tavoitteet ja periaatteet

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

Kehittämisen painopisteitä ovat kokonaisvaltainen johtaminen, riskien tunnistaminen ja ennaltaehkäisy sekä tietojen suojaaminen. Kehittämisen avulla varmistetaan yhtenäinen toimintaympäristö ja -tapa. Tavoitteena on kunnan palveluiden käyttäjien, yhteistyökumppaneiden ja työntekijöiden luottamus Kangasniemen kunnan palveluihin ja niiden tietoturvaan ja tietosuojaan.

Tietosuojan toteuttamisessa Kunnan tavoite on varmistaa tietosuojalainsäädännön ja toimialakohtaisen lainsäädännön vaatimusten toteutuminen käsiteltävien henkilötietojen elinkaaren ajan. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja tietojen käyttötarkoituksen mukaan. Tietosuoja huomioidaan jo hankintojen suunnitteluvaiheessa silloin, kun hankinnan kohde sisältää henkilötietojen käsittelyä. Henkilötietojen käsittelyyn liittyvät vaatimusmäärittelyt lisätään osaksi tarjouspyyntöä. Tietosuojavastaava osallistuu vaatimusten määrittelyyn.

Kangasniemen kunta rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee teknisen ympäristön ja toimenpiteet haluamansa tason mukaan. Tietosuojariskien hallinta on osa kunnan riskienhallintaprosessia. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Henkilötietojen käsittely toteutetaan noudattamalla tietosuojaperiaatteita.

Vaikutustenarviointi suoritetaan sellaisten henkilötietojen käsittelytoimenpiteille, joiden suunnitteluvaiheessa ilmenee, että toimenpiteisiin liittyy henkilön oikeuksien ja vapauksien kannalta merkittäviä riskejä. Vaikutustenarvioinnin tuloksia käytetään niiden hallintakeinojen määrittelemisessä, joilla pyritään pienentämään henkilötietojen käsittelyn riskitasoa.

Strateginen painopiste	Tavoite	Arviointi ja mittarit
Tietoturvaan ja tietosuojaan kohdistuvien uhkatekijöiden tunnistaminen	• Tuloksellinen ja kokonaisvaltainen riskienhallinta • ICT-varautumisen kehittäminen • Tietosuoja; tarvittaessa vaikutuksenarviointi	• Vakavien uhkatekijöiden tunnistaminen ja niihin liittyvät toimenpiteet • Tehokas tietoturva- ja tietosuojatyö ja raportointi • Tietotilinpäätös
Palveluiden jatkuvuuden ja tietojen turvaaminen	• Luotettava ICT-infrastruktuuri • Lakisääteisten velvoitteiden täyttäminen • Häiriötilanteiden hallinta ja tekniset ratkaisut • Häiriötilanteiden varautumis-, toipumis- ja viestintäsuunnitelmat (toimintamallit)	• Tarpeiden mukaisesti mitoitetut palvelutasot ja tietoturvaratkaisut ovat käytössä • Palvelutasojen toteutuminen • Toimintamallien arviointi • Häiriötilanteiden määrä
Henkilöstön tietoturva- ja tietosuojaosaamisen kehittäminen	• Positiivisen kulttuurin ja asenteiden kehittäminen • Selkeät vastuut, toimintamallit ja ohjeistukset • Yhtenäisten, tietoturvallisten toimintatapojen noudattaminen • Koulutus ja ohjeistus on ehdoton koskien työtehtäviä, joissa käsitellään henkilötietoja tai erityisiä henkilötietoja	• Tietoturva- ja tietosuojapolitiikan ja -ohjeiden noudattaminen • Tietoturva- ja tietosuojakoulutusten kattavuus • Työntekijöiden osaamismittarit
Strateginen painopiste	**Tavoite**	**Arviointi ja mittarit**
Tietoturva ja tietosuoja toiminnan kehittämisen mahdollistajana	• Ratkaisut mahdollistavat toiminnan turvallisen kehittämisen • Käyttötarkoituksenmukaisuus (paras mahdollinen tekninen ja organisatorinen riskiarvioon perustuva ratkaisu) ja kustannustehokkuus ohjaavat valintoja • Toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta; osaksi tarvemäärittelyä	• Tietoturvan ja tietosuojan kypsyys ja toteutuminen osana kokonaisarkkitehtuuria

	• Ongelmanratkaisukyky	
Suositusten mukainen toiminta	• Kunnan tietoturva ja tietosuoja on kansallisesti hyvällä tasolla • Toiminnan dokumentointi on ajan tasalla • Sopimuksissa on ajan mukaiset tietoturva- ja tietosuojasisällöt • Kansallisten strategioiden, ohjeistusten ja hyvien käytäntöjen tehokas hyödyntäminen • Kansainvälisten strategioiden, ohjeistusten ja hyvien käytäntöjen hyödyntäminen	• Toiminnan arviointi vasten kansallisia ja kansainvälisiä ohjeistuksia (soveltuvat viitearkkitehtuurit, tietosuoja-asetus) • Sopimusseuranta

Tietoturva- ja tietosuojatyön vastuut

Kangasniemen kunnan tietoturva- ja tietosuojatyön toteuttamisen perustana on kunnanhallituksen hyväksymä tietoturva- ja tietosuojapolitiikka ja sen pohjalta laaditut ohjeistukset. Kunnanhallitus on päättänyt Kangasniemen kunnan osalta seudullisesta tietosuojavastaavan virasta, tietosuojatyöryhmän perustamisesta ja tietosuojatyöryhmän puheenjohtajan nimittämisestä 4.12.2017 § 363. Päätöksen tarkoituksena on luoda toimielin/toimintatavat tukemaan EU:n yleisen tietosuoja-asetuksen toimeenpanoa Kangasniemen kunnan ja kunnan konsernin henkilötietojen käsittelyssä.

Kunnanhallituksen ja kunnanjohdon vastuu

Kuntalain mukaisesti kokonaisvaltainen riskienhallinta ja sitä kautta tietoturvan ja tietosuojan toteuttamisen kokonaisvastuu on kunnanhallituksella ja kunnanjohtajalla. Kunnan johdon on sitouduttava tietoturvan ja tietosuojan jatkuvaan kehittämiseen ja huolehdittava resursoinnin riittävyydestä ja jatkuvuudesta.

Tietohallinnon vastuu

Tietohallinnon vastuulle kuuluu strategisten ICT-linjausten muodostaminen ja toteuttaminen, ICT-palveluiden järjestäminen ja niihin liittyvä riskinhallinta sekä tietoturvan ja tietosuojan kehittäminen ja hallinta.

Tietohallinnon tehtävänä on tietosuojatyöryhmää apuna käyttäen ylläpitää kunnan tietoturva- ja tietosuojapolitiikkaa ja ohjeistuksia tietoturvan osalta, suorittaa seurantaa ja arviointeja, välittää tietoa organisaatiotasolla sekä tarvittaessa järjestää koulutuksia ja jalkauttaa yhteisiä toimintatapoja.

Tietosuojavastaavan vastuu

Tietosuojavastaavan työtä ohjaa EU:n yleinen tietosuoja-asetus.

Tietosuojavastaavan tehtävät ja vastuut ovat kirjattu seudulliseen yhteistyösopimukseen ja hyväksytty Kangasniemen kunnanhallituksessa. Ydintehtäviin kuuluu Kangasniemen kunnan tietosuojan kehittäminen riskienhallinnan näkökulmasta ja Kangasniemen kunnan tietosuojaosaamisen lisääminen kunnan tietosuojatyöryhmän avulla. Tietosuojavastaava on henkilökunnan ja tietosuojavaltuutetun yhteyshenkilö.

Rekisteröidyllä on oikeus saada tarkastella omia henkilörekisteriin tallennettuja tietojaan. Tietopyyntöihin vastaamista valvoo tietosuojavastaava.

Tietosuojavastaavan tehtävänä on tietosuojatyöryhmän avulla ylläpitää kunnan tietoturva- ja tietosuojapolitiikkaa ja ohjeistuksia tietosuojan osalta sekä valvoa tietosuojan toteutumista.

Tietosuojavastaava toimii Kangasniemen kunnan tietosuojatyöryhmän puheenjohtajan kanssa yhteistyössä.

Palvelualueiden, konsernin osien vastuu ja tietosuojatyöryhmä

Palvelualueiden ja konsernin osien johtajat vastaavat tietoturva- ja tietosuojapolitiikan ja ohjeiden noudattamisesta toiminnassaan sekä oman yksikön sisällä että sopimussuhteissa ostopalveluiden toimittajiin. Kunnan tietosuojatyöryhmään on nimetty edustaja jokaiselta palvelualueelta. Liikelaitosten, taseyksiköiden ja tytäryhtiöiden edustajana tietosuojatyöryhmässä toimii hallintopäällikkö.

Tietosuojatyöryhmän jäsenien (=arkistovastuuhenkilöiden) vastuulla on tuntea toimialansa erityispiirteet ja lainsäädäntö, seurata niiden kehittymistä ja kommunikoida niistä kunnan tietosuojatyöryhmälle, tietosuojavastaavalle ja tarvittaessa myös hallintopäällikölle. Lisäksi tehtävänä on valvoa tietoturvan ja tietosuojan toteutumista ja ohjeistuksen noudattamista sekä raportoida mahdollisista poikkeamista ja kehittämistarpeista.

Tietosuojatyöryhmän tehtävät ovat kunnanhallituksen vahvistamat seudullisen tietosuojayhteistyön päätöksenteon yhteydessä.

Tietojärjestelmän omistajan vastuu

Kangasniemen kunnan tietojärjestelmien hallinnointi on keskitetty kunnanhallituksen päätöksellä tietohallintoyksikköön. Jokaisella tietojärjestelmällä tulee olla yksilöity omistaja, joka vastaa koko järjestelmän elinkaaren hallinnasta, tietosuojasta ja tietoturvan toteuttamisesta. Järjestelmien omistajuus tapahtuu toimialueilla. Järjestelmän omistajuuteen liittyvät tiedot dokumentoidaan tietohallinnon ylläpitämään tietojärjestelmäluetteloon. Henkilötietoja sisältävistä tietojärjestelmistä on oltava ajantasainen tietosuojaseloste, joka voi olla myös usean tietojärjestelmän yhteinen. Tietojärjestelmän omistajan on huolehdittava tietojenkäsittelyn luottamuksellisuudesta, tietojen oikeellisuudesta ja pääsynvalvonnasta sekä tuotettava lakisääteiset seurantaraportit.

Omistajan tulee kartoittaa yhteistyössä tietohallinnon sekä palvelu- ja järjestelmätoimittajan kanssa tietojärjestelmään kohdentuvat riskitekijät, häiriötilanteiden toimintamallit ja varmistettava toiminnan jatkuvuus. Omistajan on laadittava tietoturva- ja tietosuojaohjeet käyttäjille sekä huolehdittava, että työntekijät saavat niihin riittävän koulutuksen.

Tietojärjestelmän pääkäyttäjän vastuu

Jokaiselle tietojärjestelmälle on nimettävä pääkäyttäjä, jonka vastuulla on huolehtia järjestelmän käyttöoikeuksista. Pääkäyttäjältä vaaditaan hyvää tietoturva- ja tietosuojaosaamista.

Esimiehen vastuu

Esimiesten vastuulla on huolehtia ja noudattaa työnantajaa koskevien lakisääteistein tietoturva- ja tietosuojavelvoitteiden toteutumista. Esimiehet ja tietojärjestelmien pääkäyttäjät vastaavat työntekijöiden käyttöoikeuksista tietojärjestelmiin ja niiden tietosisältöihin työtehtävien edellyttämässä laajuudessa. He huolehtivat loppukäyttäjän riittävästä perehdytyksestä konsernin tietoturva- ja tietosuojakäytänteisiin varmistaen, että jokainen ymmärtää niiden merkityksen työtehtävissään. Tietohallinto varmistaa ja valvoo käyttöoikeuden myöntämisiä.

Esimiesten ja pääkäyttäjien vastuulla on myös huolehtia, että työtehtävien muutokset huomioidaan järjestelmien käyttöoikeuksissa. Samoin heidän on huolehdittava, että työsuhteen päättyessä työntekijät palauttavat kaiken työnantajalle kuuluvan omaisuuden sekä käyttöoikeudet tietojärjestelmistä poistetaan. Esimiehiltä odotetaan esimerkillistä sekä vastuullista tietoturva- ja tietosuojakäyttäytymistä ja heillä on raportointivelvollisuus tietoturvapoikkeamista ja kehittämistarpeista tietosuojatyöryhmälle ja hallintopäällikölle.

Työntekijän vastuu

Kunnan työntekijän velvollisuus on suorittaa hyväksytysti kulloinkin voimassa oleva tietoturva- tai tietosuojakoulutus säännöllisin väliajoin. 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. Työntekijällä on velvollisuus raportoida havaitsemistaan tietoturvaongelmista ja kehittämistarpeista esimiehelleen.

ICT-palveluiden hankintoihin liittyvät vastuut

Kunta voi ulkoistaa valitsemansa osan ICT-palvelutuotantoa tai henkilötietojen käsittelystä sopimusperusteisesti. Kunta valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa.

Kunta huolehtii sopimuksin siitä, että palveluntuottaja järjestää palvelun asianmukaisin teknisin ja organisatorisin toimenpitein sekä täyttää tietosuoja-asetuksen vaatimukset ja pystyy huolehtimaan rekisteröidyn oikeuksien toteutumisesta silloin kun palveluun sisältyy henkilötietojen käsittelyä.

ICT-palveluiden tietoturvasta ja siihen liittyvästä ohjeistuksesta vastaavat palveluntuottajat. Rekisterinpitäjän vastuulla on huolehtia siitä, että henkilötietojen käsittely ja käsittelytoimet on kuvattu sopimuksessa. Palveluntuottajien tehtävä on avustaa tietoturva- ja tietosuojaohjeiden laatimisessa ja ylläpidossa. Samoin heidän kuuluu raportoida ja tiedottaa merkittävistä tietoturvaan liittyvistä poikkeustilanteista ja riskeistä.

Tilaajan vastuulla on huolehtia, että tarjouspyyntöihin ja palvelusopimuksiin sisällytetään Kunnan tietohallinnon ylläpitämät tietoturva- ja tietosuojavaatimukset täydennettynä palvelua käyttävän

toimialaan tai yksikköön sekä palveluun itseensä mahdollisesti liittyvillä erityisvaatimuksilla. Lisäksi tarjouspyyntöihin ja sopimuksiin on sisällytettävä palvelutaso, toiminta häiriötilanteissa ja vastuunjako koko arvoketjun läpi.

Toimintamallit

Seuranta

Tietosuojatyöryhmään nimettyjen edustajien tehtävänä on raportoida tietoturvaloukkauksista, riskeistä ja kehittämiskohteista viipymättä sekä tietosuojavastaavalle, tietohallinnolle että ICT-palveluiden tuottajille. ICT-palveluiden tuottajien tehtävänä on raportoida tietoturvaloukkauksista, riskeistä ja kehittämiskohteista viipymättä sekä tietosuojavastaavalle, tietohallinnolle että Kunnan nimeämälle palvelun omistajalle tai pääkäyttäjälle.

Tietohallinto ylläpitää kokonaiskuvaa tietoturvasta ja siihen liittyvistä riskeistä ja raportoi siitä osana sisäisen tarkastuksen prosessia.

Tietosuojatyöryhmä tietosuojavastaavan avustuksella ylläpitää kokonaiskuvaa tietosuojasta ja siihen liittyvistä riskeistä ja raportoi siitä osana sisäisen tarkastuksen prosessia.

Arviointi

Tietohallinnon tehtävänä on säännöllisesti arvioida tietoturvaa järjestelmäkohtaisesti ja kokonaisuutena. Arvioinnit voivat kohdistua sekä Kunnan ja sen sidosryhmien että ICT-palveluntuottajien toimintaan. Arvioinnin kohteena on tietoturvan kolmen pääkäsitteen - saatavuuden, eheyden ja luottamuksellisuuden - toteutuminen ja tavoitteena on tunnistaa niihin liittyviä riskejä ja kehittämiskohteita.

Tietohallinto priorisoi arviointikohteet. Priorisointiperusteena on järjestelmän tai palvelun vaikutus Kunnan palvelutuotantoon.

Tietosuojan toteutumisen arviointi lisätään osaksi sisäisen tarkastuksen toimintaan vuosittain toteutuvaksi. Kangasniemen kunnassa laaditaan vuosittain tietotilinpäätös jossa kuvataan tietosuojatoimenpiteet.

Kehittäminen

Tietohallinto tarkentaa tietoturvan ja tietosuojan kehittämisen tavoitteet vuosittain tavoitteiden pohjalta huomioiden sekä seurannan että arviointien tuottaman tiedon. Tietohallinto huomioi kehittämistavoitteet Kunnan kokonaisarkkitehtuurin kehittämisen yhteydessä.

Tiedottaminen

Kunnan sisäisestä tietosuojaan liittyvästä tiedottamisesta vastaa tietohallinnossa tietosuojatyöryhmän puheenjohtaja ja hallintopäällikkö tietosuojavastaavan ohjeiden mukaisesti. Toimialat ja liikelaitokset vastaavat lisäksi tiedon välittämisestä oman organisaation sisällä.

ICT-palvelun tai tietojärjestelmän operatiivisista ongelmista ja häiriöistä tiedottaminen on Kunnan johdon nimeämän omistajan tai hallintopäällikön vastuulla. Ulkoisesta tiedottamisesta vastaa hallintopäällikkö yhdessä markkinointisihteerin kanssa.

Toiminta häiriötilanteissa

Kunnan toiminta kriisitilanteissa perustuu lakisääteiseen valmiussuunnitteluun. Palvelualueet, liikelaitokset, taseyksiköt ja yhtiöt laativat kukin valmiussuunnitelman omalta osaltaan. Suunnittelussa tulee varautua pieneen, keskisuureen ja suureen toimintahäiriöön sekä soveltuvin osin poikkeusoloihin.

Kunnanvaltuusto hyväksyy kuntaa ja konsernia koskevat Sisäisen valvonnan ja riskienhallinnan periaatteet. Periaatteissa on kuvattu eri toimijoiden tehtävät ja vastuut sisäisen valvonnan ja riskienhallinnan jatkuvassa prosessissa.

Kunnan ICT-infrastruktuurin tai tietojärjestelmien toimintaa, tietoturvaa tai tietosuojaa uhkaavissa tilanteissa vastatoimenpiteet on aloitettava välittömästi ja niistä on raportoitava hallintopäällikölle ja kunnanjohtajalle.
Tietoturva- ja tietosuojarikkomukset käsitellään tapauskohtaisesti. Hallintopäälliköllä tai tietohallinnon sopimuksin valtuuttamalla taholla on oikeus sulkea tietoliikenneyhteys, järjestelmä, käyttäjätunnus tai laite uhkatilanteen vahinkojen minimoimiseksi. Hallintopäällikkö informoi asianosaisia suoritetuista toimenpiteistä ja mahdollisista jatkotoimenpiteistä mahdollisimman pian.
Henkilötietojen tietoturvaloukkauksen sattuessa kunnalla on rekisterinpitäjänä ilmoitus-velvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturva-loukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä.

Lisätietoja: Tietoturvaan ja tietosuojaan liittyviä ohjeita ja lakeja

Kansallisia ohjeita

Sisältö	Sijainti
VAHTI, voimassaolevat ohjeet	http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp
VM:n VAHTI, julkisen hallinnon digitaalisen turvallisuuden johtoryhmä	http://vm.fi/vahti
VAHTI - ohjesivusto	https://www.vahtiohje.fi/web/guest/home
EU:n tietosuojauudistus	http://www.tietosuoja.fi/1554.htm

Kunnan tietoturva- ja tietosuojatyötä ohjaavaa lainsäädäntöä

Laki	Sisältö tietoturvan näkökulmasta
Arkistolaki 831/1994	Arkistointia on hoidettava siten, että se tukee arkistonmuodostajan tehtävien suorittamista sekä yksityisten ja yhteisöjen oikeutta saada tietoja julkisista asiakirjoista, että yksityisten ja yhteisöjen oikeusturva samoin kuin tietosuoja on otettu asianmukaisesti huomioon ja että yksityisten ja yhteisöjen oikeusturvaan liittyvien asiakirjojen saatavuus on varmistettu sekä että asiakirjat palvelevat tutkimuksen tiedon lähteinä.
Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1030/1999	Viranomaisen on viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 18 §:n 1 momentin 4 kohdassa tarkoitettujen toimenpiteiden suunnittelua ja toteuttamista varten arkistolaissa (831/1994) tarkoitettua arkistonmuodostussuunnitelmaa hyväksi käyttäen selvitettävä ja arvioitava asiakirjansa ja tietojärjestelmänsä sekä niihin talletettujen tietojen merkitys samoin kuin asiakirja- ja tietohallintonsa.
Hallintolaki 434/2003	Tämän lain tarkoituksena on toteuttaa ja edistää hyvää hallintoa sekä oikeusturvaa hallintoasioissa. Lain tarkoituksena on myös edistää hallinnon palvelujen laatua ja tuloksellisuutta.
Henkilötietolaki 523/1999	Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. (1§) Tätä lakia sovelletaan henkilötietojen automaattiseen käsittelyyn. Myös muuhun henkilötietojen käsittelyyn sovelletaan tätä lakia silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa henkilörekisteri tai sen osa. (2 §)
Laki julkisen hallinnon tietohallinnon ohjauksesta 634/2011	Tämän lain tarkoituksena on tehostaa julkisen hallinnon toimintaa sekä parantaa julkisia palveluja ja niiden saatavuutta säätämällä

	julkisen hallinnon tietohallinnon ohjauksesta ja tietojärjestelmien yhteentoimivuuden edistämisestä ja varmistamisesta. (1 §)
Laki kansainvälisistä tietoturvallisuusvelvoitteista 588/2004	1. kansainvälisellä tietoturvallisuusvelvoitteella sellaista Suomea sitovaan kansainväliseen sopimukseen sisältyvää määräystä sekä sellaista muuta Suomea koskevaa velvoitetta, jota Suomen on noudatettava ja joka koskee erityissuojattavan aineiston suojaamiseksi tarvittavia toimenpiteitä; 2. erityissuojattavalla tietoaineistolla sellaisia salassa pidettäviä asiakirjoja ja materiaaleja sekä asiakirjoista ja materiaaleista saatavissa olevia tietoja sekä näiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka kansainvälisen tietoturvallisuusvelvoitteen mukaisesti on turvallisuusluokiteltu; 3. turvallisuusluokitellulla sopimuksella sopimusta, jonka toisen valtion viranomainen tai siellä kotipaikkaansa pitävä yritys taikka kansainvälinen järjestö tai toimielin aikoo tehdä tai on tehnyt kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitetulla tavalla Suomessa kotipaikkaansa pitävän elinkeinonharjoittajan kanssa, jos tarjouskilpailuun osallistuminen tai sopimuksen toteuttaminen voi edellyttää pääsyä erityissuojattavaan tietoaineistoon. (2 §)
Laki potilaan asemasta ja oikeuksista 785/1992	Potilaan asemaan ja oikeuksiin terveyden- ja sairaanhoitoa järjestettäessä sovelletaan tätä lakia, jollei muussa laissa toisin säädetä.
Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista 22.9.2000/812	Tämän lain tarkoituksena on edistää asiakaslähtöisyyttä ja asiakassuhteen luottamuksellisuutta sekä asiakkaan oikeutta hyvään palveluun ja kohteluun sosiaalihuollossa.
Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007	Tämän lain tarkoituksena on edistää sosiaali- ja terveydenhuollon asiakastietojen tietoturvallista sähköistä käsittelyä. Lailla toteutetaan yhtenäinen sähköinen potilastietojen käsittely- ja arkistointijärjestelmä terveydenhuollon palvelujen tuottamiseksi potilasturvallisesti ja tehokkaasti sekä potilaan tiedonsaantimahdollisuuksien edistämiseksi. (1§) Tässä laissa säädetään sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. Tätä lakia sovelletaan julkisten ja yksityisten sosiaalihuollon ja terveydenhuollon palvelujen antajien järjestäessä taikka toteuttaessa sosiaalihuoltoa tai terveydenhuoltoa (2 §).
Laki sähköisestä asioinnista viranomaistoiminnassa 13/2003	Tämän lain tarkoituksena on lisätä asioinnin sujuvuutta ja joutuisuutta samoin kuin tietoturvallisuutta hallinnossa, tuomioistuimissa ja muissa lainkäyttöelimissä sekä ulosotossa edistämällä sähköisten tiedonsiirtomenetelmien käyttöä. Laissa säädetään viranomaisten ja näiden asiakkaiden oikeuksista, velvollisuuksista ja vastuista sähköisessä asioinnissa. (1 §)
Laki sähköisestä lääkemääräyksestä 61/2007	Jollei tästä laista muuta johdu, sähköistä lääkemääräystä laadittaessa, toimitettaessa ja käsiteltäessä on noudatettava, mitä muualla säädetään potilaan asemasta ja oikeuksista, lääkkeen määräämisestä ja toimittamisesta, henkilötietojen käsittelystä,

	viranomaisten toiminnan julkisuudesta, sähköisestä viestinnästä ja asioinnista sekä sähköisistä allekirjoituksista. (2 §, 3. kappale)
Laki tietoyhteiskunnan palvelujen tarjoamisesta 458/2002	Tässä laissa säädetään tietoyhteiskunnan palvelujen tarjoamiseen liittyvistä seikoista, erityisesti palvelujen tarjoamisen vapaudesta, palvelun tarjoajien velvollisuudesta antaa tietoja, sopimusta koskevien muotovaatimusten täyttämisestä sähköisesti sekä välittäjänä toimivien palvelun tarjoajien vastuuvapaudesta. (1 §)
Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 617/2009	Tässä laissa säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä niihin liittyvien palveluiden tarjoamisesta niitä käyttäville palveluntarjoajille ja yleisölle. (1 §)
Laki viranomaisten toiminnan julkisuudesta 621/1999	Laissa säädettyjen tiedonsaantioikeuksien ja viranomaisten velvollisuuksien tarkoituksena on toteuttaa avoimuutta ja hyvää tiedonhallintatapaa viranomaisten toiminnassa sekä antaa yksilöille ja yhteisöille mahdollisuus valvoa julkisen vallan ja julkisten varojen käyttöä, muodostaa vapaasti mielipiteensä sekä vaikuttaa julkisen vallan käyttöön ja valvoa oikeuksiaan ja etujaan. (3 §)
Laki yksityisyyden suojasta työelämässä 759/2004	Tämän lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä. (1 §) Tässä laissa säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä testeistä ja tarkastuksista sekä niitä koskevista vaatimuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin hakemisesta ja avaamisesta. Mitä tässä laissa säädetään työntekijästä, sovelletaan myös virkamieheen, virkasuhteessa olevaan ja näihin verrattavassa julkisoikeudellisessa palvelussuhteessa olevaan sekä soveltuvin osin työnhakijaan. (2 §)
Rikoslaki 39/1889	34 luku, 9 a § Vaaran aiheuttaminen tietojenkäsittelylle 38 luku, Tieto- ja viestintärikoksista
Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 30.3.2009/298	Tätä asetusta sovelletaan potilaan hoidon järjestämisessä ja toteuttamisessa käytettävien asiakirjojen laatimiseen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämiseen. (2 §)
Suomen perustuslaki 731/1999	Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. (10 §)
Sähköisen viestinnän tietosuojalaki 516/2004	Lain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä. (1 §)
Terveydenhuoltolaki 1326/2010	Käytettäessä toisen terveydenhuollon toimintayksikön tietoja tietojärjestelmien välityksellä, on potilastietojen käyttöä seurattava sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetun lain (159/2007) 5 §:n edellyttämällä tavalla. Hoitosuhde potilaan ja luovutuspyynnön tekijän välillä on varmistettava tietoteknisesti. (9 §, 4 kappale)

	Sairaanhoitopiirin kuntayhtymän on vastattava yhteisen potilastietorekisterin edellyttämistä koordinointitehtävistä sekä huolehdittava siitä, että tietojärjestelmien välityksellä tapahtuvissa tietojen luovutuksissa noudatetaan 2 ja 3 momentissa säädettyjä velvoitteita. Kukin terveydenhuollon toimintayksikkö vastaa omassa toiminnassaan syntyneiden potilasasiakirjojen rekisterinpidosta henkilötietolain (523/1999) mukaisesti. (9 §, 5 kappale)

Yhteistyöryhmä, § 24,16.10.2018
Kunnanhallitus, § 189, 22.10.2018