

Tietosuojapolitiikka

Kunnanhallitus 21.5.2018

Sisällys

Johdanto	3
Tietojen hankinta ja käsittely	3
Tietosuojan tavoitteet ja periaatteet	4
Asianhallinta	4
Rekisteröidyistä muodostetut tietoryhmät	5
Tietojen luovuttaminen asiakkaille	5
Yhteistyö eri intressiryhmien ja viranomaisten kanssa	5
Kansainvälisyys	5
Tietosuoja valvoa viranomainen	6
Tietosuojaperiaatteiden päivittäminen	6
Liitteet	6
Liite 1 Tietosuojarikkomusten seuraamustaulukko	10
Liite 2 Keskeiset käsitteet	7
Liite 3 Tietosuojavastuut	11

Johdanto

Tietosuojapolitiikan tarkoitus Pyhtään kunnassa on määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Pyhtään kunnan tietosuojan toteuttamisessa ja kehittämisessä. Henkilötiedot ovat tärkeässä roolissa Pyhtään kunnassa. Tietosuojan tavoitteena on turvata kuntalaisten, asiakkaiden ja muiden sidosryhmien henkilötiedot. Pyhtään kunta käsittelee henkilötietoja EU:n tietosuoja-asetuksen (GDPR) mukaisesti ja luottamuksellisesti.

Pyhtään kunnan tahtotila on saavuttaa laaja digitalisaatio-aste vuoden 2019 aikana. Kustannustehokas digitalisointi edellyttää tietoturvallisuuden kaikkien osa-alueiden huomioimisen lisäksi myös tietosuojan huomioimista jo suunnitteluvaiheessa.

Kunnan tietosuojapolitiikka ja tietosuojaselosteet ovat saatavilla kaikille kuntalaisille kunnan Internet-sivuilla. Tällä halutaan varmistaa avoimuus ja vahvistaa luottamusta kunnan asukkaita ja muita sidosryhmiä kohtaan.

Tietosuojapolitiikka koskee koko kuntaorganisaatiota ja sen henkilöstöä mukaan lukien kuntakonsernin sekä niitä Pyhtään kunnan sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Pyhtään kunnan omistamaa tai hallinnoimaa tietoa. Poliitiikka kattaa Pyhtään kunnan omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tietojen hankinta ja käsittely

Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Tämä tarkoittaa, että henkilötietojen käsittelyn on yhtäältä oltava asianmukaista ja toisaalta sen on aina tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Henkilötietojen suojalla tarkoitetaan myös jokaiselle turvattua oikeutta tutustua niihin tietoihin, joita hänestä on kerätty ja tarvittaessa myös saada hänestä kerätyt tiedot muutetuiksi tai poistetuiksi, mikäli tietojen oikaisu on tarpeen tai tietojen säilyttämiselle ei ole perustetta.

Pyhtään kunta käsittelee vain sellaista henkilötietoa, jolla on selkeä oikeusperuste. Perusteet käsitellä henkilötietoa ovat:

- henkilön suostumus
- sopimus
- lain vaatimus
- henkilön yleinen etu

Pääosa Pyhtään kunnan käsittelemistä henkilötiedoista liittyy lakisääteisten palveluiden tuottamiseen kunnan asukkaille ja muille sidosryhmille.

Tietojärjestelmät ja tietojärjestelmäpalvelut hankitaan ostopalveluina ja toimittaja vastaa tietojärjestelmien ja palveluiden tietoturvasta. Tietojärjestelmien keskitetty identiteetin- ja pääsynhallinta on tulossa vuoden 2018 aikana käyttöön.

Noudatamme hyviä tietosuojaperiaatteita läpi organisaation. Pyhtään kunnalla on tietosuojavastaava, joka vastaa tietosuojaperiaatteiden jalkauttamisesta. Tietosuojavastaava johtaa tietosuojaryhmää, jossa on Pyhtään kunnan keskeisimmät toimialueet edustettuina. Henkilöstön tietosuojaosaamista ylläpidetään tarpeen mukaan pidettävillä koulutuksilla.

Henkilötietoja käsittelevät kunnan palveluksessa olevat henkilöt sitoutuvat olemaan käyttämättä hyväkseen ja ilmaisematta sivullisille, mitä ovat saaneet tietoonsa työssään tai muutoin työnantajan tai asiakkaiden asioista. Työntekijä sitoutuu noudattamaan vaitiolovelvollisuutta allekirjoittamalla työsopimuksen.

Pyhtään kunta voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. Pyhtään kunnan ja erikseen valitun henkilötietojen käsittelijän välille laaditaan sopimus, joka on kirjallinen. Tietosuoja-asetuksen mukaan sopimuksessa tulee määritellä henkilötietojen käsittelyn kohde, tarkoitus ja kesto sekä sopia käsiteltävät henkilötiedot. Sopimuksen sisältö vaatimuksineen tulee määritellä mahdollisimman tarkasti.

Tietoturvan osalta Pyhtään kunnassa on laadittu erillinen tietoturvaohje, jossa on määritelty tarkemmin ohjeet tietojen käsittelystä. Tietojen käsittelyn tarkemmat kuvaukset on kuvattu rekisterien tietosuojaselosteissa.

Tietosuojan tavoitteet ja periaatteet

Pyhtään kunnan lähtökohtana tietosuojassa on riskilähtöisyys. Pyhtään kunta rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet. Tietosuojariskien hallinta on osa Pyhtään kunnan riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osi-
tusvelvollisuuden toteuttamista.

Pyhtään kunnan tavoitteena on huolehtia tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisesta dokumentoimalla ja ohjeistamalla henkilötietojen käsittelyn käytänteet sekä huolehtimalla käyttäjäkoulutuksesta toteuttaakseen laadukasta ja lainmukaista henkilötietojen käsittelyä.

Henkilötietojen käsittely toteutetaan noudattamalla alla lueteltuja periaatteita:

- henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä läpinäkyvästi
- henkilötietoja käsitellään suunnitellun käyttötarkoituksen mukaisesti
- henkilötietoja kerätään käyttötarkoituksen mukainen määrä, ei enempää
- henkilötietojen käsittely toteutetaan täsmällisesti
- henkilötietoja säilytetään käyttötarkoituksen kannalta tarkoituksenmukainen aika
- henkilötietojen käsittelyssä toteutetaan henkilötietojen eheyden ja luottamuksellisuuden periaatetta

Asianhallinta

Tietosuojan merkitys asianhallinnassa korostuu entisestään EU:n tietosuoja-asetuksen myötä. Asianhallinta tarkoittaa Pyhtään kunnan toimintaprosesseihin sisältyvien asioiden ja asiakirjojen käsittelyn ohjaamista niiden koko elinkaaren ajan. Asianhallinta pyrkii tehostamaan asioiden valmistelua, käsittelyä, päätöksentekoa, julkaisemista ja arkistointia sekä asiakirjamuodossa olevien tietojen (asiakirjalliset tiedot) hallintaa. Pyhtään kunnassa on käytössä Dynasty-asianhallintaohjelmisto, mistä on olemassa erillinen toimintatapaohje.

Asiakirjalliset tiedot ovat osa Pyhtään kunnan pääomaa, jolloin niiden laatuvaatimukset on turvattava, käsittelykäytännöt suunniteltava huolellisesti ja suojaaminen varmistettava. Asiakirjallisten tietojen laatuun liittyviä vaatimuksia ovat alkuperäisyyden, eheyden, luotettavuuden ja käytettävyyden takaaminen.

Tiedolla puolestaan tarkoitetaan eri muodoissa tallennettavaa, käsiteltävää tai siirrettävää tietoa. Tieto voi olla esimerkiksi yksittäisessä asiakirjassa, puheessa, sähköposti- tai tekstiviestissä, tietokannassa, tietokoneen tai matkapuhelimen muistissa, ääni- tai kuvanauhassa tai vaikkapa yksittäisen ihmisen muistissa. Tietoa on tarkasteltava tiedon koko elinkaaren ajalla, jolloin tietoturvanäkökulmasta merkittäviä käsittelyvaiheita ovat mm. tiedon luominen, käyttäminen, muuttaminen, tallettaminen, siirtäminen, jakelu, kopioiminen, arkistointi ja hävittäminen.

Rekisteröidyistä muodostetut tietoryhmät

Pyhtään kunnan käsittelemät tietoryhmät koostuvat seuraavista tiedoista:

- Asiakastiedot
- Henkilöstötiedot
- Yhdistys- ja yritystiedot
- Kiinteistötiedot

Henkilörekistereistä laaditaan tietosuojaselosteet. Selostetta käytetään kansalaisten perusoikeuksien, yleisen tiedonsaantioikeuden toteuttamiseksi ja rekisteröidyn informoimiseksi. Tietosuojaseloste laaditaan sekä jo käytössä olevista henkilörekistereistä että perustettavista rekistereistä. Selosteet pidetään julkisesti nähtävillä.

Tietojen luovuttaminen asiakkaille

Rekisteröidyllä on oikeus saada selville mitä tietoja hänestä on kerätty. Pyhtään kunta toimii tietojen luovuttamisessa tietosuojavaltuutetun toimiston ohjeiden mukaan. Rekisteröidyn tulee toimittaa tietopyyntö Pyhtään kunnanvirastolle ja todistaa samalla henkilöllisyytensä. Pyhtään kunta toimittaa keräämänsä henkilötiedot 30 päivän sisällä tietopyynnön vastaanottamisesta.

Yhteistyö eri intressiryhmien ja viranomaisten kanssa

Pyhtään kunta käsittelee tietoja seuraavien tahojen kanssa:

- Maistraatti
- VRK
- Poliisi
- Pelastustoimi
- Maanmittauslaitos
- Verohallinto
- Sosiaali- ja terveydenhuoltopalveluita tuottavat tahot
- Sopimuskumppanit (mm. talous-, henkilöstö- ja tietohallintopalveluita tuottavat yhtiöt)
- Lähialueen muut kunnat

Pyhtään kunta tekee yhteistyötä eri intressiryhmien ja viranomaisten kanssa EU-tietosuojasetuksen, kuntalainsäädännön ja erillislainsäädännön mukaisesti.

Kansainvälisyys

Pyhtään kunta ei toimita henkilötietoja EU-alueen ulkopuolelle.

Tietosuoja valvova viranomainen

Tietosuojavaltuutettu on viranomainen, joka ohjaa, neuvoo ja valvoo henkilötietojen käsittelyä henkilötietolain mukaisesti. Tietosuojavaltuutettu käyttää päätösvaltaa tarkastusoikeuden toteuttamista ja tiedon korjaamista koskevissa asioissa sekä antaa ratkaisuja rekisterinpidon lainmukaisuudesta ja rekisteröityjen oikeuksien toteutumisesta.

Henkilötietojen tietoturvaloukkauksen sattuessa Pyhtään kunnalla on rekisterinpitäjänä ilmoitusvelvollisuus valvontaviranomaisen sekä rekisteröidyn suuntaan. Valvontaviranomaiselle tehdään ilmoitus tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä.

Tietosuojaperiaatteiden päivittäminen

Tietosuojaperiaatteet ovat tämän hetken käytäntöme mukaiset. Päivitämme periaatteita säännöllisesti ja tiedotamme muutoksista yhteistyökumppaneillemme.

Rikkomukset ja seuraamukset

Tietosuojarikkomukset käsitellään tapauskohtaisesti ja mahdollisiin seuraamuksiin sovelletaan liitteissä olevaa tietosuojarikkomusten seuraamustaulukkoa (liite 1).

Liitteet

Liite 1 Keskeiset käsitteet

Liite 2 Tietosuojavastuut

Liite 3 Tietosuojarikkomusten seuraamustaulukko

Liite 2 Keskeiset käsitteet

Tietosuoja

Tietosuojalla tarkoitetaan toimenpiteitä, joiden tarkoituksena on suojata henkilön yksityisyys henkilötietojen käsitte-lyssä.

Tietoturva

Järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Tietoturvallisuus on riskienhallintaa ja osa yritysturvallisuutta.

Tietosuojapolitiikka

Johdon hyväksymä näkemys tietosuojan päämääristä, periaatteista ja toteutuksesta.

Henkilötieto

Kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot (esim. nimi, henkilötunnus, kuva, biometrinen tai geneettinen tieto). Tunnistettavissa olevana pidetään henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, sijaintitiedon, verkkotunnistetietojen tai yhden tai useamman henkilölle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

Henkilötietojen erityiset tietoryhmät, arkaluonteiset henkilötiedot

Tiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, geneettisiä tietoja, terveyttä koskevia tietoja, tai seksuaaliseen käyttäytymiseen liittyviä tietoja. Erityisiä tietoryhmiä koskeva käsittely on erikseen säänneltyä.

Henkilötietojen käsittelijä

Luonnollinen tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta.

Henkilötietojen käsittely

Kaikenlaiset toiminnot, joita kohdistetaan henkilötietoihin joko automaattista tietojenkäsittelyä hyödyntäen tai manuaalisesti. Käsittelyä ovat esimerkiksi henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen, haku, käyttö, luovuttaminen, levittäminen tai saattaminen muutoin saataville, yhteensovittaminen, yhdistäminen, rajoittaminen, poistaminen ja hävittäminen.

Henkilötietojen tietoturvaloukkaus

Tietoturvaloukkaus, jonka seurauksena on henkilötietojen lainvastainen käsittely. Loukkauksesta seuraa siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai saanti.

Osoitusvelvollisuus

Osoitusvelvollisuuden (accountability) avulla organisaation tulee kyetä osoittamaan, että se on huolehtinut seuraavista henkilötietojen käsittelyn osa-alueista:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen ja
- eheys ja luottamuksellisuus.

Rekisterinpitäjä

Luonnollinen tai oikeushenkilö, julkinen viranomainen, virasto tai muu elin, joka yksin tai yhteistyössä muiden kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Rekisteröity

Henkilö, jonka henkilötietoja käsitellään.

Tietosuojavastaava

Tietosuoja-asetuksen määrittelemä rooli, jonka rekisterinpitäjän ja henkilötiedon käsittelijän on nimettävä määrittelyissä tilanteissa:

- jos tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin (muu kuin tuomioistuin),
- ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät rekisteröityjen säännöllistä ja järjestelmällistä seuranta laajassa mitassa, tai
- ydintehtävät muodostuvat käsittelytoimista, jotka kohdistuvat henkilötietojen erityisiin tietoryhmiin, rikostuomioihin tai rikoksia koskeviin tietoihin.

Asetus määrittelee myös tietosuojavastaavan aseman ja toimenkuvan. Yritysryhmä voi nimittää yhden tietosuoja-vastaavan samoin kuin yksi tietosuojavastaava voidaan nimittää useampaa viranomaista tai julkishallinnon elintä varten.

Hallinnollinen sakko

Valvontaviranomainen voi määrätä rekisterinpitäjälle tai henkilötietojen käsittelijälle sakon tietosuoja-asetuksen vaatimusten laiminlyönnistä. Sakon suuruus määräytyy rikkomuksen luonteen perusteella. Sakon enimmäismäärä on 20 milj. € tai 4 % yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta.

Hallinnolliset seuraamukset

Valvontaviranomaisen määräämät seuraamukset koskien tietosuoja-asetuksen vaatimusten laiminlyöntejä.

Anonymisointi

Henkilötiedon tunnistettavuuden poistaminen siten, että yhdistäminen rekisteröityyn ei enää ole mahdollista.

Pseudonymisointi

Henkilötietojen käsittelemistä niin, että tietoja ei voida enää suoraan yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja. Tällaiset lisätiedot tulee säilyttää erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei tällaista yhdistämistä tunnistettuun tai tunnistettavissa olevaan henkilöön tapahdu.

Rekisteriseloste, tietosuoja seloste

Dokumentti, joka rekisterinpitäjän tulee laatia ja pitää yleisesti saatavilla. Sen tulee kuvata henkilötietojen käsittely tiiviisti esitettyinä, avoimessa ja helposti ymmärrettävässä muodossa.

Tietotilinpäätös

Tietotilinpäätös on organisaation laatima vapaaehtoinen raportti, joka antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta. Raportti on tarkoitettu johdon työkaluksi ja lisäämään sidosryhmien luottamusta siihen, että organisaatio noudattaa hyvää sääntelyn mukaista tietojenkäsittelytapaa henkilötietojen käsittelyssä. Tietotilinpäätöstä voidaan käyttää yhtenä keinona tietosuoja-asetuksen osoitusvelvollisuuden (accountability) toteuttamisessa.

Vaikutustenarviointi

Suunniteltujen henkilötietojen käsittelytoimien vaikutusten arviointi tietosuojaan ja yksilön vapauksiin. Jos käsittely todennäköisesti aiheuttaa yksilön oikeuksien ja vapauksien kannalta suuren riskin, rekisterinpitäjän on ennen käsittelytoimien aloittamista toteutettava tietosuojaan vaikutustenarviointi ja määriteltävä toimenpiteitä, joilla riskiä voidaan hallita. Valvontaviranomainen tulee julkaisemaan luettelon käsittelytoimista, jotka vaativat vaikutustenarvioinnin laatimisen.

Lapsen henkilötietojen käsittely

Alle 16-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman suostumusta. Jäsenvaltioilla on mahdollisuus soveltaa alemmaa ikärajaa, joka voi alimmillaan olla 13 vuotta.

Sisäänrakennettu ja oletusarvoinen tietosuojaja

Tietosuojaperiaatteiden sisällyttäminen aikaisessa vaiheessa henkilötietojen käsittelyn osaksi. Periaatteiden huomioiminen käsittelytapojen määrittelyyn ja itse käsittelyn yhteydessä, siten että varmistetaan käsittelyn vastaavuus tietosuojaja-asetuksen vaatimusten kanssa. Rekisterinpitäjän tulee toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt, jotta mm.

- oletusarvoisesti kerätään vain henkilötietoja, jotka ovat välttämättömiä ja tarpeellisia käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on tarpeellista kyseiseen tarkoitukseen
- henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville
- taataan rekisteröityjen oikeuksien toteutuminen

Tietosuojaja-asetuksen vaatimusten toteutuminen tulee taata määrittelyvaiheesta aina koko käsiteltävien henkilötietojen elinkaaren loppuun.

Liite 3 Tietosuojarikkomusten seuraamustaulukko

Teon tahallisuuden aste

R
i
k
k
o
m
u
k
s
e
n
v
a
k
a
v
u
u
s

	Tietämättömyys Osaamattomuus Huolimattomuus Vahinko Tahattomuus	Piittaamattomuus Törkeä huolimattomuus Välinpitämättömyys Tahallisuus Toistuvuus	Rikoksetarkoitus (vahingonteko, luvaton käyttö, vakoilu, salassapito-rikos, aseman/väärinkäyttö) Hyötymistarkoitus
Mahdollinen toimenpide			
Vakava rikkomus/rikos Potilastiedon tai liikesalaisuuden luvaton käsittely ja luovuttaminen Hakkerointi, tunkeutuminen Rikoslain alaisen materiaalin oikeudeton käsittely Tekijänoikeuslain alaisen materiaalin laiton levittäminen Virusten tahallinen levittäminen	Työnantaja käynnistää palvelussuhteen päättämisenettelyn Tutkintapyyntöä poliisille harkitaan Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämisenettelyn Tutkintapyyntö poliisille Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämisenettelyn Tutkintapyyntö poliisille
Rikkomus (vakava väärinkäyttö tai turvallisuuden vaarantaminen) Ohjelmien ja pelien luvaton kopiointi Luvattomien ohjelmien asentaminen Ylläpitäjän työkalujen luvaton hallussapito Palvelun luvaton pystytys Tunnuksen luovuttaminen Tiedon luottamuksellisuuden vaarantaminen	Kirjallinen varoitus Huomautus	Työnantaja käynnistää palvelussuhteen päättämisenettelyn Käyttöoikeuden peruminen Kirjallinen varoitus	Työnantaja käynnistää palvelussuhteen päättämisenettelyn Tutkintapyyntö poliisille Kirjallinen varoitus
Lievä rikkomus (väärinkäytös) Henkilökohtaisen tietoturvan laiminlyönti Epäasiallinen käyttö Haitan aiheuttaminen Resurssien tuhlaus Virustorjunnan laiminlyönti Luvaton kaupallinen tai poliittinen toiminta Kulunvalvontasääntöjen rikominen	Huomautus Opastus Puheeksi ottaminen	Kirjallinen varoitus Opastus Huomautus Puheeksi ottaminen	Tutkintapyyntöä poliisille harkitaan Kirjallinen varoitus

Liite 3 Tietosuojavastuut

Tietosuojavastuut Pyhtään kunnassa

Tämä dokumentti kuvaa tietosuojan vastuut ja velvollisuudet Pyhtään kunnassa.

Tietosuojan vastuujärjestelyn tulee seurata kunnan toiminnan mahdollisia muutoksia. Monet alla mainituista vastuista voivat kuulua samankin henkilön tehtäviin ja vastuisiin. Olennaista on, että näiden tehtävien hoito on järjestetty, myös varahenkilöiden osalta.

Yleinen vastuu tietosuojan valvonnasta ja ylläpitämisestä

Tietosuojan toteutumisen valvontaan ja ylläpitämiseen osallistuu jokainen kunnan henkilöstöön ja järjestelmien ja palveluiden käyttäjiin kuuluva osana omaa yleistä toimintavastuutaan.

Tietosuoja on osa työtehtäviä

Suurin osa tietosuojan toteuttamiseksi tehdystä työstä sisältyy Pyhtään kunnassa työskentelevien normaaleihin tehtäviin. Tietosuojan ohjaustehtävissä ja kehittämisessä tarvitaan sen lisäksi erityisasiantuntemusta ja nimettyjä vastuuhenkilöitä.

Tietosuojan vastuutaulukko

Rooli	Vastuu	Valvontavastuu
Kunnanhallitus	Tietosuojapolitiikan hyväksyminen	Tietosuojaryhmä
Kunnan johtoryhmä	Tietosuojapolitiikan käsittely Tietojen omistajien määrittäminen - yksikkökohtaisten erityisvaatimusten määrittäminen Tiedon ja tietojärjestelmien omistajien nimeäminen	Tietosuojaryhmä valvoo, että asia valmistellaan ja viedään päätöksentekoon.
Tietosuojaryhmä	Tietosuojapolitiikan valmistelu Tietosuojapolitiikan ylläpitäminen Tietosuojan hallinnointi, ohjeistus ja koordinointi Organisaation järjestelmien tietosuojan toteutumisen valvonta Organisaation tietosuojaan liittyvä tiedottaminen Tietosuojakoulutuksen suunnittelu Tietosuojatietämyksen hankkiminen ja ajan tasalla pitäminen sekä tietämyksen jakaminen Poikkeustilanteiden koordinointi Organisaation tietosuojaratkaisujen määrittäminen, kehittäminen ja muutoksien hyväksyminen Viestiä tietosuoja-asioista ja tietosuojapuutteiden ja poikkeamien käsittelyn käynnistämisestä Osallistua tietosuojaperiaatteiden määrittelyyn Avustaa johtoa ja yksiköitä tietosuoja-asioiden toimeenpanossa Tietosuojasuunnitelman valmistelu osana kunnan riskienhallintaa Tietosuojan mittariston valmistelu ja tietosuoja koskevan seurannan järjestäminen Raportointi ylimmälle johdolle tietosuojan tilanteesta Kunnan tietosuojaohjeiden- ja käytäntöjen kehittäminen, valmistelu ja muutosten hallinta Vastuu poikkeustilanteiden käsittelystä Organisaation tietosuojaratkaisujen ja niihin liittyvien ohjeiden määrittämisen ja kehittämisen valmistelu	Tietosuojavastaava

Tietosuojavastaava	Tietosuojaryhmän johtaminen Tietuoja-asioiden neuvonta ja opastus Tietuoja-asetuksen noudattamisen seuranta Yhteistyö valvontaviranomaisen kanssa	Kunnanhallitus
Tiedon omistaja	Tietojen luottamuksellisuuden ja käytettävyyden varmistaminen lakien, asetusten, tietosuojapolitiikan ja ohjeiden mukaisesti. Pääkäyttäjien nimeäminen vastuulla olevien järjestelmien osalta.	Ao. esimies
Henkilötietojen käsittelijä (ulkoistettu)	Henkilötietojen huolellinen käsitteleminen Pyhtään kunnan lukuun kirjallisen sopimuksen ja rekisterinpitäjän ohjeiden mukaisesti	Sopimuksen vastuuhenkilö(t)
Tietojärjestelmien omistajat	Käyttövaltuushallinnan määrittely, kuvaaminen ja ohjeistus	Ao. esimies
Vastuualueiden ja toimintayksiköiden esimiehet	Tietosuojaan toteutuminen alaisessaan toiminnassa	Johtoryhmä
Esimies	Tietosuojaan toteutumisen valvonta Tiedon omistajien määrittäminen johtamisjärjestelmän vastuiden mukaisesti Oman yksikkönsä tietosuojakoulutukseen osallistumisesta huolehtiminen Vastaa, että yksiköllä on sen oman toiminnan erityisvaatimukset huomioiden tarkennetut tietosuojatavoitteet ja periaatteet	Ao. esimies