



PUOLANGAN KUNNAN
TIETOTURVA- JA TIETOSUOJAPOLITIikka

Hyväksytty kunnanhallituksessa 04.09.2018

Sisällysluettelo

1. JOHDANTO	3
2. KÄSITTEET	3
Henkilörekisteri	3
Henkilötieto.....	3
Henkilötietojen käsittelijä	4
Henkilötietojen käsittely	4
Rekisterinpitäjä	4
Tietosuoja	4
Tietosuojavastaava.....	4
3. POLITIIKAN SOVELTAMINEN JA TAVOITE	5
4. ORGANISOINTI, VASTUUT JA TOIMIVALTUUDET	6
5. REKISTERÖITYJEN TIETOPYYNTÖPROSESSI	7
6. TIETOTURVA- JA TIETOSUOJAKOULUTUS JA -OHJEET	7
7. TIETOTURVALLISUUDESTA TIEDOTTAMINEN	7
8. TIETOTURVALLISUUDEN TOTEUTUMISEN VALVONTA	8
9. RIKKOMUKSET JA SEURAAMUKSET	8
10. LAIT JA SÄÄDÖKSET	8
Tietosuojaan liittyvä keskeinen lainsäädäntö.....	8

1. Johdanto

Tietoturvasta ja tietosuojasta huolehtiminen ovat keskeisiä osia Puolangan kunnan vastuullisista toimintaperiaatteista. Tietoturva- ja tietosuojapolitiikka tiivistävät keskeisimmät tietosuojaan liittyvät toimintatavat, periaatteet, toimivallat, valvonnan, vastuut ja seuraamusjärjestelmän, joita kunnassa noudatetaan asiakkaiden, työntekijöiden sekä muihin sidosryhmiin kuuluvien henkilöiden oikeuksien turvaamiseksi. Kunnan toiminnot ovat jatkuvasti entistä riippuvaisempaa ICT-teknologiasta ja – palveluista sekä niiden toimintavarmuudesta, joten niihin liittyviä riskejä pitää tunnistaa ja hallita aktiivisesti.

Kaikkien henkilöiden, jotka käsittelevät henkilötietoja Puolangan kunnassa tulee varmistua siitä, että henkilötietoja käsitellään aina laillisesti ja turvallisesti siten, että tietojen yksityisyys sekä edut ja oikeusturva ovat turvattuina. Kunnan tavoitteena on olla luotettava toimija sekä asiakkaille että muille sidosryhmille.

Tietoturva- ja tietosuojapolitiikan tietoturvaperiaatteet perustuvat kansallisiin, yleisiin ja toimialakohtaisiin tietoturvaan, henkilörekistereitä, hyvää tiedonhallintatapaa ja tiedon laatua ohjaaviin ja velvoittaviin säädöksiin, ohjeisiin ja standardeihin.

Tietoturva- ja tietosuojapolitiikka on laadittu ja tarkoitettu Puolangan kunnan henkilöstölle, luottamusmiehille ja kunnan tietoja sekä tietojärjestelmiä tai toimitiloja käyttäville muille henkilöille. Asiakirja on annettu henkilöstölle tiedoksi. Tämä on saatavilla myös asianhallintajärjestelmä Dynastyssä sekä Kuntien Yhteiset tiedostot Y-asemalta.

Tietoturva- ja tietosuojapolitiikka on voimassa toistaiseksi ja asiakirjaa päivitetään tarvittaessa. Päivitystarvetta seuraa hallintojohtaja sekä tietosuojavastaava. Asiakirja on julkinen ja se on saatavilla Puolangan kunnan internet-sivuilla.

2. Käsitteet

Henkilörekisteri

Henkilörekisteri on mikä tahansa jäseneltyä henkilötietoa sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein. Henkilörekisteri sisältää samaa käyttötarkoitusta varten henkilötietoja. Esim. jäsenrekisteri ja käyttäjärekisteri ovat henkilörekistereitä.

Henkilötieto

Henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen, käyttäjätunnuksen tms. taikka yhden tai useamman

hänelle tavanomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.

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

Henkilötietojen käsittelijä

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

Henkilötietojen 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.

Lapsen henkilötietojen käsittely

Alle 16-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman suostumusta.

Rekisterinpitäjä

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

Tietosuoja

Tietosuojalla tarkoitetaan kansalaisten yksityisyyden suojaamista, luottamuksen turvaamista sekä oikeuksien, etujen, vapauksien ja oikeusturvan turvaamista henkilötietoja käsiteltäessä. Tietojen ja tietojärjestelmien käyttöä seurataan ja väärinkäytöksiin puututaan.

Tietosuojavastaava

Nimetty henkilö, jonka tehtävänä on mm. seurata henkilötietojen käsittelyn lainmukaisuutta ja auttaa organisaatiota toteuttamaan lainsäädännön asettamat velvoitteet. Asema on itsenäinen ja riippumaton. Tietosuojavastaava raportoi suoraan rekisterinpitäjän ylimmälle johdolle, joka on päävastuussa henkilötietojen käsittelyn lainmukaisuudesta. Tietosuojavastaava voi tehtävänsä ohella suorittaa muita tehtäviä, mutta nämä tehtävät eivät saa aiheuttaa intressiristiriitoja.

Tietoturva

Tietoturva tarkoittaa tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi sekä normaali- että poikkeusoloissa.

Tietoturvan tavoitteena on varmistaa tiedon

- Luottamuksellisuus
 - ✓ Tieto on vain tietoon oikeutettujen käyttäjien ja tietojärjestelmien käytettävissä sovitulla tavalla ja sovittuun aikaan
 - ✓ Tietoa ei paljasteta tai muutoin saateta sivullisten tietoon
- Eheys
 - ✓ Tieto on koko elinkaaren ajan luotettavaa, oikeellista ja ajantasaista
 - ✓ Tieto ei pääse muuttumaan tahallisesti tai tahattomasti, eikä se voi muuttua laitteistosta tai ohjelmistosta johtuvan vian tai teknisen häiriön seurauksena
- Käytettävyys
 - ✓ Tiedon, tietojärjestelmän tai palvelun tulee olla siihen oikeutettujen henkilöiden ja tietojärjestelmien satavilla sekä käytettävissä silloin kun sitä tarvitaan.
- Kiistämättömyys
 - ✓ Tietoon kohdistuvat käsittelytoimenpiteet suoritetaan siten, että käsittelyn osapuolet voidaan aina yksiselitteisesti tunnistaa sekä toimenpiteiden aikana että jälkikäteen koko tiedon elinkaaren aikana.

3. Poliitiikan soveltaminen ja tavoite

Puolangan kunnan tietoturva- ja tietosuojapolitiikkaa sovelletaan kaikissa kunnan toiminnoissa.

Yksityisyydensuoja ja henkilötietojen suoja on jokaisen perusoikeus. Puolangan 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.

Puolangan 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 ja tietoturvan 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.

Tietoturvan ja tietosuojan hallintamenetelmät kohdistuvat kaikkeen tietojenkäsittelyyn sekä manuaaliseen että sähköiseen ja pitävät sisällään myös puhutun ja kirjoitetun tiedon.

Hyvä tietoturva ja tietosuoja parantavat osaltaan Puolangan kunnan toiminnan tehokkuutta ja tuloksellisuutta.

4. Organisointi, vastuut ja toimivaltuudet

Puolangan kunta noudattaa lakeja ja asetuksia sekä kehittää toimintaansa vastaamaan voimaan tulevia toimialan viranomaissuosituksia.

Ylin vastuu tietoturva- ja tietosuojapolitiikasta on kunnanhallituksella, jonka tehtävänä on valvoa kokonaisturvallisuutta, riskienhallinnan ja sisäisen valvonnan toteutusta.

Hallintojohtajalla on vastuu koko kunnan teknisen ja hallinnollisen tietoturvan ja tietosuojan järjestämisestä, kehittämisestä ja seurannasta.

Osastopäälliköt vastaavat oman osastonsa vastuualueiden tietoturvaturvallisuuden ja tietosuojan toteutumisesta ja ohjeistuksesta. Esimiehet puolestaan vastaavat omista yksiköistään.

Jokaisen henkilörekisterin rekisterinpitäjä vastaa kyseisen henkilörekisterin osalta hyvän henkilötietojen käsittelytavan ja lainsäädännön edellyttämän korkean tietoturvan ja tietosuojan tasosta sekä rekisterin tietojen käsittelyyn liittyvistä linjauksista.

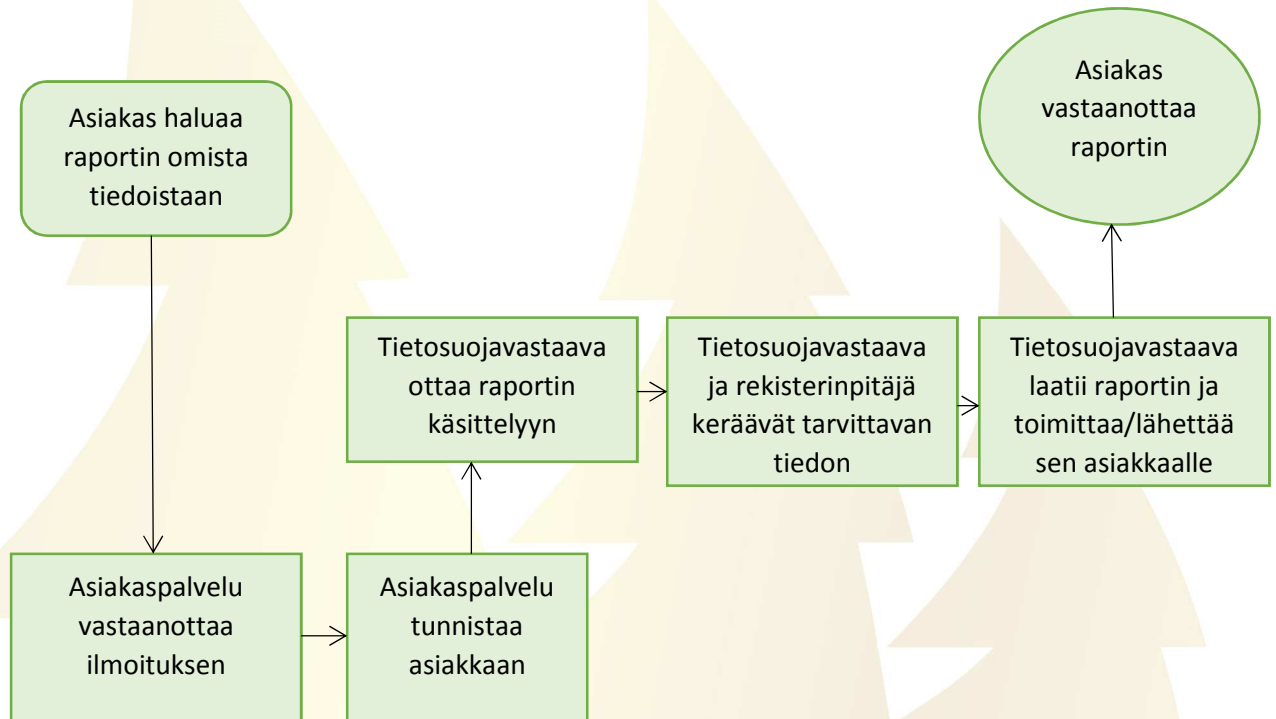
Tietojärjestelmien omistajalla on vastuu tietojärjestelmän toimintavarmuudesta ja dokumentoinnista sekä riskien hallinnasta.

Jokainen tietoja käsittelevä työntekijä, tietojärjestelmien ja sovellusten ylläpitäjä ja käyttäjä on vastuussa tietoturvallisuuden toteuttamisesta omalta osaltaan. He ovat velvollisia ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista ohjeistetulla tavalla. Henkilöstön tietoturva- ja tietosuojaosaamista ylläpidetään tiedottein ja koulutuksin.

Esimiesten tehtävänä on vastata siitä, että työntekijöillä on oikeudet tehtävän edellyttämässä laajuudessa tarvittaviin tietojärjestelmiin ja tietoihin. Esimiesten tehtävänä on ilmoittaa muutokset työtehtävissä, jotta voidaan huomioida käyttöoikeuksien tarpeellisuudet. Työsuhteen päättyessä käyttöoikeudet järjestelmistä poistetaan.

Tietosuojavastaavan tehtävänä on asiantuntijana auttaa ylintä johtoa veloitteittensa toteuttamisessa rekisterinpitäjänä. Osallistuu suunnittelutoimintaa, ohjeiden valmisteluun ja ylläpitoon sekä tietosuojakoulutuksen toteutukseen. Tietosuojavastaavan tehtävänä on seurata ja valvoa henkilötietojen käsittelyä ja suojausmenettelyä, tukea ja ohjata henkilökuntaa ja rekisteröityjä tietosuoja-asioissa, toimia yhdyssiteenä valvontaviranomaisiin sekä raportoida johdolle tietosuojan tilasta ja kehittämistarpeista. Tietosuojavastaavalla on oikeus suorittaa tehtävänsä ja niihin liittyvä suunnittelu, seuranta ja raportointi itsenäisesti.

5. Rekisteröityjen tietopyyntöprosessi



6. Tietoturva- ja tietosuojakoulutus ja – ohjeet

Esimiehet vastaavat siitä, että hänen alaisuudessaan oleva henkilöstö saa tehtäviensä hoitamiseen vastaavan perehdytyksen lisäksi tietoturva- ja tietosuojaohjeistuksen. Esimies varmistaa, että henkilöstö hallitsee tietoturvan ja tietosuojan perusteet käymällä asiaa läpi kehityskeskusteluissa.

Tietoturvaan ja tietosuojaan liittyvien ohjeiden sisällöstä ja ajantasaisuudesta vastaa tietosuojavastaava.

7. Tietoturvallisuudesta tiedottaminen

Tietoturva- ja tietosuoja-asioista tiedotetaan tarpeen mukaan. Tietoturva-asioiden sisäisestä tiedottamisesta vastaavat tietosuojavastaava yhdessä viestinnästä vastaavan tahon kanssa.

Tietoturva- ja tietosuoja-asioista ei aktiivisesti tiedoteta ulkopuolisille, mutta jos tiedottamistarvetta ilmenee, sen hoitaa tietosuojavastaava.

Henkilötietojen tietoturvaloukkauksen sattuessa Puolangan kunnalla on rekisteripitäjänä ilmoitusvelvollisuus valvontaviranomaiselle sekä rekisteröidylle. Ilmoituksen valvontaviranomaiselle tekee tietosuojavastaava tietosuoja-asetuksen mukaisesti 72 tunnin kuluessa siitä, kun henkilötietojen tietoturvaloukkaus on tullut ilmi. Rekisteröidylle henkilötietojen tietoturvaloukkaus ilmoitetaan ilman aiheetonta viivytystä.

8. Tietoturvallisuuden toteutumisen valvonta

Jokainen organisaation tietoja ja tietojärjestelmiä käyttävä on velvollinen ilmoittamaan havaitsemistaan tietoturvallisuuden puutteista, uhkista tai menettelyvirheistä kunnan tietosuojavastaavalle tai omalle esimiehelleen.

Tietoturvallisuudesta annettujen ohjeiden toteutumisesta vastaa kukin toimintayksikkö tai organisaatiolle palveluja tuottava yritys omalla vastuualueellaan. Esimiesten tulee valvoa, että henkilöstö noudattaa tietoturvasta ja tietosuojasta annettuja määräyksiä ja ohjeita. Esimiesten tulee raportoida tietosuojavastaavalle valvonnan tuloksista.

9. Rikkomukset ja seuraamukset

Jokainen Puolangan kunnan tietojenkäsittelyjärjestelmien käyttäjä on velvollinen noudattamaan hyväksytyjä käytösääntöjä ja tietoturvaohjeita.

Puolangan kunnan tietosuoja- ja tietoturvapolitiikkaa sekä siihen liittyviä ohjeita vastaan havaitut rikkomukset raportoidaan organisaation johdolle. Rikkomuksen tekijä saatetaan edesvastuuseen teostaan ja häntä vastaan ryhdytään rikkomuksen vaatimiin toimenpiteisiin.

10. Lait ja säädökset

Puolangan 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.

Tietosuojaan liittyvä keskeinen lainsäädäntö:

- EU:n yleinen tietosuoja-asetus (679/2016)
- Suomen perustuslaki (731/1999)
- Hallintolaki (434/2003)
- Hallintolainkäyttölaki (586/1996)
- 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)
- 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)