Seinäjoki

Seinäjoen kaupungin tietosuojapolitiikka

Kh 4.11.2024, § 279

Sisällys

Johdanto

Tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut, valvonnan ja seuraamusjärjestelmän, joita noudatetaan Seinäjoen kaupungin tietosuojan toteuttamisessa ja kehittämisessä. Tämä tietosuojapolitiikka koskee niiden henkilötietojen käsittelyä, jossa Seinäjoen kaupunki toimii rekisterinpitäjänä.

Seinäjoen kaupungin vuoteen 2029 ulottuvassa strategiassa turvallinen kaupunki on nostettu teemana vahvasti esiin. Seinäjoki haluaa tarjota niin kuntalaisille, yrityksille kuin kaupunkia kehittämässä oleville muille kumppaneille arjen sujuvuutta. Digiälykäs Seinäjoki nojaa vahvasti palvelutuotannossaan sujuviin nykyaikaisiin ICT-ratkaisuihin, ajantasaiseen tietoon ja sen tietoturvalliseen käsittelyyn sekä tietoturvallisiin toimintamalleihin. Palvelutuotannon nojautuessa yhä enemmän digitalisaatioon, korostuu henkilötiedon tietosuojan tärkeys entisestään.

Tietosuojaosaamisella voidaan lisätä organisaation tuottavuutta ja tehokkuutta sekä säästää kustannuksia. EU:n yleisen tietosuoja-asetuksen sekä muun tietosuojalainsäädännön myötä tietosuojasta, tietosuojatyön organisoinnista ja itse tietosuojatyöstä, sekä koko henkilöstön tietosuojaosaamisesta on tullut organisaatioiden operatiivisen toiminnan menestystekijä.

Tekoälyn hyödyntäminen on organisaatioissa voimakkaassa kasvussa. Tekoäly luo mahdollisuuden entisestään tehostaa toimintaa, mutta aiheuttaa myös erityisesti henkilötietojen käyttöön tietosuojaa koskevia uhkia, jotka on huomioitava tekoälypalveluita käyttöönottaessa. Seinäjoen kaupunki huolehtii myös tekoälyn käyttöön liittyvästä tietosuojan toteutumisesta riittävin ohjeistuksin ja periaattein.

Seinäjoen kaupungin johto tietosuojatoiminnan omistajana määrittelee tässä tietosuojapolitiikassa johtamiseen, palveluihin ja toimintoihin liittyvät tietosuojaperiaatteet, vastuut ja tavoitteet. Tietosuojapolitiikka toimii perustana Seinäjoen kaupungin tietosuojaa koskeville ohjeille, joiden tehtävänä on tarkentaa tietosuojapolitiikassa annettuja määräyksiä ja ohjeistaa niiden soveltamista käytäntöön.

Tietosuojapolitiikka koskee koko kaupunkiorganisaatiota ja sen henkilöstöä mukaan lukien kaupunkikonsernin sekä niitä Seinäjoen kaupungin sidosryhmien edustajia, jotka toimeksiantojensa puitteissa käsittelevät Seinäjoen kaupungin omistamaa tai hallinnoimaa tietoa. Tietosuojapolitiikka kattaa Seinäjoen kaupungin omistaman tiedon riippumatta sen esitystavasta, muodosta, suojaustasosta tai elinkaaren vaiheesta.

Tämä tietosuojapolitiikka on saatavissa asianhallintajärjestelmässä (LAARI), intranetissä (AALTONETTI) ja kaupungin internetsivulla. Tietosuojapolitiikka liitetään tarvittaessa Seinäjoen kaupungin toimeksianto- ja hankintasopimuksiin.

Tietoturvaa käsitellään tarkemmin Seinäjoen kaupungin tietoturvapolitiikassa.

Tietosuojan määritelmä

Tietosuojalla tarkoitetaan yksityisyyden suojaamista henkilötietoja käsiteltäessä. Oikeus henkilötietojen suojaan on jokaiselle kuuluva perusoikeus. Tämä tarkoittaa, että henkilötietojen käsittelyn on oltava asianmukaista ja 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.

Tietosuojan tavoitteet ja periaatteet

Seinäjoen kaupungin lähtökohtana tietosuojassa on riskilähtöisyys. Seinäjoen kaupunki rekisterinpitäjänä arvioi henkilötietojen käsittelyyn liittyvät riskit ja valitsee arvioidun riskitason mukaan tarvittavat hallintatoimenpiteet.

Tietosuojariskien hallinta on osa Seinäjoen kaupungin riskienhallintaprosessia, jolloin erityisesti merkittävän tason riskit raportoidaan johdolle saakka. Riskilähtöisyys ohjaa organisaation henkilötietojen käsittelyä ja on erittäin tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista. Riskienhallintaprosessin mukaisesti toimialat raportoivat tietosuojariskeistä hallintosäännössä määritellyille lautakunnille. Kaupunki- ja kaupunkikonsernitason raportointi tapahtuu kaupunginhallitukselle.

Ennen henkilötietoja sisältävien tietojärjestelmien käyttöönottoa on tehtävä vaikutustenarviointi ainakin silloin, kun henkilötietojen käsittelystä muodostuu merkittävä riski. Vaikutustenarvioinnin yhteydessä tietoturvaan liittyvät hallintakeinot on tunnistettava ja määritettävä. Seinäjoen kaupunki tekee vaikutustenarvioinnin kaikille uusille henkilötietoja sisältäville järjestelmille. Vaikutustenarviointi suoritetaan myös merkittävissä henkilötietoja sisältävien järjestelmien muutoksissa.

Seinäjoen kaupungin toiminnassa toteutetaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta. Tietosuoja otetaan huomioon monipuolisesti perustoiminnan yhteydessä mm. johtamisessa, hankinnoissa, kehitystyössä sekä toimintaprosesseissa. Tietosuojan oikeanlainen toteutuminen varmistetaan myös käyttämällä tilannekohtaisesti parhaita mahdollisia teknisiä ja organisatorisia riskiarvioon perustuvia ratkaisuja.

Seinäjoen kaupungin tavoitteena on huolehtia rekisteröityjen oikeuksien toteutumisesta dokumentoimalla ja ohjeistamalla henkilötietojen käsittelyn käytännöt sekä huolehtimalla käyttäjäkoulutuksesta toteuttaakseen laadukasta ja lainmukaista henkilötietojen käsittelyä.

Henkilötietojen käsittelyssä noudatetaan seuraavia tietosuojaperiaatteita kaikissa henkilötietojen käsittelyvaiheissa:

- henkilötietoja käsitellään lainmukaisesti, asianmukaisesti sekä rekisteröidyn kannalta läpinäkyvästi
- henkilötietoja kerätään vain tarpeellinen määrä henkilötietojen käsittelyn tarkoitukseen nähden
- henkilötietoja kerätään ja käsitellään tiettyä nimenomaista ja laillista tarkoitusta varten
- henkilötietojen käsitellään luottamuksellisesti ja turvallisesti
- henkilötietoja päivitetään aina tarvittaessa
- epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä
- henkilötiedot säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoituksen toteuttamista varten

Tietosuojatoimintaa ohjaavat tekijät

Seinäjoen kaupungin tietosuojatoimintaa velvoittavat ja ohjaavat yleiset lainsäädäntövelvoitteet sekä toimialakohtaiset erityislainsäädäntövelvoitteet. Lisäksi muut tietosuojaa ohjaavat velvoitteet, määräykset ja ohjeet kuten esimerkiksi toimittajien kanssa tehdyt tietosuojasopimukset. Lisäksi noudatetaan soveltuvin osin muuta tietosuojaa liittyvää ohjeistusta (Euroopan tietosuojaneuvoston ja Suomen tietosuojavaltuutetun ohjeet).

Seinäjoen kaupungin johdon tehtävänä on ohjata tietosuojatoiminnan kehittämistä strategisella tasolla yhdessä tietosuojasta vastaavien kanssa.

Tietosuojaan liittyvä organisointi ja vastuut

Seinäjoen kaupungin tietosuojaan liittyvät vastuut on kuvattu liitteessä 1.

Tietosuojavastuut Seinäjoen kaupungin ja keskeisten sidosryhmien ja yhteistyökumppaneiden osalta tulee kuvata ja sopia kirjallisesti. Sopimisesta vastaavat kyseisistä palveluista vastaavat henkilöt yhteistyössä tietosuoja- ja tietoturvatyöryhmän, tietohallinnon ja hankintapalveluiden kanssa.

Seinäjoen kaupunkikonsernin tietosuojapolitiikan ja sen muutokset hyväksyy kaupunginhallitus. Yksittäisten tietosuojaa koskevan ohjeistuksesta poikkeavan menettelyn hyväksyy tietosuoja- ja tietoturvatyöryhmä. Tietosuojaohjeistukset ja niiden muutokset hyväksyy tietosuoja- ja tietoturvatyöryhmä.

Tietosuojan hallintajärjestelmä

Tietosuojapolitiikka on osa Seinäjoen kaupungin tietoturvallisuuden ja tietosuojan hallintajärjestelmää. Hallintajärjestelmään kuuluvat kaikki tietoturvallisuuden ja tietosuojan hallintaan käytetyt toimintamallit, hallintakeinot ja dokumentit, joista

keskeisimmät on määritelty liitteessä 4.

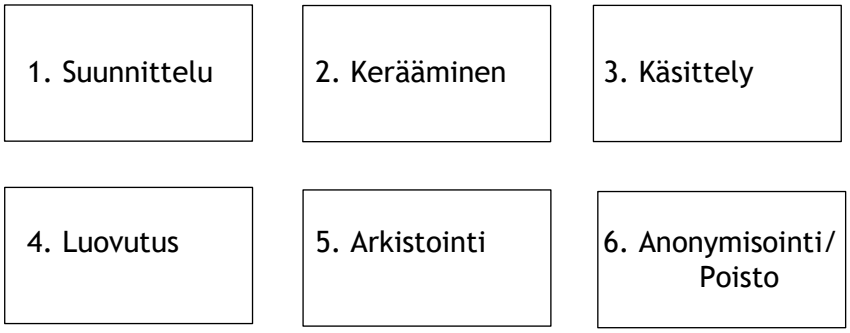
Tietosuojan toteuttaminen

Seinäjoen kaupunki toteuttaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta ja sisällyttää tietosuojaperiaatteet ja -vaatimukset jo aikaisessa vaiheessa osaksi henkilötietojen käsittelyä. Seinäjoen kaupunki toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet ja menettelyt tietosuojan varmistamiseksi.

Edellä mainittujen toimenpiteiden avulla varmistetaan mm, että:

- kerätään vain sellaisia henkilötietoja, jotka ovat välttämättömiä käsittelytarkoituksen kannalta
- tietoja ei kerätä eikä säilytetä suurempia määriä eikä kauemmin kuin on välttämätöntä kyseiseen käsittelytarkoitukseen
- henkilötietoja ei saateta rajoittamattoman henkilömäärän saataville
- taataan rekisteröityjen oikeuksien toteutuminen
- taataan henkilötietojen suoja tarvittavin tietoturvakeinoin
- tietosuojan toteuttamiseen liittyvät eri osapuolet tunnistavat vastuunsa

Tietosuojan toteuttamisessa Seinäjoen kaupunki haluaa varmistaa tietosuojalainsäädännön vaatimusten toteutumisen koko käsiteltävien henkilötietojen elinkaaren ajan.



Kuva: Henkilötietojen elinkaaren vaiheet

Seinäjoen kaupungin järjestelmä- ja sovelluskehitysprosesseissa on mukana työvaiheet, joissa analysoidaan henkilötietojen käyttötarkoituksiin sovellettavat tietosuojavaatimukset. Sovellettavat tietosuojavaatimukset vaihtelevat kerättävien henkilötietojen ja tietojen käyttötarkoituksen mukaan. Tekninen toteutus suunnitellaan siten, että se vastaa käsittelyn riskitasoa. Riskitason perusteella valitaan tilanteeseen sopivat hallintakeinot riskitason hallitsemiseksi ja vaatimustenmukaisuuden saavuttamiseksi. Hallintakeinojen valinnassa huomioidaan parhaat mahdolliset käytännöt tietoturvan suhteen.

Seinäjoen kaupunki voi rekisterinpitäjänä ulkoistaa valitsemansa osan henkilötietojen käsittelystä toimeksisaajalle, henkilötietojen käsittelijälle. Seinäjoen kaupunki valitsee sopimuskumppanikseen vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa asianmukaisten teknisten ja organisatoristen toimenpiteiden avulla sekä täyttävät tietosuojaan liittyvät lainsäädännölliset ja kaupungin asettamat vaatimukset ja pystyvät huolehtimaan rekisteröidyn oikeuksien toteutumisesta. Henkilötietojen käsittelyä sisältävien hankintojen kohdalla tietosuojaan liittyvät näkökohdat huomioidaan jo hankinnan suunnitteluvaiheessa ja saatetaan ne osaksi tarjouspyyntöä.

Seinäjoen kaupungin 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. Sopimuksiin liitetään myös tietosuojan toteuttamiseen liittyvät tietoturvaa koskevat vaatimukset.

Seinäjoen kaupungilla on erilliset ohjeet henkilötietojen käsittelyyn, jotka koskevat kaupungin omaa henkilöstöä sekä ulkoistettuja palveluntuottajia.

Rekisteröityjen tieto- ja oikaisupyynnöt

Seinäjoen kaupungissa rekisteröityjen tieto- ja oikaisupyynnöt käsitellään määritellyn toimintaprosessin mukaisesti. Kirjalliset tietopyynnöt käsitellään kunkin rekisterin määritellyn yhteyshenkilön toimesta. Pyynnöt tehdään ensisijaisesti Seinäjoen kaupungin verkkosivujen kautta (www.seinajoki.fi/tietosuoja) sähköisesti vahvasti tunnistautuen.

Henkilöstön tietosuojakoulutus

Seinäjoen kaupunki huolehtii henkilöstön riittävästä tietosuojaosaamisesta henkilöstökoulutuksien ja informaation välittämisen kautta. Myös organisaatioon tulevat uudet työntekijät perehdytetään tietosuoja-asioihin järjestelmällisesti. Erityisesti tämä korostuu niissä rooleissa, joissa käsitellään henkilötietoja ja toteutetaan rekisteröityjen oikeuksien toteuttamisprosesseja.

Toiminta tietoturva- ja tietosuojapoikkeamatilanteissa sekä ilmoitusvelvollisuus

Seinäjoen kaupungissa on määritetty toimintaprosessi ja ohje liittyen toimintaan tietoturvaloukkausten ja tietosuojapoikkeamien tapahtuessa. Tämän prosessin mukaista toimintatapaa noudatetaan ko. tilanteessa.

Kaupungin varautuminen häiriötilanteisiin ja poikkeusoloihin perustuu

lakisääteiseen valmiussuunnitteluun. Kaupungin palveluista vastaavat toimialat ja konsernipalvelut laativat kukin omat valmiussuunnitelmansa Seinäjoen kaupunginhallituksen hyväksymän valmiusohjeen mukaisesti. Suunnitelmat muodostavat yhdessä Seinäjoen kaupungin valmiussuunnitelman. Kaupungin varautumista johtaa kaupunginjohtaja yhdessä kaupunginhallituksen kanssa.

Seinäjoen on hyväksynyt ohjeen ”Sisäinen valvonta ja kokonaisvaltainen riskienhallinta Seinäjoen kaupungissa”. Ohjeessa on kuvattu eri toimijoiden tehtävät ja vastuut sisäisen valvonnan ja riskienhallinnan jatkuvassa prosessissa.

Seinäjoen kaupungin on rekisterinpitäjänä ilmoitettava henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle, jos siitä voi aiheutua riski luonnollisen henkilön oikeuksille tai vapauksille.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava valvontaviranomaiselle ilman aiheetonta viivästystä ja mahdollisuuksien mukaan 72 tunnin kuluessa siitä, kun Seinäjoen kaupunki rekisterinpitäjänä on tullut tietoiseksi tietoturvaloukkauksesta.

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava rekisteröidylle, jos se todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille. Asiasta on ilmoitettava rekisteröidylle ilman aiheetonta viivästystä, jotta hänellä on mahdollisuus suojata itseään. Ilmoitus rekisteröidylle henkilötietojen tietoturvaloukkauksesta voidaan jättää tekemättä vain tietosuoja-asetuksessa määritellyissä tilanteissa.

Rikkomukset ja seuraamukset

Tietosuojarikkomukset käsitellään tapauskohtaisesti ja mahdollisiin seuraamuksiin palvelussuhteessa oleville sovelletaan Liitteen 3 mukaista tietosuoja- ja tietoturvarikkomusten seuraamustaulukkoa. Luottamushenkilöiden tekemien tietosuojarikkomuksien seuraamukset määräytyvät kuntalain (410/ 2015) ja muun lainsäädännön mukaisesti.

Liitteet

Liite 1 Tietosuojavastuut
Liite 2 Keskeiset käsitteet
Liite 3 Tietosuoja- ja tietoturva rikkomusten seuraamustaulukko
Liite 4 Tietoturvallisuuden ja – suojan hallintajärjestelmä

Liite 1 Tietosuojavastuut

Tämä dokumentti kuvaa tietosuojan vastuut ja velvollisuudet Seinäjoen kaupungissa. Tietosuojan vastuujärjestelyn tulee seurata kaupungin toiminnan mahdollisia muutoksia.

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

Suurin osa tietosuojan toteuttamiseksi tehdystä työstä sisältyy Seinäjoen kaupungissa työskentelevien normaaleihin tehtäviin. Tietosuojan ohjaustehtävissä ja kehittämisessä tarvitaan sen lisäksi erityis- asiantuntemusta ja nimettyjä vastuuhenkilöitä.

Tietosuojan vastuutaulukko

VASTUUTAHO	TEHTÄVÄ
Kaupunginhallitus	• Tietosuojapolitiikan hyväksyminen • Valmiussuunnitelman hyväksyminen
Kaupunginjohtaja	• Nimeää tietosuoja- ja tietoturvatyöryhmän sekä tietosuojavastaavat • Valmiussuunnitelmissa määriteltyjen vakavien poikkeus- ja häiriötilanteiden johtaminen
Kaupungin johtoryhmä/ toimialojen johto	• Tietojen turvaluokittelujärjestelmä • Tiedon ja tietojärjestelmien omistajien nimeäminen • Tietosuojan toteutumisen valvonta • Tietosuojan hallintaprosessien hyväksyminen • Tietosuojapolitiikan ja riskienhallinnan sekä valmiussuunnittelun yhteensovittaminen • Tietosuojan poikkeustilanteiden prosessien hyväksyminen • Valmiussuunnitelmissa määriteltyjen vakavien poikkeus- ja häiriötilanteiden johtoryhmätoiminta
Hallintojohtaja	• Tietosuoja- ja tietoturvatyöryhmän johtaminen • Tietosuojaa koskevien asioiden raportointi ja valmistelu kaupungin johtoryhmälle ja hallitukselle • Poikkeustilanteiden koordinointi

Tietosuoja- ja tietoturvatyöryhmä	• Tietosuojapolitiikan valmistelu ja ylläpito • Tietosuoja-asioiden tiedottaminen • Avustaa osaltaan johtoa ja yksiköitä tietosuoja-asioiden toimeenpanossa • Tietosuojaohjeistuksista poikkeavien menettelytapojen hyväksyminen • Tietosuojan toteutumisen valvonnan suunnittelu ja seurannan järjestäminen • Tietosuojaohjeiden- ja käytäntöjen kehittäminen, valmistelu ja muutosten hallinta • Tietosuojan hallintaprosessien suunnittelu ja valmistelu • Tietosuojan poikkeustilanteiden prosessien suunnittelu ja valmistelu • Tietosuojaan liittyvien koulutuksiin liittyvät linjaukset
Tietosuojavastaavat	• Tietosuoja-asioiden neuvonta ja opastus • Tietosuojasääntöjen noudattamisen seuranta • Vaikutusten arviointeihin liittyvä neuvonta • Yhteistyö valvontaviranomaisen kanssa • Tietosuojakoulutuksen suunnittelu, organisointi ja toteuttaminen • Yhteyshenkilönä toimiminen rekisteröidyille • Tietosuoja- ja tietoturvatyöryhmän toimintaan osallistuminen
Tietohallinnon ohjausryhmä	• Organisaation tietosuojaan liittyvien teknisten hankkeiden hyväksyminen
Tietohallinto	• Teknisten tietosuojaan liittyvien hankkeiden määrittäminen ja kehittäminen • Tietosuojaan liittyvien asioiden huomioiminen järjestelmien hankinnassa ja teknisissä muutoksissa • Tietosuoja-asioista viestiminen osaltaan • Avustaa yksiköitä ja johtoa tietosuoja-asioiden toimeenpanossa teknisesti • Vaikutustenarviointien tietoturvaan liittyvä asiantuntijatuki tietojärjestelmän omistajalle
Tiedon omistaja	• Tietosuojan varmistaminen tiedon koko elinkaaren ajan lakien, asetusten, tietoturva- ja tietosuojapolitiikan ja ohjeiden mukaisesti.

Tietojärjestelmien omistajat	• Käyttövaltuushallinnan määrittely, kuvaaminen, toteutus ja ohjeistus • Tietojärjestelmän käytönaikainen tietoturvallisuus. • Pääkäyttäjien nimeäminen vastuullaan olevien järjestelmien osalta.
Tiedon käsittelijä	• Tiedon huolellinen käsitteleminen ja ohjeiden noudattaminen
Henkilötiedon käsittelijä (ulkoinen	• Henkilötietojen huolellinen käsitteleminen Seinäjoen kaupungin lukuun kirjallisen sopimuksen ja rekisterinpitäjän ohjeiden mukaisesti • Järjestelmäkohtaisten sopimusten ja ohjeiden mukainen tietoturvan hallintakeinojen toteuttaminen ja toimintatapojen noudattaminen
Tulosalueen johtajat / esihenkilöt	• Tietosuojan toteutuminen oman organisatorisen vastuu-alueensa osalta • Tiedonantovelvoitteen noudattaminen omalla vastuu-alueella • Yksikkökohtaisten erityisvaatimusten määrittäminen • Käyttövaltuushallinnan organisoiminen • Oman yksikkönsä tietosuojakoulutukseen osallistumisesta huolehtiminen • Vastaa, että yksiköllä on sen oman toiminnan erityisvaatimukset huomioiden tarkennetut tietosuojatavoitteet ja periaatteet • Raportoi tietosuojaa koskevista asioista annetun ohjeistuksen mukaisesti esihenkilöään, tietosuojavastaavaa sekä tietohallintoa. • Kriisiviestintäohjeen mukainen viestintävastuu yhdessä viestintäpäällikön kanssa oman toimialan osalta
Konsernin tytäryhtiöiden johtajat	• Oman liikelaitoksen tai yhtiönsä tietosuojatyön johtaminen ja organisointi konserniohjeistuksen mukaisesti

Liite 2 Keskeiset käsitteet

Tietosuoja
Tietosuojalla tarkoitetaan toimenpiteitä, joiden tarkoituksena on suojata henkilön yksityisyys henkilötietojen käsittelyssä.

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 määritellyissä tilanteissa:

- jos tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin (muu kuin tuomioistuin),
- ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät rekisteröityjen säännöllistä ja järjestelmällistä seurantaa 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.

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.

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 tietosuojan vaikutustenarviointi ja määriteltävä toimenpiteitä, joilla riskiä voidaan hallita.

Lapsen henkilötietojen käsittely
Alle 13-vuotiaiden lasten henkilötietojen käsittely ei ole sallittua ilman vanhemman suostumusta. Lapsen henkilötietoihin liittyvä ikäraja on määritelty Suomessa tietosuojalaissa.

Sisäänrakennettu ja oletusarvoinen tietosuoja
Henkilötietojen käsittelijöillä on velvollisuus antaa rekisterinpitäjälle riittävät takeet siitä, että niiden puolesta suoritettava henkilötietojen käsittely on tietosuoja-asetuksen vaatimusten mukaista ja rekisteröityjen oikeuksien suojaaminen on varmistettu. Tämä merkitsee erityisesti sitä, että

- tietosuojaperiaatteet sisään rakennetaan rekisterinpitäjille tarjottaviin työkaluihin, tuotteisiin, sovelluksiin tai palveluihin
- työkalut, tuotteet, sovellukset tai palvelut takaavat oletusarvoisesti, että käsittely rajoittuu vain käsittelyn tarkoituksen kannalta tarpeellisiin henkilötietoihin. Käsittelyn rajaamisessa on huomioitava tiedon määrä, käsittelyn laajuus, tietojen säilytysaika ja tietojen käyttöön oikeutettujen henkilöiden lukumäärä.

Liite 3 tietosuoja- ja tietoturvarikkomusten seuraamukset

Tietosuoja- ja tietoturvarikkomusten seuraamukset

(palvelussuhteessa olevat)

RIKKOMUKSEN VAKAVUUS	**Lievä rikkomus (asiaton toiminta),** esim. *Henkilökohtaisen tietoturvan laiminlyönti *Epäasiallinen käytös *Haitan aiheuttaminen *Resurssien tuhlaus * Virustorjunnan laiminlyönti * Luvaton kaupallinen tai poliittinen toiminta *Kulunvalvontasääntöjen rikkominen	**Rikkomus (Vakava väärinkäyttö tai turvallisuuden vaarantaminen),** esim. * ohjelmien ja pelien luvaton käyttö * Luvattomien ohjelmien asentaminen * Ylläpitäjän työkalujen luvaton hallussapito * Palvelun luvaton pystytys * Tunnuksen luovuttaminen * Tiedon luottamuksellisuuden vaarantaminen	**Vakava Rikkomus/rikos (lain mukaan rikkomuksena tai rikoksena tuomittava teko)**, esim. * Henkilötietojen tai liikesalaisuuden luvaton käsittely ja luovuttaminen * Hakkerointi, tunkeutuminen * Rikoslain alaisen materiaalin oikeudeton käsittely * Tekijänoikeuslain alaisen materiaalin laiton levittäminen * Virusten tahallinen levittäminen
Teon arviointi	**Mahdolliset seuraamukset**		
Osaamattomuus **Huolimattomuus** **Tahattomuus**	Huomautus	Kirjallinen varoitus	Kirjallinen varoitus Tutkintapyyntöä poliisille harkitaan
Piittaamattomuus **Törkeä huolimattomuus** **Välinpitämättömyys** **Tahallisuus** **Toistuvuus**	Huomautus Kirjallinen varoitus	Kirjallinen varoitus Käyttöoikeuden peruminen Palvelussuhteen päättäminen	Kirjallinen varoitus Tutkintapyyntö poliisille Palvelussuhteen päättäminen
Rikoksentekotarkoitus (vahingonteko, luvaton käyttö, vakoilu, salassapitorikos, virka-aseman väärinkäyttö yms.) **Hyötymistarkoitus**	Kirjallinen varoitus Tutkintapyyntöä poliisille harkitaan Palvelusuhteen päättäminen	Tutkintapyyntö poliisille Palvelussuhteen päättäminen	Tutkintapyyntö poliisille Palvelussuhteen päättäminen

Liite 4 Tietoturvallisuuden ja tietosuojan hallintajärjestelmä

Seinäjoen kaupungin tietoturvallisuuden ja tietosuojan hallintajärjestelmään kuuluvat kaikki niiden hallintaan tarvittavat toimintamenetelmät, hallintakeinot ja dokumentit. Osa dokumenteista on turvaluokiteltuja.

Hallintajärjestelmään kuuluvia toimintamalleja ovat muun muassa:

- Tietosuoja- ja tietoturvatyöryhmän toiminta.
- Tietohallinnon ohjausryhmän toiminta.
- Tietohallinnon sisäiset toimintamallit ICT-palvelutuotannon tietoturvassa.
- Tietohallinnon ylläpitämä digitaalisen turvallisuuden tilannekuva.
- ICT-palveluiden toimittajien tietoturvaan liittyvät toimintamallit ja raportointi.
- Tietoturvapoikkeamien käsittely.
- Henkilötietojen tietosuojapoikkeamien ja -selvitysten käsittely.
- Poikkeamien lakisääteinen ilmoittaminen valvontaviranomaisille.
- Tietoturvan ja tietosuojan varhaisessa vaiheessa huomioiminen sopimuksissa, prosesseissa ja projekteissa.
- Tietoturvaan ja tietosuojaan liittyvien vaatimusten määrittely ICT-hankinnoissa.
- Tietoturva- ja tietosuojakoulutus.
- Tietoturvaan ja tietosuojaan liittyvien asioiden huomioiminen projektien, toimittajahallinnan ja organisaatioiden riskienhallinnassa.
- Omistajien ja/tai vastuuhenkilöiden määrittäminen tiedoille, tietojärjestelmille ja henkilörekistereille.
- Henkilötietoa sisältävien järjestelmien vaikutustenarvioinnit
- Tietoturvan ja tilannekuvan kannalta tärkeiden lokitietojen kerääminen, analysointi ja reagointi
- Tietojärjestelmien ylläpidossa huomioidaan tiedonhallintalain vaatimukset ja niihin liittyvät tiedonhallintalautakunnan suositukset.
- Seinäjoen kaupungin käyttövaltuusperiaatteiden noudattaminen ICT-ympäristön ja tietojärjestelmien käyttövaltuuksien hallinnassa.
- Vuosittaiset tietotilinpäätökset.

Hallintajärjestelmään liittyviä dokumentteja ovat muun muassa:

- Seinäjoen kaupungin tietoturvapolitiikka (tämä dokumentti)
- Seinäjoen kaupungin tietosuojapolitiikka
- Seinäjoen tietohallinnon sisäiset ohjeistusdokumentit ICT-palvelutuotannon toteuttamisessa
- Seinäjoen kaupungin pilviympäristöjä koskevat ohjeistukset
- Seinäjoen kaupungin tekoälypalveluihin liittyvät ohjeistukset
- Seinäjoen kaupungin tietoturvapoikkeamiin liittyvät ohjeistukset
- Seinäjoen kaupungin valmiussuunnitelmat liitteineen
- Ohje ”Sisäinen valvonta ja kokonaisvaltainen riskienhallinta Seinäjoen kaupungissa”
- Tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus
- Seinäjoen intranetin tietoturvaohjeistus sekä koulutusvideot
- Muut tietoturvaan ja tietosuojaan liittyvät määräykset, linjaukset, suunnitelmat sekä ohjeistus. Esimerkiksi:
  - Hallintosääntö
  - Henkilöstöhallinnon käsikirja
  - Kriisiviestintäohje
- Tietosuojaa koskevien henkilörekisterin käsittelytoimien selosteet sekä vaikutustenarvioinnit.