



Savonlinna

HENKILÖTIEDON KÄSITTELYN YLEISOHJE

Voimassa 1.6.2026 alkaen



Kaupunginhallitus 25.5.2026

SAVONLINNA.FI





Sisällys

1	Johdanto	3
2	Henkilötietojen käsittelyyn liittyvät roolit.....	4
3	Henkilötietojen käsittely	4
3.1	Mitä on henkilötieto ja henkilötiedon käsittely?.....	4
3.2	Tietosuojaperiaatteet	5
3.3	Erityiset henkilötietoryhmät ja henkilötunnuksen käsittely	6
3.4	Tietojen julkisuus, salassapito ja vaitiolovelvollisuus	6
3.5	Kuka saa käsitellä tietoja ja milloin?	7
3.6	Tietojen luovuttaminen	8
3.7	Henkilötiedon käsittely verkkotiedottamisessa.....	9
3.8	Henkilötietojen käsittely tekoälyjärjestelmissä	9
3.9	Miten käsittelen henkilötietoja oikein?.....	9
3.10	Mistä saan tukea?	10
4	Rekisterinpitäjän velvollisuudet	10
4.1	Riskien arviointi.....	10
4.2	Rekisteröidyn informointi.....	11
4.3	Seloste käsittelytoimista	11
4.4	Osoitusvelvollisuus.....	11
4.5	Käsittelijän toiminnan valvominen.....	12
4.6	Henkilötietojen tietoturvaloukkausten käsittely	12
5	Rekisteröidyn oikeudet.....	13
6	Liitteet	15
	Liite 1 Tietosuojan muistilista työntekijälle.....	15
	Liite 2 Tietosuojan muistilista esihenkilölle	16

1 JOHDANTO

EU:n yleisen tietosuoja-asetuksen (GDPR) tarkoituksena on suojella luonnollisen henkilön oikeuksia ja vapauksia henkilötietojen käsittelyssä. Sitä on sovellettu EU-tasoisesti kaikessa henkilötietojen käsittelyssä vuodesta 2018 lähtien. Kansallinen tietosuojalaki täsmentää ja täydentää yleistä tietosuoja-asetusta ja sen kansallista soveltamista. Lisäksi henkilötietojen käsittelystä säännellään Suomessa myös useissa erityislaeissa.

Miten tämä koskee organisaation työntekijöitä ja luottamushenkilöitä? On tärkeää, että lainsäädännön mukaiset velvoitteet huomioidaan kaikessa henkilötietojen käsittelyssä. Tietosuoja-asetus antaa rekisteröidylle täsmennettyjä oikeuksia ja toisaalta rekisterinpitäjälle ja henkilötietojen käsittelijälle velvollisuuksia.

Yksi keskeisistä velvollisuuksista on osoitusvelvollisuus. Rekisterinpitäjän tulee pystyä esimerkiksi erilaisin dokumentein, ohjein, koulutuksin, prosessikuvauksin osoittamaan, että se on huomionnut lainsäädännön asettamat velvollisuudet toiminnassaan.

Tietosuojavaltuutetun toimisto on kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista. Henkilötietojen virheellisestä käsittelystä voidaan antaa huomautus, varoitus tai käsittelykielto ja viime kädessä rekisterinpitäjä tai henkilötietojen käsittelijä voidaan velvoittaa maksamaan vahingonkorvauksia rekisteröidylle, mikäli tämän tietoja on käsitelty turhaan, virheellisesti tai jos tiedot päätyvät asiattomien saataville.

Tämä materiaali on tarkoitettu Savonlinnan kaupungin henkilökunnan ja luottamushenkilöiden käyttöön; avuksi henkilötietojen lainmukaiseen käsittelyyn ja rekisteröidyn oikeuksien toteuttamiseen. Tämä ohje ja sen liitteet korvaavat aiemmat, vuonna 2019 hyväksytyt henkilötiedon käsittelyn ohjeet.

Lisätietoja:

[EU:n tietosuoja-asetus](#)

[Tietosuojalaki](#)

[Tietosuojavaltuutetun toimisto](#)

2 HENKILÖTIETOJEN KÄSITTELYYN LIITTYVÄT ROOLIT

Rekisteri tarkoittaa rekisteröityjen henkilötiedoista koostuvaa tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. Käytännössä rekisteri voi siis koostua yhdestä tai useammasta, eri paikoissa sijaitsevasta ja eri muodossa olevasta tietolähteestä. **Loogisen rekisterin** käsite tarkoittaa sitä, että samaan käyttötarkoitukseen kerätyt henkilötiedot kuuluvat samaan henkilörekisteriin. Yhteen rekisteriin voi siis sisältyä monenlaisia ylläpitotapoja/järjestelmiä tai vaikkapa manuaalisesti tehtyjä listauksia ja Excel-raportteja, jotka kaikki liittyvät yhteen ja samaan tietojen käsittelytarkoitukseen.

Rekisterinpitäjällä tarkoitetaan sitä tahoaa, jonka käyttötarkoituksia varten tietoja kerätään. Rekisterinpitäjä määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot, ja vastaa käsittelyn lainmukaisuudesta. Rekisterinpitäjänä voi toimia luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin. Rekisterinpitäjyys voi määräytyä lainsäädännön perusteella joko suoraan tai epäsuorasti, tai se määritetään käsittelyä koskevien tosiseikkojen arvioinnin perusteella. Tämä tarkoittaa sitä, että rekisterinpitäjä on taho, joka tosiasiallisesti käyttää ratkaisevaa vaikutusvaltaa käsittelyn tarkoituksiin ja keinoihin nähden. Savonlinnan kaupungin hallintosäännössä on määritelty rekisterinpitäjyydet ja rekisterinpitäjän vastuut. Jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat **yhteisrekisterinpitäjiä**.

Henkilötietojen käsittelijä on taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Esimerkiksi sopimuskumppani tai palveluntuottaja voi olla henkilötietojen käsittelijä. Henkilötietojen käsittelijällä ei tarkoiteta rekisterinpitäjän alaisuudessa toimivia työntekijöitä, jotka käsittelevät henkilötietoja osana työtehtäviään.

Rekisteröidyllä tarkoitetaan sitä luonnollista henkilöä, jonka tietoja rekisterissä käsitellään. Se voi olla rekisteristä riippuen esimerkiksi asiakas, kuntalainen tai organisaation työntekijä.

Tietosuojavastaava on organisaation sisäinen asiantuntija, joka seuraa henkilötietojen käsittelyä ja auttaa tietosuojasäännösten noudattamisessa. Säännösten noudattaminen on rekisterinpitäjän vastuulla.

Tietosuojavaltuutettu on Suomen kansallinen valvontaviranomainen tietosuoja-asioissa. Tietosuojavaltuutettu valvoo henkilötietojen käsittelyn lainmukaisuutta ja tietosuojoikeuksien toteutumista.

3 HENKILÖTIETOJEN KÄSITTELY

3.1 Mitä on henkilötieto ja henkilötiedon käsittely?

Tietosuoja-asetuksen mukaan **henkilötietoa** on kaikki sellainen tieto, josta luonnollinen henkilö eli rekisteröity voidaan suoraan tai epäsuorasti tunnistaa. Tällaisia tunnistetietoja ovat esimerkiksi nimi, henkilötunnus, sijaintitieto, verkkotunnistetieto tai jokin fyysinen, fysiologinen, geneettinen, psyykinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä tai näiden tietojen yhdistelmä. Epäsuora tunnistaminen tarkoittaa sitä, että henkilö voidaan tunnistaa yhdistämällä tietoja useammasta lähteestä, esimerkiksi useammasta tietojärjestelmästä.

Henkilötiedon käsittelyllä puolestaan tarkoitetaan henkilötietoihin tai tietojoukkoihin liittyvää toimintaa, on se sitten automaattista, tietojärjestelmällä sähköisesti tapahtuvaa tai manuaalista käsittelyä, esimerkiksi tulostettujen asiakirjojen mapittamista. Tiedon käsittelyä on tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen tai asettaminen saataville, tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poisto tai tuhoaminen. Erityisesti tulee

huomioida, että myös tiedon katseleminen tai haku sähköisestä järjestelmästä on henkilötietojen käsittelyä.

Henkilötiedon käsittelyä on myös pääsyy mahdollistaminen henkilötietoon esimerkiksi silloin, kun henkilötiedon käsittely - palkanlaskenta, tukipalvelut tms. - ulkoistetaan rekisterinpitäjän ulkopuolelle ns. sopimuskumppanille. Käsittelyä on myös pelkästään tietojärjestelmässä tapahtuva, automatisoitu tiedon käsittely, jossa esimerkiksi arvioidaan henkilön piirteitä tai ominaisuuksia. Henkilötietojen käsittelysäännöt koskevat kaikenlaista henkilötietojen käsittelyä, olivatpa tiedot asiakkaiden, sopimuskumppaneiden tai oman henkilökunnan tietoja. Henkilötiedon käsittelyssä tulee myös muistaa lainmukainen käsittely koko tiedon elinkaaren ajan; tiedon käsittelyn suunnittelusta (käsittelyn oikeusperuste) tiedon lainmukaiseen hävittämiseen/arkistointiin saakka.

Henkilötietojen käsittelyn yhteydessä saatat törmätä **pseudonymisoinnin** ja **anonymisoinnin** käsitteisiin. Tietoja, joista henkilö on tunnistettavissa vain epäsuorasti, kutsutaan pseudonymisoiduiksi tiedoiksi. On tärkeää huomioida, että pseudonymisoitu tieto on edelleen henkilötieto ja siihen sovelletaan tietosuojaa-asetusta. Pseudonymisointi on siis ennen kaikkea tiedon suojaamistoimenpide, jota käytetään esim. tilanteissa, joissa yksilön tiedot korvataan jollain tunnisteella, mutta tunnisteiden avulla tiedot voidaan myöhemmin vielä palauttaa ja yhdistää luonnolliseen henkilöön. Anonymisoitujen henkilötietojen tunnistettavuus on poistettu siten, ettei rekisteröidyn tunnistaminen ole mahdollista edes yhdistämällä tiedot muualta saataviin tietoihin. Anonymisoituja tietoja käsitellään mm. tilasto- ja tutkimustarkoituksia varten. Tietosuojaa-asetus ei koske anonymisoituja henkilötietoja. Sekä tietojen pseudonymisoinnissa ja anonymisoinnissa tulee huolehtia siitä, että se tehdään sellaisella mallilla ja algoritmilla, johon ei liity haavoittuvuutta tai muuta mahdollisuutta palauttaa alkuperäiset tiedot.

3.2 Tietosuojaperiaatteet

Tietosuojaa-asetusta sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn. Henkilötietojen käsittelyyn liittyvää lainsäädäntöä on laajasti myös erityislainsäädännössä, joka luonnollisesti täytyy huomioida varsinaisen tietosuojalainsäädännön - tietosuojaa-asetuksen ja tietosuojalain - lisäksi.

Kaikissa henkilötiedon käsittelyn vaiheissa on noudatettava tietosuojaperiaatteita. Ne on otettava huomioon jo siinä vaiheessa, kun suunnitellaan henkilötietojen käsittelyä, esimerkiksi sisäisiä toimintamalleja tai palvelun hankkimista ulkopuolelta. Rekisterinpitäjän on myös pystyttävä osoittamaan, että tietosuojaperiaatteet toteutuvat tehokkaasti henkilötietojen käsittelyssä.

1. Henkilötietojen käsittely on oltava **lainmukaista, asianmukaista ja läpinäkyvää**. Käsittelylle on aina oltava lain mukainen peruste eikä henkilötietoja saa käyttää väärin. Lisäksi rekisteröidyille tulee kertoa siitä, miten heitä koskevia tietoja kerätään ja käytetään sekä missä määrin henkilötietoja käsitellään.
2. Henkilötietojen kerääminen on kytköksissä niiden käyttötarkoitukseen (**käyttötarkoitussidonnaisuus**). Tiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten eikä kerättyä tietoa saa käyttää myöhemmin muuhun tarkoitukseen ilman, että tämä uusi käyttötarkoitus on yhteensopiva alkuperäisen käyttötarkoituksen kanssa.
3. Henkilötietoja ei saa kerätä tai käsitellä laajemmin kuin on välttämätöntä käyttötarkoituksen kannalta (**tietojen minimointi**). Henkilötietojen on oltava asianmukaisia ja olennaisia, ja niiden käsittelyn pitää rajoittua vain tarpeelliseen.
4. Käsiteltävien henkilötietojen on oltava **täsmällisiä** ja päivitettyjä. Epätarkat ja virheelliset henkilötiedot on oikaistava tai poistettava viipymättä.
5. Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojen käyttötarkoitusten toteuttamista varten (**säilytyksen rajoittaminen**). Asiakirjojen arkistointia ja säilytysaikoja ohjaa kaupungin tiedonohjaussuunnitelma.

6. Henkilötietojen käsittelyn on oltava **luottamuksellista ja turvallista**. Tähän sisältyy suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Suojatoimien riittävyttä on punnittava suhteessa olosuhteisiin ja riskeihin.

3.3 Erityiset henkilötietoryhmät ja henkilötunnuksen käsittely

Henkilötietoja on erilaisia ja osaa tiedoista tulee käsitellä erityisen huolellisesti. Tietosuojasetuksessa on määritelty erityiset henkilötietoryhmät: etninen alkuperä, poliittinen mielipide, uskonnollinen tai filosofinen vakaumus, ammattiliiton jäsenyys, terveyttä koskevat tiedot, seksuaalista käyttäytymistä tai suuntautumista koskevat tiedot sekä geneettiset ja biometriset tiedot. Näitä tietoja on suojeltava erityisen tarkasti, koska niiden käsittely voi aiheuttaa huomattavia riskejä henkilön perusoikeuksille ja -vapauksille.

Erityisiin henkilötietoryhmiin liittyvien tietojen käsittely on lähtökohtaisesti kiellettyä ja sallittua vain erikseen määritellyissä tilanteissa, kuten

- rekisteröidyn antama nimenomainen suostumus
- rekisterinpitäjän tai rekisteröidyn veloitteiden ja erityisten oikeuksien noudattaminen työoikeuden, sosiaaliturvan ja sosiaalisen suojelun alalla siltä osin, kuin se sallitaan lainsäädännössä tai työehtosopimuksessa
- rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaaminen, kun rekisteröity on fyysisesti tai juridisesti estynyt antamasta suostumustaan
- käsittely on tarpeen tärkeää yleistä etua koskevasta syystä lainsäädännön nojalla
- käsittely on tarpeen ennalta ehkäisevää tai työterveydenhuoltoa koskevia tarkoituksia varten, työntekijän työkyvyn arvioimiseksi, lääketieteellisiä diagnooseja varten, terveys- tai sosiaalihuollollisen hoidon tai käsittelyn suorittamiseksi taikka terveys- tai sosiaalihuollon palvelujen ja järjestelmien hallintoa varten
- käsittely on tarpeen yleisen edun mukaista arkistointia, tieteellistä ja historiallista tutkimusta tai tilastointia varten lainsäädännön nojalla.

Henkilötunnusta saa käsitellä rekisteröidyn suostumuksella tai, jos käsittelystä säädetään laissa. Henkilötunnusta saa käsitellä, jos rekisteröidyn ja hänen henkilötietojensa yksiselitteinen erottaminen muista rekisteröidyistä ja heidän henkilötiedoistaan (yksilöiminen) on tärkeää esim. lakisääteisen tehtävän tai rekisteröidyn/rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi. Henkilötunnusta ei tule tarpeettomasti merkitä tulostettuihin tai laadittuihin asiakirjoihin. Rekisteröidyn henkilöllisyyden selvittämiseen (tunnistaminen) ei saa käyttää yksinomaan henkilötunnusta tai henkilötunnuksen ja rekisteröidyn nimen yhdistelmää.

3.4 Tietojen julkisuus, salassapito ja vaitiolovelvollisuus

Tärkeimmät organisaation toimintaa koskevat lait ovat

- **julkisuuslaki** eli laki viranomaisen toiminnan julkisuudesta (621/1999), joka määrittelee, mitkä viranomaisen asiakirjat ovat julkisia ja mitkä asiakirjat ja tiedot salassa pidettäviä sekä
- **hallintolaki** (434/2003), jossa määritellään hyvän hallinnon perusteet sekä asian käsittelystä ja oikaisuvaatimusmenettelystä
- **kuntalaki** (410/2015), jossa säännellään kunnan hallinnon toiminnasta ja talouden järjestämisestä.

Pääsääntöisesti kaikki viranomaiselle toimitetut asiakirjat ja tehdyt päätökset ovat julkisia. Valmisteluasiakirjojen osalta organisaatio voi käyttää harkintavaltaa tiedottamisen tai tietojen

luovuttamisen osalta. Sisäiset muistiot tai esimerkiksi omat muistiinpanot eivät ole julkisia, eivätkä siten kuulu lainkaan julkisuuslain piiriin.

Salassa pidettäviä asiakirjoja (julkisuuslain 24 §) ei saa näyttää tai luovuttaa eikä niiden sisällöstä saa keskustella ulkopuolisten kanssa. Yleisimmät salassa pidettävät asiat koskevat erityisiä henkilötietoryhmiä, sosiaali- ja terveystietoja ja näihin liittyvää asiakkuutta, oppilashuoltoa tai kunnan liike- ja ammattisalaisuuksia.

Vaitiolovelvollisuus koskee paitsi salassa pidettävää asiakirjaa, myös muuta tietoa, jonka henkilö - virkamies, työntekijä, harjoittelija jne. - saa tietoonsa työtehtäviä hoitaessaan. Jokaisen organisaation työntekijän tulee noudattaa organisaation henkilötiedon käsittelyn ohjeita sekä olemaan paljastamatta salassa pidettäviä tai muuten luottamuksellista tietoa ulkopuoliselle työsuhteen aikana tai sen jälkeen. Vaitiolovelvollisuudesta säädetään mm. julkisuuslaissa (23§) ja sen rikkomisesta on määritelty rangaistus rikoslaissa (luku 38).

Aina, kun käsittelet luottamuksellisia tai salaisia tietoja, huomioi

- ettei tällaisia tietoja sisältäviä tulosteita jää muiden näkyviin.
- tiedon tallennuspaikka - ettet erehdyksessä tallenna tietoa internetiin tai väärille levyasemille (esim. työaseman kiintolevyille).
- sähköpostiosoitteen tarkistus, ettei tieto joudu väärälle henkilölle.
- ettet keskustele asiasta niin, että tietoa paljastuu ulkopuolisille.

Lisätietoja julkisuudesta ja tietosuojasta kunnan toiminnassa löytyy Kuntaliiton ohjeistuksista: [julkisuus ja tietosuoja | Kuntaliitto.fi](https://www.kuntaliitto.fi/julkisuus-ja-tietosuoja)

3.5 Kuka saa käsitellä tietoja ja milloin?

Henkilötietojen käsittelylle täytyy lähtökohtaisesti olla aina jokin peruste. Julkisella sektorilla se on yleensä lakisääteinen oikeus tai velvollisuus käsitellä tietoja. Henkilötietoja ei saa kerätä ilman syytä, vaikka tiedot olisivat vapaasti saatavilla esimerkiksi internetistä. Tietoja ei myöskään saa katsella esimerkiksi tietojärjestelmistä tai tulosteilta/kopioilta muuten vain, ilman asiallista syytä. Salassa pidettäviä tietoja ei lähtökohtaisesti saa käsitellä lainkaan, elleivät työtehtävät sitä edellytä. Niistä ei myöskään tule keskustella ulkopuolisten kanssa.

Ellei tietojen käsittely perustu lainmukaiseen oikeuteen tai velvollisuuteen tai esimerkiksi rekisteröidyn kanssa tehtävään sopimukseen, tulee henkilötietojen käsittelyyn pyytää suostumus. Rekisteröity saa koska tahansa peruuttaa suostumuksensa, ja peruuttamisen tulee olla yhtä helppoa kuin suostumuksen antamisenkin. Annettu suostumus on pystyttävä jälkikäteen osoittamaan.

Henkilötietoja saa käsitellä esimerkiksi seuraavissa tilanteissa

- siihen on olemassa rekisteröidyn vapaaehtoinen **suostumus**
- käsittely on tarpeen organisaation **lakisääteisten velvoitteiden noudattamiseksi**
- käsittely on tarpeen **yleistä etua koskevan tehtävän** suorittamiseksi tai rekisterinpitäjälle kuuluvan **julkisen vallan käyttämiseksi** (tehtävä tai valta on annettu lailla tai muilla oikeudellisilla säännöksillä)

- rekisteröity on tehnyt **sopimuksen**, johon käsittely perustuu; käsittely voi olla tarpeen esimerkiksi sopimuksen täytäntöön panemiseksi tai sopimuksen tekemistä edeltävien toimenpiteiden (esim. laskutuksen) toteuttamiseksi tai
- käsittely on tarpeen rekisterinpitäjän **oikeutettujen etujen toteuttamiseksi**.

Huomaa, ettet voi vapaasti keskustella rekisteröityjen - olivatpa he kansalaisia, kuntalaisia, asiakkaita tai henkilökuntaamme kuuluvia - henkilötiedoista kollegoidenkaan kanssa tai näyttää heihin liittyviä tai muuten salassa pidettäviä tietoja tietojärjestelmästä sillä perusteella, että molempia osapuolia koskevat salassapitosäännöt mukaan lukien vaitiolovelvollisuus.

Henkilötietojen käsittelylle, esimerkiksi tietojen katselulle, tulee aina löytyä myös henkilötietoja käsittelevän työntekijän työrooliin perustuva oikeus.

3.6 Tietojen luovuttaminen

Tietosuoja-asetus sääntelee tietojen luovuttamista tai siirtoa rekisterinpitäjältä toiselle tai rekisterinpitäjältä henkilötietojen käsittelijälle, esimerkiksi ostopalvelutilanteissa. Virallisten asiakirjojen julkisuudesta ja tietojen luovuttamisesta esimerkiksi viranomaistaholta toiselle säännellään kansallisessa lainsäädännössä - julkisuuslaissa ja eri alojen erityislaeissa.

Tietojen luovutuksessa on huomioitava, että luovuttaja vastaa aina luovutusten laillisuudesta. On siis syytä pohtia, missä tilanteissa ja mihin tarkoituksiin tietoja luovutetaan. Tiedon luovutukset tulee aina dokumentoida, eikä ilman kirjallista pyyntöä tietoja ole syytä luovuttaa, ellei kyseisestä tarkoituksesta ja luovutuksensaajasta voida olla täysin varmoja.

Henkilötietojen luovuttaja vastaa siitä, että:

- tiedon pyytäjällä on oikeus saada tiedot ja
- tietojen luovutukset tehdään sähköisesti suojatusti, kirjepostilla tai paikan päällä organisaatiossa siten, että pyytäjän henkilöllisyys varmistetaan.

Mikäli et ole täysin varma siitä, voiko tietoa luovuttaa, on syytä kääntyä esihenkilön, tietosuojavastaavan tai kaupunginlakimiehen puoleen.

Tietopyyntöjen käsittelystä ohjeistetaan tarkemmin Santrassa: [Hallinnon ohjeet](#)

3.7 Henkilötiedon käsittely verkkotiedottamisessa

Kunnalla on lakisääteinen velvollisuus tiedottaa kunnan toiminnasta ja päätöksenteosta. Kaikkea julkistakaan tietoa ei voi sellaisenaan viedä verkkoon, mutta erityistä huomiota tulee kiinnittää henkilötietojen julkaisemiseen yleisessä tietoverkossa. Henkilötietojen viemistä verkkoon on syytä välttää ottaen huomioon väärinkäytösten mahdollisuus.

Viranomaisen julkaistaessa esityslistaa/pöytäkirjaa se saa sisältää ainoastaan tiedonsaannin kannalta välttämättömät henkilötiedot. Henkilötiedot eivät yleensä itse päätöksen tiedoksiannon kannalta ole olennaisia. Toimielinten on syytä pitää henkilötietoja sisältävät kokousasiakirjat verkkosivuilla vain tehokkaan tiedottamisen vaatiman rajoitetun ajan (esim. oikaisuvaatimus- tai valitusaika), ja on suositeltavaa poistaa ne viimeistään vuoden kuluttua niiden julkaisemisesta. Jos kokousasiakirjoissa ei ole henkilötietoja, voidaan asiakirjoja pitää verkkosivuilla pidempään. **Henkilötietojen vieminen verkkoon edellyttää aina tapauskohtaista harkintaa.**

Salassa pidettäviä tiedot tulee kirjata salassa pidettäviin liitteisiin, ei itse pöytäkirjaan. Tällöin julkinen pöytäkirja voidaan julkaista salassa pidettävien liitteiden tulematta sivullisen tietoon. Henkilövaalia koskevissa asioissa valitun ja varalle valitun henkilön nimitietojen sekä mahdollisesti ammattia ja koulutusta koskevien tietojen julkaiseminen voi joskus olla tarpeellista. Lisäksi voidaan todeta esimerkiksi, että julkiset tiedot muista hakijoista ovat saatavilla kunnanvirastossa. Asianosaisilla on oikeus pyydettäessä saada myös salassa pidettäviä tietoja. Myös luottamushenkilöitä koskevissa asioissa, kuten henkilön valinta toimielimeen ja sieltä eroaminen, voidaan henkilön nimiä julkaista verkossa.

3.8 Henkilötietojen käsittely tekoälyjärjestelmissä

Tietosuojasääntelyä on noudatettava kaikessa henkilötietojen käsittelyssä teknologiasta riippumatta, myös tekoälyjärjestelmissä. Henkilötietojen käsittely tekoälyjärjestelmillä voi aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille, joten tekoälyjärjestelmää käyttöön otettaessa on tehtävä huolellista riskiarviointia. Henkilötietoja saa käsitellä vain niillä tekoälyjärjestelmillä, jotka on organisaatiossa arvioitu ja hyväksytyt.

Lisätietoja ja ohjeita Santran Tekoäly-sivustolla: [Tekoäly](#)

3.9 Miten käsittelen henkilötietoja oikein?

Henkilötietojen käsittelyssä pienilläkin asioilla on suuri merkitys. Tärkeintä on huomioida arjen työtehtävissä toimenpiteet, joilla tietoa pyritään suojaamaan sivullisilta, käsiteltiinpä henkilötietoja sitten sähköisesti tietojärjestelmissä, paperilla, kuvina tai keskusteluissa. Huomioi aina, etteivät ulkopuoliset pääse kuulemaan tai näkemään käsittelemiäsi tietoja.

Oikeudet verkkolevyille tai erilaisiin tietojärjestelmiin myönnetään henkilökohtaisesti ja työtehtäväperusteisesti. Tietojärjestelmissä toimitaan aina henkilökohtaisilla tunnuksilla ja omaan työrooliin kuuluvilla oikeuksilla. Toisten henkilöiden tunnuksia ei saa käyttää, eikä omia tunnuksia saa lainata tai luovuttaa toiselle. Tämä on myös oikeusturvakysymys; useimpien tietojärjestelmien käyttöä valvotaan yhä laajemmin, jotta voidaan tarvittaessa jälkikäteen todentaa, kuka henkilötietoja on katsonut tai muuten käsitellyt.

Ole erityisen huolellinen lähettäessäsi sähköpostia myös organisaation sisällä - varsinkin kun sähköposti sisältää henkilötietoa tai erityisiin henkilötietoryhmiin kuuluvaa tietoa. Tarkista aina, että vastaanottaja on varmasti oikea eikä nimikaima organisaation sisältä tai ulkopuolelta. Salassa pidettävää (tai muuten arkaluonteista tietoa, kuten henkilötunnus, pankkitilinro, tms.) ja erityisiin henkilötietoryhmiin kuuluvaa tietoa ei saa lähettää tavallisella sähköpostilla, vaan on aina käytettävä turvasähköpostia.

Suojattavaa tietoa ovat esimerkiksi paperitulosteet ja muistitikut, jotka sisältävät sellaista henkilötietoa, josta henkilö voidaan yksilöidä. Tietosuojattava materiaali tulee käsitellä, kerätä, varastoida ja hävittää niin, ettei tietosuoja vaarannu - älä siis jätä henkilötietoja sisältävää materiaalia pöydille muiden nähtäväksi, älä varastoi sitä esimerkiksi pahvilaatikoihin myöhemmin hävitettäväksi tai heitä tulosteita tavalliseen roska-astiaan tai paperinkeräykseen.

Esimerkkejä hyvistä ja suositeltavista toimintatavoista:

- Lukitse työasemasi aina kun poistut työpisteeltä hetkeksikin.
- Suojaa näytön tiedot käyttämällä näytönsuojakalvoa.
- Huomioi tietosuoja myös työmatkoilla ja etätyössä; estä ulkopuolisten pääsy näkemään tai kuulemaan tietoja.
- Pidättäydy keskustelemasta luottamuksellisista tai salassa pidettävistä asioista edes muiden työkavereiden kanssa.
- Henkilötietoja sisältävät tulosteet kuuluvat tietosuojattavan jätteen astiaan, ei tavalliseen paperinkeräykseen tai roska-astiaan eikä niitä saa varastoida myöhemmin hävitettäväksi.
- Älä tallenna henkilötietoja sisältävää materiaalia työaseman kovalevyille/työpöydälle, suojaamattomille muistitikuille tai muille ulkoisille lisämuisteille. Työnantajan määrittelemällä verkkolevylläsi tiedot ovat turvassa, vaikka joku varastaisi työaseman.
- Huomioi, että työajan ulkopuolellakin sinua koskee vaitiolovelvollisuus - älä puhu työasioista ulkopuolisten kuullen.

Sähköpostin tietoturva- ja tietosuojaohje: [Microsoft-Outlook-tietoturva--ja-tietosuojaohjeistus](#)

Tietosuojajätteen käsittelyohje: [Tietosuojajätteen-käsittely](#)

Lisätietoa tietoturvallisista toimintatavoista löytyy Santrasta: [IT-tuki ja -ohjeet](#)

3.10 Mistä saan tukea?

Tukea ja ohjausta henkilötietojen oikeaoppiseen käsittelyyn saat kaupungin tietosuojavastaavalta. Santran tietosuoja käsittelevät sivut sisältävät paljon hyvää tietoa ja ohjausta. Navisec-verkkokoulutusympäristössä on tarjolla tietoturvaan ja tietosuojaan liittyvää koulutusta. Henkilökunta suorittaa Henkilöstön tietosuoja ja tietoturva -verkkokoulutuksen vuosittain. Esihenkilöt ovat vastuussa siitä, että työntekijät saavat riittävän koulutuksen ja perehdytyksen henkilötietojen käsittelyyn. Jokaisen työntekijän vastuulla on osallistua työssään tarvitsemiinsa tietosuojakoulutuksiin, perehtyä ohjeisiin ja noudattaa niitä sekä huomioida tietoturva ja tietosuoja työtehtävissään.

[Navisec](#)-koulutusympäristö

[Tietosuoja ja henkilötiedon käsittely](#) Santrassa

4 REKISTERINPITÄJÄN VELVOLLISUUDET

Rekisterinpitäjän tulee toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että tietosuoja-asetuksessa säädetyt vaatimukset täyttyvät. Velvoite on varsin laaja.

4.1 Riskien arviointi

Rekisterinpitäjän on arvioitava henkilötietojen käsittelyyn liittyviä riskejä aina, ennen kuin se ryhtyy käsittelemään henkilötietoja. Riskianalyysin avulla rekisterinpitäjä tunnistaa jo suunnitteluvaiheessa ne toimenpiteet, joihin sen on ryhdyttävä riskien hallitsemiseksi ja henkilötietojen asianmukaisen

käsittelyn turvaamiseksi. Rekisterinpitäjän on varmistettava myös tietosuojaperiaatteiden tehokas toteutuminen suhteessa käsittelyyn liittyvään riskiin.

Tietosuoja-asetuksen mukainen riskiarvio on tehtävä rekisteröidyn näkökulmasta eli rekisterinpitäjän on arvioitava, mitä rekisteröidyn vapauksia ja oikeuksia käsittely voi vaarantaa ja mitä vahinkoa rekisteröidylle voi aiheutua suunnitellusta henkilötietojen käsittelystä. Riskien arviointi on jatkuvaa toimintaa: toimenpiteiden riittävyttä suhteessa käsittelyyn liittyvään riskiin on arvioitava jatkuvasti ja päivitettävä tarvittaessa. Rekisterinpitäjällä on myös osoitusvelvollisuus riskiperusteisen lähestymistavan noudattamisesta.

Kun suunniteltu käsittely voi aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille, on tehtävä tietosuojan **vaikutustenarviointi**. Vaikutustenarvioinnin tavoitteena on arvioida, onko jäljelle jäänyt riski oikeutettu ja hyväksyttävissä kyseisissä olosuhteissa. Rekisterinpitäjän on pyydettävä tietosuojavastaavan neuvoja vaikutustenarvioinnin tekemisessä.

4.2 Rekisteröidyn informointi

Rekisterinpitäjän tulee informoida rekisteröityjä henkilötiedon käsittelystä. Tiedot on annettava tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Kaupunki toteuttaa rekisteröityjen informoinnin pääasiassa kotisivuilta löytyvillä tietosuojaselosteilla. [Tietosuojaselosteet - Savonlinna](#)

4.3 Seloste käsittelytoimista

Rekisterinpitäjän on ylläpidettävä selosteita käsittelytoimista. Selosteet käsittelytoimista ovat yleisiä kuvauksia siitä, miten rekisterinpitäjä käsittelee henkilötietoja. Selosteet käsittelytoimista laaditaan sisäiseen käyttöön ja valvontaviranomaista varten. Kaupungin tiedonhallintamalliin on sisällytetty seloste käsittelytoimista.

4.4 Osoitusvelvollisuus

Osoitusvelvollisuus tarkoittaa, että rekisterinpitäjän on pystyttävä osoittamaan noudattavansa tietosuojalainsäädäntöä. Tämä edellyttää, että henkilötietojen käsittelyyn liittyvät prosessit ja tietosuojaperiaatteiden käytännön toteuttaminen dokumentoidaan. Osoitusvelvollisuuden tarkoituksena on myös näyttää, miten rekisterinpitäjä kunnioittaa rekisteröityjen eli henkilötietojen käsittelyn kohteena olevien tietosuoja. Osoitusvelvollisuuden toteuttaminen lisää luottamusta rekisterinpitäjän toimintaan. Osoitusvelvollisuutta toteutetaan erilaisilla dokumenteilla ja toimenpiteillä, kuten:

- seloste käsittelytoimista
- toimintamallit ja ohjeistukset henkilötietojen käsittelyyn liittyen
- rekisteröityjen informoinnit, tietosuojaselosteet
- käsittelyn oikeusperustetta koskevat arviot
- tietosuojan vaikutustenarvioinnit
- henkilötietojen tietoturvaloukkausten prosessi ja dokumentointi
- rekisteröidyn oikeuksiin liittyvien pyyntöjen dokumentointi
- henkilötietojen käsittelyyn liittyvät sopimukset
- koulutukset

4.5 Käsittelijän toiminnan valvominen

Kaupungille palveluja tuottava yritys, yhdistys, säätiö tai toinen viranomainen voi käsitellä henkilötietoja kaupungin puolesta. Tällöin kaupunki on rekisterinpitäjä ja kaupungin puolesta tietoja käsittelevä yritys on käsittelijä. Kaupunki saa rekisterinpitäjänä käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät tekniset ja organisatoriset suoja-toimet, ja käsittely täyttää tietosuojalainsäädännön vaatimukset. Tällä varmistetaan rekisteröidyn oikeuksien suoje-lu myös silloin, kun käsittelyn suorittaa kaupungin puolesta joku muu.

Henkilötietojen käsittelijän kaupungin puolesta suorittamasta käsittelystä on määritettävä sopimuksella, joka sitoo henkilötietojen käsittelijää suhteessa rekisterinpitäjään ja jossa vahvistetaan käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet. Henkilötietojen käsittelijä saa käsitellä henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti.

Henkilötietojen käsittelijä ei saa käyttää toisen henkilötietojen käsittelijän palveluksia ilman rekisterinpitäjän erityistä tai yleistä kirjallista ennakkolupaa. Kun kyse on kirjallisesta ennakkoluvasta, henkilötietojen käsittelijän on kerrottava rekisterinpitäjälle kaikista suunnitelluista muutoksista, jotka koskevat muiden henkilötietojen käsittelijöiden lisäämistä tai vaihtamista, ja annettava siten rekisterinpitäjälle mahdollisuus vastustaa tällaisia muutoksia.

4.6 Henkilötietojen tietoturvaloukkausten käsittely

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tilannetta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai pääsy tietoihin. Tietomurtojen lisäksi tämä tarkoittaa siis myös esimerkiksi tilanteita, joissa henkilötietoa päätyy vahingossa ulkopuolisten saataville, esimerkiksi

- henkilötietoja (asiakas-, henkilökunta- tai esimerkiksi yhteystietoja) sisältävää materiaalia katoaa tai joutuu hukkaan (esimerkiksi mappi tai kansio)
- henkilötietoja sisältävä muistitikku tai muu tallennusväline katoaa tai joutuu hukkaan
- työasemasi varastetaan, ja työasemaan on liitetty ulkoinen muistiväline
- henkilötietoja sisältäviä asiakirjoja tai tulosteita löytyy varastoituna julkisista valvomattomista tiloista
- henkilötietoja sisältäviä aineistoja päätyy tai löytyy erehdyksessä internet-sivuilta (julkinen sivusto)
- tulostat erehdyksessä henkilötietoja sisältäviä dokumentteja väärälle tulostimelle
- postitat väärän henkilön asiakirjoja kirjepostilla tai sähköisesti sivulliselle

Henkilötietojen tietoturvaloukkauksesta tulee **aina ilmoittaa viipymättä tietosuojavastaavalle:**

1. Santran etusivulta löytyvän lomakkeen kautta, tai
2. olemalla yhteydessä tietosuojavastaavaan, p. 050 302 3377, tietosuojavastaava@savonlinna.fi

Tietosuojalainsäädännön mukaan tietoturvaloukkauksen jatkoselvittelyyn kuuluu huolellinen riskiarviointi ja dokumentointi sekä riskiarvioinnin tulosten perusteella ilmoitusvelvollisuus tietosuojavaltuutetun toimistoon (72 tunnin sisällä) ja loukkauksen kohteelle ilman aiheetonta viivytyksiä. Tietoturvaloukkauksesta voi seurata esimerkiksi identiteettivarkaus tai petos, maineen vahingoittuminen tai salassapitovelvollisuuden alaisten henkilötietojen paljastuminen. Riskiarvioinnin perusteella tehdään tarvittaessa ilmoitus myös Kyberturvallisuuskeskukseen ja Poliisille. Ilmoitusten avulla myös opimme organisaationa, löydämme kehittämiskohteita ja pystymme toteuttamaan tietosuojaa parantavia toimenpiteitä.

5 REKISTERÖIDYN OIKEUDET

Tietosuoja-asetus takaa henkilölle, jonka tietoja käsitellään (rekisteröity), erilaisia oikeuksia. Oikeuksia sovelletaan eri tavalla riippuen henkilötietojen käsittelyperusteesta. Henkilöllä on mm. oikeus tietää, käsitelläänkö hänen henkilötietojensa ja mitä henkilötietoja käsitellään sekä pyytää itseään koskevat tiedot. Henkilöllä on myös oikeus vaatia virheelliset henkilötiedot oikaistavaksi.

Tietojen tarkastusoikeus (oikeus saada pääsy tietoihinsa, artikla 15)

Henkilöllä on oikeus tietää, käsitelläänkö hänen henkilötietojensa vai ei, ja mitä henkilötietoja hänestä on tallennettu. Organisaatio varmistaa pyytäjän henkilöllisyyden ja toimittaa rekisteröidyn pyynnöstä tiedot mahdollisimman pian ilman aiheetonta viivytystä (kuukauden sisällä). Mikäli tietopyyntö on poikkeuksellisen monimutkainen ja laaja, määräaika voidaan jatkaa kahdella kuukaudella.

Rekisteröidyn tiedot toimitetaan lähtökohtaisesti maksutta. Jos jäljennöksiä pyydetään useampia, organisaatio voi kuitenkin periä niistä hallinnollisiin kustannuksiin perustuvan kohtuullisen maksun. Mikäli tietopyyntö on ilmeisen perusteeton ja kohtuuton, erityisesti jos tietopyyntöjä esitetään toistuvasti, organisaatio voi periä tietojen toimittamisesta aiheutuneet hallinnolliset kustannukset tai kieltäytyä kokonaan toimittamasta tietoja. Tällaisessa tapauksessa organisaatio osoittaa pyynnön ilmeisen perusteettomuuden tai kohtuuttomuuden.

Tietosuojalainsäädännössä (34 §) on määritelty rajoitukset, milloin rekisteröidyllä ei ole oikeutta tutustua hänestä kerättyihin tietoihin. Oikeutta ei ole, jos tiedon antaminen saattaisi vahingoittaa kansallista turvallisuutta, puolustusta tai yleistä järjestystä ja turvallisuutta taikka haitata rikosten ehkäisemistä tai selvittämistä. Lisäksi, jos tiedon antamisesta saattaisi aiheutua vakavaa vaaraa rekisteröidyn terveydelle tai hoidolle taikka rekisteröidyn tai jonkun muun oikeuksille.

Mikäli organisaatio ei toimita tietoja, annetaan asiasta kirjallinen todistus. Samassa yhteydessä kerrotaan oikeudesta tehdä valitus valvontaviranomaiselle.

Oikeus tietojen oikaisemiseen (artikla 16)

Henkilöllä on oikeus vaatia, että häntä koskevat virheelliset, epätarkat tai puutteelliset henkilötiedot oikaistaan tai täydennetään ilman aiheetonta viivytystä. Lisäksi henkilöllä on oikeus vaatia, että tarpeettomat henkilötiedot poistetaan. Tarpeettomuutta ja virheellisyyttä arvioidaan tietojen tallennushetken mukaan.

Ellei organisaatio hyväksy oikaisupyyntöä, annetaan asiasta kirjallinen todistus, jossa mainitaan ne syyt, joihin perustuen vaatimusta ei ole hyväksytty. Samoin tiedotetaan oikeudesta tehdä valitus valvontaviranomaiselle.

Oikeus tulla unohdetuksi (artikla 17)

Henkilöllä on vain tietyissä poikkeustapauksissa oikeus saada henkilötietonsa kokonaan poistettua organisaation rekistereistä (oikeus tulla unohdetuksi). Tällaista oikeutta ei kuitenkaan ole niissä tapauksissa, kun henkilötietojen käsittely on tarpeellista lakisääteisen velvoitteen noudattamiseksi tai organisaatiolle kuuluvan julkisen vallan käyttämistä varten. Tietojen säilyttämisessä ja poistamisessa noudatetaan organisaation tiedonohjaussuunnitelmaa ja lainsäädännön velvoittamia tietojen säilytysaikoja.

Oikeus käsittelyn rajoittamiseen (artikla 18)

Henkilöllä voi tietyissä tilanteissa olla oikeus pyytää henkilötietojensa käsittelyn rajoittamista siksi aikaa, kunnes hänen tietonsa on asianmukaisesti tarkistettu ja korjattu tai täydennetty.

Oikeus siirtää tiedot järjestelmästä toiseen (artikla 20)

Oikeus ei koske sellaista henkilötiedon käsittelyä, joka on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Näin ollen pääsääntöisesti oikeutta ei sovelleta kaupungin henkilörekistereihin liittyen.

Vastustamisoikeus (artikla 21)

Henkilöllä on oikeus henkilökohtaiseen, erityiseen tilanteeseensa perustuen milloin tahansa vastustaa henkilötietojensa käsittelyä silloinkin, kun käsittely perustuu yleistä etua koskevan tehtävän suorittamiseen tai organisaatiolle kuuluvan julkisen vallan käyttämiseen. Tässä tapauksessa tietoja voidaan käsitellä edelleen vain, jos käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka voidaan osoittaa.

Oikeus olla joutumatta automaattisen päätöksenteon tai profiloinnin kohteeksi (artikla 22)

Henkilöllä on oikeus vaatia, että häntä koskevat päätökset tekee ihminen. Hänellä on oikeus olla joutumatta sellaiseen pelkäämään automaattiseen käsittelyyn, jolla on häntä koskevia oikeusvaikutuksia tai muita merkittäviä vaikutuksia. Kieltoon on kuitenkin poikkeuksia.

Oikeus saada tieto henkilötietojen tietoturvaloukkauksesta (artikla 34)

Henkilötietojen tietoturvaloukkauksesta on ilmoitettava henkilölle, jos se todennäköisesti aiheuttaa korkean riskin tämän oikeuksille ja vapauksille. Asiasta on ilmoitettava ilman aiheetonta viivytystä, jotta rekisteröidyllä on mahdollisuus suojautua negatiivisilta vaikutuksilta. Ilmoitukseen on sisällytettävä selkeä kuvaus henkilötietojen tietoturvaloukkauksesta, sen todennäköisistä seurauksista sekä tehdyistä ja aiotuista toimenpiteistä asian suhteen. Lisäksi kerrotaan tietosuojavastaavan yhteystiedot ja lisätietoja antava taho.

Oikeus tehdä valitus viranomaiselle (artikla 77)

Henkilöllä, jonka henkilötietoja on kaupungin henkilörekistereissä, on oikeus tehdä valitus valvontaviranomaiselle, jos hän katsoo, että häntä koskevien henkilötietojen käsittelyssä rikotaan EU:n yleistä tietosuojaa-asetusta. Suomessa tämä valvontaviranomainen on tietosuojavaltuutettu. Tämän lisäksi henkilöllä on oikeus käyttää muita hallinnollisia muutoksenhakukeinoja sekä oikeussuojakeinoja.

6 LIITTEET

Liite 1 Tietosuojaan muistilista työntekijälle

Tietosuoja on perusoikeus, joka turvaa henkilön oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojalainsäädäntöä sovelletaan aina, kun käsitellään henkilötietoa, paperiaineistosta tekoälysovelluksiin.

1. Noudata annettuja ohjeita henkilötiedon käsittelyssä

- Pehdy henkilötiedon käsittelyn ohjeistuksiin Santran tietosuojaan sivuilla ja niiden linkeissä: [Tietosuoja ja henkilötiedon käsittely](#)
- Ymmärrä oma roolisi ja vastuusi henkilötietojen käsittelyssä.
- Huomio tiedon elinkaari, säilytysajat ja tietoturallinen poistaminen.
- Pehdy käsittelemiesi tietojen tietosuojaoselosteeseen: [Tietosuojaoselosteet - Savonlinna](#)
[Tietosuojaoselosteet](#)
Käsittele henkilötietoja vain määritellyn käsittelytarkoituksen mukaisesti.
- Pehdy tietoturvallisiin toimintamalleihin [IT-tuki ja -ohjeet](#)
- Kysy, jos olet epävarma. Esihenkilöltäsi tai tietosuojaavastaavalta saat apua.

2. Käsittele henkilötietoja yksityisyyden suoja huomioiden

- Varmista, että ulkopuoliset eivät kuule tai näe henkilötietoja. Ulkopuolisia ovat myös työkaverit, joiden työtehtäviin kyseinen asia ei kuulu. Huomio etätyötilanteet. Käytä näytönsuojakalvoa.
- Noudata puhtaan pöydän periaatetta. Säilytä henkilötietoja sisältävät paperiaineistot lukituissa kaapeissa. Hävitä paperiaineistot tietosuojaajätteeseen.
- Vältä henkilötietoja sisältävien paperien tulostusta ja kopiointia. Käytä turvatulostusta.
- Lukitse työasemasi aina kun poistut sen ääreltä.
- Ole tietoinen, että henkilöllä, jonka tietoja käsitellään, on oikeus saada tietoa henkilötietojensa käsittelystä sekä oikeus pyytää omat tietonsa.
- Vaikka asiakirja on julkinen, sen sisältämiä henkilötietoja tulee käsitellä tietosuojaoselosteiden mukaisesti. Ole tarkkana asiakirjojen julkaisussa tai luovuttamisessa.
- Henkilötietoja luovuttavan tulee varmistua, että pyytäjällä on oikeus saada tiedot. Varmistu pyytäjän henkilöllisyydestä ja kirjaa tietojen luovutukset Dynastyyn.
- Käytä turvasähköpostia, kun lähetät sähköpostitse asiakkaiden tietoja myös organisaation sisällä. Varmistu, että sähköpostiosoite on oikein. Älä ohjeista asiakasta lähettämään esim. henkilötunnusta tavallisella sähköpostilla.

3. Edistä tietosuojaan toteutumista

- Tunnista henkilötietojen tietoturvaloukkaukset ja ilmoita niistä välittömästi: [Tietoturvaloukkaukset](#)
- Toimi esimerkkinä ja tuo epäkohtia rohkeasti esille.

Lisätietoja: tietosuojaavastaava@savonlinna.fi

Liite 2 Tietosuoja muistilista esihenkilölle

Tietosuoja on perusoikeus, joka turvaa henkilön oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojalainsäädäntöä sovelletaan aina, kun käsitellään henkilötietoa, paperiaineistosta tekoälysovelluksiin.

Tällä muistilistalla ohjeistetaan esihenkilön vastuista.

1. Hallitse oikeaoppinen henkilötietojen käsittely.

- Kaikelle henkilötietojen keräämiselle ja käsittelylle pitää olla laillinen peruste.
- Tarpeettomia tietoja ei saa kerätä eikä säilyttää enempää kuin on tarve.
- Tietoja ei saa käyttää muuhun tarkoitukseen, kuin mihin ne on kerätty.
- Tietojen oikeellisuudesta ja täsmällisyydestä pitää huolehtia.
- Tietoja pitää käsitellä ja säilyttää huolellisesti ja ne tulee hävittää turvallisesti.
- Tietoja ei saa luovuttaa ulkopuolisille, jos luovuttamiselle ei ole laillista perustetta.
- Rekisteröidyllä on oikeus saada tietoa siitä, mitä tietoja hänestä on tallennettuna.

2. Tunne tehtäväalueesi rekisterit ja käsiteltävät henkilötiedot.

- Erityisten henkilötietoryhmien (esim. terveystiedot) käsittely vaatii erityistä tarkkuutta.

3. Tiedosta ja arvioi henkilötietojen käsittelyyn liittyviä riskejä vastualueellasi.

4. Tunne alaistesi tehtävät ja roolit henkilötietojen käsittelyssä.

- Työntekijän käyttöoikeudet tietoihin tulee olla rajattu tarkasti työtehtävien mukaiseksi. Tämä on huomioitava myös työntekijän siirtyessä toisiin tehtäviin organisaation sisällä.
- Käyttöoikeudet on päätettävä/lukittava, kun työntekijä jää pois organisaation palveluksesta myös tilapäisissä tilanteissa.
- Poisjäävän työntekijän hallussa olevat aineistot on hävitettävä/arkistoitava/otettava talteen ennen poisjääntiä.

5. Tiedosta oikeat käytännöt tietojen luovutuksessa.

6. Ohjeista työntekijöitä henkilötietojen oikeaoppisesta käsittelystä.

- Esihenkilöllä on velvollisuus varmistaa, että työntekijöillä on käytössään riittävä ohjeistus työtehtäviensä suorittamiseen tietosuojalainsäädännön mukaisesti.
- Varmista, että työntekijöillä on käytettävissä mm. näytönsuojakalvot, tietosuojajäteastia ja lukittavat kaapit paperiaineiston säilytykseen.

7. Huolehdi, että työntekijät osallistuvat säännöllisesti tietosuojakoulutuksiin.

8. Ohjeista yhteistyökumppanit henkilötietojen oikeaoppisesta käsittelystä.

9. Huolehdi, että tietosuoja on huomioitu uuden toiminnan suunnittelussa, hankinnoissa ja sopimuksissa.

- Ota tietosuojavastaava alusta alkaen mukaan suunnitteluun, kun toimialueellenne suunnitellaan jotain uutta, johon liittyy henkilötiedon käsittelyä (esim. hankkeet, toiminnot, palvelut, hankinnat).
- Sopimushallinnassa tietosuojaan huomioiminen toteutetaan tietosuojaliitteellä, joka liitetään pääsopimukseen. Sopimuskumppani tulee myös ohjeistaa rekisterinpitäjän lukuun toteutettavaan henkilötiedon käsittelyyn.

10. Tunne työelämän tietosuojalaki

- [Laki yksityisyyden suojasta työelämässä | 759/2004 | Lainsäädäntö | Finlex](#)

11. Tiedosta väärinkäytösten rikosoikeudellinen luonne

- Kansallisessa tietosuojalaissa on viittaukset rikoslakiin tietosuojarikoksen (esim. henkilötietojen käsittely vastoin käsittelyn yleisiä edellytyksiä), tietomurron (tekijä käyttää hänelle kuulumatonta käyttäjätunnusta) ja salassapitorikoksen (paljastaa salassa pidettävän seikan) osalta.

12. Reagoi tietosuoja- ja tietoturvapoikkeamiin

- Ole välittömästi yhteydessä tietosuojavastaavaan tai tietohallintopäällikköön.

Lisätietoa saa tietosuojavastaavalta, tietosuojavastaava@savonlinna.fi