# Tietosuojapolitiikka

## Sipoon kunta

SIPOO
SIBBO

# Sisällys

# 1 Tietosuojapolitiikan keskeisiä käsitteitä

| | |
|---|---|
| **Tietosuoja** | Tietosuoja tarkoittaa perusoikeutta, joka turvaa jokaisen oikeuksia ja vapauksia henkilötietojen käsittelyssä. Tietosuoja määrittelee ne periaatteet, milloin, millä edellytyksillä ja miten henkilötietoja voidaan käsitellä. |
| **Tietoturva** | Tietoturvalla varmistetaan tietojen luottamuksellisuus, eheys, saatavuus ja käytettävyys. Tietoturva liittyy läheisesti tietosuojaperiaatteiden toteuttamiseen. |
| **Henkilötieto** | Henkilötietoa on kaikki tieto, joiden avulla henkilö on tunnistettavissa. Henkilö on tunnistettavissa, jos tieto voidaan liittää henkilöön joko suoraan tai välillisesti esimerkiksi yhdistämällä tieto johonkin toiseen tietoon. |
| **Henkilötietojen käsittely** | Henkilötietojen käsittely tarkoittaa kaikkia henkilötietoihin kohdistettavia toimia, kuten kerääminen, tallentaminen, säilyttäminen, muokkaaminen, muuttaminen, hakeminen, luovuttaminen ja poistaminen. |
| **Rekisterinpitäjä** | Rekisterinpitäjä tarkoittaa ihmistä tai organisaatiota, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot tai jonka tehtäväksi henkilötietojen käsittely on lailla säädetty. Rekisterinpitäjä on vastuussa suorittamastaan henkilötietojen käsittelystä. |
| **Rekisteröity** | Rekisteröity tarkoittaa henkilöä, jonka henkilötietoja rekisterinpitäjä käsittelee. EU:n tietosuoja-asetus antaa erilaisia oikeuksia rekisteröidyille henkilötietojen käsittelyperusteesta riippuen. |
| **Henkilötietojen käsittelijä** | Henkilötietojen käsittelijä tarkoittaa ihmistä tai organisaatiota, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Esimerkiksi rekisterinpitäjän käyttämä palveluntarjoaja. Henkilötietojen käsittelijällä ei tarkoiteta organisaation omia työntekijöitä. |
| **Tietosuojan vaikutustenarviointi** | Tietosuojan riskejä on arvioitava aina, kun henkilötietoja käsitellään. Tietosuojan vaikutustenarviointi on ennen henkilötietojen käsittelyn aloitusta tehtävä arvio, jossa arvioidaan tarkemmin suunnitellun käsittelyn sisältöä, oikeasuhtaisuutta suhteessa rekisteröityyn ja henkilötiedoille aiheutuvia riskejä. Vaikutustenarviointi on tehtävä, mikäli käsittelystä todennäköisesti aiheutuu korkea riski luonnollisen henkilön oikeuksille ja vapauksille. |

# 2 Tietosuojapolitiikan merkitys

Tietosuojapolitiikka on ylin tietosuojan toteutusta ja hallintaa määrittävä dokumentti. Tietosuojapolitiikan tarkoituksena on määritellä ne keinot, joilla Sipoon kunta pyrkii varmistamaan noudattavansa henkilötietojen käsittelyssä tietosuoja-asetusta ja muuta henkilötietojen käsittelyyn soveltuvaa lainsäädäntöä. Tietosuojapolitiikka määrittää ne periaatteet, toimintatavat, vastuut ja valvonnan, joita noudatetaan Sipoon kunnan tietosuojan toteuttamisessa ja kehittämisessä. Tietosuojapolitiikan mukaisia periaatteita ja niiden soveltamista voidaan tarkentaa linjauksilla ja vaatimuksilla, käytännöillä, ohjeistuksilla ja muulla tietosuojan ja tietoturvan dokumentaatiolla. Tietosuojapolitiikalla Sipoon kunta sitoutuu käsittelemään henkilötietoja vastuullisesti, reilusti ja rekisteröityjen oikeuksia kunnioittaen.

Tietosuojapolitiikka velvoittaa Sipoon kunnan henkilöstöä, johtoa, luottamushenkilöitä, viranhaltijoita, sekä muita kunnan tietoja käsitteleviä henkilöitä, kuten konsultteja, alihankkijoita ja sidosryhmiä riippumatta siitä, missä muodossa käsiteltävä tieto on. Tietosuojapolitiikka tulee huomioida myös kunnan käyttämien palveluntuottajien ja sidosryhmien toiminnassa. Tietosuojapolitiikka koskee kaikkea Sipoon kunnan toimintaa.

Kunnanhallitus on hyväksynyt tietosuojapolitiikan. Tietosuojapolitiikkaa katselmoidaan vuosittain ja tarvittaessa useammin merkittävien muutosten johdosta tietosuojakäytännöissä, lainsäädännössä tai viranomaisohjeistuksessa. Katselmoinnin tarkoituksena on varmistaa politiikan ajantasaisuus ja vaikuttavuus. Tietosuojapolitiikan katselmoinnista vastaa Sipoon tietosuojavastaava.

# 3 Tietosuojan roolit ja vastuut

Tietosuojan roolit ja vastuut jakautuvat Sipoon kunnassa alla olevan taulukon mukaisesti:

| | |
|---|---|
| **Kunnanhallitus** | Vastaa tietosuoja-asioiden johtamisesta ja resurssoinnista sekä valvonnasta. |
| **Kunnanjohtaja** | Toimii tietosuojan omistajana kunnassa luoden edellytykset tietosuojan asianmukaiselle toimeenpanolle. |
| **Tietosuoja- ja tietoturvatyöryhmä** | Sipoon kunnalla on kunnanjohtajan viranhaltijapäätöksellä 8.11.2021 asetettu tietosuoja- ja tietoturvatyöryhmä. Työryhmän tehtävänä on seurata tietosuojan toteutumista, tehdä kehitysehdotuksia ja toimia tietosuojavastaavan sekä järjestelmien pääkäyttäjien tukena. Työryhmä toimii tietosuojan kehityksen asiantuntijana ja edistäjänä organisaatiossa sekä sovittaa yhteiset mallit oman organisaation toimintaan.<br><br>Työryhmän puheenjohtajana toimii tietosuojavastaava. |

| | |
|---|---|
| **Tietosuojavastaava** | Sipoon kunnalle nimetty tietosuoja-asetuksen mukainen tietosuojavastaava on ilmoitettu tietosuojasta vastaavalle valvontaviranomaiselle. Tietosuojavastaavan tehtäviin kuuluu tietosuoja-asetuksen mukaiset lakisääteiset tehtävät.<br><br>Tietosuojavastaava neuvoo henkilötietojen lainmukaisessa käsittelyssä, valvoo tietosuojalainsäädännön ja hyvien tietosuojakäytänteiden noudattamista ja toimii yhteyspisteenä valvontaviranomaiselle.<br><br>Tietosuojavastaava raportoi tietosuojan toteutumisesta kunnan ylimmälle johdolle. |
| **Toimialan johto** | Vastaa tietosuojan toteutuksesta johtamansa toiminnan osalta. |
| **Esimiehet** | Vastaavat tietosuoja toteutumisesta alaisessaan toiminnassa. Esimiehet raportoivat näistä asioista toimialajohdon lisäksi tietosuojavastaavalle. |
| **Viranhaltijat, työntekijät, luottamushenkilöt ja muut työntekijäsuhteeseen rinnastettavat henkilöt** | Vastaavat omalta osaltaan tietosuojan toteutumisesta omissa työtehtävissään. Jokaisen vastuulla on havaitsemiensa tietosuojaan liittyvien uhkien, riskien tai rikkomusten ilmoittaminen viipymättä esimiehelle, palvelusta tai toiminnasta vastuulliselle taholle ja tietosuojavastaavalle. |
| **Tiedon, tietojärjestelmän tai palvelun omistaja** | Vastaa omistukseensa liittyvästä käyttäjien ja heidän käyttöoikeuksiensa määrittelystä ja hyväksynnästä, riskienhallinnan toteuttamisesta, tiedon eheyden varmistamisesta ja tietojen luokittelusta (julkisuuden ja salassapidon määrittely sekä arkistonmuodostus). |

# 4 Keskeiset dokumentit

Sipoon kunta sitoutuu tietosuoja-asetuksen edellyttämän osoitusvelvollisuuden mukaisesti näyttämään, että se noudattaa toiminnassaan tietosuojalainsäädäntöä.

Sipoon kunnan ylläpitämät keskeiset dokumentit vaatimuksenmukaisuuden ja osoitusvelvollisuuden täyttämiseksi ovat:

| | |
|---|---|
| **Tietosuojapolitiikka** | Tietosuojapolitiikka kuvaa tietosuojan periaatteet, tietosuojan hallinnan tavoitteet, tietosuojan organisoinnin ja vastuut sekä toimintatavan. |
| **Tietoturvapolitiikka** | Tietoturvapolitiikka määrittää Sipoon tietoturvaa koskevan toimintatavan. |
| **Seloste käsittelytoimista** | Seloste käsittelytoimista on sisäinen kuvaus organisaation tekemästä henkilötietojen käsittelystä ja käsittelyn tarkoituksista. |
| **Rekisteröityjen informointidokumentit** | Tietosuojaselosteet ja muut rekisteröityjen informointiin tarkoitetut dokumentit, joilla kerrotaan rekisteröidyille henkilötietojen käsittelystä läpinäkyvästi. |
| **Tietosuojan arvioinnit ja riskiarvioinnit** | Kunnan suorittamat tietosuojan esiarvioinnit, tietosuojan vaikutustenarvioinnit ja oikeutetun edun tasapainotestit. |
| **Tietosuojan vuosisuunnitelma** | Tietosuojan vuosisuunnitelmaan kirjataan tietosuojatyölle suunnitellut tehtävät kuukausitasolla. Tietosuojan vuosisuunnitelman avulla seurataan tietosuojatyön etenemistä. |
| **Koulutussuunnitelma** | Määrittelee kunnan henkilöstölle suunnitellut tietosuojakoulutukset. |
| **Tietojenkäsittelysopimuspohja** | Määrittää henkilötietojen käsittelijöiden kanssa sovellettavat sopimusehdot. |
| **Käsittelyn oikeusperusteeseen liittyvät dokumentit** | Suostumukseen liittyvä dokumentaatio ja tarvittavat arvioinnit, kuten oikeutetun edun tasapainotestit. |
| **Rekisteröityjen pyyntöjen käsittelyyn liittyvät dokumentit** | Rekisteröityjen oikeuksien toteuttamiseen liittyvät ohjeistukset, pyyntöihin liittyvät lomakkeet ja dokumentointiin liittyvät asiakirjapohjat. |
| **Tietoturvaloukkausten käsittelyyn liittyvät dokumentit** | Tietoturvaloukkausten hallintaan liittyvät ohjeet ja dokumentointi. |

# 5 Suunnittelu ja raportointi

Sipoo suunnittelee tietosuojatyötä vuosittaista tietosuojan vuosisuunnitelmaa hyväksikäyttäen. Suunnitelmassa tietosuojatyössä toteutettavat tehtävät on jaettu toteutettavaksi pitkin vuotta. Vuosisuunnitelman pohjalta tehtäviä voidaan delegoida vastuussa oleville henkilöille.

Vuoden lopussa kunnan tietosuojatyö kootaan tietotilinpäätökseen. Tietotilinpäätös on kunnan tilinpäätöksen liitteenä, jonka hyväksyy kunnan valtuusto.

# 6 Henkilötietojen käsittely

## 6.1 Henkilötietojen käsittelyn periaatteet

Sipoon kunta noudattaa asiakkaiden, kuntalaisten, kunnan henkilöstön ja muiden sidosryhmien henkilötietojen käsittelyssä voimassa olevaa lainsäädäntöä. Sipoon kunta noudattaa alla olevia tietosuoja-asetuksen mukaisia henkilötietojen käsittelyn periaatteita kaikessa henkilötietojen käsittelyssä.

| | |
|---|---|
| **Lainmukaisuus, asianmukaisuus ja läpinäkyvyys** | Henkilötietojen käsittelyssä noudatetaan tietosuoja-asetusta ja muuta henkilötietojen käsittelyyn soveltuvaa sääntelyä. Henkilötietoja käsitellään asianmukaisesti ja kohtuullisesti suhteessa käsittelyn tarkoituksiin, ottaen huomioon informointivelvollisuus ja käyttötarkoitussidonnaisuus. Käsittelystä kerrotaan rekisteröidyille selkeällä ja ymmärrettävällä tavalla. |
| **Käyttötarkoitussidonnaisuus** | Henkilötietojen käsittely suunnitellaan etukäteen ja käsittely perustuu aina tiettyyn selvästi määritettyyn ja nimenomaiseen sekä lailliseen tarkoitukseen. Henkilötietoja ei käsitellä alkuperäisten tarkoitusten kanssa yhteensopimattomalla tavalla myöhemmin. Uusista käyttötarkoituksista kerrotaan rekisteröidylle ennen käsittelyn aloittamista. |
| **Täsmällisyys, minimointi ja säilytyksen rajoittaminen** | Henkilötietojen oikeellisuus pyritään varmistamaan. Virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.<br><br>Henkilötietoja kerätään ja käsitellään vain siinä määrin, kuin on tarkoituksenmukaista ja välttämätöntä tarkoitukseen nähden. Käsiteltyjen tietojen tulee olla asianmukaisia eli tiedoille on oltava olemassa määritetty käyttötarkoitus. Tietojen on oltava olennaisia ja rajoitettuja eli välttämättömiä käyttötarkoituksen kannalta.<br><br>Henkilötietoja säilytetään ainoastaan niin kauan kuin on tarpeen määritetyn käyttötarkoituksen kannalta. Henkilötietojen säilytysajat määritetään ja dokumentoidaan. |

| | |
|---|---|
| **Tiedon luottamuksellisuus ja turvallisuus** | Tietoja käsitellään luottamuksellisesti ja turvallisesti. Suojatoimenpiteet suhteutetaan arvioimalla käsittelyyn liittyvät riskit ja käsittelyyn liittyvät olosuhteet. Henkilötiedot suojataan teknisillä ja organisatorisilla suojatoimilla asianmukaisen eheyden, luottamuksellisuuden ja turvallisuuden varmistamiseksi, mukaan lukien suojaus luvattomalta tai laittomalta käsittelyltä sekä vahingossa tapahtuvalta katoamiselta, tuhoutumiselta tai vahingoittumiselta.<br><br>Henkilöstön ja sopimuskumppaneiden on noudatettava käsittelyyn liittyviä ohjeita ja tietoturvakäytäntöjä. |

## 6.2 Riskiperusteinen lähestymistapa ja riskien hallinta

Sipoon kunta noudattaa riskiperusteista lähestymistapaa kaikessa henkilötietojen käsittelyssä ja suunnittelee toimenpiteet sekä suojakeinot suhteuttaen ne käsittelyyn liittyviin tietosuojariskeihin. Henkilötietojen käsittely suunnitellaan ja toteutetaan koko elinkaaren ajan tietosuojaperiaatteiden ja muiden käsittelyyn soveltuvien vaatimusten mukaisesti, jotta sisäänrakennetun ja oletusarvoisen tietosuojan periaatteet toteutuvat.

Sipoo arvioi henkilötietojen käsittelyyn liittyviä riskejä toiminnassaan, mukaan lukien uusien järjestelmien hankinta, yhteistyö uusien toimittajien kanssa sekä olemassa olevat käsittelytoimet. Riskitasoa arvioidaan ja lain edellyttämissä tilanteissa käsittelytoimille tehdään tietosuoja-asetuksen mukainen tietosuojan vaikutustenarviointi. Vaikutustenarvioinnin tulosten avulla määritellään hallintakeinoja, joilla henkilötietojen käsittelystä aiheutuvia riskejä minimoidaan.

## 6.3 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sipoon kunta noudattaa sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita. Tietosuojaperiaatteet huomioidaan kaikessa toiminnassa mahdollisimman varhaisesta vaiheesta lähtien. Riskitasoon nähden asianmukaiset tekniset ja organisatoriset toimenpiteet toteutetaan.

## 6.4 Rekisteröityjen oikeudet

Sipoon kunta varmistaa tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien toteutumisen ylläpitämällä ja kehittämällä tarvittavia käytäntöjä.

Rekisteröityjen oikeudet toteutetaan siten, kuin ne kussakin tilanteessa soveltuvat huomioiden käsittelyn oikeusperusteen ja käsittelytilanteen. Rekisteröityjä informoidaan henkilötietojen käsittelystä läpinäkyvästi. Rekisteröidyllä on käsittelyn oikeusperusteiden mukaisesti oikeus saada tietoa henkilötietojensa käsittelystä, oikeus saada tutustua omiin tietoihinsa, oikaista tietojaan, poistaa tiedot, rajoittaa tietojensa käsittelyä, siirtää tiedot järjestelmästä toiseen, vastustaa tietojensa käsittelyä ja olla joutumatta automaattisen päätöksenteon kohteeksi.

Rekisteröityjen pyynnöt käsitellään lain edellyttämällä tavalla ja aikarajoissa. Rekisteröityjen pyyntöjen käsittelylle on määritetty asianmukaiset toimintaprosessit.

## 6.5 Henkilötietojen tietoturvaloukkaukset

Sipoon kunta pyrkii minimoimaan henkilöihin kohdistuvia tietoturvaloukkauksia suunnittelemalla henkilötietojen käsittelyn tietosuojaperiaatteiden mukaisesti sekä toteuttamalla tekniset ja organisatoriset suojatoimenpiteet, jotka suhteutetaan henkilötietojen käsittelyyn liittyvään riskiin rekisteröidyille.

Henkilötietojen tietoturvaloukkausten havaitsemiseen, ilmoittamiseen ja käsittelyyn on asianmukaiset prosessit, ohjeet ja dokumentointikäytännöt. Henkilötietojen tietoturvaloukkaukset käsitellään lain edellyttämällä tavalla ja aikarajoissa. Jos henkilötietojen tietoturvaloukkaus on jo tapahtunut, toimitaan tilanteisiin laaditun ohjeistuksen mukaan.

Jokaisella organisaation palveluksessa olevalla ja sen lukuun työskentelevällä on velvollisuus ilmoittaa huomaamastaan henkilötietoihin kohdistuvasta riskistä, havaitsemastaan poikkeamasta tai muusta vastaavasta tilanteesta.

## 6.6 Kolmannet osapuolet ja henkilötietojen siirrot

Tietosuoja huomioidaan kunnan ja eri osapuolten välisissä sopimuksissa. Sopimuksia tehdessä varmistetaan, että sopimusehdoissa varmistutaan tietosuojasäädöksien vaatimusten noudattamisesta. Kirjalliset ja tietosuojalainsäädännön mukaiset tietojenkäsittelysopimukset solmitaan kaikkien Sipoon kunnan käyttämien henkilötietojen käsittelijöiden kanssa.

Kolmansiin osapuoliin liittyviä tietosuojariskejä arvioidaan ja hallitaan tekemällä asiaankuuluvia riskiarviointeja ja asettamalla vähimmäisvaatimukset tietojen käsittelylle ennen kuin aloitetaan yhteistyö kolmansien osapuolten kanssa.

Sipoo ei lähtökohtaisesti siirrä henkilötietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle. Mahdollisten siirtojen osalta noudatetaan voimassa olevia lakeja ja asetuksia ja tietojen siirto toteutetaan asianmukaisella siirtoperusteella.

# 7 Koulutus ja tietoisuuden lisääminen

Henkilötietojen käsittelyyn liittyvää ohjeistusta tehdään sellaisiin työtehtäviin, joissa henkilötietoja käsitellään. Ohjeistukset tulee laatia tietosuojapolitiikan periaatteet huomioon ottaen. Tietosuoja-asioista viestitään organisaatiossa läpinäkyvästi.

Sipoo järjestää tietosuojan peruskoulutuksen henkilöstölleen perehdytyksen yhteydessä. Tietosuojapolitiikan sisällön omaksuminen on yhtenä osana uuden työntekijän perehdytystä. Tietosuojan peruskoulutusta tarjotaan säännöllisesti ja tehtäväkohtaisten tarpeiden mukaisesti järjestetään syventävää koulutusta. Osaamisen varmistamiseksi koko henkilöstöltä edellytetään vuosittain tietoturva- ja tietosuojakoulutuksen suorittamista.

Tietosuojan koulutukset suunnitellaan ja koulutussuunnitelmaa seurataan säännöllisesti.

# 8 Dokumentin tiedot ja versiohistoria

| Dokumentin tiedot | Selite |
|---|---|
| **Dokumentin nimi** | Sipoon tietosuojapolitiikka |
| **Omistaja** | Tietosuojavastaava |
| **Hyväksyjä** | Kunnanhallitus |
| **Hyväksymispäivämäärä** | 24.10.2022 |
| **Dokumenttia päivitetty** | 14.6.2022 |

| Versio | Pvm. | Muutokset | Tekijä |
|---|---|---|---|
| **1.0** | 24.10.2022 | Ensimmäinen hyväksytty versio | Privaon Oy |