
Tietoturvapäällikön tietosuojaopas

Matti Laakso, 2025
Tietojesiturvaksi.fi

Mitä ja kenelle?

Mitä kaikkea tietoturvapäällikön tulee tietää tietosuojasta?

Tietoturva ja tietosuoja ovat kaksi eri asiaa. Tämän lyhyen oppaan tarkoituksena on korostaa tietoturvan ja tietosuojan eroavaisuuksia, jotta molemmat aiheet saavat ansaitsemansa huomion organisaatioiden arjessa.

Tietoturvapäällikön tietosuojaopas on suunnattu kaikille tietoturvaa ja tietosuojaa kehittäville ja aiheista kiinnostuneille. Tietoturvapäällikkönä saat perustiedot tietosuojasta ja tietosuojavastaavan tehtävästä. Löydät oppaasta vinkkejä siihen, miten käytät asiantuntemustasi hyödyksi myös tietosuojatyössä.

Toimitko tietoturva-asiantuntijana tai tietoturvavastaavana? *Ihan sama, mitä tittelissäsi lukee!* Tässä oppaassa tietoturvapäälliköllä tarkoitetaan nimittäin kaikkia niitä organisaation arjen tekijöitä, jotka ovat vastuussa tietoturvan edistämisestä.

Tietosuojavastaavat ja tietosuoja-asiantuntijat saavat myös oppaasta uuden näkökulman omaan työhönsä. Johtajat ja muut rekrytoinnista vastaavat löytävät oppaasta vinkkejä siihen, millaista asiantuntijaa organisaatiosi tarvitsee.

Opas perustuu tietoturvablogini sisältöön. Löydät lisää tietoturvaan, tietosuojaan, kyberturvallisuuteen ja riskienhallintaan liittyviä julkaisuja osoitteesta **Tietoesituturvaksi.fi**

Oppaan sisältö

Tunne ainakin nämä tietosuojakäsitteet.....	3
Mitä eroa on tietosuojavastaavalla ja tietoturvapäälliköllä?.....	4
Voiko tietoturvapäällikkö olla tietosuojavastaava?.....	5
Miten tietoturvapäällikkö osallistuu tietosuojatyöhön?.....	6
Miten huomioit tietosuojavaatimukset tietoturvapäällikön työssä?.....	7

Tunne ainakin nämä tietosuojakäsitteet

Organisaatiosi käsittelee aina jonkun ihmisen henkilötietoja. Tämä henkilö on **rekisteröity**. Hän voi olla oman organisaatiosi työntekijä, yhteistyökumppanin edustaja tai asiakas. Rekisteröidyllä on **rekisteröidyn oikeudet**, jotka tulee huomioida osana henkilötietojen käsittelyä.

Henkilötietoja ovat kaikki tunnistettuun tai tunnistettavissa olevaan henkilöön liittyvät tiedot, kuten nimi, sähköpostiosoite jne. Henkilötietojen **käsittelyä** ovat kaikki henkilötietoihin kohdistetut toimet, kuten tietojen kerääminen, tallentaminen, siirtäminen ja poistaminen.

Rekisterinpitäjä on se, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Eli miksi tietoja käsitellään ja millä tavalla. Henkilötietojen **käsittelijä** käsittelee henkilötietoja rekisterinpitäjän puolesta. Rekisterinpitäjä kertoo, miten tietoja tulee käsitellä ja millaisia turvallisuusvaatimuksia tulee noudattaa. Tämä kirjataan **henkilötietojen käsittelysopimukseen**. Organisaation rooli henkilötietojen käsittelyssä on tiedettävä, jotta voidaan tunnistaa omaan organisaatioon liittyvät vaatimukset.

Henkilötietojen käsittelyssä on noudatettava aina ns. **tietosuojaperiaatteita**, jotka ovat:

- Lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- Käyttötarkoitussidonnaisuus
- Tietojen minimointi
- Tietojen täsmällisyys
- Säilytyksen rajoittaminen
- Eheys ja luottamuksellisuus
- Osoitusvelvollisuus

Periaatteista eheys ja luottamuksellisuus, eli käytännössä tietoturvallisuus, ovat tietysti tietoturvatyön näkökulmasta se olennaisin osio. Tutustuessasi periaatteiden sisältöön tarkemmin huomaat kuitenkin, että tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen ja osoitusvelvollisuus liittyvät myös tietoturvallisuuteen.

Tietosuojatyöhön liittyy keskeisesti **riskien arviointi**. Kuten tietoturvatyöhönkin. Näkökulma vain on eri. Tietosuojassa riskejä on arvioitava rekisteröidyn oikeuksien ja vapauksien näkökulmasta. Tietosuojaan **vaikutustenarviointi** on yksi tapa toteuttaa kattava riskiarvio. Vaikutustenarviointi on pakollinen tietyissä tilanteissa.

Organisaatiossasi voi työskennellä myös **tietosuojavastaava**. Hän on henkilötietojen käsittelyyn ja tietosuojalainsäädäntöön perehtynyt asiantuntija.

Henkilötiedot ovat suojeltavia kohteita, kuten muutkin tiedot ja tietojärjestelmät. Henkilötietojen suojaamisen merkitys on niin suuri, että organisaatioosi kohdistuu tietosuojavaatimuksia lainsäädännöstä, yhteistyökumppaneilta ja asiakkailta. Vaatimusten noudattaminen edellyttää suunnitelmallista ja riskilähtöistä toimintamallia.

(Sivun käsitteiden lähde GDPR lakiteksti <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>)

Mitä eroa on tietosuojavastaavalla ja tietoturvapäälliköllä?

Tietosuojavastaavan tehtävänä on valvoa, että yritys käsittelee henkilötietoja tietosuojalainsäädännön edellyttämällä tavalla. Tietosuojatyön tarkoituksena on suojata ihmisten henkilötietoja ja niihin liittyviä oikeuksia. Ihmisillä on esimerkiksi oikeus tietää, miten organisaatiot käsittelevät heidän tietojan, oikeus korjata vääriä tietoja, pyytää poistamaan tietoja jne.

Jokaisella on myös oikeus siihen, että tietojen turvallisuudesta huolehditaan. Eli tiedot eivät päädy ulkopuolisille, tai kukaan ei pääse urkkimaan niitä. Tämä on puolestaan sitä tietoturvaa ja tietoturvapäällikön tehtäväkenttää. Tietosuojavastaava on siis organisaation pääasiantuntija tietosuojan ja henkilötietoihin liittyvissä asioissa.

Tietoturvapäällikkö on puolestaan asiantuntija tietoturvaan ja kyberturvallisuuteen liittyvissä asioissa. Tietoturvapäällikön tehtävänä on varmistaa, että tiedot ja järjestelmät pysyvät turvallisina. Eli käytännössä pyritään suojelemaan ihmisiä ja järjestelmiä niin, että ei jouduta esimerkiksi kiristysahdettajien tai muiden kyberhyökkäysten uhriksi. Tai että organisaation tietoja ei pääse vuotamaan rikollisille.

Käytännössä siis huolehditaan käyttäjätunnuksista ja salasanoista, palomureista, virusohjelmien yms. teknisistä asioista. Lisäksi koulutetaan työntekijöitä toimimaan järkevästi netissä ja sähköpostissa sekä tehdään tietoturvaan liittyviä ohjeita ja sääntöjä.

Kuvan taulukkoon on koottu keskeisiä tietoturvapäällikön ja tietosuojavastaavan tehtävien eroja.

TIETOTURVAPÄÄLLIKKÖ	TIETOSUOJAVASTAAVA
Tietoturvallisuuden asiantuntija	Henkilötietojen suojan asiantuntija
Tehtävät organisaatiokohtaisia	Tehtävät lakisääteisiä
Vastaa tietoturvatyön ohjaamisesta	Valvoo tietosuojasäännösten noudattamista
Valvoo tietoturvatyötä	Valvoo myös tietoturvapäällikköä
On päättämässä tietojen suojaamisesta	Ohjaa, mutta ei voi päättää
Organisaation edustaja, voi ottaa vastaan ohjeita	Riippumaton taho, ei saa ottaa vastaan ohjeita
Toimii yhteistyössä toisen kanssa ja mahdollistaa fiksun ja turvallisen toiminnan	

Käytännössä tietosuojavastaava keskittyy henkilötietojen suojaan liittyviin näkökulmiin, kun taas tietoturvapäällikkö tarkastelee aihetta laajemmin. Tietosuojavastaavan tehtävänkuva on kerrottu GDPR:ssä, mutta molemmilla voi olla organisaation osoittamia (lisä)tehtäviä. Tietoturvapäällikön työ liittyy toteuttamiseen, tietosuojavastaavan tehtävät ovat riippumatonta ohjausta ja valvontaa.

Voiko tietoturvapäällikkö olla tietosuojavastaava?

Ei voi olla.

Houkutus näiden roolien yhdistämiselle on kuitenkin suuri. Se johtuu siitä, että tietoturvapäällikön ja tietosuojavastaavan tehtävät mielletään helposti samanlaisiksi ja toisiaan tukeviksi.

Kun asioita pohtii hieman pidemmälle, roolien erot alkavat hahmottua. Viimeistään käytännön työssä huomaa, että näiden roolien yhdistämisessä ei ole järkeä.

Pääsyy roolien erottamiselle on eturistiriita. GDPR:n mukaan tietosuojavastaavalla voi olla myös muita tehtäviä ja velvollisuuksia, mutta ne eivät saa aiheuttaa eturistiriitoja. Tässä muutamia mahdollisia ristiriitoja, jos tietoturvapäällikkö toimisi tietosuojavastaavana:

Tietoturvapäällikkö tekee päätöksiä suojatoimenpiteistä, joilla henkilötietoja suojataan. Tietosuojavastaava ei saa tehdä näitä päätöksiä. **Tietoturvapäällikkö ei saisi olla päättämässä oman vastuualueensa keskeisistä asioista.**

Tietosuojavastaavan tehtävänä on valvoa henkilötietojen käsittelyä. **Tietoturvapäällikön pitäisi valvoa myös itse itseään.**

Tietoturvapäällikkö edustaa rekisterinpitäjää ja suojelee ensisijaisesti organisaation etua. Tietosuojavastaavana hänen tulisi edustaa ensisijaisesti rekisteröityä. **Kenen etu on tärkein?**

Tietosuojavastaavan tehtävänä on neuvoa rekisterinpitäjää henkilötietojen käsittelyssä. **Tietoturvapäällikkö joutuisi neuvomaan itse itseään.**

Jos tietoturvapäällikkö olisi tietosuojavastaava, niin tilanne olisi erikoinen:
*Hän edustaa kaikkia tahoja. Hän neuvoo itse itseään ja keskustelee itsensä kanssa ratkaisuihin.
Lopuksi hän valvoo kaikkia – myös itseään. Huh!*

Käytännössä ongelmat konkretisoituvat esimerkiksi tietoturvatyökalujen hankinnan ja käyttöönoton yhteydessä. IT-ympäristön suojelemiseksi on olemassa erilaisia työkaluja, joilla pystyy seuraamaan, mitä ympäristössä tapahtuu ja mitä henkilöt tekevät. Tietosuojan näkökulmasta henkilötietoja pitää käsitellä mahdollisimman vähän ja kaikki pitää pystyä yksityiskohtaisesti perustelemaan. Tietoturvan takaamiseksi halutaan puolestaan nähdä mahdollisimman paljon. Ja tiedon on oltava tarkkaa, etenkin poikkeamatilanteiden selvittämistä varten.

Organisaation kannalta on hyödyllisintä, jos tietoturvapäällikkö ja tietosuojavastaava ovat eri henkilöitä, mutta he tekevät tiivistä yhteistyötä keskenään. Tietoturvapäällikön kannattaa olla hyvin perillä tietosuojavaatimuksista. Sekin auttaa, että tuntee tietosuojavastaavan tehtäväkenttää. Tietosuojavastaavan kannattaa puolestaan oppia ymmärtämään, mitä kaikkea tietoturvaan kuuluu ja mitä kaikkea teknisillä ratkaisuilla pystytään tekemään.

Miten tietoturvapäällikkö osallistuu tietosuojatyöhön?

Tietoturvapäälliköllä on luontainen ja tärkeä rooli myös organisaation tietosuoja-asioiden edistämisessä. Tietoturvan asiantuntijana hän katsoo samaa aihepiiriä eri näkökulmasta.

Tietosuojatyön ja tietoturvatyön yhteisenä tavoitteena on suojella ihmisten henkilötietoja ja niihin liittyviä oikeuksia. Tietoturvatyön kautta haetaan hallinnollisia ja teknisiä ratkaisuja, joilla henkilötietoja suojellaan.

Tietoturvapäällikkö ei voi ulkoistaa itseään tästä aiheesta. On kaikkien etu, kun asioita edistetään yhdessä.

Organisaatiot myös odottavat sitä, että tietoturva-asiantuntija osallistuu myös tietosuojatyöhön. Tämä on nähtävissä esimerkiksi tietoturvapäälliköiden rekrytointi-ilmoituksissa.

Tehtäviä, joissa tietoturvapäällikkö osallistuu tietosuojatyöhön:

Henkilötietojen käsittelyn turvaaminen osana perustyyötä

Tietoturvapäällikön perustyyö on tietojen suojaamista. Myös henkilötietojen suojaamista. Tietoturvan asiantuntijana hän osallistuu mm. turvallisten tietojenkäsittelyratkaisujen suunnitteluun.

Henkilötietojen suojaan liittyvien riskien arviointi ja DPIA

Henkilötietojen käsittelyyn liittyy aina tietoturvariskejä. Tietoturvapäällikkö on tärkeässä roolissa näiden riskien arvioinnissa. Ja suojatoimenpiteiden toteuttamisessa.

DPIA-prosessi* voidaan rakentaa sellaiseksi, että tietoturvapäällikkö antaa lausuntonsa suunnitellusta henkilötietojen käsittelystä. Kun vaihe on osa prosessia, tietoturva huomioidaan asianmukaisesti etukäteen. (Data Protection Impact Assessment, tietosuojan vaikutustenarviointi)

Henkilötietojen tietoturvaloukkausten käsittely

Tietoturva-asiantuntijat ovat mukana organisaation tietoturvaloukkausten käsittelyssä.

Henkilötietojen tietoturvaloukkauksia, pienempiä ja suurempia, tapahtuu jatkuvasti.

Tietosuojavaaltuutetun toimiston toimintakertomuksessa todetaan, että vuonna 2024 TSV:lle tuli vireille 7152 tietoturvaloukkausilmoitusta. (Lähde <https://tietosuoja.fi/toimintakertomus-2024>)

Auta tietosuojavastaavaa onnistumaan

Tietoturvapäällikkönä voit edesauttaa tietosuojaa omassa roolissasi ja toimia tietosuojavastaavan apuna:

- Tuo tietosuoja-asioita ja -vaatimuksia esille muille työntekijöille myös oman työsi kautta.
- Tarjoa ratkaisuja, tai edes ehdotuksia, tietosuojatyön tueksi.
- Osallistu tietosuojatyöhön konkreettisesti. Molemmat hyötyvät.
- Älä vaikeuta tietosuojatyötä omilla puheillasi. Puhutko tietosuoja vaatimuksista negatiiviseen sävyyn?

Miten huomioit tietosuojavaatimukset tietoturvapääallikön työssä?

Tietosuojavaatimukset ulottuvat myös tietoturvatyöhön. Tietoturvavastaavana olet yhtä lailla velvollinen huomioimaan tietosuojavaatimuksia omassa työssäsi, ja suunnittelemaan ratkaisuja henkilötietojen suoja huomioiden.

GDPR ja muu tietosuojalainsäädäntö edellyttävät, että henkilötietojen tietoturvallisuudesta huolehditaan. Tietoturva on keskeinen osa henkilötietojen suoja, joten tietojen turvaamisella voidaan helposti yrittää perustella lähes mitä vain.

Se ei silti tarkoita, että tietoturva-asiantuntijat voivat ohittaa tietosuojavaatimukset:

Tietoturva-asiantuntijoilla ei ole vapaalippua kaikkeen tekemiseen.

Tietoturvatyössä käsitellään yhtä lailla henkilötietoja. Tietoturvatyössä käytettävät työkalut ovat myös astetta rajummat.

Oletko koskaan pohtinut, mihin kaikkialle sinulla ja IT-henkilöstöllä on pääsy? Millaisia työkaluja käytätte? Mitä kaikkea näillä työkaluilla voi tehdä ja nähdä?

Mieti esim. mitä kaikkea näet, ja voit tehdä näiden järjestelmien kautta:

- Lokienhallintatyökalut – mitä ihmiset tekevät järjestelmissä?
- AV ja EDR – mitä työasemilla ja palvelimilla tapahtuu?
- Palomuuuri ja VPN – millaista tietoliikennettä verkossa liikkuu?
- Microsoft 365 ja Teams, sähköposti, pikaviestisovellukset yms. – millaista viestiliikennettä organisaatiossa on?
- Käyttäjätunnukset – mihin henkilöstö kirjautuu?

Haluatko ymmärtää paremmin tietoturvatyöhön liittyviä tietosuojavelvollisuuksia? Tee näin:

1. Selvitä millaisia tietoturva- tai muita valvontatyökaluja organisaatiossasi on käytössä.
2. Keskustele työkaluista tietosuojavastaavan kanssa.
3. Toteuta tietosuojariskien arviointi jollekin käytössä olevalle ylläpito- tai tietoturvatyökalulle.

Tietoturvapääallikön tietosuojaopas

**Lisää vinkkejä organisaatiosi tietoturvan, tietosuojan,
kyberturvallisuuden ja riskienhallinnan kehittämiseen löydät
osoitteesta [Tietojesiturvaksi.fi](https://tietojesiturvaksi.fi)**

Matti Laakso, 2025
[Tietojesiturvaksi.fi](https://tietojesiturvaksi.fi)