



**Suomen Hissiyhdistys ry**

**Tietosuoja ja henkilötietojen käsittely**

## Sisälllys

Johdanto.....	3
Roolit .....	4
Miksi tietoa kerätään ja miten sitä säilytetään .....	5
Jäseneksi hakeutuminen .....	5
Jäsenrekisteri .....	5
Jäsentiedotus .....	5
Tietojen edelleen luovutus.....	5
Riskit ja riskienhallinta.....	6
Riskit .....	6
Johtaminen.....	6
Toimitilat .....	6
Tietojärjestelmien suojaus .....	6
Henkilöstön toiminta .....	6
Suhteet sidosryhmiin .....	7
Kehittäminen ja toiminnan jatkuvuus .....	7
Sisäänrakennettu tietosuoja .....	7
Oikeus saada tietoa henkilötietojen keräämisestä ja käsittelystä .....	7
Oikeus päästä omiin tietoihin ja tietojen oikaisuun.....	7
Oikeus tulla unohdetuksi.....	8
Oikeus siirtää tiedot järjestelmästä toiseen .....	8
Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle .....	8

## Johdanto

Suomen Hissiyhdistys ry on hissialalla toimivien yritysten toimialajärjestö, joka vaikuttaa alan viranomaissäädöksiin, edistää alan ammattipätevyyttä ja arvostusta ja auttaa turvaamaan pätevän henkilöstön saatavuutta. Toiminnan keskiössä on alan hyvien käytäntöjen kehittäminen ja julkaiseminen, hissialan työturvallisuuskoulutuksen järjestäminen sekä alan toimintaympäristöä edistävä sidosryhmäyhteistyö. Toiminnastamme voit lukea lisää osoitteessa [www.hissiyhdistys.fi](http://www.hissiyhdistys.fi).

Henkilötietojen käsittelyyn voimassa olevan lainsäädännön mukaisesti on kiinnitetty erityistä huomiota jo ennen 25.5.2018 voimaan tullutta EU:n tietosuoja-asetusta (General Data Protection Regulation, GDPR). GDPR tietosuoja-asetus on tarkentanut henkilötietojen käsittelyä omalta osaltaan. Tässä dokumentissa kuvataan, miten Suomen Hissiyhdistys ry:ssä toimitaan. Tietosuoja-asetuksen perustarkoitus on pitää yritysten hallussa olevat henkilötiedot ajan tasalla, turvassa ja saatavilla ja vain niille, jotka tietoa tarvitsevat.

Noudatamme tietosuoja-asetuksen ydinhengen mukaisesti sisäänrakennetun tietosuojan (Privacy by Design) periaatteita. Olemme päivittäneet sähköiset järjestelmämme toimintavarmiksi ja turvallisiksi tätä henkeä silmällä pitäen.

Otamme mielellään vastaan tietosuojaan liittyvää palautetta ja kysymyksiä toimintamme parantamiseksi. Tietoturvaan ja tietosuojaan liittyvissä asioissa voit olla yhteydessä asiamieheemme Olli Vitikka

[olli.vitikka@stul.fi](mailto:olli.vitikka@stul.fi).

## Roolit

Ohessa on lyhyesti kerrottu keskeisiä tietosuoja-asetuksessa käytettyjä termejä.

### Rekisterinpitäjä

Suomen Hissiyhdistys ry toimii rekisterinpitäjänä. Rekisterinpitäjä tekee sisältöön, prosesseihin ja henkilötietoihin käyttöoikeuksiin liittyvät päätökset.

### Yhteisrekisterin pitäjä

Jos eri rekisterinpitäjät yhteisesti määräävät henkilötietojen käsittelystä, voivat he toimia yhteisrekisterin pitäjänä. Yhteisrekisterin pitäjät voivat yhdessä määrittellä mikä rekisterinpitäjä toimii yhteyspisteenä rekisteröidyille. Suomen Hissiyhdistys ry on ulkoistanut palvelusopimuksella jäsenrekisterin ylläpitämisen Sähkö- ja Teleurakoitsijaliitto STUL ry:lle. Sähkö- ja Teleurakoitsijaliitto STUL ry:n rekistereitä ylläpitää sen kustannusyhdistiö Sähköinfo Oy. Sähköinfo Oy toimii yhteisrekisterin pitäjänä STUL ry:lle ja sen jäsenjärjestöille, jollainen Suomen Hissiyhdistys ry on.

### Henkilötietojen käsittelijä

Palveluntarjoajat, jotka tuottavat meille järjestelmiä toimivat henkilötietojen käsittelijöinä. Palveluntarjoajat käsittelevät tietoja ainoastaan tuottaakseen nimettyä järjestelmää. Palveluntarjoajat ovat vastuussa meille sopimusperusteisesti sekä tietysti suoraan viranomaisille. Käsittelemme eri palveluntarjoajat myöhemmin tässä dokumentissa.

### Rekisteröity

Rekisteröity-termillä tarkoitetaan henkilöitä, joiden tietoja käsitellään.

### Oikeus käsitellä henkilötietoja

Oikeus käsitellä tietoja voi perustua hakemukseen, jonka yritys lähettää jäsenyyttä hakiessaan, sopimukseen tai oikeutettuun etuun.

*Suostumuksella* tarkoitetaan sitä, kun rekisteröity antaa suostumuksen tietojen käsittelyyn esim. tuoteoston yhteydessä.

*Sopimuksen* myötä syntyvä käsittelyoikeus edellyttää sopimuksen kautta syntyvää oikeutta sopimuksen ehtojen toimeenpanemiseksi.

*Oikeutettuun etuun* perustuva käsittelyoikeus muodostuu, kun tietojen käsittely on tarpeen etuuden tuottamiseksi, esimerkiksi Jäsen sopimukset.

*Lakisääteinen oikeus* muodostuu, kun rekisterinpitäjällä on velvoite käsitellä tietoja.

## Miksi tietoa kerätään ja miten sitä säilytetään

### Jäseneksi hakeutuminen

Suomen Hissiyhdistys ry:n jäseniä ovat hissialalla toimivat yritykset. Yritykset ilmoittavat jäsenhakemuksella yhteyshenkilön yhteystiedot. Yhteystietoja käytetään jäsenviestintään ja jäsenetujen toimittamiseen.

Suomen Hissiyhdistys ry:n hallitus käsittelee kaikki jäsenhakemukset ja hyväksyy jäsenyyden ehdot täyttävät yhdistyksen jäseniksi. Hallituksella on pääsy jäsenhakemustietoihin, mutta heille ei jää kopioita hakemuksista. Hallituksen voimassa olevan kokoonpanon saa yhdistysrekisteristä tai yhdistyksen asiamieheltä [olli.vitikka@stul.fi](mailto:olli.vitikka@stul.fi).

Jäsenhakemus toimitetaan yhdistykselle joko kirjeitse postin välityksellä tai sähköpostin liitteenä. Paperilla toimitetut hakemukset skannataan sähköiseen arkistoon, eikä paperiversioita säilytetä. Kaikki hakemukset säilytetään sähköisessä muodossa tietojärjestelmässä. Hakemuksen sähköiseen muotoon tallentamisen jälkeen paperihakemus hävitetään tietoturvaisella tavalla.

Sähköisesti tiedostot ovat tallennettuina Sähköinfon lukuun Decens Oy:n ylläpitämillä tiedostopalvelimilla EU:n alueella. Sähköposti tuotetaan Sähköinfon lukuun Microsoftin O365 -palvelulla Decens Oy:n toimesta.

### Jäsenrekisteri

Suomen Hissiyhdistys ry on ulkoistanut jäsenrekisterin ylläpidon palvelusopimuksella Sähkö- ja Teleurakoitsijaliitto STUL ry:lle. STUL ry:n jäsenrekisteriä ylläpitää yhteisrekisterinpitäjänä Sähköinfo Oy. Jäsenrekisteri on sähköinen ja sitä tuottaa Sähköinfon lukuun Business Databases Oy.

Sivustolla [www.hissiyhdistys.fi](http://www.hissiyhdistys.fi) on erillinen extranet vain jäsenten käyttöön. Kullakin jäsenellä on henkilökohtainen käyttäjätunnus ja salasana. Jäsensivuja ja siellä käytettäviä salasanoja hallinnoi Sigmatic Oy.

### Jäsentiedotus

Eräs keskeisimmistä toiminnoistamme on tiedottaminen hissialaan liittyvistä asioista. Hoidamme tiedotusta verkkosivujen ja sähköpostin kautta. Jäsentiedotusta varten henkilöiden tietoja ylläpidetään jäsenrekisterissä ja viestit lähetetään O365 Outlook -sähköpostiohjelmistolla aina piilokopioina.

### Jäsenkoulutus

Suomen Hissiyhdistys ry tuottaa hissialaan liittyvää osaamista kehittävää ja ylläpitävää koulutusta yhteistyössä Sähköinfo Oy:n kanssa. Koulutuksen järjestelyistä vastaa palvelusopimuksella Sähköinfo Oy. Koulutuksiin osallistujien osalta noudatetaan Sähköinfo Oy:n tietosuojakuvausta.

### Tietojen edelleen luovutus

Suomen Hissiyhdistys ry on Sähkö- ja teleurakoitsijaliitto STUL ry jäsenjärjestö. Jäsenjärjestönä Suomen Hissiyhdistys ry:n jäsenet ovat oikeutettuja saamaan STUL ry:n jäsenetuja. Näiden etujen toimittamiseksi Suomen Hissiyhdistys ry luovuttaa jäsentietonsa Sähkö- ja teleurakoitsijaliitto STUL ry:lle.

Suomen hissiyhdistys ry on ulkoistanut palvelusopimuksella toimistopalveluidensa ja järjestelmiensä hallinnan Sähkö- ja teleurakoitsijaliitto STUL ry:lle. Sähkö- ja teleurakoitsijaliitto STUL ry:lle näitä palveluita tuottaa Sähköinfo Oy, STUL:n 100 % omistusyhtiö.

Suomen Hissiyhdistys ry:n toiminnan tarkastajina toimivat vuosikokouksessa valitut toiminnan tarkastajat. Toiminnan tarkastajiksi valittujen henkilöiden nimet saa asiamieheltä [olli.vitikka@stul.fi](mailto:olli.vitikka@stul.fi).

## Riskit ja riskienhallinta

Tietoriskien hallinta muodostuu riskien tunnistamisesta ja olennaiset osat riskien hallinnasta liittyvät tekniseen suojaamiseen ja henkilöstön osaamisen varmistamiseen.

Tietoriskien kannalta tärkeitä on että,

- tiedot ovat oikeita, luotettavia ja ajan tasalla
- tiedot ovat oikeutettujen henkilöiden saatavilla
- tiedot eivät joudu asiaankuulumattomille henkilöille.

## Riskit

Henkilötietoihin liittyvät riskit ovat tietojen oikeellisuus, oikea-aikainen saatavuus oikeille henkilöille, tietojen väärinkäyttö tai tietojen katoaminen. Henkilötietoja ylläpidetään säännöllisesti ja niihin tehdään tarkennuksia rekisteröidyn ilmoituksen perusteella tai ulkoisista lähteistä.

Tietojärjestelmiä varmistetaan niin, että ne ovat saatavilla oikeille henkilöille silloin, kun niitä tarvitaan. Järjestelmäkumppaneiden kanssa on sovittu erikseen sopimuksilla erillisistä palvelutasoista, milloin tietojen pitää olla käytettävissä häiriötilanteissa.

Tietojen väärinkäyttöä estetään käyttöä suojaamalla ja henkilöstöä opastamalla. Suurin tietoriski on henkilöiden toiminta, tätä hallitaan kouluttamalla ja ohjeistamalla henkilöstö tietojen oikeanlaiseen käsittelyyn.

Sellaisessa tilanteessa, jossa tietoja päätyisi väärin käsiin, noudatetaan tietosuoja-asetuksen ilmoittamismenettelyä. Ilmoitusmenettelystä on sovittu ja dokumentoitu toimintamallit.

## Johtaminen

Johto on tietoinen yrityksen hallussa olevista tietovarannoista ja siitä, miten niitä käytetään ja suojataan. Johto vastaa tietoturvapoliittikan ylläpitämisestä ja käytäntöön viemisestä. Johto vastaa siitä, että henkilöstöllä on riittävät mahdollisuudet tietoturvaliiseen tietojen käsittelyyn.

## Toimitilat

Toimitilat on suojattu ulkopuolisilta. Mekaanisten lukitusten lisäksi käytössä on elektroninen kulunvalvonta. Arkaluontoista tietoa sisältävät fyysiset arkistot säilytetään lisäksi lukituissa tiloissa. Avainhallinta on keskitettyä ja henkilöstön ulkopuolelle annetut kulkuoikeudet on dokumentoitu. Virustorjunta ja palomuurit ovat ajan tasalla ja palomuriavaukset dokumentoitu.

Arkaluontoisten dokumenttien tuhoamista varten on käytettävissä silppureita tai erillinen lukittu tietosuoja-säiliö, jonka tietoturvaliisesta tyhjennyksestä ja dokumenttien tuhoamisesta vastaa MTB Tietopalvelut Oy.

## Tietojärjestelmien suojaus

Tietojärjestelmien hallinta on ulkoistettu ja konesalin turvallisuudesta vastaa Decens Oy. Kunkin käytetyn järjestelmän kohdalla on kuvattu kyseiseen tietoon liittyvä kumppani. Etäkäyttö on mahdollista vain suojatun VPN-yhteyden kautta. Käyttöä suojataan käyttöoikeuksin.

## Henkilöstön toiminta

Jokainen työntekijä on koulutettu tietoturvaliiseen tietojen käsittelyyn. Henkilöstön kanssa on käyty läpi tietoturvapoliittikka aina sen muututtua olennaisesti. Tietojen käsittelystä on selkeät toimintaohjeet.

Henkilöstön kanssa on käyty läpi myös henkilötiedoista keskustelun periaatteet. Julkisissa tiloissa yhdistyksen asioista ja asiakkaista keskusteleminen on tietoturvaohjeessa kielletty.

## Suhteet sidosryhmiin

Alihankkijoita valitessa ja kumppanuussopimuksia solmittaessa turvallisuuden hallintaan liittyvät asiat on käyty läpi. Sopimukset ovat ajan tasalla ja niitä päivitetään säännöllisesti. Luottamushenkilöt ymmärtävät luottamusasemansa tuomat oikeudet tietovarantoihin ja niiden luottamukselliseen käsittelyyn.

## Kehittäminen ja toiminnan jatkuvuus

Tietosuojakuvaukset ja tietovarannot on dokumentoitu, samoin tietotekniset järjestelmät. Tietoteknisestä ympäristöstä on tehty palautumis- ja jatkuvuussuunnitelma ja tiedot on varmistettu. Toiminnan jatkuvuuden kannalta avainhenkilöt on tunnistettu.

*GDPR tarkentaa tiettyjä rekisteröidyn oikeuksia. Esitämme seuraavassa, miten olemme huomioineet nämä muutokset.*

## Sisäänrakennettu tietosuoja

Henkilötietojen yksityisyys ja tietoturva ovat prosessiemme perusteissa. Toimintaamme sisältyy henkilötietojen käsittelyä, ja sekä yksityisyys että tietosuojan noudattaminen ovat olennainen osa palveluamme, niin palvelun kehityksessä, ylläpidossa, tuessa kuin myynnissä ja markkinoinnissakin. Yksityisyys on tärkeä osa myös kaikkia kehityshankkeitamme. Tietojen käsittelyjärjestelmämme on tehty mahdollisimman turvalliseksi. Käytämme turvallisuutta ja hallintaa kumppanien valintaperusteissa ja kehitämme sekä teknisiä että omia toimintatapojamme taataksemme henkilötietojen turvallisen käsittelyn.

## Oikeus saada tietoa henkilötietojen keräämisestä ja käsittelystä

*Rekisteröidyillä on oikeus saada tietää, milloin ja mitä heitä koskevia henkilötietoja käsitellään ja mitä tallennetaan.*

- Keräämme vain tietoa, joka on tarpeen palveluiden tuottamiseksi.
- Säilytämme henkilötietoja huolellisesti. Säilytämme tietoja ainoastaan sähköisesti. Sähköisiä tietoja säilytämme tietojärjestelmissä, joissa tietojen käsittelyä suojataan käyttöoikeuksin.
- Tietosuoja- ja rekisteriselosteenne ovat jatkuvasti nähtävillä verkkopalvelussamme.
- Jos jokin tietojen käsittelyyn vaikuttava lainsäädäntö muuttuu olennaisesti, tiedotamme muutoksista.

## Oikeus päästä omiin tietoihin ja tietojen oikaisuun

*Rekisteröidyillä on oikeus saada pääsy omiin tietoihinsa ja saada epätarkat ja virheelliset tiedot korjattua.*

- Rekisteröidyillä on oikeus saada jäljennös hallussamme olevista tiedoista. Pyynnöstä toimitamme jäljennöksen tiedoista sähköisesti. Jäljennöksen voi pyytää sähköpostitse yhdistyksen asiamieheltä  
[olli.vitikka@seti.fi](mailto:olli.vitikka@seti.fi)
- Toimitamme pyynnöt viivyttämättä ja tietosuoja-asetuksen mukaisessa määräajassa 1 kk.
- Ylläpidämme tietoja ja päivitämme yhteystietoja ilmoituksesta.

## Oikeus tulla unohdetuksi

*Rekisteröidyillä on oikeus saada tietonsa poistetuksi, kun tiedon käsittely ei ole enää aiheellista.*

- Unohdetuksi tulemisen vaihtoehtoina voi käyttää postikieltoa, passivointia tai rajoitetusti poistoa.
- Tuotteiden myyntiin ja toimittamiseen liittyen tietoja voidaan pyynnöstä poistaa, ei kuitenkaan niiltä osin, kun niihin liittyy lakisääteisiä säilytysaikoja esim. laskuttamiseen liittyen.

## Oikeus siirtää tiedot järjestelmästä toiseen

*Rekisteröidyillä on oikeus saada omat tietonsa helposti luettavassa muodossa sekä siirtää kyseiset tiedot toiselle rekisterinpitäjälle.*

- Tallennetut tiedot voidaan pyynnöstä toimittaa asiakkaalle sähköisessä muodossa tietojen siirtämistä varten.
- Paperimuotoiset tiedot toimitetaan sähköisenä PDF-muodossa.
- Muut henkilötiedot toimitetaan sähköisenä CSV-tiedostona.

## Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle

*Tietoturvaloukkaukset tulee raportoida viranomaisille 72 tunnin kuluessa.*

- Olemme valinneet järjestelmätoimittajat tarkasti ja luotamme suomalaisiin kumppaneihimme, joten tietojasi säilytetään huolellisesti ja valvotusti.
- Tietokanta- ja tiedostopalvelimet ovat asiantuntevien kumppaneidemme hallinnassa ja niitä säilytetään Decens Oy:n lukuun EU:n alueella. Ne täyttävät seuraavat standardit: TIA-942, ISO/IEC 27001:2005, ISO 9001:2008, ISO 14001:2004. Salit ovat Tier 3 - tason tiloja.
- Olemme sopineet kumppaneiden kanssa menettelystä, jolla tietoturvaloukkauksista informoidaan.
- Henkilökuntamme on koulutettu luottamuksellisen tiedon käsittelyyn.
- Epätodennäköisessä tilanteessa, jossa tietoturvaloukkaus tapahtuisi, ilmoitamme rekisteröidylle ja viranomaiselle.