Tietosuojavastaavan nimittäminen ja tehtävät

14.9.2022

Harto Pönkä
Innowise

Kuva: Pixabay

Milloin tietosuojavastaava tulee nimetä?

- Tietosuojavastaavan (eng. Data Protection Officer, DPO) tehtävä perustuu yleensä EU:n yleiseen tietosuoja-asetukseen (GDPR art. 37-39).
- SOTE-alan palveluntuottajien ja apteekkien on pitänyt asettaa tietosuojavastaava vuodesta 2007 lähtien (lait 61/2007 ja 159/2007).
- Tietosuojavastaavan nimittäminen on monessa tapauksessa **pakollista**:
  - Rekisterinpitäjä on julkishallinnon toimija (poislukien tuomioistuimet tiettyjen tehtäviensä osalta)
  - Ydintehtävät edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa
  - Ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin (mm. terveys, entinen alkuperä, poliittiset mielipiteet, uskonnollinen vakaumus, seksuaalinen suuntautuminen) tai rikostuomioita tai rikkomuksia koskeviin tietoihin.
- Ydintehtäviä eivät ole tavalliset tukitoiminnot kuten palkanmaksu ja IT-tuki.
- Jos organisaation on nimitettävä tietosuojavastaava, tulee sellainen olla **koko ajan**. Esim. vakituisen tietosuojavastaavan loman ajaksi voidaan nimittää sijainen.

Lisätietoa: Tietosuoja-asetuksen 4 jakso,
http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL#d1e3702-1-1

Mitä on ”laajamittainen” henkilötietojen käsittely?

- Rekisteröityjen lukumäärä – joko täsmällinen lukumäärä tai osuus väestöstä
- Käsiteltävä tietomäärä ja/tai käsiteltävien tietotyyppien määrä
- Tietojen käsittelytoiminnan kesto tai pysyvyys
- Käsittelytoiminnan maantieteellinen laajuus

- Esimerkkejä laajamittaisesta henkilötietojen käsittelystä:
  - Potilastietojen käsittely sairaalan tavanomaisessa toiminnassa
  - joukkoliikennejärjestelmän käyttäjien matkatietojen käsittely
  - Kansainvälisen pikaruokaketjun asiakkaiden reaaliaikaisten sijaintitietojen käsittely
  - Asiakastietojen käsittely vakuutusyhtiön tai pankin liiketoiminnassa
  - Henkilötietojen käsittely käyttötottumuksia seuraavaa mainontaa varten
  - Puhelin- tai internetpalveluntarjoajien suorittama tietojenkäsittely

- Sen sijaan esim. yksittäisen lääkärin tai asianajajan toimintaa ei katsottane laajamittaiseksi

Lähde: WP243 liite, usein kysyttyä tietosuojavastaavista, https://tietosuoja.fi/documents/6927448/8316711/Tietosuojavastaavat+UKK+fi.pdf/006f8dcb-540a-403e-a29d-b8a4b7c4814f/Tietosuojavastaavat+UKK+fi.pdf.pdf/Tietosuojavastaavat+UKK+fi.pdf.pdf

Mitä tarkoitetaan ”säännöllisellä ja järjestelmällisellä seurannalla”?

- GDPR:ssä ei määritellä säännöllisen ja järjestelmällisen seurannan käsitettä, mutta siihen sisältyy ainakin seuraaminen ja profilointi internetissä, myös mainontaa varten.
- ”Säännöllisellä” tarkoitetaan:
  - toiminta jatkuu tai toteutetaan tietyin aikavälein tietyn ajan
  - toiminta toistuu tai toistetaan määritettyinä aikoina
  - toiminta on jatkuvaa tai ajoittaista.
- ”Järjestelmällisellä” tarkoitetaan:
  - toiminta on järjestelmän mukaista
  - toiminta on ennalta järjestettyä, organisoitua tai menetelmällistä
  - toiminta toteutetaan osana yleistä tiedonkeruusuunnitelmaa
  - toiminta toteutetaan osana strategiaa.
- Esimerkkejä: tietoliikenneverkkojen ja -palvelujen ylläpito, uudelleenmarkkinointi sähköpostitse, dataohjattu markkinointitoiminta, profilointi ja pisteyttäminen riskinarviointia varten, sijainnin seuraaminen, kanta-asiakasohjelmat, videovalvonta, IoT-laitteet kuten älymittarit, älyautot ja kodin automaatio.

Lähde: WP243 liite, usein kysyttyä tietosuojavastaavista, https://tietosuoja.fi/documents/6927448/8316711/Tietosuojavastaavat+UKK+fi.pdf/006f8dcb-540a-403e-a29d-b8a4b7c4814f/Tietosuojavastaavat+UKK+fi.pdf.pdf/Tietosuojavastaavat+UKK+fi.pdf.pdf

Muuta tietosuojavastaavan nimittämisessä huomioitavaa

- **Eturistiriitojen välttämiseksi tietosuojavastaava ei saisi olla asemassa, jossa hän päättää henkilötietojen käsittelyn tarkoituksista tai keinoista.**
  - Ylempi johtoasema (esim. hallintojohtaja, talousjohtaja, johtava lääkäri, markkinointipäällikkö, henkilöstöpäällikkö tai IT-päällikkö) voi aiheuttaa eturistiriidan.
  - Myöskään tietoturvavastaavaa ei tulisi nimittää tietosuojavastaavaksi.

- Tietosuojavastaavan voi nimittää myös **vapaaehtoisesti**
  - Jos tietosuojavastaava nimitetään, sen rooli määräytyy GDPR:n mukaisesti.
  - Yleensä on suositeltavampaa nimittää tietosuojasta vastaava henkilö tms. kuin vapaaehtoisesti tietosuojavastaava.

- Konsernilla sekä usealla julkishallinnon organisaatiolla voi olla yhteinen tietosuojavastaava.
- Tietosuojavastaava voi olla ulkoistettu palveluntarjoaja.
- Jos tietosuojavastaavaa ei nimitetä, kannattaa dokumentoida sen perustelut.

Lisätietoa: Tietosuoja-asetuksen 4 jakso,
http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN&toc=OJ:L:2016:119:FULL#d1e3702-1-1

Tietosuojavastaavan pätevyys

- Asiantuntemus kansallisesta ja EU:n tietosuojalainsäädännöstä ja alan käytänteistä, myös GDPR:n perusteellinen tuntemus
- Suoritettujen käsittelytoimien tuntemus
- Tietojärjestelmien ja tietoturvan tuntemus
- Toimialan ja organisaation tuntemus
- Valmiudet edistää tietosuojakulttuuria organisaatiossa

→ Ei muodollisia vaatimuksia, vaan tehtävään sopiva osaaminen.

→ Itsenäinen ja rehellinen, rohkeus viestiä ja tuoda asiat esiin.

Lähde: Tietosuojatyöryhmä: Tietosuojavastaavia koskevat ohjeet, 2016, https://tietosuoja.fi/documents/6927448/8316711/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf/

Kenellä on vastuu tietosuojasta?

Rekisterinpitäjä

- Vastuussa rekisterin henkilötietojen käsittelyn lainmukaisuudesta
- Voi olla yksi tai useampi henkilö, yritys tai muu organisaatio

Organisaation johto ja esimiehet

- Kokonaisvastuu henkilötietojen käsittelyn lainmukaisuudesta
- Esimerkin näyttäminen

Rekisterinpitäjä päättää ”tarkoitukset ja keinot” ja toimeenpanee ne. Velvollisuus kuulla tietosuojavastaavaa.

Tietosuojavastaavalla on tärkeä rooli riskiarvioinnissa, vaikutustenarvioinnissa ja suositusten annossa!

Tietosuojavastaava

- Vastaa neuvonnasta, kehittämisestä ja seurannasta sekä yhteydenpidosta valvontaviranomaiseen

Henkilöstö

- Jokainen on vastuussa toiminnastaan
- Ohjeiden noudattaminen
- Ongelmista ilmoittaminen

Tietosuojavastaavan asema

- **Tietosuojavastaavalla tulee olla johdon tuki ja hän raportoi suoraan johdolle.**

- **Organisaation on varmistettava, että tietosuojavastaava otetaan mukaan kaikkien henkilötietoja koskevien kysymysten käsittelyyn.**
  - Jos tehdään kyseenalaisia päätöksiä, tietosuojavastaavalle olisi annettava tilaisuus esittää eriävä mielipiteensä ylimmälle johdolle ja päätöksentekijöille.

- **Tietosuojavastaavalle ei saa antaa tehtäviä, jotka aiheuttaisivat ristiriidan tehtävän hoidolle.**

- Tehtävä on luonteeltaan pysyvä, joten työsuhteen olisi hyvä olla jatkuva.
- Riippumaton: ei saa ottaa vastaan ko. tehtävien hoitoa koskevia ohjeita.
- Ei saa erottaa, rangaista tai uhata seurauksilla tehtävään liittyvien toimenpiteidensä vuoksi.

Lähde: Tietosuojatyöryhmä: Tietosuojavastaavia koskevat ohjeet, 2016, https://tietosuoja.fi/documents/6927448/8316711/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf/

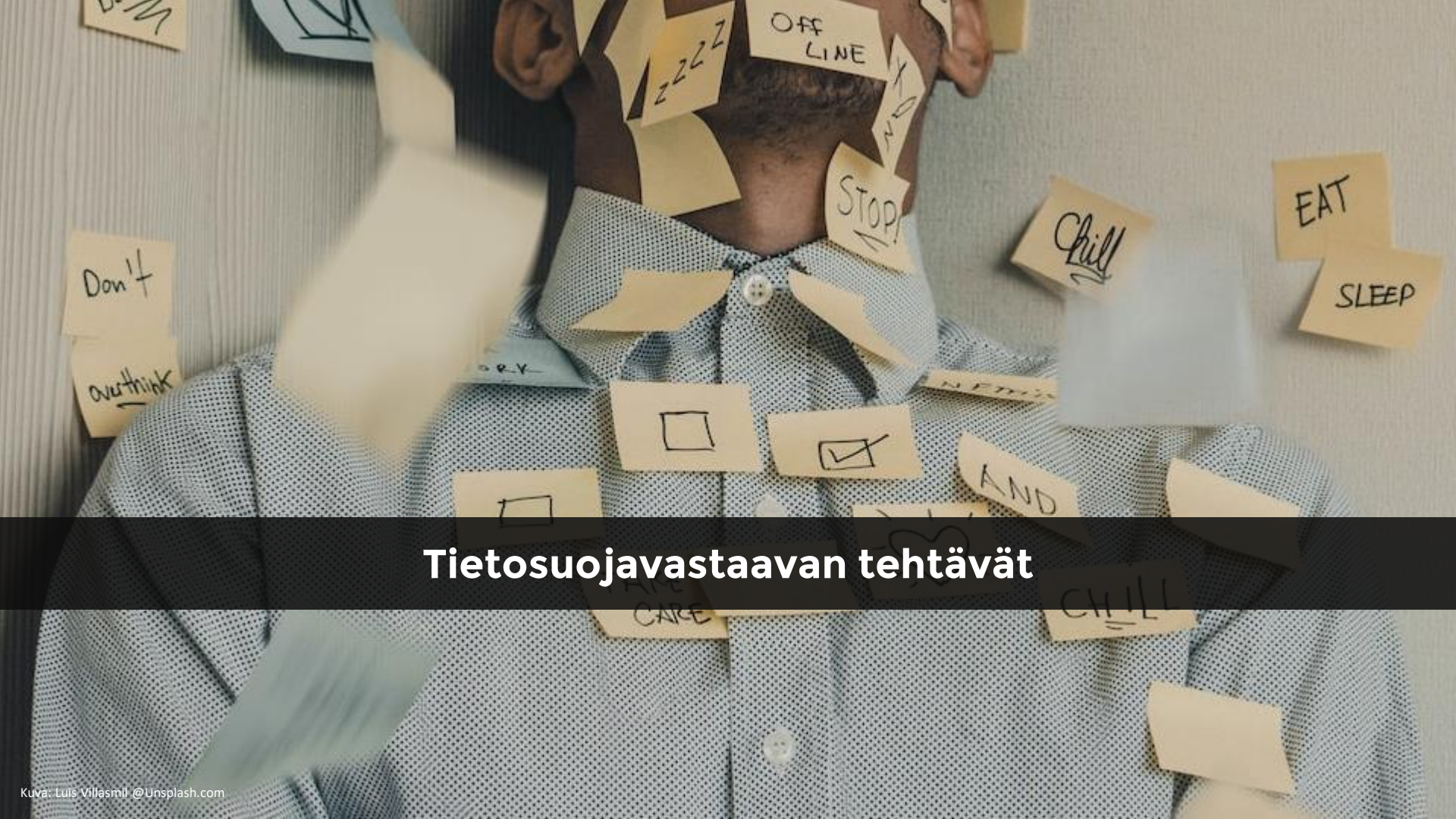
Tietosuojavastaavan salassapitovelvollisuus

38 artikla

5. Tietosuojavastaavaa sitoo hänen tehtäviensä suorittamista koskeva salassapitovelvollisuus unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti.

- Lisäksi tietosuojalain 35 §:n vaitiolovelvollisuus on kaikilla henkilötietoja käsittelevillä.
- Tietosuojasuojavastaava voi luovuttaa tietojaan vain niille henkilöille, joilla on asemansa tai tehtäviensä perusteella oikeus saada kyseisiä tietoja.
- Salassapitovelvollisuus ei estä ottamasta yhteyttä valvontaviranomaiseen ja pyytämästä neuvoja missä tahansa henkilötietoihin liittyvässä kysymyksessä (GDPR art. 39).
- Tietosuojavastaava on tehtäviensä hoidossa itsenäinen, joten hän voi kysyä valvontaviranomaiselta myös sellaisista asioista, joista rekisterinpitäjä ei ehkä haluaisi kysyttävän.
- Valvontaviranomaisella on ”oikeus salassapitosäännösten estämättä saada maksutta tehtäviensä hoidon kannalta tarpeelliset tiedot” (tietosuojalaki 18 §).

Lähde: EU:n yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR), 2016/679, http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.FIN



Tietosuojavastaavan tehtävät

Kuva: Luis Villasmil @Unsplash.com

Tietosuojavastaavan tehtävät 1/2

39 artikla

1) Tietosuoja-asioiden neuvonta ja ohjeistus

- Tekee ohjeistuksia, kouluttaa ja neuvoo työntekijöitä tietosuoja-asioissa.
- Antaa tietoa ja neuvoja tietosuojasääntelyn mukaisista velvollisuuksista johdolle.

2) Tietosuoja-asetuksen noudattamisen seuranta

- Kerää tietoa henkilötietojen käsittelytoimista, analysoi niitä ja tarkistaa, ovatko ne vaatimusten mukaisia, sekä tuo esiin havaitsemiaan puutteita.
- Priorisoi toimiaan ja keskittyy kysymyksiin, jotka aiheuttavat tavallista suurempia tietosuojariskejä (riskiperusteinen lähestymistapa).
- Raportoi organisaation johdolle asioiden kiireellisyys huomioiden (esim. tietoturvaloukkaukset välittömästi ja pitkäaikainen seuranta vuosittain toimintakertomuksena tai tietotilinpäätöksenä).

Lähde: Tietosuojatyöryhmä: Tietosuojavastaavia koskevat ohjeet, 2016, https://tietosuoja.fi/documents/6927448/8316711/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf/

Tietosuojavastaavan tehtävät 2/2

3) Rooli tietosuojaa koskevissa vaikutustenarvioinneissa

- Antaa pyydettäessä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoo vaikutustenarviointien toteutusta.

4) Yhteyshenkilö rekisteröidyille ja valvontaviranomaiselle

- On rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa.
- On tietosuojavaltuutetun toimiston yhteyshenkilö ja yhteistyötaho.

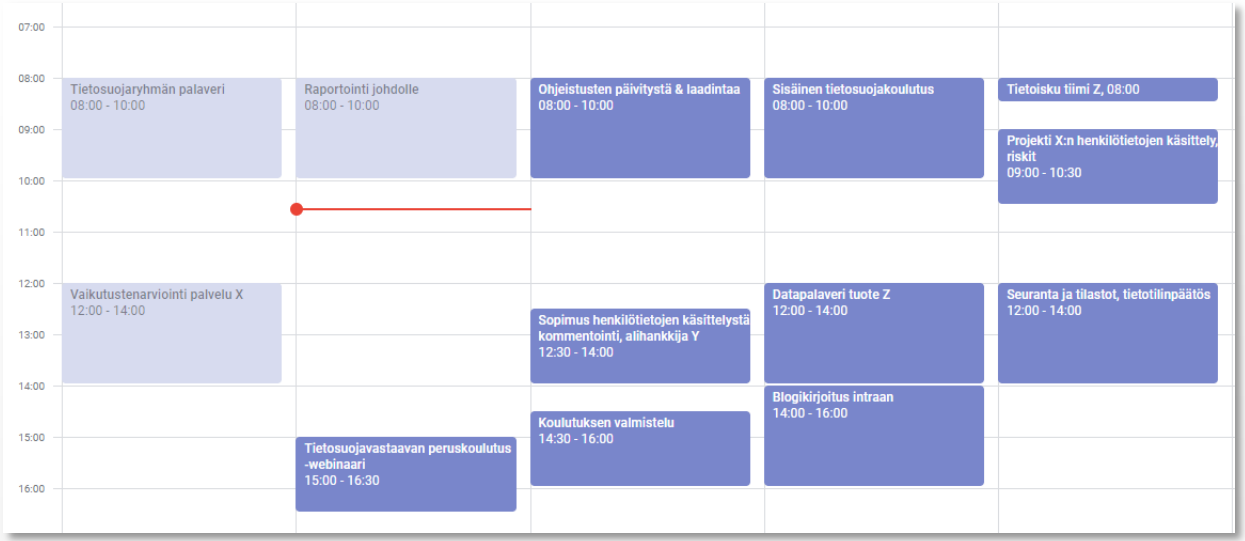
5) Mahdolliset muut annetut tehtävät

- Muihin tehtäviin sopii ylläpitää sisäistä selostetta henkilötietojen käsittelytoimista.
- Organisaation johto voi antaa tietosuojavastaavalle lisäksi muita tehtäviä, mutta ne eivät saa aiheuttaa eturistiriitoja: tietosuojavastaava ei saa olla vastuussa päätöksistä, joita hän valvoo.

Lähde: Tietosuojatyöryhmä: Tietosuojavastaavia koskevat ohjeet, 2016, https://tietosuoja.fi/documents/6927448/8316711/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf/

Tarvittavat resurssit, yhteistyö ja toimintakulttuuri

Tietosuojavastaavan tärkein resurssi = aika



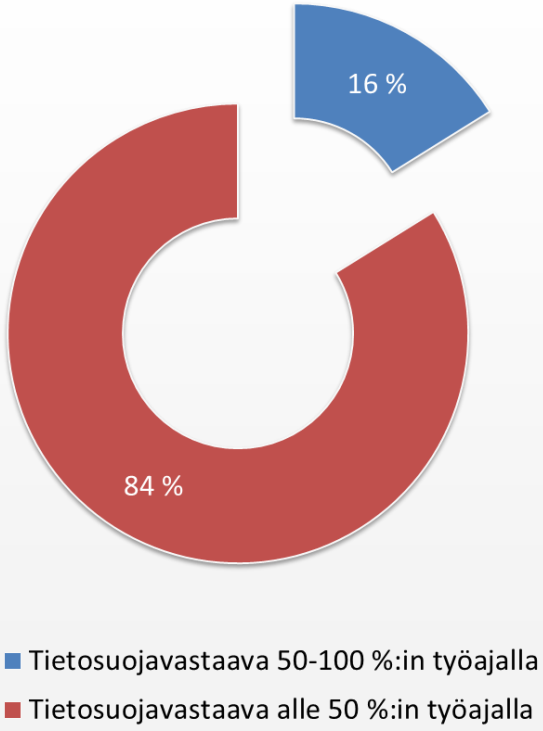
Tietosuojavastaavan kannattaa pitää kalenteri väljänä, jotta kiireisille tehtäville jää aikaa!

- Yhteydenpito eri tahoihin
- Tietosuojatyön suunnittelu ja koordinointi
- Palaverit, arvioinnit, kommentoinnit
- Sisäiset koulutukset ja materiaalit
- Henkilötietojen käsittelyn seuranta
- Raportointi johdolle ja sen avustaminen
- Osaamisen ylläpito, tietosuojaan liittyvien uutisten seuraaminen, kouluttautuminen

“

Tietosuojasta huolehtiminen on kaikkien vastuulla, mutta tietosuojavastaavan tehtävänä on varmistaa, että siitä tullaan tietoiseksi ja osataan toimia oikein.

Useilla tietosuojavastaavilla ei ole edellytyksiä tehdä työtään hyvin



”

Vaikka kaupungilla on ollut tietosuojavastaava ja tietosuojaryhmä heti, kun tietosuoja-asetus sitä edellytti, niin asetusta ei noudateta.

Varsinkin uusien ohjelmistojen tai muutosten teon yhteydessä asioista ei tiedoteta tietosuojavastaavalle, riskianalyysit ja vaikutusten arvioinnit jäävät tekemättä ja henkilörekistereitä saatetaan käyttää vastoin asiakkaiden suostumusta tai tietosuojaselosteessa ilmoitettua tapaa.

Tähän pitää saada muutos ja kaupungin esihenkilöiden, etenkin johtoryhmässä olevien, **pitäisi ottaa tietosuoja-asetus tosissaan ja antaa tietosuojavastaavan tehdä työnsä kunnolla.**

- Anonyymi tietosuojavastaava

Kuvaaja: Tietosuojavastaavan peruskoulutuksen suorittaneiden tietosuojavastaavien vastaukset 2019-2022 (N=93), lainaus erään kurssilaisen tehtävästä luvan kanssa.

Tule syksyn kurssille!

Tietosuojavastaavan peruskoulutus (2 op) S22

Ajankohta
01.11.2022 - 15.11.2022

Paikka
Etäopetus

Opintopisteet
2 op

Hinta
250,00 €

Ilmoittaudu viimeistään
24.10.2022

Ilmoittaudu koulutukseen | Ryhmäilmoittautumiset

https://snellmanedu.fi/tuote/tietosuojavastaavan-peruskoulutus-2-op-4/

Kysymyksiä tai kommentteja?

Yhteystiedot

Harto Pönkä
0400500315
@hponka
harto.ponka@innowise.fi
https://www.innowise.fi/