



TAMPEREEN KAUPUNKI

Osaava tietosuojavastaava - Käytännön kokemuksia ja havaintoja tietosuojavastaavan elämässä

Juhta-Vahti-tietosuojatyöpaja VI

17.11.2017, Ari Andreasson tietosuojavastaava



Kuka, mitä, häh, tä?

- Ari Andreasson
 - Sote-palvelujen tietosuojavastaavana 2008-2017
 - 10/2017- Tampereen kaupungin konsernihallinnon johtoryhmä nimitti Arin koko ”peruskunnan” tietosuojavastaavaksi
 - Asemoituu Konsernihallinnon Strategia- ja kehittämissyksikköön
 - Esimies tietohallintojohtaja
 - Lähin työkaveri tietoturvapäällikkö
 - Tehtävänimike on tietosuojavastaava ja 100% työajasta käytetään ko. tehtävän hoitamiseen
 - Tietosuojavastaavalle on nimetty virkapäätöksellä varahenkilö
 - Sivutoiminen tietokirjailija ja yrittäjä
 - Yhtenä harrastuksena oman tietosuojatietouden kasvattaminen ja tarvittaessa väittely aiheesta alan harrastajien kanssa

Tietosuojavastaavat (1/2)

- Ovat keskiössä GDPR:n toimeenpanon varmistamisessa
- Voivat olla avainhenkilöriskejä tai uupuneita
- Pitää olla mukana DPIA-arvioita laatiessa
- Ovat välillä johdon suosikkilistalla ja välillä sen ulkopuolella
- Pitää olla määrätietoisia ja rohkeita- muttei tyhmänrohkeita
- Ovat asemassa, jossa voi vaatia itselleen asiaankuuluvaa asiantuntijan palkkatasoa sekä pääsyä koulutuksiin ja johtoryhmiin
- Ovat selkeä parannus lainsäädännön vaatimuksissa!!!



Tietosuojavastaavat (2/2)

- Ei ole järkevää vain nimetä tietosuojavastaavaa, vaan varmistaa, että hän saa riittävät resurssit ja mahdollisuuden kouluttautua osaavaksi tietosuojavastaavaksi
- Pahimmillaan ”ei osaava” tietosuojavastaava voi olla pahin tietosuojariski organisaatiolle
- Tietosuojavastaavan pitää itse uida johtoportaan työryhmiin ja pystyä määrätietoisesti tuomaan asiantuntevia mielipiteitään esille
- Pitää muistaa, että tietosuojan ei pidä olla liian tiukka eikä tarpeettoman löysä!
- Pitää muistaa verkostoitua!

Arin tämä viikko & 100+ sähköpostia/pvä

	MAANANTAI	TIISTAI	KESKIVIIKKO	TORSTAI	PERJANTAI
	13	14	15	16	17
8				straken aamukahvipalaveri 2. kerroksen kahvihuone	
9	Kameravalvonnan tallenteiden käsittelyohjeiden päivittäminen	Tietosuojariskien raportointi	Tietoturva- ja tietosuojaryhmä TRE Virastotalo neuvotteluhuone (17+7 hlö)		Iuennoin: JUHTA tietosuojatyöpaja #6 Skype (tai Hesa)
10		Riskienhallintakuulumisia TRE Virastotalo neuvotteluhuone		Turvallisuus- ja tietosuojan aja	
11				Kameravalvontamateriaalin läpikä	
12			lokiraportointi	Kameravalvontaohje / tiedonluovutus TRE Virastotalo neuvotteluhuone K... 12 hlö	
13	Kehittämisen ohjausfoorumi TRE Virastotalo neuvotteluhuone K... (7 hlö)	Tietoturva ja tietosuoja pelastuslaitoksella	tietosuojabrieffi puhelinpalaveri		
14				Potilastietojen käsittelyohjeen päi	
15				esitys VM:ään ja sohvi-telluseminaariin	
16				GDPR-sopimuskommentit	

Työtehtävät liittyvät käytännössä

- Ulkoistussopimuksien liitteisiin (henkilötietojen käsittely)
- Vaatimusmäärittelyihin eri (hankinta) ICT-projekteissa
- Yksittäisten työntekijöiden kysymyksiin (mutta silloin joku sakkaa, jos vastauksia ei saa esimiehiltä tai olemassa olevista ohjeista –voi olla perehdyttämisen ongelma)
- Johdon esittämiin todella vaikeisiin kysymyksiin, joissa tarvitaan myös kansallisia asiantuntijoita kaupungin asiantuntijoiden lisäksi
- Kansalaisten viikoittain esittämiin kysymyksiin ”Minä veronmaksajana vaadin saada tietää...” Yli puolella kysyjistä on Arin havaintojen mukaan henkisiä ongelmia esim. vainoharhaisuutta ja asian selvittelyssä pitää olla erityisen hienotunteinen, jottei pahenna tilannetta (esim. terveydenhuollon hoitosuhdetta) entisestään.

Yksi kasvava vyyhti on lokiselvitykset

- Kuka tietojani käsitteli sähköisesti tai miksi?
- Vaatii tarkempia valtakunnallisia linjauksia, että mitä edes tarkoitetaan sanoilla ”käyttö- ja luovutusloki” ja millä tarkkuudella niitä pitää pystyä kansalaisille tuottamaan. Asiaan liittyy myös kustannusvaikutuksia sekä tietojärjestelmien toimintaan liittyviä (toiminnan hidastavia) asioita, joten asiaa pitää kansallisesti pohtia tarkasti.
- Tampereella on tarkoin määritelty soten asiakastietojen käsittelyn lokiselvitysprosessi, jossa otetaan tarvittaessa lausunto myös psykiatrian ylilääkäriltä, kun arvioidaan lokien luovutuksia tai niistä kieltäytymistä.
- Syytä on dokumentoida kuinka tietojen käsittelyä on valvottu lokitietojen avulla. Esim. Tampereella potilastietojärjestelmä-Pegasoksen lokitietojen käsittelystä tallentuu myös loki.

Johdon ja tietosuojavastaavan yhteistyö – Varmista perusedellytykset

- 1) Tietosuojavastaava: Nosta tietosuoja johdon agendalle ja pidä se siellä
- 2) Nimetkää yhdessä avainhenkilöt ja varmistakaa riittävä resursointi
- 3) Laatikaa pelisäännöt
- 4) Panostakaa henkilöstön kouluttamiseen
- 5) Seuratkaa ja kehittäkää, sekä puuttukaa poikkeamiin





Riskejä GDPR-valmiuden nostossa

- Avainhenkilöriskit organisaation sisällä
- Kansallinen ohjaus ontuu, EU-tasoiset soveltamisohjeet osin puuttuu
- Uutta lainsäädäntöä tulee Suomeen (mm. Tietosuojalaki, ehkä ”Tiedonhallintalaki”, sote- ja maakuntalakupaketti jne.)
- Paljon uutta terminologiaa kaikille osapuolille
- Sopimusliitteitä tai niiden ehdotuksia alkaa tulemaan ovista ja ikkunoista
- Miten tietosuojavastaava osaa keskittyä oleelliseen?

Mitä riskejä voi esiintyä 2018-

- Alkuinnostuksen jälkeen organisaatioiden avainhenkilöiden voimat ehtyvät ja johdon kiinnostus laimenee
- Huomataan, että kyseessä oli enemmän GDPR-projekti kuin se, että lopputuloksena olisi jatkuva prosessi, jota kehitetään
- **Tietosuojavastaavan** työaika kuluu epäoleelliseen ja yksittäisten kysymyksien ja ongelmien ratkaisemiseen
- Kansalaiset voivat esittää enenevästi tiedusteluja ”Kuka tietojani käsittelee ja miksi?”, ”Haluan tietoni poistettavaksi kaikista järjestelmistä”
- Vakavista tietosuojalaiminlyönneistä tai tietovuodoista voi seurata tuntevia seuraamuksia ml. imago tappioita



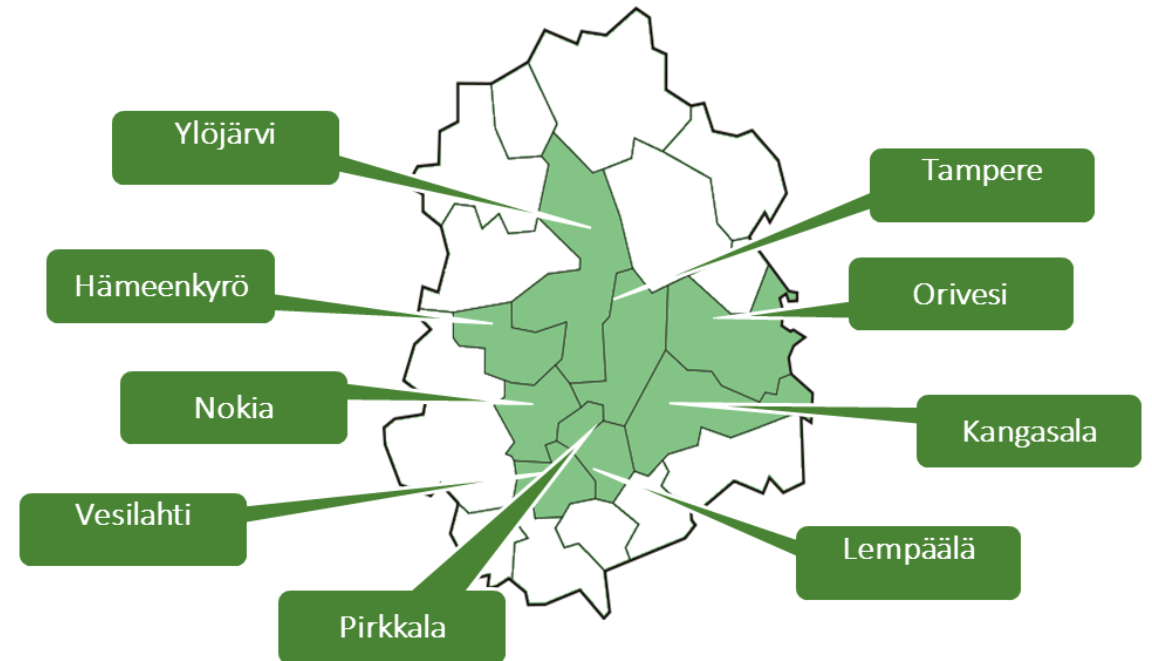
Varautuminen

- Suunnitelkaa tietosuojatyön organisointi huolella
- Toteuttakaa sitä suunnitelman mukaisesti
- Käyttäkää tarvittaessa ulkopuolisia asiantuntijoita –kukaan ei pärjää ”yksin”
- Tehkää vaikutustenarviointi isoriskisessä henkilötietojen käsittelyssä (DPIA=Data Protection Impact Assessment)
- Muistakaa riittävä dokumentointi
- Pitäkää tiedon elinkaaren hallinta keskiössä
- Verkostoitukaa kollegojen kanssa niin paljon kuin mahdollista ja vertailkaa käytäntöjä!

Käytännön esimerkkejä kuntayhteistyöstä

Tampereen seudun tietoturva- ja tietosuoja yhteistyö

- seudun yhteinen tietoturvaryhmä, jossa jäsenet myös isoimmilta ICT-sopimuskumppaneilta
- seudun yhteinen tietoturvapoliittikka
- seudun yhteinen henkilöstön tietoturva- ja tietosuojaopas
- seudun yhteinen tietojen ja tietojärjestelmien käyttö- ja salassapitositoumus (sähköinen hyväksyntä)
 - mukana myös Pirkanmaan sairaanhoitopiiri
- seudun yhteinen mobiilipoliittikka
- seudun yhteiset käyttövaltuusperiaatteet
- seudun yhteiset sähköisten viestintävälineiden käytösäännöt



Lisätietovinkkejä

- www.tietosuoja.fi
 - Tietosuojavastaavia koskevat ohjeet [suomeksi](#)
- www.arjentietosuoja.fi
- www.tietosuojavastaavat.fi
- http://shop.kunnat.net/product_details.php?p=3362 (hyvä julkaisu hankintojen tietosuojaan liittyen)
- Yksi linkki asetukseen <http://www.privacy-regulation.eu/fi/>
- Kirjavinkki: Osaava tietosuojavastaava, Tietosanoma Oy, 2017