

Keskustelukysymykset

1. Mikä on se yksi asia, jossa mielestänne onnistuitte parhaiten siirtymäaikana ja miten sen teitte?

1. Sisäinen koulutus ja tietämyksen taso +4
→ hyvä verkkokoulutus, sisäiset asiantuntijaluennot, task forcen muodostaminen, ulkoinen koulutus, ”jatkuva rummutus”, kohderyhmälähtöisyys
2. Tietosuojakiinnostuksen herättäminen ja positiivisen asenteen luominen +1
→ ”keskustelu, keskustelu, keskustelu”
3. Teimme hyvän ja kattavan analyysin tietovirroista. +1
→ kaikkien järjestelmien ja projektien läpikäynti, ”isot talkoot: IT-ihmiset, legal, markkinointi”
4. Ylinopeuden ja paniikin välttäminen +1
→ riskiperusteinen lähestyminen, tiedon jakaminen ja koulutukset, sisäinen konsultointi, tietosuojavastavaan rekrytointi ja tietosuojatyöryhmän perustaminen
5. Kartoitus tietosuoja tila nyt ja mitä pitää tehdä gdpr:n takia.
6. Pidimme yllä avointa keskustelua haasteista, ratkaisuksista ja liiketoimintamahdollisuuksista
7. Rekisteröityjen informoiminen
8. Insinöörien ja juristien sitoutunut yhteistyö
9. Kansalaisten huomioiminen
→ sähköinen asiointi
10. Tunnistamaan asiakkaita eniten kiinnostavat asiat.
11. Aloitettiin varautuminen ajoissa
12. Asiat olivat lähtökohtaisesti kunnossa: prosessien dokumentoiminen
13. Tietosuoja- ja tietoturvatyöryhmä
→ tiedon jakaminen ryhmän kautta, osastojen aktivointi
14. Liiketoiminnan ymmärryksen lisääminen
→ laillisen perustan selkeytys, rekisteröidyn oikeudet

2. Mikä on se yksi asia, johon kiinnitätte loppuvuoden ajan vielä erityistä huomiota?

1. Toimintatapojen kehittäminen ja testaaminen yleisesti +3
2. Sisäisten prosessien kuvaus, muutostenhallinta ja hyvien oppien levittäminen +2
3. Privacy by default -ajattelun jalkauttaminen päivittäiseen työhön +1
4. Tietosuoja-asioiden pysyminen mielessä jatkossakin, ohjeistus ja kertaus +1
5. Sopimukset ml. hankintasopimukset +1
6. Tietopyyntöprosessien toimivuuden varmistaminen
7. Rekisteröityjen oikeuksien toteuttaminen
8. Dokumentaatio
9. Väärien tulkintojen nitistäminen
10. Sisäinen tietosuojaverkoston toiminta ja koulutus
11. Yrityksen sisällä hajanaisista käytännöistä kohti yhteistä kehittämistä
12. Isojen kolmansien palveluntarjoajien huonot käytännöt/asenne/ehdot eli vaihtoehtoja etsittävä
13. Parhaiden käytäntöjen vieminen koskemaan myös muuta dataa kuin henkilötietoa
14. Riskitaso: virheiden välttämisestä mahdollisuuksiin

3. Mistä yhdestä asiasta toivoisitte viranomaisilta lisäohjausta? (verkkokeskustelu)

1. Minkälaisista tietoturvaloukkauksista viranomaiselle tulee ilmoittaa? +5
2. Oikeutetun edun käyttö käsittelyperusteena +4
3. Moni isompi rekisterinpitäjä pyrkii vyöryttämään omia vastuitaan (sanktioista) käsittelijän suuntaan käsittelysopimuksen puitteissa. Ohjaus vastuukysymyksiin liittyvästä sopimisesta olisi tarpeen. +4
4. Käsittelyperuste ”oikeutettu etu”, mihin tietojenkäsittelyyn EI sovi Tästä paljon ylioptimistisia käsityksiä mm verkkomainonnan toimijoilla +2
5. Pienille organisaatioille ja yhdistyksille kädestä pitäen ohjaavaa pakettia ja pohjia, jota voi käyttää kun tietosuojasta ja rekistereistä on vastuussa yksi maallikko oman toimen ohella. +1
6. Toivomme parempaa mallia rekisteröityjen informointiin. Nyt ohjeet tuntuvat vaikeaselkoisilta ja monitulkintaisilta. +2
7. Kuinka yksityiskohtaisesti pitää vastata kun rekisteröity pyytää tietojaan? "Maija käsittelee tietojasi" vai "Maija korjasi virheen tiistaina klo 13.44 ja perjantaina klo 15.15 tulosti laskusi"? +2
8. Selvennystä siihen, että henkilötietojen siirtyessä eri tahojen välillä kyseessä ei ole aina DPA't vaatima RP-käsittelijälle siirto, vaan tietoja voi luovuttaa myös itsenäisten RP'n välillä tai yhteisRP'den kesken. (Suomen rajojen sisällä / ulkopuolella on paljon epäselvyyttä asiasta) +1
9. Selvennystä siihen, milloin tietosuojavaltuutettu tulee nimittää ja milloin ei esimerkiksi kun kyseessä on yrityksen sisäinen työterveydenhuolto - riittääkö kansallisen lain mukainen tietosuojavastaava vai tulisiko seurata GDPRää?