Haaga-Helia
ammattikorkeakoulu Oy

Tutkimus Nurmijärven kunnassa tehdyistä EU GDPR toimenpiteistä sekä tarvittavista lisätoimenpiteistä

Tomi Ahonen

Opinnäytetyö
YTI 2016
2019

Tekijä
Ahonen Tomi

Koulutusohjelma
Tietojärjestelmäosaamisen koulutusohjelma

Opinnäytetyön nimi	**Sivu- ja liitesivumäärä**
Tutkimus Nurmijärven kunnassa tehdyistä EU GDPR toimenpiteistä sekä tarvittavista lisätoimenpiteistä.	53 + 25
Ohjaaja Ari Alamäki	

Tässä tutkimuksessa kuvataan Nurmijärven kunnassa toteutettu, ennen tietosuoja-asetuksen voimaantuloa 25.5.2018, toteutettu projekti, siinä tehdyt toimenpiteet sekä asetuksen voimaantulon jälkeen tarvittavat lisätoimenpiteet.

Lisäkoulutustarve kartoitettiin kyselytutkimuksella. Tutkimuskysymykset olivat seuraavat:

- Tarvitseeko henkilö työssään lisäkoulutusta liittyen tietosuoja-asetukseen?
- Minkä koulutusmuodon henkilöt katsovat parhaiten palvelevan heitä?
- Mitkä ovat tietosuoja-asetuksen osa-alueet, joissa lisätietoa tarvitaan?

Kyselytutkimus toteutettiin syyskuussa 2019. Tutkimustulosten analysoinnin jälkeen annetaan jatkotoimenpide-ehdotukset, joiden toteutusaikatauluksi suunnitellaan alkuvuotta 2020.

Tutkimuksen viitekehyksenä käytettiin tietosuoja-asetusta.

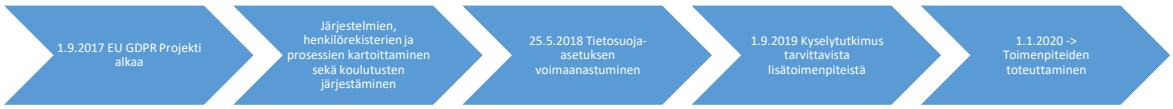
Asiasanat
Tietosuoja-asetus, EU GDPR, Henkilörekisteri, Tietosuojaseloste, Nurmijärven kunta

Sisällys

1 Johdanto

Tässä tutkimuksessa kuvataan Nurmijärven kunnassa toteutettu, ennen tietosuoja-asetuksen voimaantuloa 25.5.2018, toteutettu projekti, siinä tehdyt toimenpiteet sekä asetuksen voimaantulon jälkeen tarvittavat lisätoimenpiteet.

Aikajana projektille:



Syyskuussa 2019 Nurmijärven kunnan henkilökunnalle lähetettiin kysely, jonka tarkoituksena oli selvittää, tarvitseeko henkilö lisäkoulutusta liittyen tietosuoja-asetukseen. Tämän lisäksi haluttiin selvittää minkä koulutusmuodon henkilöt katsovat parhaiten palvelevan heitä. Toteutetulla kyselyllä saatiin myös tietää mitkä tietosuoja-asetuksen osa-alueilla tarvitaan lisätietoa.

1.1 Nurmijärven kunta ja EU GDPR projektin tarve

Nurmijärven kunta sijaitsee Uudenmaan maakunnassa kuuluen Helsingin seutukuntaan. Alueen päätaajamat ovat Klaukkala, Nurmijärven kirkonkylä ja Rajamäki. Asukasluku on vuonna 2019 noin 42.000 asukasta. Helsingin seutukuntaan kuuluu yhteensä 14 kuntaa. Nurmijärvi kuuluu myös KUUMA-seutualueeseen. KUUMA-seutualueita on yhteensä kymmenen: Hyvinkää, Järvenpää, Kerava, Kirkkonummi, Mäntsälä, Nurmijärvi, Pornainen, Sipoo, Tuusula ja Vihti. Näiden alueiden yhteenlaskettu väestö on vuonna 2019 yli 320 000 asukasta. Nurmijärvi on asukasluvultaan Suomen suurin kunta. (Nurmijärvi 2019.)

Nurmijärven kunnan uusi organisaatio astui voimaan 1.1.2019. Tätä ennen, toteutetun projektin aikana, Sote-puoli oli kokonaan kunnan hallinnassa. Vuoden 2019 alusta siirtyi sosiaali- ja terveyspuoli virallisesti liiketoimintakauppana Keski-Uudenmaan Sote kuntayh-

tymään (jäljempänä Keusote). Keusoten jäsenkunnat ovat: Hyvinkää, Järvenpää, Mäntsälä, Nurmijärvi, Pornainen ja Tuusula. Keusote vastaa jäsenkuntien sosiaali- ja terveyspalveluiden tuottamisesta. Kunnat ja kaupungit toimivat palveluiden tilaajina.

1.1.1 Esittely organisaatiosta ja tarvittavat toimenpiteet

Nurmijärven kunnan organisaatio 1.1.2019 alkaen:

(Nurmijärven kunta 2019.)

Tietosuoja-asetusten vaatimusten mukaisesti Nurmijärven kunnalla oli tarve perustaa tietosuojaryhmä, valita tietosuojavastaava, alkaa kartoittaa kunnan henkilörekistereitä sekä järjestelmiä. Näiden tehtävien toimenpiteiden mukaisesti laatia selvitys vaadittavista toimenpiteistä, tarkentaa tarvittavat vaatimukset sekä tehdä tarvittavat muutokset.

Aluksi tietosuoja-asioiden käsittely ja projektin seuranta toteutettiin tietohallinnon kehittämisryhmässä. Syksyllä 2017 Nurmijärven kunta palkkasi kuitenkin asianhallintapäälliköksi Hanna Elomaan joka samalla nimettiin Nurmijärven kunnan tietosuojavastaavaksi. Tietosuojaryhmän kokoonpano oli projektin alussa seuraava:

- Puheenjohtaja: hallintojohtaja Jukka Anttila
- Sihteeri: tietosuojavastaava Hanna Elomaa
- Jäsenet:
    - Kirsi Hyvämäki, sivistystoimen toimiala

- Leena Ojala, henkilöstöpalvelut
- Anita Pihala, elinkeino- ja kuntakehitys
- Ville Timmerbacka, hyvinvointitoimiala
- Arja Toivonen, tietohallinto
- Leena Vuorenpää, ympäristötoimiala

Tietosuoja-asetuksen velvoitteiden täyttäminen oli yksi tietosuojaryhmän alkuvaiheen päätavoitteista. Tämän mukaisesti tuli varmistaa, että kunnan tietoturvakäytännöt olivat asianmukaiset ja ajantasaiset. Tietoturvallisuutta tuli rakentaa mm. ohjeistuksella, koulutuksella ja neuvonnalla. Kuntaan laadittiin myös tietosuojapolitiikka. (Nurmijärven kunta 2019.)

1.2 Kunnan nykytila-analyysi projektin aloituksessa

Projektin alkaessa Nurmijärven kunnassa oli edelleen voimassa aiempi organisaatio, jonka mukaisesti aloitettiin henkilörekisterien ja tietojärjestelmien läpikäynti. Kunnan tietosuojavastaavana toimi Hanna Elomaa ja sosiaali- ja terveyspalveluiden tietosuojavastaavana toimi Ville Timmerbacka. Kaikkien kunnan rekisteriselosteiden katselmointi aloitettiin arvioimalla, olivatko sen hetkiset rekisteriselosteet:

- ajan tasalla
- säädösten mukaisia
- riittävän kattavia ja -informatiivisia sekä johdonmukaisia.

Työ aloitettiin käymällä läpi luettelo olemassa olevista tietojärjestelmistä. Käytännössä tämä tarkoitti sitä, että tietojärjestelmäluetteloon lisättiin kunkin järjestelmän kohdalle alla oleva tieto:

- Sisältääkö järjestelmä (tai välitetäänkö sen kautta) ylipäätänsä henkilötietoja?
- Tieto henkilörekisteriselosteen olemassaolosta. Esim. päiväys, jolloin seloste on viimeksi päivitetty.
- Linkki henkilörekisteriselosteeseen. Mieluiten originaaliin, mutta jollei se onnistu niin viimeksi (nettisivulla) julkaistuun.

Näin saatiin kyseiseen luetteloon talteen kaikki tarvittavat tiedot. Lähtökohtaisesti järjestelmien pääkäyttäjät tuntevat järjestelmänsä parhaiten, jonka vuoksi kyseisiä henkilöitä haastateltiin ja heiltä saatiin ajantasainen tieto järjestelmistä. Näillä tiedoilla päivitettiin aiempaa tietojärjestelmäluetteloa. Tietosuoja-asetuksen kannalta oli erittäin tärkeää tunnistaa kaikki ne järjestelmät, joissa oli henkilötietoa.

Vastaavalla tavalla käytiin läpi kaikki sen hetkiset tiedonkäsittelyprosessit sekä tietovarannot sillä tarkkuustasolla kuin käytettävissä olevan tiedon perusteella oli mahdollista.

Jos tehdyn työn perusteella löytyi henkilötietoja niin kyseisestä henkilörekisteristä piti tehdä tietosuojaseloste ja samalla päivittää vastaava tieto kunnan nettisivuille. Kartoittamisen perusteena pyrittiin määrittelemään seuraavia asioita:

- vastuut
- järjestelmät
- sopimukset, (tiedonohjaussuunnitelmaa (TOS) ei ollut vielä projektin alussa olemassa)
- järjestelmien ominaisuudet
- täyttääkö järjestelmä tietosuoja-asetuksen vaatimukset
- onko järjestelmissä loki ominaisuus
- kuinka tiedot poistetaan / arkistoidaan, kun niitä ei enää tarvita tehtävien hoitamiseen.

Sopimuksien osalta kunta on vastuussa omiin tehtäviinsä liittyvistä henkilötiedoista. Jos taas joku muu taho käsittelee henkilötietoja kunnan lukuun, niin tehtävät ja vastuut on määriteltävä sopimuksessa erikseen. Kuntaliiton juristit olivat laatineet kunnille mallin sopimuksissa käytettävästä henkilötietojen käsittelystä. Tulevissa sopimuksissa tuli huomioida tietosuoja-asiat.

Työpajoja varten laadittiin toimiala ja yksikkökohtaiset tarkistuslistat. Työpajoissa käytiin myös: henkilörekisterit, sopimukset, riskit ja toimintatavat.

1.3 Valmistautuminen tietosuoja-asetuksen mukanaan tuomiin muutoksiin

Uusi tietosuoja-asetus astui voimaan 25.5.2018 ja siihen mennessä tuli tehdä kaikki tarvittavat muutokset olemassa oleviin järjestelmiin ja tunnistaa ne järjestelmät, joissa käsiteltiin henkilötietoja. Varsinaisen tietosuojaprojektin aikana toteutettiin KUUMA-kuntien välistä yhteistyötä.

Kyseisen yhteistyön toimintamalli oli seuraavanlainen:

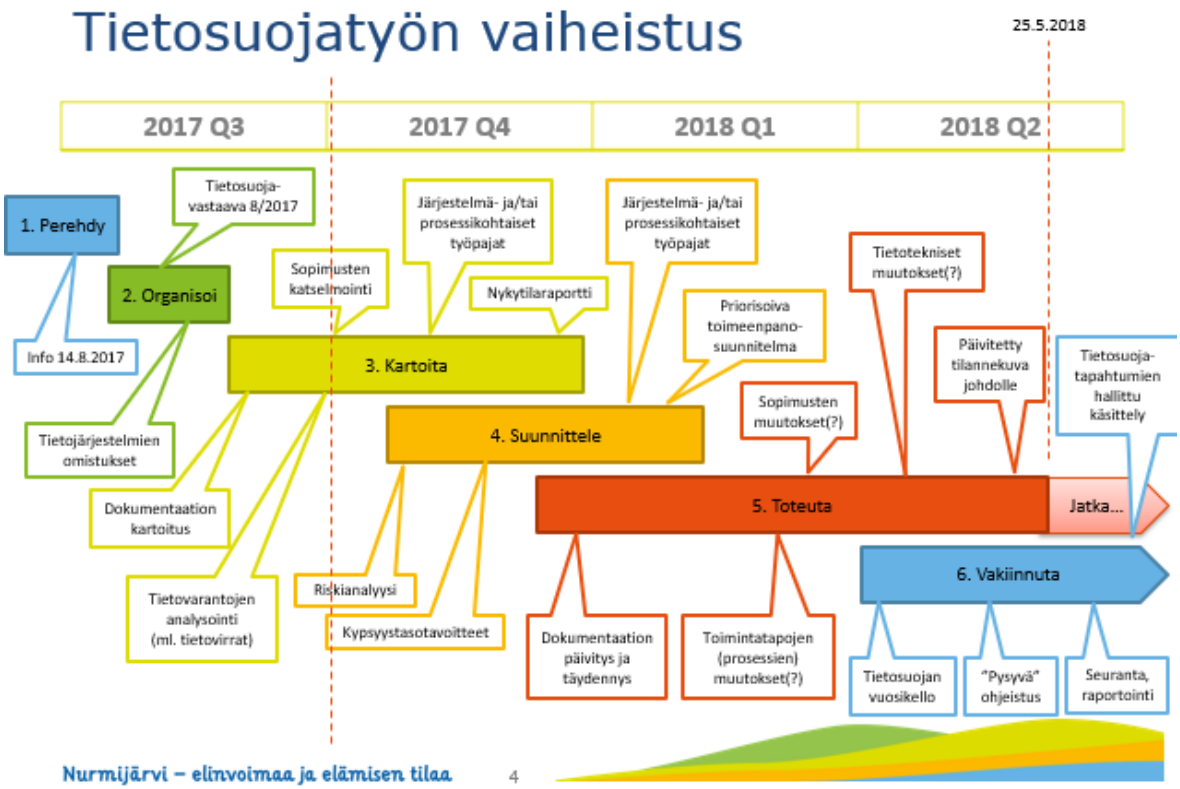
- ohjausryhmänä toimi tietosuojaryhmä
    - Tietosuojaryhmä koostui toimialojen edustajista sekä Nurmijärven kunnan käyttämästä Tieran (Kuntien Tiera Oy – Kuntatoimijoiden omistama ICT-yhtiö) asiantuntijapalveluista

- KUUMA kuntien tietosuojavastaavien kanssa tehtiin yhteistyötä, yhteiset koulutustilaisuudet ja yleistä pohdintaa toimintatavoista.

Kunnan johto on viimekädessä vastuussa tietosuojatyöstä ja sen organisoinnista. Asianhallintapäällikkönä hoiti oman työn ohella tietosuojatyötä sekä työn koordinointia. Toimialojen edustajat velvoitettiin valvomaan tietosuojatyön etenemistä omilla vastuualueillaan. Sosiaali- ja terveyspalveluilla oli jo entuudestaan nimetty tietosuojavastaava. Tietosuojaryhmän kokouksissa Tieran konsultti antoi ohjeita ryhmälle etenemisestä käytännössä. Ryhmä tutustui myös VAHTI (Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän ohjesivusto) ohjeistukseen Valtiovarainministeriön sivuilla.

1.4 Tietosuojatyön projektin aikataulu

Tietosuoja-asetuksen voimaantulo päivämäärä 25.5.2018 asetti projektin valmistumiselle selkeän takarajan. Julkishallinnon osalta lainsäätäjä oli määritellyt, että mahdollisia asetuksen puutteellisuuksia ei tulla sanktioimaan. Tästä huolimatta Nurmijärven kunnalla oli tavoitteena saada projekti päättymään sekä kaikki lainmukaisuuden saavuttamiseksi tarvittavat toimenpiteet suoritettua asetuksen voimaantulopäivään mennessä. Tämän mukaisesti määriteltiin projektille tietosuojatyön vaiheistus alla olevan mukaisesti:



Kaikkia suunniteltuja asioita ei onnistuttu loppuun saattamaan niille määritetyssä aikataulussa, mutta kaikki asetuksen määrittämät vaatimukset saatiin toteutettua 25.5.2018 mennessä. Tämä piti sisällään mm.: kaikki uudet tietosuojaselosteet päivitettyinä Nurmijärven kunnan nettisivuilla.

2 Tietosuoja-asetus viitekehyksenä

Tässä opinnäytetyössä käytetään tietosuoja-asetusta teoreettisena viitekehyksenä.

2.1 Tietosuoja-asetus

Tietosuoja-asetus 679/2016 (Euroopan unionin virallinen lehti 2019) astui voimaan 25.5.2018 ja sääntelee henkilötietojen käsittelyä kaikissa EU-maissa.

Tietosuoja-asetus korvaa 1.6.1999 voimaan tulleen henkilötietolain (523/1999), joka on ollut tietosuojaa koskeva yleislaki. Tämä laki korvasi vuodelta 1988 olevan henkilörekisterilain ja -asetuksen. (Andreasson, Koivisto & Ylipartanen 2015, 28.)

Uuden tietosuoja-asetuksen pykälien (artikla) rikkomisesta on seurauksena hallinnollinen sanktio ja enimmäisrangaistus on 4 prosenttia edellisen vuoden liikevaihdosta tai 20 miljoonaa euroa, sen mukaan kumpi on suurempi. Korkeampiin seuraamuksiin sovelletaan seuraavia artikloja: 5,6,7,9,12-22. Tämän lisäksi asetuksen mukaan seuraavista artiklojen rikkomisesta saa alhaisemman sakon, jonka maksimi 10 miljoonaa euroa. Artiklat ovat: 8,11,25-39 ja 42-43. (EU GDPR 2018, Ch3.)

EU:n yleinen tietosuoja-asetus ja kansallinen tietosuojalaki määrittelevät henkilötietojen käsittelyn Suomessa. Henkilötietolaki on kumottu tietosuojalailla. Sosiaali- ja terveydenhuollon osalta ovat omat erityissääntelynsä potilastietojen erityisen arkaluonteisuuden vuoksi. (Andreasson, Riikonen & Ylipartainen 2019, 28.)

Nurmijärven kunnassa oli jo erittäin hyvin laadittu tietosuojaselosteet, varsinkin sosiaali- ja terveyspuolella. Kyseisellä toimialalla on lainsäädäntö edellyttänyt jo näitä aiemmin. Aiemmin olemassa olleet rekisteriselosteet päivitettiin uudelle tietosuoja-asetuksen vaatimalle pohjalle.

EU tietosuoja-asetus edellyttää tietosuojavastaavan nimittämistä julkisella sektorilla, pois lukien tuomioistuimet. Asetus velvoittaa myös yritykset nimeämään tietosuojavastaavan, mikäli yrityksen toiminnassa käsitellään arkaluonteisia henkilötietoja. Yrityksen johto voi muutenkin nimittää tietosuojavastaavan, jos he katsovat sen tarpeelliseksi riskiperusteisuuden mukaan. (Andreasson, Riikonen & Ylipartainen 2019, 14.)

Asetusta sovelletaan Euroopan unionin alueella riippumatta siitä, onko rekisterinpitäjä EU:n alueella. Asetus saattaa amerikkalaiset yritykset tämän uuden asetuksen noudattajiksi. Tietosuoja-asetuksessa on määritelty huomattavia sanktioita, mikäli tietosuoja-asetusta ei noudateta. Lain tarkoituksena on ollut yhtenäistää EU:n jäsenvaltioiden tietosuojalakeja. (Kauppakamari 2019, 1.)

Tietosuojalla pyritään saavuttamaan myös organisaation tehokkuutta ja tuottavuutta sekä kustannusten säästöä. Tietosuojalla tarkoitetaan perinteisesti tietosuojan yleislain ja henkilötietojen käsittelyssä koskevien oikeuksien ja velvollisuuksien huomioimista. Rekisterinpitäjän tulee käsitellä henkilötietoja hyvin ja suojata tiedon kohteen yksityiselämää, oikeuksia, etuja ja vapauksia. Henkilötietolainsäädäntö asettaa rajat, joita rekisterinpitäjän on noudatettava arkaluonteisia henkilötietoja käsiteltäessä. Tietosuoja ja tietoturva ovat jokaisen organisaation arkipäivää. Kyseiset asiat tulee ottaa huomioon yrityksen liiketoiminnassa. Tulee myös huomata, kyseiset asiat eivät ole pelkästään tietotekniikkaan liittyviä. Tietosuojaan liittyvät asiat tulee ennakoida ja ehkäistä etukäteen. Turvallisuuden toteuttamiseksi tulee suunnitella toimintatapoja ja turvamekanismeja, tietoverkkojen ja laitteiden suojaamiseksi. (Andreasson, Riikonen & Ylipartainen 2019, 10, 20.)

Organisaatioilla on myös velvoite tehdä arvio tietosuojan nykytilasta. Asetus muuttaa kansallisia henkilötietojen käsittelyn käytäntöjä ja tuo uusia velvoitteita rekisterinpitäjälle, että henkilötietojen käsittelijöille. Uuden asetuksen artiklaan 25 sisältyy sisäänrakennetun tietosuojan (data protection by design) ja oletusarvoisen tietosuojan (data protection by default) periaatteet. EU:n yleinen tietosuoja velvoittaa suunnittelemaan hyvissä ajoin ennen uuden sovelluksen käyttöönottoa, kuinka henkilötietoja tullaan käsittelemään. Nämä periaatteet ohjaavat yksittäistapauksissa henkilötietoja käsittelyä. (Andreasson, Riikonen & Ylipartainen 2019, 23-24.)

Tietosuoja-asetuksen mukaan rekisteröidyllä on oikeus tulla unohdetuksi. Rekisteröity voi vaatia, että hänestä olevat tiedot poistetaan, myös siinäkin tapauksessa, että hän on antanut suostumuksensa tietojen käsittelyyn. Tiettyjä poikkeuksia lukuun ottamatta organisaatiolla ei ole mahdollisuutta kieltäytyä poistamasta kyseisiä tietoja. Näin ollen rekisterinpitäjän on ryhdyttävä kohtuullisin toimenpitein poistamaan tietoja. Tietosuojaviranomaiset haluavat pystyä todentamaan, että kaikki tietojen poistot on toteutettu asianmukaisesti. (EU GDPR 2018, Ch3.)

Rekisterinpitäjällä on velvollisuus seurata ja valvoa asiakastietojen käyttöä. Sosiaali- ja terveydenhuoltoalan rekisterinpitäjiä on velvoitettu väärinkäytösten ehkäisemiseksi tekemään aktiivisesti tarkastuksia lokitietoihin. Terveydenhuollon puolella on käytäntönä tehdä pistokokeita erityisesti niihin lokitietoihin, jotka koskevat tunnettuja henkilöitä. Lokitietojen tarkastamisella halutaan valvoa, että vain hoitosuhteessa olevat henkilöt ovat käsitelleet ja katsoneet kyseisiä henkilötietoja.

Jo tällä hetkellä rekisteröidyn on mahdollista katsella omia lokitietoja esim. Kanta-palvelusta. Jokaiselle henkilörekisterille on määriteltävä rekisterinpitäjä ja tästä on myös laadittava tietosuojaseloste. Näin ollen lokirekisterillekin on määriteltävä rekisterinpitäjä. Lainsäädännön mukaiset asiakas- ja potilasrekisteritietojen suojauskeinot kuuluvat organisatorisisiin eli käyttäjähallinnollisiin tai teknisiin keinoihin. (Andreasson, Koivisto & Ylipartanen 2013, 81.)

Vastaavanlaisia palveluja ovat kehittäneet vaikka mm. Kesko ja S-ryhmä. Näistä tiedoista kuluttaja voi tilata omat rekisteritietonsa ja löytää näin esim. kanta-asiakastietonsa tai tiedon hakemuksestaan, mikäli on hakenut töihin kyseisen yrityksen palvelukseen.

Nykyään on mahdollista automatisoida lokivalvonta ja sitä kautta varmistaa tietojen käytön luvallisuus. Lokidataa voidaan analysoida esim. reaaliaikaisesti tai kerran vuorokaudessa. Järjestelmiin voidaan myös rakentaa raportteja ja hälytyksiä. Aiemmin tehdyissä ohjelmissa ei välttämättä ole loki ominaisuutta. Lokiohjelmien käyttö saattaa hidastaa kyseisen ohjelmien käyttöä. Tähän tarkoitukseen on olemassa apuna erillisiä ohjelmia, joilla voidaan kuitenkin seurata loki tapahtumia. (Andreasson, Koivisto & Ylipartanen 2013, 82.)

EU:n tietosuoja-asetus merkitsee oikeuksia rekisteröidylle ja vastaavasti vaatimuksia rekisterinpitäjälle. Rekisteröidyn on mahdollista päästä omiin tietoihinsa käsiksi kohtuullisessa ajassa. Rekisteröidyn pyytäjän on tunnistauduttava vaatiessaan omia tietojaan ja hänen on tarkasti määriteltävä mitä tietoja hän haluaa ja miltä ajalta. Tietopyyntöihin on vastattava määrä- tai kohtuullisessa ajassa. Tietosuoja on huomioitava koko ohjelman elinkaaren ajalle kaikkiin niihin vaiheisiin, jolloin tietojenkäsittelyä on tehty.

Vuonna 2016 EU:n ja Yhdysvaltojen välillä allekirjoitettiin uusi sopimus Yhdysvaltojen Safe Harbour sopimuksen korvaamiseksi. Tämän uuden sopimuksen mukaan yhdysvaltalaisten organisaatioiden on todistettava noudattavansa ja täyttääkseen GDPR:n vaatimukset. (EU GDPR 2018, Ch3.)

2.1.1 Tietosuoja-asetuksen soveltaminen

Tietosuoja-asetusta sovelletaan, mikäli EU kansalaisen henkilötietoja käsitellään yrityksessä, riippumatta siitä missä maassa tietoja tullaan lopulta käsittelemään. EU kansalaisen henkilötietoja käsittelevän EU:n ulkopuolisen yrityksen on nimettävä EU:ssa toimiva edustaja.

Yleistä tietosuoja-asetusta ei sovelleta jos:

- rekisteröity on kuollut
- rekisteröity on oikeushenkilö

Henkilötiedoilla tarkoitetaan kaikkia tietoja, joista henkilön voi tunnistaa tai henkilö on tunnistettavissa.

Tunnistettavia henkilötietoja ovat esimerkiksi:

- nimi
- osoite
- IP-osoite
- passin numero
- tulotiedot
- terveydenhuollossa olevat tiedot, sairaala/lääkäri

Erityiset henkilötiedot, joihin liittyviä tietoja yritys ei saa käsitellä, ovat mm.:

- rotua tai etnistä alkuperää
- sukupuolista suuntautumista
- poliittisia mielipiteitä
- uskonnollisia tai filosofista vakaumusta
- ammattiliittoon kuulumista
- geneettisiä, biometrisiä tai terveydellisiä tietoja, erityistapauksissa jos käsittelylle on annettu suostumus, tai käsittely on tarpeen yleisen edun vuoksi tai kansallisen lainsäädännön vuoksi.
- rikostuomioita tai rikkomuksia ellei lainsäädäntö EU tai kansallinen lainsäädäntö salli sitä. (Euroopan Unioni 2019.)

2.2 Organisaatioiden oma-aloitteinen osoitusvelvollisuus

Tietosuoja-asetuksen mukaan ei enää riitä, että rekisterinpitäjä noudattaa lakeja, vaan on pystyttävä osoittamaan eri tavoin, että organisaatio noudattaa tietosuojavaatimuksia. Rekisterin pitäjällä on oltava kirjallisia suunnitelmia, joilla voidaan osoittaa henkilötietojen käsittelyn olevan lainmukaista. Tämä voidaan todentaa esim. tietotilinpäätöksen, dokumenttien tai muiden sääntöjen avulla. (Andreasson, Riikonen & Ylipartainen 2019, 25.)

Tietosuojan suunnittelu on otettava huomioon tietojärjestelmien käyttöönottoa suunniteltaessa. Tietosuoja-asetus ei suoraan määrittele järjestelmään rakennettavien turvallisuustoimintojen laajuutta. Tietosuoja-asetuksen vaatimuksen mukaisesti rekisterinpitäjän tulee toteuttaa tekniset ja organisatoriset toimenpiteet asianmukaisesti. (EU GDPR 2018, Ch3)

2.3 Tietosuojavastaavat viranomaisilla

Suomessa lainsäädäntö on jo vuodesta 2007 alkaen edellyttänyt tietosuojavastaavien nimittämiseen sosiaali- ja terveydenhuollon palvelujen tuottajilla sekä apteekeilla. Kehitystä on tapahtunut viimeisen kymmenen vuoden ajalla, mutta silti henkilökuntaa ei ole aina ohjeistettu ja koulutettu henkilötietojen ja potilastietojen käsittelyyn. (Andreasson, Riikonen & Ylipartainen 2019, 25.)

Tietosuojavastaavan tehtävä on seurata seuraavia asioita:

- tietosuojalainsäädännön noudattamista
- rekisterinpitäjän ja henkilötietojen käsittelijän toimintamenettelyjä, jotka liittyvät henkilötietojen suojaan
- henkilöstön koulutus ja tarkastukset.

Tietosuojavastaavat hoitavat tehtäväänsä seuranta- ja valvontasuunnitelman pohjalta. Tätä toimintaa tukemaan on usein laadittu tietosuojavuosikellon.

Nurmijärven tietosuojavastaava tekee yhteistyötä säännöllisesti Kuuma-kuntien tietosuojavastaavien kanssa. Yhteistyömuotoja on mm. yhteiset koulutukset, tapaamiset sekä työpajat. Näissä tilaisuuksissa pohditaan yhdessä, kuinka eri tilanteissa tulee toimia. Teams ohjelmalla mahdollistetaan tietojen jakoa. Tässä yhteistyössä osallisena ovat KUUMA-ICT: Sipoo, Mäntsälä, Nurmijärvi, Kirkkonummi, Porvoo, Järvenpää, Kerava, Vihti, Tuusula ja Hyvinkää. Osalla Kuuma-kunnista on käytössä myös Arc-ohjelmisto, jonka avulla osallistujat voivat jakaa keskenään tietoa parhaista käyttötavoista. Yhteisen ARC alustan kautta jaetaan tietoja ja kaavioita.

Yhtenä yhteistyömuotona julkinen hallinto harjoittelee henkilötietojen tietoturvaloukkausten hallintaa yhteisissä TAISTO-harjoituksissa 2018-2021. Ensimmäinen TAISTO-harjoitus järjestettiin syksyllä 2018 Väestörekisterikeskuksen toteuttamana. (Taistoharjoitus 2018.)

Nurmijärven kunta osallistui valtionvarainministeriön ja Väestörekisterikeskuksen järjestämään Taisto18 harjoitukseen 22.11.2018. Harjoituksen jälkeen osallistujat saivat palautteen, jonka perusteella voitiin arvioida ne osa-alueet, jotka oli jo toteutettu asetuksen vaatimalla tavalla sekä ne kohdat, joita piti vielä parantaa. Kyseinen harjoitus oli hyvä tapa testata organisaation valmiutta toimia tietosuojaloukkausten tapahduttua.

Tietosuojavastaava ei kunnassa vastaa yksin tietosuojan toteutumisesta kunnassa, vaan vastuu yleisvastuu kuuluu kunnan johdolle.

Yleisvastuu jakautuu seuraavien osapuolien kesken:

- Luottamuselimet
- Johto
- Tietosuojavastaava
- Tietohallinto
- Prosessien omistajat

2.4 Palautetta GDPR:stä ja Suomen tietosuojalaista

Oikeusministeriö kerää parhaillaan (syyskuussa 2019) tietoa ja palautetta GDPR:n ja kansallisen tietosuojalain toimivuudesta. GDPR:ään ja yleisesti laajentuneeseen tietosuojakeskusteluun on tullut myönteistä kehitystä. Tietosuojakeskustelujen myötä eri tahojen tietoisuus on lisääntynyt yksityisyyden suojasta. GDPR tavoitteet eivät ole harmonisoituneet EU:ssa tavoitteiden mukaisesti. Kansalliset tietosuojalait ja viranomaisten linjaukset eivät ole täysin samassa linjassa, joten voidaan katsoa, että harmonisointi ei ole vielä täysin onnistunut. Voidaan myös todeta, että EU:n tietosuojaneuvoston antamat ohjeet koetaan raskaiksi ja usein jo antovaiheessa vanhentuneiksi. Tämän lisäksi tietoturvaloukkausten tekemisen kriteereihin pitäisi saada yhtenäiset ohjeet ja kriteerejä pitäisi tarkistaa, koska eri maiden tekemissä tietoturvaloukkauksissa on suurta hajontaa. Myöskään EU maissa annetut GDPR-sakot eivät ole linjassa keskenään. Nähdään myös, että viranomaisten valtuuksien piiriin tulisi saada hallinnolliset sakot. Yleisenä huomiona voidaan nähdä, että GDPR:n voimaantulon jälkeen markkinaosuuksia ovat kasvattaneet EU:ssa Google, Amazon ja Facebook. (Sähköpostiviesti www.asml.fi 11.9.2019)

2.5 Tietosuoja-asetuksen pääkohdat

Rekisteröidyllä tarkoitetaan henkilöä, jonka tietoja käsitellään ja/tai johon kohdistuvat tietosuoja-asetuksessa mainitut toimenpiteet. Tietosuoja-asetuksen mukaan rekisteröidyllä on pääpiirteittäin seuraavat oikeudet:

- ”saada tietoa henkilötietojensa käsittelystä
- saada pääsy tietoihin
- oikaista tietoja
- poistaa tiedot ja tulla unohdetuksi
- rajoittaa tietojen käsittelyä
- siirtää tiedot järjestelmästä toiseen
- vastustaa tietojen käsittelyä
- olla joutumatta automaattisen päätöksenteon kohteeksi.” (www.tietosuoja.fi)

Rekisteröity ei voi käyttää mainittuja oikeuksiaan kaikissa tilanteissa, vaan käytön taustalla on henkilötiedon käsittelyperuste. (Tietosuojavaltuutetun toimisto 2019.)

2.5.1 Henkilötietojen käsittelyä koskevat periaatteet 5 artikla

Seuraavassa esitetään rekisteröidyn oikeuksien turvaamisen varmistaminen.

> ”5 artikla Henkilötietojen käsittelyä koskevat periaatteet: 1. Henkilötietojen suhteen on noudatettava seuraavia vaatimuksia:”
>
> ”a) lainmukaisuus, kohtuullisuus ja läpinäkyvyys: niitä on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi”

Tämä tarkoittaa, että henkilötietoja käsitellään lainmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Samalla rekisterinpitäjän on kyettävä osoittamaan, että henkilötietoja käsitellään kyseisen artiklan vaatimalla tavalla.

> ”b) käyttötarkoitussidonnaisuus: ne on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla; myöhempää käsittelyä yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten ei katsota 89 artiklan 1 kohdan mukaisesti yhteensopimattomaksi alkuperäisten tarkoitusten kanssa”

Tämä tarkoittaa, että tietoja saa kerätä, vaikka yhtä yksittäistä tapahtumaa varten, mutta tietoja ei saa yhdistää uusiin tuleviin tapahtumiin.

> ”c) tietojen minimointi: henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään”

Tämä tarkoittaa, että voidaan kerätä vain sellaisia tietoja, jotka todella ovat välttämättömiä, mutta ylimääräisiä tietoja ei saa kerätä talteen.

> ”d) täsmällisyys: henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä”); 4.5.2016 FI Euroopan unionin virallinen lehti L 119/35 (1) Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/1535, annettu 9 päivänä syyskuuta 2015, teknisiä määräyksiä ja tietoyhteiskunnan palveluja koskevia määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä (EUVL L 241, 17.9.2015, s. 1).”

Tämä tarkoittaa, että henkilötietojen tulee olla ajan tasalla ja virheettömiä.

> ”e) säilytyksen rajoittaminen: ne on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten; henkilötietoja voidaan säilyttää pidempiä aikoja, jos henkilötietoja käsitellään ainoastaan yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten 89 artiklan 1 kohdan mukaisesti edellyttäen, että tässä asetuksessa vaaditut asianmukaiset tekniset ja organisatoriset toimenpiteet on pantu täytäntöön rekisteröidyn oikeuksien ja vapauksien turvaamiseksi”

Tämä tarkoittaa, että artiklan 89 kohdan 1 mukaiset suojatoimet otetaan käyttöön, esimerkiksi henkilötietojen pseudonymisoinnilla, jolloin henkilöitä ei ole mahdollista tunnistaa aineiston sisältä.

> ”f) eheys ja luottamuksellisuus: niitä on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia.”

Tämä tarkoittaa, että tiedot on käsiteltävä suljetuissa tietojärjestelmissä, joissa tulee olla loki päällä tai käytettävissä oltava erillinen loki ohjelma. Tietoja ei saa tallentaa työkoneen C:\-asemalle vaan tietojen pitää olla suojatuilla ja varmistetuilla verkkolevyillä tai OneDrive Businessversiossa.

2.5.2 Käsittelyn lainmukaisuus 6 artikla

> ”6 artikla Käsittelyn lainmukaisuus: 1. Käsittely on lainmukaista ainoastaan, jos ja vain siltä osin kuin vähintään yksi seuraavista edellytyksistä täyttyy:
> a) rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten.
> b) käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä”
> c) käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi;
> d) käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi;
> e) käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi;
> f) käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn

edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi.
Ensimmäisen alakohdan f alakohtaa ei sovelleta tietojenkäsittelyyn, jota viranomaiset suorittavat tehtäviensä yhteydessä.
2. Jäsenvaltiot voivat pitää voimassa tai ottaa käyttöön yksityiskohtaisempia säännöksiä tässä asetuksessa vahvistettujen sääntöjen soveltamisen mukauttamiseksi sellaisessa käsittelyssä, joka tehdään 1 kohdan c ja e alakohdan noudattamiseksi määrittämällä täsmällisemmin tietojenkäsittely- ja muita toimenpiteitä koskevat erityiset vaatimukset, joilla varmistetaan laillinen ja asianmukainen tietojenkäsittely muun muassa muissa erityisissä käsittelytilanteissa siten kuin IX luvussa säädetään.
3. Edellä olevan 1 kohdan c ja e alakohdassa tarkoitetun käsittelyn perustasta on säädettävä joko
a) unionin oikeudessa; tai
b) rekisterinpitäjään sovellettavassa jäsenvaltion lainsäädännössä.
Käsittelyn tarkoitus määritellään kyseisessä käsittelyn oikeusperusteessa tai, 1 kohdan e alakohdassa tarkoitetussa käsittelyssä, sen on oltava tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Kyseinen käsittelyn oikeusperuste voi sisältää erityisiä säännöksiä, joilla mukautetaan tämän asetuksen sääntöjen soveltamista, muun muassa: yleisiä edellytyksiä, jotka koskevat rekisterinpitäjän suorittaman tietojenkäsittelyn lainmukaisuutta; käsiteltävien tietojen tyyppiä; asianomaisia rekisteröityjä, yhteisöjä joille ja tarkoituksia joihin henkilötietoja voidaan luovuttaa; käyttötarkoitussidonnaisuutta; säilytysaikoja; sekä käsittelytoimia ja -menettelyjä, mukaan lukien laillisen ja asianmukaisen tietojenkäsittelyn varmistamiseen tarkoitetut toimenpiteet, kuten toimenpiteet
4.5.2016 L 119/36 Euroopan unionin virallinen lehti FI
muita IX luvussa esitettyjä erityisiä tietojenkäsittelytilanteita varten. Unionin oikeuden tai jäsenvaltion lainsäädännön on täytettävä yleisen edun mukainen tavoite ja oltava oikeasuhteinen sillä tavoiteltuun oikeutettuun päämäärään nähden.
4. Jos käsittely tapahtuu muuta kuin sitä tarkoitusta varten, jonka vuoksi tiedot on kerätty, eikä käsittely perustu rekisteröidyn suostumukseen eikä unionin oikeuteen tai jäsenvaltion lainsäädäntöön, joka muodostaa demokraattisessa yhteiskunnassa välttämättömän ja oikeasuhteisen toimenpiteen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi, rekisterinpitäjän on otettava huomioon muun muassa seuraavat asiat varmistaakseen, että muuhun tarkoitukseen tapahtuva käsittely on yhteensopivaa sen tarkoituksen kanssa, jota varten tiedot alun perin kerättiin:
a) henkilötietojen keruun tarkoitusten ja aiotun myöhemmän käsittelyn tarkoitusten väliset yhteydet;
b) henkilötietojen keruun asiayhteys erityisesti rekisteröityjen ja rekisterinpitäjän välisen suhteen osalta;
c) henkilötietojen luonne, erityisesti se, käsitelläänkö erityisiä henkilötietojen ryhmiä 9 artiklan mukaisesti tai rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja 10 artiklan mukaisesti;
d) aiotun myöhemmän käsittelyn mahdolliset seuraukset rekisteröidyille;
e) asianmukaisten suojatoimien, kuten salaamisen tai pseudonymisoinnin, olemassaolo.”

2.5.3 Henkilötietojen lainmukainen käsittely

Aiemmin kohdassa 2.5.2 Artiklan 6 mukaisesti henkilötietojen käsittely on lainmukaista, jos yksikin Artikla 6:n kohdista toteutuu:

a) rekisteröidyn suostumus

Suostumuksessa käsittelyperusteena rekisterinpitäjän on pysyttävä osoittamaan, että lainmukainen suostumus on olemassa. Henkilö voi aina peruuttaa suostumuksensa ja silloin tiedot pitää poistaa välittömästi ja viipymättä rekisteristä. Suostumus voi olla vaikka, nettisivuilla rastiruutuun suostumus.

b) sopimus

Sopimus on tietosuoja-asetuksen mukaan käsittelyperusteena sallittu, mikäli rekisteröity on sopimuksen toinen osapuoli, esim. kauppakirjassa. Käsittelyperuste kattaa muun muassa ennen luottosopimuksen syntyä tehtävät selvitykset henkilön luottokelpoisuuden arvioimisesta.

c) rekisterinpitäjän lakisääteinen velvoite

Lakisääteisenä tehtävä voidaan mainita esimerkiksi tilanne, jossa työnantaja ilmoittaa työntekijänsä palkkatiedot veroviranomaisille tai kun pankki ilmoittaa epäilyttävästä rahaliikenteestä tai liiketoiminnasta viranomaiselle.

d) elintärkeän edun suojaaminen

Elintärkeiden etujen suojaaminen on sallittu silloin kun on kysymys elämästä tai kuolemasta eli tilanteesta, joka voisi johtaa rekisteröidyn tai jonkun muun loukkaantumiseen tai muuten olla terveydelle vaarallinen esim. epidemiat ja pandemiat.

e) yleinen etu ja julkinen valta

Yleinen etu käsittelyperusteena soveltuu vain julkissektoriin ei elinkeinoelämään. Kunnan ja viranomaisen toiminnassa henkilötietojen käsittely perustuu pitkälti juuri lakisääteiseen velvoitteeseen ja yleiseen etuun.

f) rekisterinpitäjän oikeutettu etu tai kolmannen osapuolen oikeutettu etu

Oikeutettu etu on sallittua silloin kun on kyseessä rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. Tietojen käsittely on tarpeen jonkin perusoikeuden toteuttamiseksi esim. sananvapaus, elinkeinovapaus.

2.6 Kansallinen tietosuojalaki

Alkuperäisen suunnitelman mukaisesti kansallisen tietosuojalain oli suunniteltu tulevan voimaan saman aikaisesti tietosuoja-asetuksen kanssa. Lain käsittely kuitenkin viivästyi ja sen voimaantuloon asti sovittiin noudatettavan henkilötietolakia niissä kysymyksissä, joita tietosuoja-asetus ei kata.

Eduskunta hyväksyi tietosuojalain (Tietosuojalaki 1050/2018.), astumaan voimaan 1.1.2019. Kyseinen laki täydentää tietosuoja-asetusta.

2.7 Mitä on tietosuoja? (Data Privacy)

Tietosuojalla tarkoitetaan luonnollisen henkilön yksityiselämän ja yksityisyyden suojaamista. Käytännössä tietosuojalla tarkoitetaan erityisesti henkilötietojen suojaamista. Jokaisen ihmisen perusoikeus on henkilötietojen suojaus ja yksityisyyden suojaaminen. Tietosuojaperiaatteita sovelletaan kaikkeen tietoon, joka koskettaa tunnistettavissa tai tunnistettua luonnollista henkilöä. Henkilötiedoilla on nykyään yhä suurempi merkitys, jonka lisäksi kyseisillä tiedoilla on huomattava taloudellinen merkitys yritysten liiketoiminnalle sekä yhteiskunnalle. Tämän mukaisesti myös henkilötietojen väärinkäytökset ovat lisääntyneet. (Ijäs, 2018.)

> ”Facebookin mukaan analyysiyhtiö Cambridge Analytica on päässyt käsiksi jopa 87 miljoonan Facebook-käyttäjän tietoihin, joita on sitten käytetty mm. presidentti Donald Trumpin presidentinvaalikampanjassa hyväksi.” (Yle uutiset 11.4.2018)

Henkilötietoja suojaavat EU:n perusoikeussäännökset. Artiklan 7:n mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejä kunnioitetaan.

Henkilötietojen suoja pitää sisällään seuraavat oikeudet:

- tietojen käsittelyn on oltava asianmukaista ja tapahduttava tiettyä tarkoitusta varten, rekisterin pitäjällä tulee olla henkilön suostumus tai muu laissa säädetty oikeus tietojen säilyttämiseen
- jokaisella on oikeus saada tietoa omista kerätyistä tiedoista
- mahdollisuus oikaista väärät tiedot
- viranomaisella on velvollisuus valvoa sääntöjen noudattamista (Ijäs 2018.)

”Tietosuoja on henkilötietojen suojaa
Tietosuoja tarkoittaa henkilötietojen suojaamista ja niiden asiallista käsittelyä. Henkilötiedolla tarkoitetaan kaikenlaisia luonnollista henkilöä takka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. EU:n tietosuoja-asetus, jota sovelletaan kansallisesti 25.5.2018 alkaen, asettaa entistä tiukemmat vaatimukset henkilötietojen käsittelylle, ja niihin kuuluu osoitusvelvollisuus. Rekisterinpitäjällä on velvollisuus osoittaa, miten se käsittelee henkilötietoja ja miten yksityisyyden suoja turvataan. Tietosuojapolitiikassa määritellään henkilötietojen käsittelyn ja suojaamisen yleiset periaatteet kunnassa, ja ne muodostavat samalla perusteet osoittamisvelvollisuudelle. Periaatteita noudattamalla tavoitellaan luottamusta: Nurmijärven kunnassa henkilötietoja käsitellään tavalla, johon kuntalaiset ja muut rekisteröidyt sekä yhteistyökumppanit voivat luottaa. Tämä vaatii sitä, että periaatteet ovat riittävän selkeät ja konkreettiset, ja että rekisteröidyillä on saatavilla riittävästi informaatiota tietosuojan toteutumisesta Nurmijärven kunnassa. Tietosuojapolitiikkaa täydentävät henkilötietojen käsittelyä koskevat käytännön ohjeet, jotka julkaistaan kunnan intranetissä. Tietosuoja liittyy läheisesti tietoturvaan, eli tietojen saatavuuden, eheyden ja luottamuksellisuuden varmistamiseen. Tietoturvaan kuuluu muun muassa tietoaineistojen, laitteistojen, ohjelmistojen, tietoliikenteen ja toiminnan turvaaminen. Siihen liittyvät periaatteet on kuvattu kunnan tietoturvapolitiikassa ja tietoturvaohjeissa. Tietosuojapolitiikka täydentää niitä henkilötietojen turvallisen käsittelyn osalta.” (Nurmijärven kunta 2019.)

2.7.1 Henkilötietojen suojaaminen

EU:n tietosuoja-asetuksella taataan henkilötietojen suojaaminen mm. internet-ostoksissa. Tietosuojalla on merkittävä rooli internetissä asioivien asiakkaiden kohdalla, koska juuri henkilötietoja käytetään hyväksi markkinoinnissa ja palveluissa. Asiakkaiden halukkuus antaa henkilötietoja palveluntuottajan käyttöön vaihtelee huomattavasti. Asiakkaat ovat yhä enenevässä määrin huolissaan yksityisyydestään sekä, siitä kuinka heidän henkilötietojaan käytetään. GDPR on tuonut tullessaan luvantarpeen henkilötietojen hyödyntämiseen. Viimevuosina yrityksien käytettävissä olevat digitaaliset työkalut ovat yleistyneet, jonka lisäksi markkinointidataa kerätään talteen monin tavoin. Tämä on saanut kuluttajat huolestumaan mahdollisesta yksityisyyden loukkaamisesta. Edellä mainitun lisäksi uutisissa kerrotut tapahtumat digitaalisten palveluiden tietojen vuotamisesta heikentävät ihmisten luottamusta yksityisyyden suojaan entisestään. Poistaakseen ihmisten huolta yritysten tulee ottaa huomioon yksityisyyden suojaan liittyvät asiat digitaalisia palveluita suunnitellessaan. (Alamäki A. & Mäki 2019.)

2.8 Huoli yksityisyydestä (Privacy Concern)

Lehdistössä kerrotaan erilaisista kuluttajan näkökulmasta toteutuneesta yksityisyyden suojaan liittyvistä artikkeleista. Ihmiset ovat hyvin huolissaan omien tietojensa joutumisesta kolmansille osapuolille ja siitä, kuinka heidän tietojaan käytetään hyväksi ja yhdistetään muihin tietoihin. Käytännössä saatetaan kokea, että jos henkilö haluaa käyttää

Googlen, Microsoftin, Facebook tai muiden suurten yritysten pilvipalveluita, niin käytännössä henkilö joutuu sallimaan omiin tietoihinsa pääsyn. Yritysten osalta pilvipalveluyritykset takaavat, että ainakin osaa tiedoista säilytetään EU:n alueella.

Yhtenä esimerkkinä voidaan mainita tapaus jossa, Hollannin tietosuojaviranomaiset huomasivat, että Microsoftin Windows 10 ohjelma kerää tietyissä tapauksissa käyttäjistä heidän henkilökohtaista tietoansa. Tämä tarkoittaa, että ihmisten on syytä olla hyvin tarkkana, kun asentavat ohjelman tai säätävät yksityisyysasetuksia. GDPR:n peruslähtökohtana onkin suojata ihmisten tietoja, ettei ylimääräisiä tietoja kerätä tarpeettomasti. (Tekniikka & Talous 2019.)

Syksyllä 2019 kävi myös ilmi, että Suomessa verottaja lähetti ihmisille kirjeitä, joissa oli osin toisten asiakkaiden tietoja. Syynä tähän arveltiin olevan tulostusohjelmassa väärin määritellyt parametrit, joiden perusteella määriteltiin mistä mitäkin tietoa poimitaan tai vaihtoehtoisesti kovakoodattu lähdekoodi oli ohjelmoitu virheellisesti. Verottaja lupasi tiedottaa asianomaisille tapahtuneesta. (Tivi 2019.)

Ihmisten tietosuojasta aiheutuneen huolen voitaneen katsoa olevan aiheellinen, sillä henkilöistä kerätään dataa lähes kaikesta, eikä vielä edes tiedetä mihin kerättyä dataa tullaan käyttämään. Lainsäädäntö kehittyy tulevaisuudessa olemassa olevan tiedon ja sen mahdollisen jatkojalostus mahdollisuuden mukaisesti. Laitevalmistajat asettavat jo tällä hetkellä laitteisiin sensoreita, joilla voidaan seurata käyttäjän toimia. Näin saatua tuotteen käyttödataa käytetään yritysten markkinointiin ja tuotekehitykseen. Yhtenä esimerkkinä voidaan mainita nykyiset televisiot, jotka on poikkeuksetta varustettu kameralla. Tulevaisuudessa kyseisten komponenttien hintojen laskiessa sensoreita alettaneen asentamaan myös esim. leivänpaahtimiin. Näiden sensoreiden avulla hankittuja tietoja hyödynnettäneen ainoastaan valmistajien ja markkinoinnin tarpeisiin. Tuotteen käyttäjille niistä ei liene suoranaista hyötyä. Tästäkin näkökulmasta katsottuna käyttäjän huoli tietosuojasta voidaan olettaa olevan aiheellinen.

Artiklan 22 mukaan automatisoidut yksittäispäätökset ja profilointi saattavat aiheuttaa mielenkiintoisia tilanteita rekisteröidyn kannalta. Tämä sen vuoksi, että päätöksenteko pohjautuu suoraan tietokannoista saataviin tietoihin. Tehdyt päätökset voivat olla kyseisen henkilön kannalta huonoja, koska hän ei esim. saa vakuutusta tai lainaa. Lain mukaan automaattisen päätöksenteon, joka perustuu ainoastaan tietokoneen tekemään päätökseen, on lähtökohtaisesti kielletty. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 259.)

Henkilötiedoksi katsotaan tieto, joka kerätään luonnollisista henkilöistä, jotka ovat tunnistettavissa tai tunnistettuja. Rekistereihin kerätään usein nimi, osoite, sotu/henkilötunnus, puhelinnumero, sijaintitieto, verkkotunnistetieto IP-osoite/Mac-osoite, asuinpaikka, sormenjäljet, autojen rekisteritunnukset, bonuskorttien tiedot, sähköpostiosoitteet, valokuvat, katujen videovalvontatiedot jne. Tätä kaikkea tietoa voidaan käyttää henkilöiden tunnistamiseen. Lain mukaan näistä tiedoista saa käyttää vain kulloisenkin käyttötarkoituksen kannalta tarpeelliseksi katsottuja tietoja.

Tietosuoja-asetuksen mukaan henkilöiden, jotka ovat alle 13-vuotiaita on saatava vanhempien lupa käyttääkseen niitä verkkopalveluita, joihin vaaditaan henkilötieto.

Tutkimuksessa ja jossa tieto piti siirtää organisaatioiden yli nimettömänä, eli anonymisoituna kävi ilmi, että datasta ei saatu riittävästi tutkimustietoa. Kävi myös ilmi, että tietojen siirto organisaatioiden välillä vaatii yhteistyötä uusien liiketoimintamallien luomiseksi. Tutkimuksessa kävi ilmi, että tekoäly ei vielä pysty tulkitsemaan keskusteluja riittävän hyvin, vaan ihmisten tulee opettaa ohjelmaa. Tämä tarkoittaa sitä, että Ihmistä tarvitaan vielä koneoppimisen eri vaiheissa. GDPR salli tietojen toissijaisen käytön artiklan 89 mukaan. (Alamäki, Aunimo, Ketamo & Parvinen 2019.)

Artikla 89:n mukaan yleisen edun mukaisia arkistotilanteita, tieteellisiä, historiallisia tutkimustarkoitusta tai tilastollista tarkoitusta varten tapahtuvaa tietojen käsittelyä varten on kyseisessä artiklassa määritelty erilliset suojatoimet. Näillä suojatoimilla suojellaan rekisteröidyn oikeuksia ja vapauksia. On siis varmistettava, että käytetään teknisiä ja organisatorisia suojatoimia, joilla tietoja minimoidaan esim. pseudonymisoinnilla. Tutkimalla arkistoituja tietoja ja yhdistämällä niitä muiden tietolähteiden tietoihin saadaan luotettavia tutkimustuloksia. Viranomaisilla, jotka ylläpitävät yleistä etua koskevia tietoja, on lakisääteinen velvoite hankkia, säilyttää, arvioida, järjestää, kuvailla, levittää, välittää sekä myöntää pääsy tietoihin, joilla on yleistä etua koskeva merkitys. Jäsenvaltiot voivat takautuvasti säätää lakeja, joilla henkilötietoja voidaan käsitellä erityistietojen hankkimiseksi poliittisesta toiminnasta, kansanmurhista, rikokset ihmisyyttä vastaan ja erityisesti sotarikoksista. (Korpisaari, Pitkänen & Warma-Lehtinen 2018, 608- 610.)

Organisaatiot tulee suojata asiakkaidensa yksityisyyttä anonymisoimalla henkilötietoja silloin kun käyttävät kyseisiä tietoja omissa analyyseissään. Näin kuluttajan luottamus yrityksiä kohtaan säilyy sekä varmistetaan, että organisaatiot noudattavat lakia. Anonymisointi saattaa kuitenkin vähentää datasta muuten saatavaa informaatiota. Tutkimuksen tavoitteena oli saada tietoa ja luoda malleja anonymisoinnin ja informaation välisistä suhteista. (Alamäki, Aunimo, Ketamo & Parvinen 2019.)

2.9 Pseydonymisointi ja anonymisointi

Pseudonymisoinnilla tarkoitetaan toimenpiteitä, joilla henkilötietojen jälkikäteinen yhdistäminen tiettyyn rekisteröityyn henkilöön käyttämättä lisätietoja ei onnistu. Lisätiedot on säilytettävä erillään ja niihin on tullut sellaisia teknisiä toimenpiteitä, joilla voidaan varmistaa, ettei henkilötietojen yhdistämistä tapahdu tunnistettuun tai tunnistettavissa olevaan henkilöön. Tämä tarkoittaa sitä, että asiakkaan henkilötiedot salanimetään. Tieto on kuitenkin vielä henkilötietoa. Hätätilanteissa salaus voidaan purkaa ja selvittää kuka on ostanut jonkin vaarallisen tuotteen. Anonyymiä tieto on vasta silloin, kun siitä ei voida tunnistaa kohtuullisesti yksittäistä henkilöä. Anonymisoinnin tulee olla peruuttamatonta, jotta henkilötieto on tosiasiallisesti sellaista, että siitä ei voida tunnistaa henkilöä. (Ijäs 2018.)

3 Mitä on tietoturva

Tietoturvan määritelmä on tiedon saatavuuden, luottamuksellisuuden ja eheyden ylläpitämistä, turvattava tieto voi olla erilaisissa muodoissa. Tietoturvalla tarkoitetaan tietoturvallisuutta, tietojen suojaamista, on sitten kyse verkko-, puhelinliikenteestä, tietojärjestelmistä tai erilaisista muista palveluista. Tietoturvalla pyritään suojaamaan tietoja tietojärjestelmistä. Kyse on toiminnoista ja tavoista, joilla suojataan yrityksen tai henkilön tietoja tai tiloja.

Tietoturvaa on myös kulunvalvonta, kiinteistöjen ja tilojen lukitus sekä käyttöoikeuksien hallinta. Asiakirjojen säilyttäminen lukituissa tiloissa, niin ettei niihin pääse käsiksi ulkopuoliset tai henkilöt, joilla ei ole oikeutta tietoa nähdä.

3.1 Tietoturvaloukkaukset

Nurmijärven kunnalla on ohjeistus, tapa toimia tietoturvaloukkauksissa, jotka ovat kohdistunet tietovarantoihin tai järjestelmiin. Samaa mallia voidaan soveltaa henkilötietojen käsittelyn osalta tietosuojaloukkauksiin. Oletuksena mallissa on, että järjestelmille löytyy pääkäyttäjä ja omistaja. Kunnan henkilöstö on koulutettu ja ohjeistettu, sekä heille on tiedotettu yleisistä periaatteista tietoturvaan ja tietosuojaan liittyen. Tietosuojavastaavana toimii Hanna Elomaa ja tietoturvapäällikkönä Arja Toivonen.

Tietoturvaloukkaus on tahaton tai tahallisesti aiheutettu poikkeama kunnan tietojärjestelmiin. Vastaavasti tietosuojaloukkaus on kyseessä silloin, kun kunnan henkilötietoihin on kohdistunut rikkomus.

Nurmijärven kunnan helpdesk tarkkailee omassa työssään palvelupyyntöjen hallinnan kautta, ilmeneekö niissä epäilyttäviä tapauksia. Kaikki tapahtumat eivät ole tietoturvaloukkauksia ja näin osa epäillyistä ei ole aiheellisia.

4 Tietosuoja-asetuksen vaatimusten linkittäminen kunnassa tehtäviin toimenpiteisiin

Kunnan työntekijöiden tulee saada tietoa tietosuoja-asetuksesta, jonka vuoksi kunnan tulee työnantajana järjestää koulutuksia henkilökunnalle. Muun koulutuksen toteuttamiseen kunnassa oli jo käytössä Navisec verkkokoulutukset -nettiohjelmisto ja -testit. Navisecissa on kaikki ne koulutukset, jotka työntekijän tulee vuosittain käydä läpi ja suorittaa hyväksytysti. Koulutuksen toteutumista seurataan kehityskeskusteluissa. Kyseistä verkkokoulutus alustaa oli tarkoitus hyödyntää tietosuoja-asetus koulutukseen.

Tarvittavan koulutuksen aluksi organisoitiin tietosuojaryhmä, jonka tehtävänä oli valvoa ja avustaa tietosuojatyötä tekeviä ihmisiä. Nimettiin projektiin liittyvät henkilöt eli ne, jotka tulivat tekemään työtä tietosuoja-asetuksen parissa. Tämän jälkeen projektin jäsenille määriteltiin selkeät vastuut ja jaettiin tehtävät.

Tietojenkäsittelyn ja tietojärjestelmien dokumentointi päätettiin käydä läpi yhdessä toimialojen kanssa työpajoissa sekä tarvittaessa erikseen. Sovittiin tietosuoja ja tietoturvakoulutusten tarjoamisesta henkilöstölle. Tämä piti sisällään myös tietojärjestelmäsopimusten läpikäyntiä sekä mahdollisesti uusien sopimusten laadintaa kuntaliiton mallin mukaisesti. Tuli myös määritellä ne tietojärjestelmät, joissa ei ole erillistä loki ohjelma käytössä, sekä päättää erillisten tietosuojatyötä tukevia ohjelmistoja mahdollisesta käyttöönotosta.

5 Projekti

5.1 Projektin aloitus

Tietosuojaprojekti aloitettiin syksyllä 2017. Projektityöskentelytavaksi valittiin interaktiivinen toimialakohtainen, työpajatyyppinen lähestymistapa. Valitut kohdehenkilöt kutsuttiin työpajoihin. Projektin alussa käytiin muutama palaverin kuntien Tiera Oy:n konsultin kanssa, jonka kanssa määriteltiin millä tasolla ja mitä tullaan henkilökunnalta kysymään. Tällä haluttiin varmistaa yhtenäinen toimintatapa. Konsultin avulla laadittiin ohjeistusta, kuinka tietosuoja-asioiden hallinta olisi hyvä toteuttaa kunnassa.

5.1.1 Toimialat

Nurmijärven kunta jakaantuu seuraaviin toimialoihin:

- Elinkeino- ja kuntakehitys
- Keskushallinto
- Sivistystoimi
- Hyvinvointitoimiala ja Ympäristötoimiala

Projektin kartoitusvaiheessa määriteltiin tarpeelliseksi käydä läpi kukin toimiala erikseen.

5.2 Projektin eteneminen

Aluksi järjestelmien pääkäyttäjille ja omistajille lähetettiin sähköpostikysely (Liite 2) jossa pyydettiin vastaanottajaa toimittamaan olemassa oleva tietosuojaseloste, mikäli sellainen oli. Tämän jälkeen kartoitettiin työpajatyyppisillä kokouksilla tietojärjestelmäkohtaisesti mitä henkilörekistereitä kunnasta löytyy, tiedossa olevien rekisterien lisäksi. Projekti käynnistettiin käymällä läpi palavereissa toimialakohtaisesti tietojärjestelmät, ohjelmat ja henkilörekisterit. Käytyjen palaverien perusteella päädyttiin jaottelemaan tulevat tietosuojaselosteet alla olevan jaottelun mukaisesti:

- Asuminen, rakentaminen ja ympäristö
- Hallinto ja talous
- Kasvatus ja sivistys
- Sosiaali- ja terveystoimi
- Kunnan omia työntekijöitä koskevat rekisterit

Toimialakohtaisissa työpajoissa käytiin läpi ne toimialakohtaiset järjestelmät, joissa käsitellään henkilötietoja. Samalla kun toimialojen kanssa käytiin järjestelmiä läpi, päivitettiin poistuneet järjestelmät, ihmiset ja lisättiin puuttuvat järjestelmät.

Samanaikaisesti käytiin läpi kartoitustaulukko (Liite 3) sekä henkilörekisteritaulukko. Näiden toimenpiteiden avulla kartoitettiin kaikki ne kunnassa olevat tietojärjestelmät, joissa käsiteltiin henkilötietoja. Työpajatyyppinen lähestymistapa koettiin hyväksi, haasteena nähtiin kuitenkin ihmisten kokoon saaminen tietojärjestelmien ja henkilörekisterien läpikäymistä varten. Yleisimmin palavereihin riitti noin kaksi tuntia kerrallaan, joissain tapauksissa, kaikkien asioiden selville saamiseksi jouduttiin jatkamaan asioiden läpikäyntiä myöhemmin.

Kokouksissa käytiin läpi henkilörekisteriselosteet, jotka täydennettiin tietosuoja-asetuksen mukaisella tietosuojaselostepohjalla, jonka jälkeen kyseiset tietosuojaselosteet siirrettiin nettisivuille. Uusi laki ei velvoita laatimaan henkilörekistereistä tietosuojaselostetta, mutta tietosuojaselosteet ovat erittäin hyvä tapa osoittaa asioiden olevan kunnossa. Tämän vuoksi kaikki olemassa olevat rekisteriselosteet käytiin läpi työpajoissa ja tarvittaessa lisättiin puuttuvat tietosuojaselosteet.

Kuten edellä mainittiin, projektissa lähdettiin aluksi liikkeelle sähköpostin välityksellä kaikille osalliselle eli järjestelmien omistajille ja pääkäyttäjille. Tämä osoittautui hyväksi tavaksi, sillä tietojärjestelmätaulukon osalta oli haasteellista pitää tietoja ajan tasalla henkilöiden vaihtuessa, eikä kaikista uusista järjestelmistä ollut ajantasaista tietoa.

Jotta tarvittavat tiedot saatiin koottua sekä selvitettyä puuttuvat järjestelmät, pidettiin työpajoja aktiivisesti. Näissä hankittiin päivitetty tieto järjestelmistä, sekä niistä järjestelmistä, joissa käsitellään henkilötietoja.

Projektin alkuvaiheessa tietosuojaryhmä ja tietoturvaryhmä olivat erilliset kokoonpanot, jotka kokoontuivat säännöllisesti. Projektin edetessä ryhmät yhdistettiin ja syntyi tietosuoja- ja tietoturvaryhmä, joka toimi projektin ohjausryhmänä. Ryhmälle pidettiin säännöllisesti tilannekatsaukset ja samanaikaisesti kunnanhallitukselle pidettiin omat infonsa tietosuojavastaavan toimesta.

Helmikuussa 2018 oli käytynä kaksikymmentä rekisteriä läpi, perustiedot ja tarkistuslistat päivitetty, sekä listattu pahimmat ongelmakohdat. Työpajoissa pyrittiin selvittämään olemassa olevat sopimukset sekä missä sopimukset sijaitsivat. Kaikki sopimukset eivät välttämättä olleet vielä tallennettuina asianhallintajärjestelmä Dynastyyn. Uudet sopimukset skannattiin ja tallennettiin asianhallintajärjestelmään.

Sopimuksien osalta toimittajat olivat valmiita tekemään uusia sopimuksia, mutta sopimusehdot eivät olleet linjassa kuntaliiton sopimuspohjan kanssa. Tämän vuoksi sopimusten päivittäminen tuli viemään huomattavasti enemmän aikaa, jotta saatiin kuntaliiton edellyttämä liite voimaan.

Kunnanjohtajalle ja kunnanhallitukselle pidettiin väliarvio maaliskuussa ja toukokuussa 2018. Väliarviossa todettiin työpajatyöskentelyn alkamisesta ja jatkosuunnitelmista kaikkien henkilörekisterien ja järjestelmien kartoittamiseksi.

Maaliskuun puolivälissä 2018 tilannepäivityksenä voitiin kertoa, että rekisterikohtaisia työpajoja oli pidetty sen mukaisesti, kun kunnan työntekijöiden aikataulut olivat sallineet. Kyseiseen ajankohtaan mennessä oli saatu keskushallinnon, sivistystoimen ja hyvinvointitoimialan rekisterit hyvin pitkälle läpikäytyä. Vastaavasti samanaikaisesti oli aloitettu elinkeino-, kuntakehitys- ja ympäristötoimialan rekisterien läpikäynti. Kyseinen aikataulu tarkoitti sitä, että eritoimialojen rekisterit saatiin päivitettyä ennen tietosuoja-asetuksen 25.5.2018 voimaan astumista. Kyseisen päivämäärän jälkeen tehtiin vielä muutoksia olemassa oleviin tietosuojaselosteisiin, lähinnä tämä tarkoitti uuden tietosuojaselostepohjan käyttöönottoa.

5.2.1 Nykytilan kartoitus

Aiemmin kuvatun mukaisesti Nurmijärven kunnan tietosuojaprojekti aloitettiin nykytilan kartoituksella. Järjestelmien kartoituksen yhteydessä havaittiin tarve saada käyttöön järjestelmä tietosuoja-asioiden ylläpitämistä varten. Tässä kyseisessä järjestelmässä tultaisiin kirjaamaan kaikki tietojärjestelmät ja henkilörekisterit. Tähän käyttöön Nurmijärven kunta hankki Arter Oy:ltä Arc nimisen ohjelman, jossa oli valmiina tietosuojaosio. ARC ohjelma piti sisällään tietosuojanhallintamallin ja kokonaisarkkitehtuurin kuvantamisvälineet. Yhdessä tietosuojavastaavan kanssa projektiryhmä sai koulutuksen tähän ohjelmaan. Tämän jälkeen laadittiin henkilörekisterit, tietojärjestelmät ja linkit tietosuojaselosteisiin.

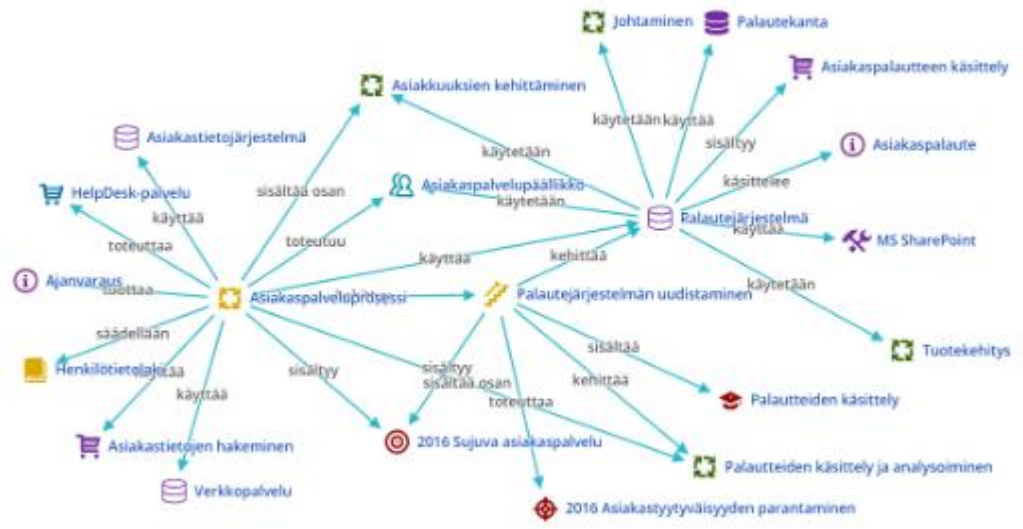
Projektin aikana kävi ilmi, että kunnan verkkolevyasemille oli tallennettu paljon erilaisia henkilötietoja. Kyseiset henkilörekisterit olivat osa jotain suurempaa rekisteriä, jonka mukaisesti kyseiset tiedot olivat olleet olemassa ehkä yhtä tiettyä käyttötarkoitusta varten. Henkilökuntaa ohjeistettiin, että tarpeettomien henkilörekisterien tiedot tulee poistaa verkkolevyiltä. Kunnassa oli otettu O365 käyttöön jo vuonna 2017, uuden ohjeistuksen mukaisesti henkilökunnan oli luovuttava omista verkkolevyasemista, jotka olivat olleet kunnan palvelimilla. Heidän tuli siirtyä käyttämään OneDrive for Business tallennustilaa. Tarkoitus oli siirtää OneDriveen omat kansiot, kansiorakenne ja samalla siivota vanhat tiedot pois. Näitä yleisiä kunnan työntekijöille suunnattuja O365 tietoiskuja pidettiin kunnan valtuustosalissa, jonne kunkin osallistujan oli helppo saapua sen keskeisen sijainnin ansiosta. Toimialakohtaisia koulutuksia pidettiin toimialojen omissa tiloissa, jotta osallistujien oli mahdollisimman helppo päästä tilaisuuksiin.

5.2.2 Tarvittavat toimenpiteet

Nykytilan kartoituksen jälkeen, työpajoissa ruvettiin käymään läpi henkilörekistereitä ja täydentämään puuttuvia tietosuojaselosteita. Tietosuojavastaavan johdolla alettiin käydä

läpi merkittävimpiä sopimuksia sekä pyytää tietosuojaliitteitä toimittajilta. Toimittajilta pyydettävien tietosuojaliitteiden suhteen tehtiin yhteistyötä KUUMA kuntien tietosuojavastaavien kanssa. Osa toimittajista kuten mm. HUS ja Attendo tarjosivat henkilötietojen käsittelyliitettä automaattisesti.

Kuten jo aiemmin mainittiin, käytiin työpajoissa läpi sekä henkilörekisterit, järjestelmät että kartoitettiin suuririskisimmät järjestelmät. Kyseiset tiedot kirjattiin Arc-ohjelmaan, jossa oli helppo nähdä kaikki toisiinsa liittyvät rekisterit ja järjestelmät. Kyseisessä ohjelmassa oli työskentelyä helpottava toiminnallisuus, jolla voitiin porautua eri osista eri taulukoihin ja tietoihin yhteyskaavion avulla, sekä ohjelmaan oli helppo rakentaa linkkejä tietosuojaselosteisiin tai sopimuksiin.



(Arter Oy 2019.)

5.3 Koulutusten järjestäminen

Tietosuojakoulutuksen tietoiskut järjestettiin infoina erilaisten tilaisuuksien alussa. KUUMA-kuntien tietosuojavastaavien kanssa yhteistyönä järjestettiin koulutuksia toimialoille heille kuuluvista tietosuoja-asioista. Koulutuksissa käytettiin ulkopuolisia konsultteja lähinnä, juristeja.

Tilaisuuksiin pystyi osallistumaan joko paikan päällä, oli myös mahdollista katsoa koulutus omalta koneelta, mennä ennalta varattuun neuvotteluhuoneeseen tai muuhun vastaavaan tilaan, josta tilaisuus näytettiin suorana isolta kankaalta esim. valtuustosalista.

Esimerkiksi KUUMA kuntien kanssa yhteistyössä järjestettiin johdon tietosuojakoulutusta, jota seurattiin kunnanhallituksen huoneessa etäyhteyden kautta. Kyseisen koulutuksen piti Suomen Kuntaliiton johtava lakimies Ida Sulin. Koulutus pidettiin Keravan kaupungintalon kaupunginhallituksen kokoushuoneessa, josta se videoitiin muiden KUUMA-kuntien katsottavaksi.

Kuntien Tieran konsultti Olli Nykänen kävi pitämässä Klaukkalan Monikkosalissa EU:n yleisen tietosuojainfon juuri ennen tietosuoja-asetuksen voimaantuloa. Kyseinen konsultti kävi myös pitämässä infoja tietosuojaryhmän palavereissa.

5.4 Tietosuojaselosteet

Tietosuojaselosteet laadittiin ja läpikäytiin tietosuojatyöpajoissa, joihin oli kutsuttu asianomaiset henkilöt. Kunnan toiminnassa oli jo aikaisemmin tehty hyvin pitkälti tietosuojaselosteita eri järjestelmistä. Nämä aikaisemmat tietosuojaselosteet eivät pitäneet sisällään kaikkia uusia tietovaatimuksia, joita uuden asetuksen mukaan tulee kertoa tietosuojaselosteessa.

Aluksi alettiin kartoittaa kunnassa olevia tietojärjestelmiä. Tähän oli jo olemassa konsulttien laatima, muutaman vuoden vanha Excel taulukko, jota ylläpidettiin tietojärjestelmien osalta. Projektiryhmällä oli myös valmiina Nurmijärven kunnan järjestelmäkartta, vuodelta 2016, jossa oli suurin osa olemassa olevista järjestelmistä. Kyseiset järjestelmät oli selkeästi eroteltu toimialoittain:

- Sosiaali- ja terveyspalvelut
- Keskushallinto
- Elinkeino- ja kuntakehitys
- Sivistystoimi
- Ympäristötoimiala
- Perhe- ja sosiaalipalvelut
- Liikuntapalvelut
- Talous- ja hallintopalvelut
- Henkilöstöpalvelut
- Asemakaavoitus ja tekninen suunnittelu
- Tekninen keskus
- Vesilaitos
- Tilakeskus.

Näiden lisäksi oli vielä kunnan omistavat yhtiöt mm.:

- Nurmijärven Sähkö Oy
- Rajamäen Uimahalli Oy

- Nurmijärven Vuokra-asunnot Oy
- sekä muita kunnan omistamia osuuksia.

Läpikäyntiin käytettiin olemassa olevaa Nurmijärven kunnan järjestelmärekisteriä, jonka voitiin katsoa olevan lähes ajan tasalla. Kyseisen järjestelmärekisterin pohjalta lähestyttiin tietojärjestelmien pääkäyttäjiä ja omistajia.

Olemassa olevaan järjestelmärekisterin, eli Excel-taulukkoon oli jo alkukartoituksessa lisätty kohdat, joita alettiin täydentää. Täydennettävät kohdat olivat:

Täydennettävät kohdat					
1. Sisältääkö järjestelmä/tai välitetäänkö sen kautta henkilötietoja	0 = ei sisällä	1 = ei sisällä tai välitä muille järjestelmille suoria henkilötietoja, mutta kylläkin tietoja, jotka muihin tietoihin liitettyinä antavat mahdollisuuden yksilön tunnistamiseen, tai muuten suojattavia lisätietoja hänen toiminnastaan	2 = kyllä sisältää yksilöiviä henkilötietoja	3 = kyllä, sisältää erityisen suojan edellyttäviä henkilötietoja, esim. terveydentila, alaikäiset	4 = ei tiedetä, sisältääkö
2. Tieto henkilörekisterin olemassaolosta. Esim. päiväys, jolloin seloste on viimeksi päivitetty					
3. Linkki henkilörekisteriselosteeseen. Mieluiten originaaliin, mutta jollei se onnistu niin viimeksi (nettisivuilla) julkaistuun					

Taulukko 1. Alkukartoituksen lisätiedot Exceliin

Aiemmin tietosuojaselosteessa oli ollut kaksitoista kohtaa ja nyt uudessa tietosuojaselosteessa tuli olemaan yhdeksäntoista kohtaa. Päivitetty tietosuojaseloste oli laadittu yhteistyössä Kuuma-kuntien tietosuojavastaavien kanssa, ja mallina oli Kirkkonummen tietosuojaseloste. Näin päivitetyt tietosuojaselosteet niputettiin Nurmijärven kunnan verkkosivuille kohtaan: ”Kuntatieto ja päätöksenteko”, jonka alla on erillinen osio, ”Tietosuoja”:

- Asuminen, rakentaminen ja ympäristö
- Hallinto ja talous
- Kasvatus ja sivistys
- Sosiaali- ja terveys
- Kunnan omia työntekijöitä koskevia rekistereitä

Päivitetylle tietosuojasivustolle on koottu yhteen paikkaan kaikki tietosuojaan liittyvät asiat. Aikaisemmin nämä tietosuojaselosteet olivat toimialojen omilla verkkosivuilla. Tämä muutos tehtiin juuri ennen tietosuoja-asetuksen voimaan astumista, toukokuussa 2018.

5.5 Henkilökunnan ohjeistus

Yhteistyössä eri toimialojen edustajien kanssa laadittiin henkilökunnalle ohjeistus tietosuoja-asioihin. Laadittiin myös opas, joka sai nimekseen Nurmijärven O365-Aapinen. Kyseinen opas sisältää ohjeet siitä, kuinka tulee työskennellä pilvipohjaisten ohjelmien kanssa, sekä mihin voi tallentaa tietoa huomioiden tietosuoja-asetuksen vaatimukset.

Kuten jo aiemmin kerrottu, henkilökunnalle järjestettiin eri koulutustilaisuuksia, joihin heidän oli mahdollista osallistua joko paikanpäälle saapumalla tai katsomalla videolähetystä. Henkilökunta sai vapaasti valita ne koulutustilaisuudet, jotka he kokivat omaan työhönsä tarpeelliseksi. Henkilökunta on myös velvoitettu tekemään kerran vuodessa Navicre Navisec Flexin yleinen tietoturva- ja tietosuoja koulutus osion, joka pitää sisällään seuraavat osiot:

- Yleistä tietoturvasta
- Yleistä tietosuojasta
- Tietojen julkisuus ja salassapito
- Henkilöstön tietoturvallinen toiminta
- Tilojen ja tietojen suojaaminen
- Tietoturva sosiaalisessa mediassa

Yllä mainittujen lisäksi tarjotaan Navisecin GDPR-Opas EU:n tietosuojakäytäntöihin -koulutus, joka on lähinnä tarkoitettu esimiehille ja vastuuhenkilöille, mutta sen voi suorittaa kuka tahansa.

Suoritettavat testit ovat: Navisec Flex yleinen tietosuoja, Navisec GDPR ja Tietosuojaa esimiehille ja vastuuhenkilöille sekä Tietoturva testi. Navisecistä löytyy myös koulutusosiot sosiaali- ja terveydenhuollon henkilöille sekä uutena tarjottiin osio opetustoimen henkilöstölle.

Suoritettujen osioiden seurantaa päätettiin alkaa valvoa ja seurata asetuksen voimaantulon jälkeen käytävissä kehityskeskusteluissa.

Yhteistyössä Kuuma-kuntien kanssa laadittiin ”Tietosuojasuositukset O365 Sähköpostiviestinnässä.” (liite4)

5.6 Tietosuojapolitiikka

Nurmijärven tietosuojapolitiikan on laatinut, tietosuojavastaava Hanna Elomaa ja sen on hyväksynyt Nurmijärven kunnanhallitus kokouksessaan 11.6.2018 ”§158 Tietosuojapolitiikan hyväksyminen.”

Tämän jälkeen Nurmijärven kunnan tietosuojapolitiikka ja yleisohje henkilötietojen käsittelystä vietiin käsiteltäväksi yhteistyöryhmän käsittelyyn.

Tietosuojapolitiikassa määritellään esim. tietosuoja on henkilötietojen suojaa:

> ”Tietosuojalla tarkoitetaan henkilötietojen suojaamista. Henkilötietoja ovat kaikki tunnistettavaan henkilöön liitettävissä olevat tiedot. EU:n tietosuoja-asetus, joka tulee voimaan 28.5.2018, asettaa entistä tiukemmat vaatimukset henkilötietojen käsittelylle, ja niihin kuuluu osoitusvelvollisuus. Rekisterinpitäjällä on velvollisuus osoittaa, miten se käsittelee henkilötietoja ja miten yksityisyyden suoja turvataan.” (Nurmijärven kunta 2018.)

Tietosuojan organisointi:

> ”Tietosuojan toteutumisesta kunnassa on viime kädessä vastuussa kunnan johto eli kunnanhallitus, joka myös hyväksyy tietosuojapolitiikan. Tietosuojatyön organisoinnista kunnassa huolehtii tietosuojavastaava, joka raportoi ylimmälle johdolle. Tietosuojavastaava on rooli, ei virkanimike. Tehtävää oman hoitavalla henkilöllä on oikeus saada työhönsä lisäresursseja tarpeen mukaan. Hänellä on oikeus tarvittaessa edellyttää muilta kunnan työntekijöiltä osallistumista tietosuojatyöhön ja tarvittavien tietojen antamista. Tietosuojatyön eteenpäin viemiseen osallistuu ja sitä valvoo tietosuojatyöryhmä, jonka puheenjohtajana toimii hallintojohtaja ja sihteerinä tietosuojavastaava. Ryhmässä on edustus kaikilta kunnan toimialoilta.” (Nurmijärven kunta 2018.)

Tietojärjestelmien turvallinen käyttö ja henkilöstön osaamisen varmistaminen:

> ”Kunnan sisäisiä henkilötietojen käsittelijöitä ovat kaikki henkilötietoja työssään käsittelevät henkilöt. Heiltä vaaditaan osaamista ja sitoutumista. Tietojärjestelmien käyttöoikeuksien saamiseksi työntekijältä edellytetään tietoturva- ja tietosuojasitoumuksen allekirjoittamista. Osaamisen varmistamiseksi koko henkilöstöltä edellytetään Navisec-tietoturva- ja tietosuojakoulutuksen suorittamista. Asia tarkistetaan vuosittain kehityskeskustelujen yhteydessä. Tietosuojakoulutusta edellytetään myös luottamushenkilöiltä. Lisäksi järjestetään vuosittain tietosuojakoulutusta kohdennetuille henkilöstöryhmille.” (Nurmijärven kunta 2018.)

Tietopyyntöihin ja poikkeamiin vastaamisesta on omat ohjeensa. Tähän tarkoitukseen alettiin käyttää tietosuojavaltuutetun lomaketta. Kaikki tietopyynnöt tulee osoittaa kunnanviraston asiakaspalveluun, josta ne toimitetaan edelleen kunnan kirjaamoon.

.

6 Kyselytutkimus

Ennen tietosuoja-asetuksen voimaantuloa 25.5.2018 sekä vähän sen jälkeen oli toteutettu edellä kuvatun mukaisesti Nurmijärven kunnan työntekijöiden keskuudessa tietosuojakoulutukset. Varmistamaan henkilökunnan, sekä koulutuksen käyneiden, että tietosuoja-asetuksen voimaan astumisen jälkeen kunnan palvelukseen tulleiden henkilöiden, tietosuoja-osaamistaso päätettiin järjestää syksyllä 2019 tutkimus. Koska tutkimuksen haluttiin olevan vastaajan kannalta sekä mahdollisimman helposti saavutettavissa että toteutettavissa, päädyttiin kunnan tietosuojavastaavan kanssa käytyjen keskustelujen perusteella toteuttaa se kyselylomakkeella. Kysely tehtiin Webropol 3.0 ohjelmalla ja linkki kyselyyn laitettiin kunnan intraan.

6.1 Kyselytutkimuksen tavoite

Kyselytutkimuksella haluttiin kartoittaa kunnan työntekijöiden tietämystä tietosuoja-asetuksesta sekä tarvittavasta lisäkoulutuksesta. Tutkimuskysymykset, joihin kyselytutkimuksella haettiin vastauksia:

1. Tarvitseeko henkilö työssään lisäkoulutusta liittyen tietosuoja-asetukseen?

    - Koska kysely oli suunnattu kaikille niille kunnan työntekijöille, joilla oli pääsy intraan, niin vastaanottajien tarve tietosuoja-asioille vaihteli suuresti.
    - Koulutuksesta saatu hyödynnettävyys työhön haluttiin myös määritellä tarkemmin.

2. Minkä koulutusmuodon henkilöt katsovat parhaiten palvelevan heitä?

    - Koska kunnan henkilökunnan työtehtävät, työajat ja toimipaikat vaihtelevat suuresti, haluttiin varmistaa, että valitut koulutusmuodot mahdollistavat joustavan koulutuksen. Niin, että koulutus ei olisi aikaan tai paikkaan sidottu.

3. Mitkä ovat tietosuoja-asetuksen osa-alueet, joissa lisätietoa tarvitaan?

    - Tietosuoja-asetus edellyttää muutoksia työntekijän tavassa luovuttaa henkilötietoja sekä käsitellä niitä. Kyselyllä haluttiin varmistaa, että työntekijän tavassa toimia kyseiset muutokset oli huomioitu.

- Koska ennen tietosuoja-asetuksen voimaantuloa sekä välittömästi voimaantulon jälkeen pidetyistä koulutuksista oli kulunut vuosi. Haluttiin tietää, minkä osa-alueen osalta syventävää koulutusta henkilökunta tarvitsi.
- Haluttiin myös varmistaa, että henkilöille, jotka ovat tulleet kunnan palvelukseen tietosuoja-asetuksen voimaantulon jälkeen, on riittävän monipuolista koulusta tarjolla.

6.2 Kyselyn toteutus

Kysely toteutettiin syksyn 2019 aikana ja tuloksia alettiin analysoida välittömästi vastausten valmistuttua. Kyselytyökaluna käytettiin koulun Webropol 3.0 ohjelmaa. Kysely avattiin kunnan Mylly-intranet sivuille. Lisäämään kyselyn kiinnostavuutta kunnan työntekijöiden keskuudessa, kysely tehtiin Nurmijärven tietosuojavastaavan nimissä.

Vastaajille annettiin noin kaksiviikkoa vastausaikaa eli vastauksia odotettiin 20.9.2019 mennessä. Kyselyn puolivälissä kyselyä nostettiin intrassa, jotta saatiin vastaajia aktivoitua. Vastausaika määriteltiin tarkoituksella riittävän lyhyeksi, jotta vastaajat saataisiin toimimaan välittömästi kyselyn saatuaan. Kunnassa aiemmin toteutettujen vastaavanlaisten kyselyjen perusteella voitiin päätellä, että henkilöt, jotka vastaavat kyselyihin, toimivat joko välittömästi kyselyn avattuaan tai jättävät vastaamatta. Näin ollen pitkällä kyselyajalla ei voitu olettaa vastausprosentin nousevan.

Kyselyyn oli tullut määräaikaan mennessä viisitoista vastausta. Tämän lisäksi kyselyn oli avannut ja/tai osittain vastannut 34 henkilöä.

Internet kyselyt ovat yleistyneet viimevuosina voimakkaasti myös Nurmijärven kunnassa. Tässäkin kyselyssä vastaajien joukko oli kaikki ne Nurmijärven kunnan työntekijät, joilla on pääsy hallinnon verkkoon ja sitä kautta pääsivät kunnan Mylly-intranettiin. Vastaajilta pyydettiin valitsemaan toimialansa, jotta tiedettiin mitä toimintoa kunnassa vastaajat edustivat. Vastaajien vastaushalukkuutta lisäämään oli kysely laadittu lyhyeksi. Asetetuilla kysymyksilläkin uskottiin saatavan riittävästi tietoa, siitä millainen tarve on jatkossa kehittää erilaisia tietoiskuja ja koulutuksia.

6.3 Kyselylomake

Kyselyn oli pääsy kunnan intranetin kautta. (lomake Liite 1)
Kyselylomake oli rakennettu pitäen sisällään seuraavat osiot:

- taustatiedot
    - toimialue ja yksikkö:

        - tietoa tarvittiin koulutustarpeen selvittämiseen, missä yksiköissä on tarvetta lisäkoulutuksille ja samalla saada tietoa siitä missä asiat ovat jo kunnossa
    - sukupuoli:
        - haluttiin myös saada tietää vastaajien sukupuolijakauma.
            - haluttiin nähdä, oliko sukupuolella merkitystä saadun koulutuksen tasoon

    - ikä
        - haluttiin selvittää karkealla tasolla vastaajien ikäjakauma suhteessa osaamiseen ja koulutustarpeeseen
            - koska koulutus oli toteutettu ns. nykyaikaisilla koulutusmetodeilla, eikä esim. aiemmin annettuna luokkahuone koulutuksina, haluttiin nähdä, oliko toteutetuilla koulutusmetodeilla vaikutusta saadun koulutuksen tasoon

- asiakysymykset

    - Osallistumiseni jo aiemmin järjestettyihin koulutuksiin?
        - tietoa aiemmin toteutetuista koulutuksista
            - minkä tyyppiset koulutukset koettiin parhaimpina

    - Käsittelenkö työssäni henkilötietoja / tietosuojaan liittyviä asioita?
        - kuinka monta prosenttia henkilökunnasta työskentelee tietosuojan parissa

    - Tarvitsenko työssäni lisäkoulutusta liittyen tietosuoja-asetukseen?
        - selvitetään lisäkoulutuksen tarve

    - Minua parhaiten palveleva koulutusmuoto?
        - minkä tyyppinen koulutusmuoto parhaiten sopii millekin työntekijäryhmälle

    - Mistä tarvitsisin lisätietoa?
        - vapaamuotoinen palaute

7 Analysointi ja aikataulutus toimeenpanoille

Kyselyn tuloksena saatiin määrällistä dataa, kvantitatiivista tietoa sekä laadullista tietoa avoimen kysymyksen kautta. Tässä tutkimuksessa toteutettiin kysely, joka analysoidaan määrällisen tutkimusmenetelmän avulla. Tavoitteena oli yleistää tulokset koskemaan koko kunnan henkilöstöä ja saada tietoa siitä, mitä henkilö oli jo oppinut ja millaista hyötyä hän oli saanut työhönsä. Kyselyn tuloksiin on laskettu prosenttilukuja ja tilastollisia lukuja Webropolista.

7.1 Tehdyn kyselytutkimuksen analysointi

Nurmijärven kunnan työntekijöille suunnatussa tutkimuskyselyssä oli tarkoituksena saada selville, miten jo pidetyistä koulutuksista on ollut hyötyä henkilön omassa työssään. Haluttiin myös tutkia, minkälaisena henkilöstö oli kokenut annetun tietosuoja koulutuksen, sekä kartoittaa jatkokoulutustarpeet. Tutkimuskysymykset ovat liitteessä nro 1.

Saadut vastaukset jakaantuivat konsernipalvelun, ympäristötoimialan, sivistys- ja hyvinvointitoimialan kesken. Kyselyyn saatiin 15 vastausta sekä 34 osittain vastattua tulosta. Saatujen vastausten lukumäärä voidaan katsoa melko alhaiseksi, eikä sen perusteella voida tehdä pitkälle meneviä johtopäätöksiä. Asetettuihin tutkimuskysymyksiin saatiin kuitenkin riittävän kattavat vastaukset tukemaan jatkotoimenpiteitä. Tämä sen vuoksi, että tutkimukseen saadut vastaukset tulivat kaikilta päätoimialoilta. Tulosten perusteella voidaan päätellä, että lisäkoulutukselle on tarvetta.

7.1.1 Kvantitatiivinen tutkimusmenetelmä

Kvantitatiivien eli määrällinen tutkimusmenetelmä on tyypillisesti lomakekysely tai strukturoitu lomakehaastattelu, jossa kysytään samoja asioita samassa muodossa isolta joukolta. Tämä joukko muodostaa otoksen tietystä perusjoukosta. Määrälliset menetelmät soveltuvat hyvin tilanteisiin, joissa halutaan testata pitääkö jokin teoria paikkansa. Tehdään hypoteeseja eli väittämiä, joita kyselyllä testataan. Väittämä voisi olla esim. ”Palveluprosessin nopeus vaikuttaa asiakastyytyväisyyteen” Kyselyn jälkeen todettaisiin pitävätkö väittämät paikkaansa ja tulos olisi tosi tai epätosi. Lomakkeen kysymyksien avulla mitataan teorian paikkansapitävyyttä. Kyselyn avulla kerätty materiaali analysoidaan tilastollisin menetelmin ja tiedot yleistetään koskemaan koko perusjoukkoa. Tutkija ei vaikuta tutkimuksen kohteeseen eikä usein edes kohtaa tutkittavia. (Ojasalo, Moilanen & Ritakoski 2015,104.)

Kyselyä voidaan käyttää monella eri tavalla, ne tuottavat tyypillisesti paljon numeroihin perustuvia tuloksia. Näitä tuloksia voidaan tutkia tilastollisesti. Tilastolliseen tutkimukseen ja raportointiin on kehitetty valmiit tilastolliset analyysitavat ja ohjelmistot esim. Excel tai monipuolisempaan käyttöön SPSS. Kysely on nopea toteuttaa suurelle joukolle. Kyselyn heikkoutena yleisesti pidetään tuotetun tiedon pinnallisuutta ja ettei pysty arvioimaan vastaajien suhtautumista kyselyyn. Vakiotulkinnan mukaan kvantitatiivisilla (määrällinen) menetelmillä saadaan pinnallista mutta luotettavaa tietoa. (Ojasalo, Moilanen & Ritakoski 2015,121.)

Määrällinen tutkimus pyrkii selittämään tutkimuksen kohteena olevia ilmiöitä havaintojen avulla. Tutkimuksen kohteena olevat ilmiöt määritellään tutkimuksen tavoitteiden perusteella. Mittauksen kohteita kutsutaan havaintoyksiköiksi, joissa tutkija valitsee havaintoyksiköiden määrän, kuinka monesta kerätään tietoa. (Ojasalo, Moilanen & Ritakoski 2015,122.)

Nettipohjaiset kyselyt ovat yleistyneet viime aikoina todella paljon. Kyselyiden toteuttamiseen on tarjolla monia ohjelmistoja. Tunnetuimmat ovat Webropol, SurveyMonkey, Digium ja Microsoftin Forms. Tyypillisiä tapoja on kotisivuille tai yrityksen omille sivuille liitetyt kyselyt sekä some alustoille.

Kysely sopii hyvin tilanteisiin, joissa tutkittava alue tunnetaan entuudestaan hyvin ja halutaan varmistua sen paikkansapitävyydestä. Kyselyn suunnittelussa on useita vaiheita, on suunniteltava, mitä tietoa tarvitaan. Myös kyselyn analysointi olisi hyvä suunnitella etukäteen. Kyselyn kysymyksiin pitää pystyä vastaamaan helposti. Tulokset ilmaistaan yleensä jakaumina ja tunnuslukuina aineistosta. Kyselytutkimusten vastausprosentit ovat pienentyneet, joka voi johtua suuresta kyselytulvasta. (Ojasalo, Moilanen & Ritakoski 2015,40-41.)

Kyselylomake on tavallisin aineiston keräämistapa määrällisessä tutkimuksessa. Kyselyn voi toteuttaa myös vakioituna eli standardikyselynä, jolloin kaikilta kysytään sama asiasisältö. Tiedonkeruuta heikentää se, että kysely ei tavoita kaikkia vastaajia, jolloin vastausprosentti jää alhaiseksi. Määrällisessä tutkimuksessa voi käyttää lähdeaineistona muiden keräämiä tutkimusaineistoja esim. Tilastokeskus. Olennaista on määrällisen, hyvän tutkimussuunnitelman laatiminen sekä tutkimusongelman asettaminen laajemmasta kokonaisuudesta. (Vilkka 2015, 61-73.)

Määrällisen tutkimuksen pätevyys (validiteetti) tarkoittaa kykyä mitata sitä mitä tutkimuksessa oli tarkoitus mitata. Tutkittavien tulee ymmärtää kyselylomakkeen kysymykset samalla tavalla kuin tutkija tarkoitti. Tutkimus on onnistunut, kun tutkija on onnistunut siirtämään tutkimuksessa käytetyn teorian kyselylomakkeelle. (Vilkka 2015, 124)

Määrällisen tutkimuksen luotettavuus (reliabiliteetti) tarkoittaa tulosten tarkkuutta, antaa eisattumanvaraisia tuloksia. Tämä tarkoittaa, että jos tutkimus toistetaan, niin saman henkilön kohdalla tulee sama mittaustulos. Tutkimuksen pätevyys ja luotettavuus muodostavat yhdessä kokonaisluotettavuuden. (Vilkka 2015, 124)

Kyselyllä voidaan mitata laadullista (avoimet kysymykset) ja määrällistä dataa, useimmiten kuitenkin painopiste tutkimuksissa on määrällisellä puolella. Määrällistä dataa voidaan

tutkia tilastollisilla analyyseillä. Tilastollisissa analyyseissä tutkimuksen perusmenetelmät voidaan jakaa kahteen ryhmään: perustaviin menetelmiin ja monimuuttujamenetelmiin. Perustavia menetelmiä ovat mm.:

- keskiluvut (moodi, mediaani, keskiarvo)
- hajontaluvut (keskihajonta, vaihteluväli, vaihteluvälin pituus, variaatiosuhde ja variaatiokerroin)
- ristiintaulukointi
- korrelaatio (Pearson)
- riippuvuusluvut (Spermann rho, kontigenssikerroin).

Monimuuttujamenetelmiä ovat mm.:

- klusterianalyysi
- varianssianalyysi
- erotteluanalyysi
- faktorianalyysi

(Ojasalo, Moilanen & Ritakoski 2015,134-135.)

7.2 Kyselytutkimuksen tulokset

Kuten jo aiemmin on todettu, kunnan Mylly-intrassa oli linkki kyselyyn, johon saatiin määräaikaan mennessä kokokyselyyn 15 vastausta, jonka lisäksi muutamia osittaisia vastauksia. Kysely oli avattu 34 kertaa ja joihinkin kohtiin myös vastattu. Tiedonkeruumenetelmänä toimi kyselytutkimus Webropol 3.0 ohjelmalla toteutettuna.

Tietosuoja-asetus Nurmijärven kunta

Seurantatilastot | Vastaajan tilastot

Näytä / piilota rivejä Näytä: n %

	Yhteensä	
	(N)	%
Vastattu kyselyyn: Julkinen nettilinkki	15	100
Kysely avattu vastaajien toimesta	34	226
Vastaaminen aloitettu	15	100

Taulukko 2. Kyselyn yhteenveto

7.2.1 Toimialue

Vastaajien määrä: 15

Alla vastaajien jakauma toimialueittain:

	n	Prosentti
Konsernipalvelut	7	46,67%
Ympäristötoimiala	4	26,67%
Sivistys- ja hyvinvointitoimiala	4	26,67%
Yhteensä	15	100%

Taulukko 3. Toimialue jakauma

Yllä olevien toimialojen jakaumat tulosyksiköittäin:

Konsernipalvelut:

- talouspalvelut 3 kpl
- hallintopalvelut 3 kpl
- Aleksia-liikelaitos 1 kpl

Ympäristötoimiala:

- maankäyttö ja yleiskaavoitus 1 kpl
- tekninen keskus 1 kpl
- asemakaavoitus suunnittelu ja tilakeskus 1kpl

Sivistys- ja hyvinvointiala:

- hyvinvointipalvelut 1 kpl
- varhaiskasvatuspalvelu 1 kpl
- kirjasto- ja kulttuuripalvelut 1 kpl
- nuorisopalvelut 1 kpl

7.2.2 Sukupuoli

Vastaajien määrä: 15

Kyselyssä vastaajien sukupuolijakauma oli lähes 50/50, alla. Todellinen henkilökunnan sukupuolijakauma toimialoittain on noin 80% naisia. Tältä osin vastaajien jakauma ei suotaan vastaa reaalitilannetta henkilökunnan osalta.

	n	Prosentti
Nainen	8	53,33%
Mies	7	46,67%

Taulukko 4. Sukupuoli jakauma

7.2.3 Ikä

Vastaajien määrä: 15

Kyselyssä vastaajien ikäjakauma painottui annetun ikäjakauman yläpäähän, alla. Tämä vastaa kunnan tämänhetkistä henkilökunnan reaali-ikäjakaumaa. Ikäjakaumaa kysyttiin vain karkealla tasolla, koska sitä käytettiin vain valittujen koulutusmenetelmien onnistumisen arviointiin.

	n	Prosentti
- 35 vuotta	2	13,33%
35 - 50 vuotta	6	40%
51- vuotta	7	46,67%

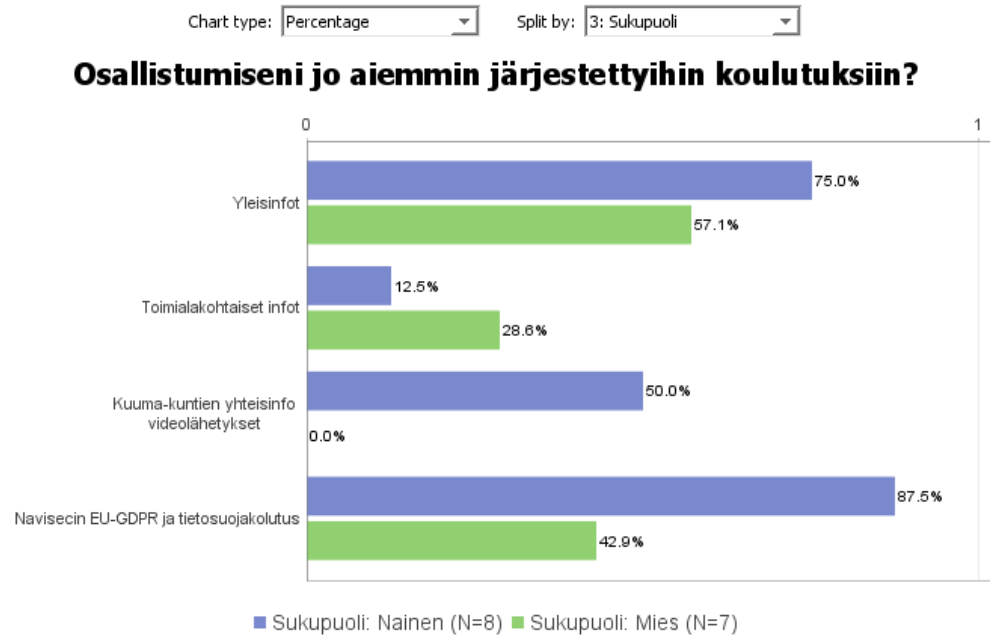
Taulukko 5. Ikä jakauma

7.2.4 Osallistuminen jo aiemmin järjestettyihin koulutuksiin

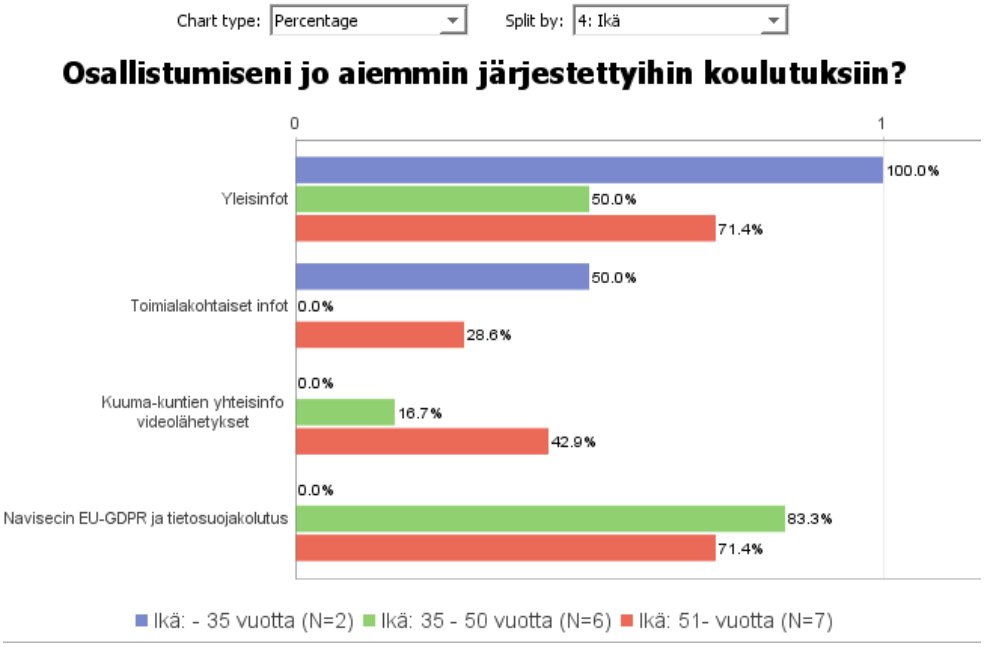
Vastaajien määrä: 15, valittujen vastausten lukumäärä: **27**

Selite	**n**	**%**
Yleisinfot	10	37%
Toimialakohtaiset infot	3	11%
Kuuma-kuntien yhteisinfo videot	4	15%
Navisec GDPR ja tietosuojakoulutus	10	37%

Saatujen vastausten mukaan vastaajat olivat osallistuneet eniten yleisinfoihin sekä Navisecissa oleviin GDPR ja tietosuojakoulutuksiin. Kuuma-kuntien kanssa yhteistyössä tehtyihin koulutuksiin, joissa on ollut erikseen tilattu asiantuntija, kertomassa aiheesta sekä toimialakohtaisiin infoihin, joita on pidetty kunnan eri tiloissa, on ollut vähiten osallistujia.



Taulukko 6. Sukupuolen mukaan jaoteltu osallistuminen



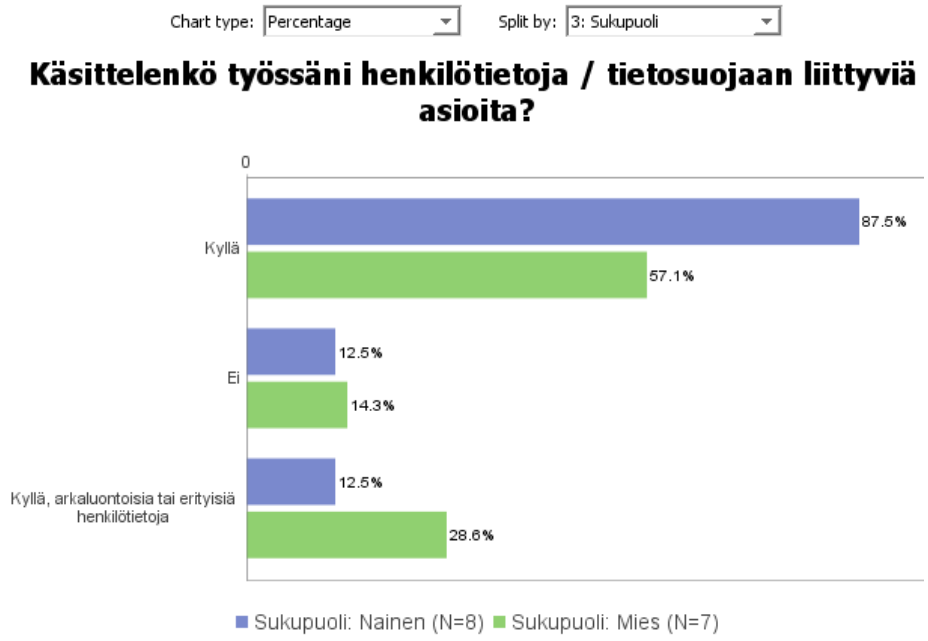
Taulukko 7. Iän mukaan jaoteltu osallistuminen

7.2.5 Käsittelenkö työssäni henkilötietoja / tietosuojaan liittyviä asioita

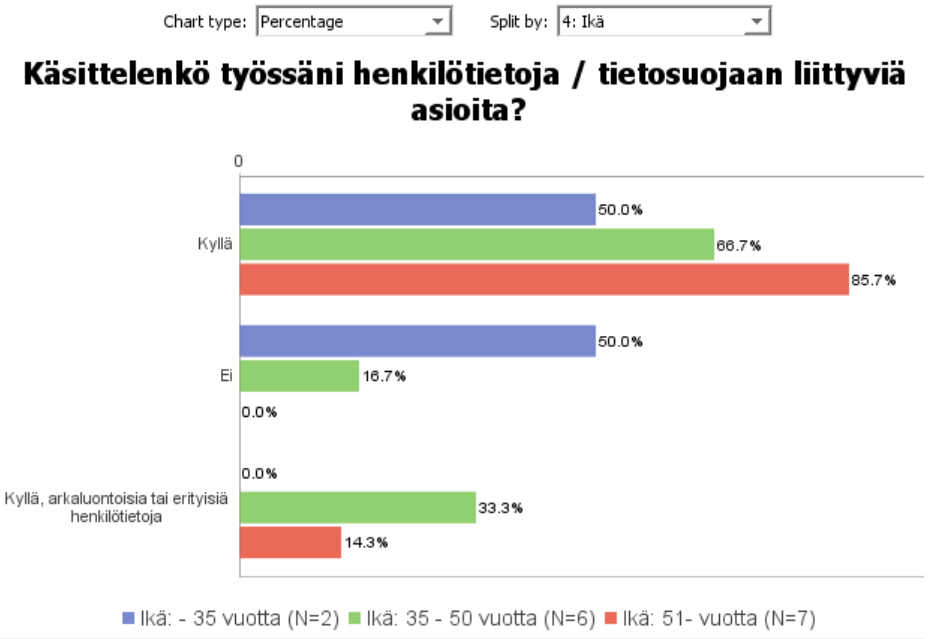
Vastaajien määrä: 15, valittujen vastausten lukumäärä: **16**

Henkilötietoja työssään käsitteli vastaajista 69%, jonka lisäksi arkaluontoisia henkilötietoja käsitteli 18,5 %. Tämän mukaisesti 87,5% vastaajista käsittelee työssään henkilötietoja. Saatu vastaus tukee aiemmin annetuissa koulutuksissa saatua tietoa.

Selite	n	%
Kyllä	11	69%
Ei	2	12,5%
Kyllä, arkaluontoisia tai erityisiä henkilötietoja	3	18,5%



Taulukko 8. Sukupuolen mukaan jaoteltu



Taulukko 9. Iän mukainen jakauma

Taulukon mukaan ikäryhmässä yli 51-vuotiaat tuntevat tarvitsevan lisäkoulutusta verrattuna muihin ikäryhmiin.

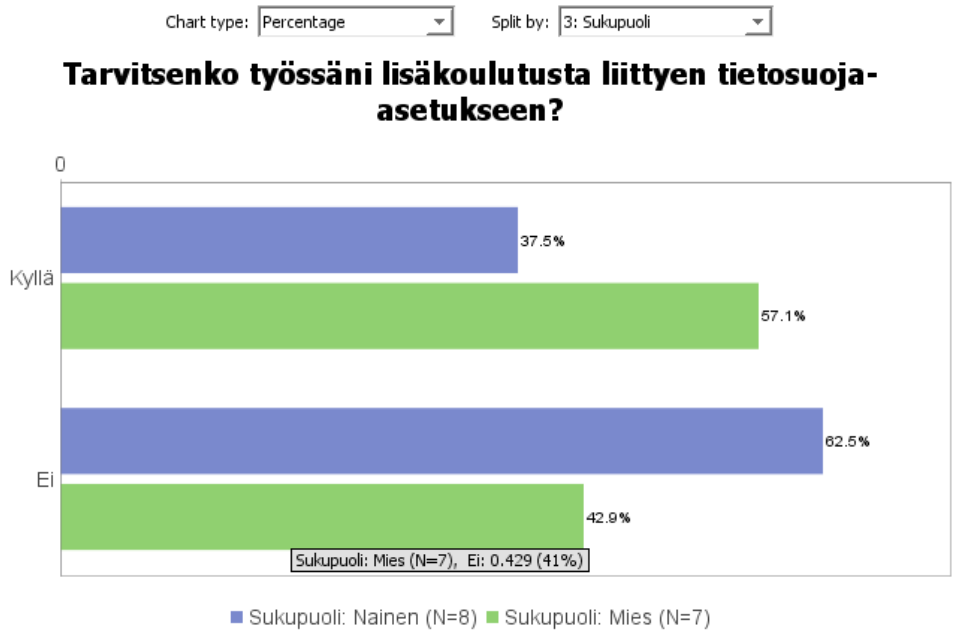
7.2.6 Tarvitsenko työssäni lisäkoulutusta liittyen tietosuoja-asetukseen

Vastaajien määrä: 15

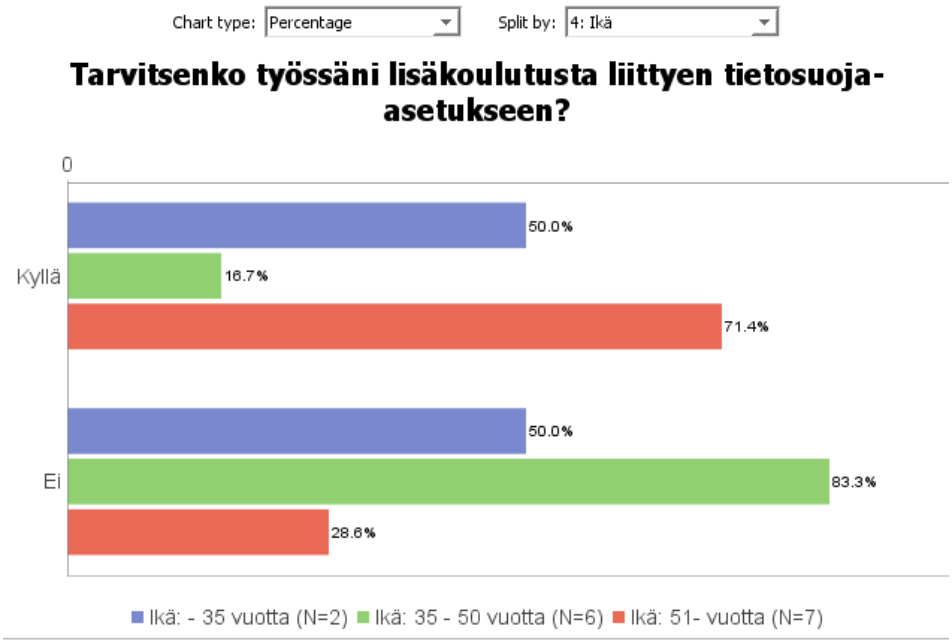
Lisäkoulutusta tietosuoja-asetukseen liittyvissä kysymyksissä kokee tarvitsevansa 46,7% vastaajista. Talous ja hallintopalveluissa toivotaan lisää koulusta enemmän verrattuna muihin.

	n	Prosentti
Kyllä	7	46,67%
Ei	8	53,33%

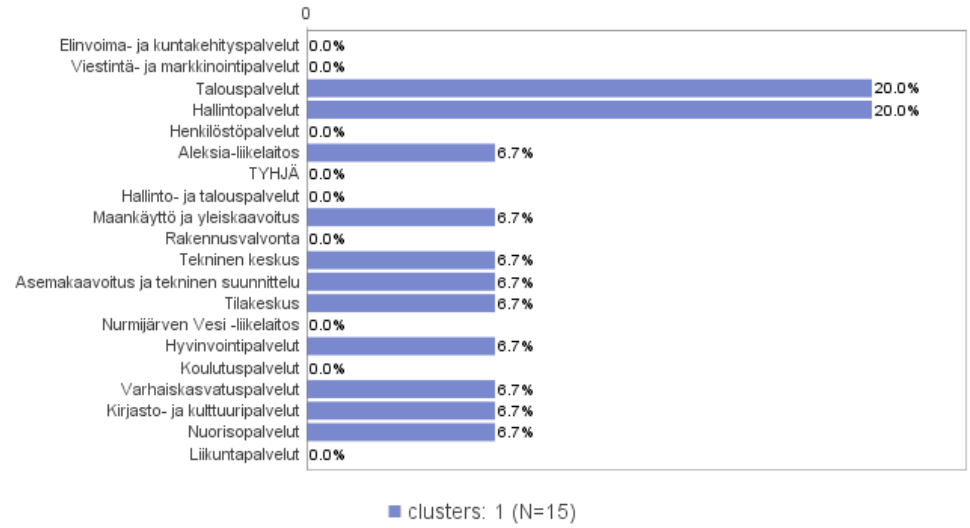
Taulukko 10. Prosenttijakauma



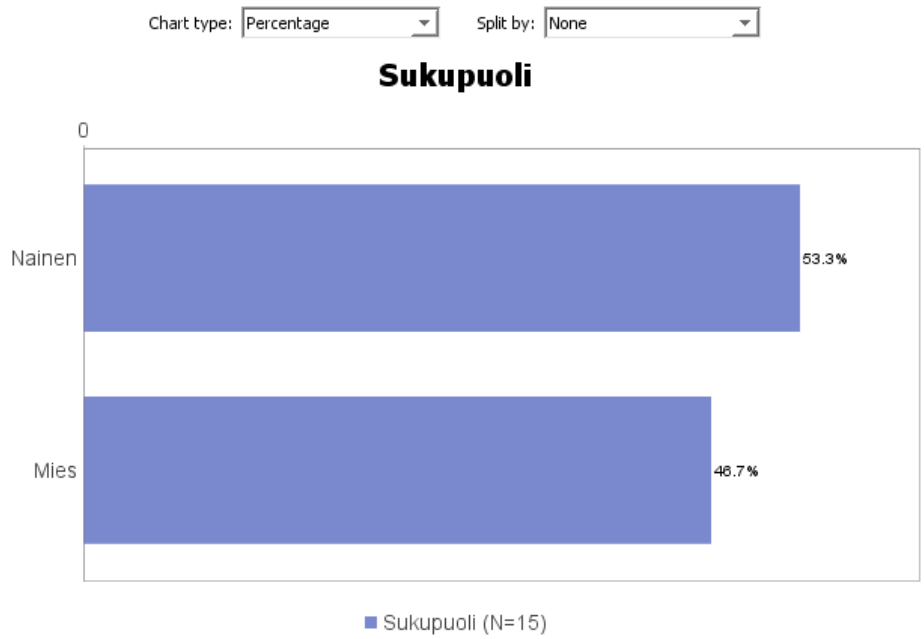
Taulukko 11. Prosenttijakauma



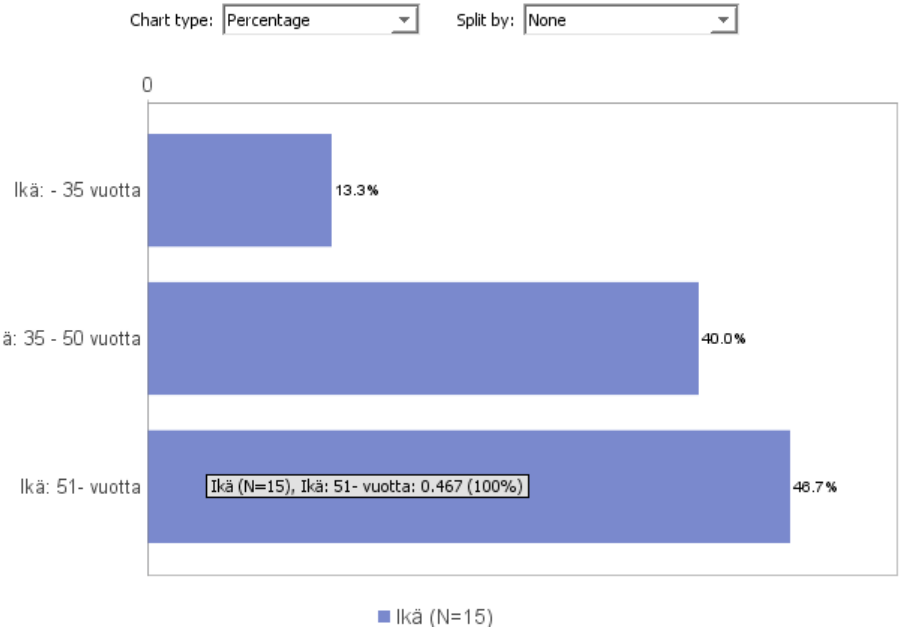
Taulukko 12. Ikäjakauma



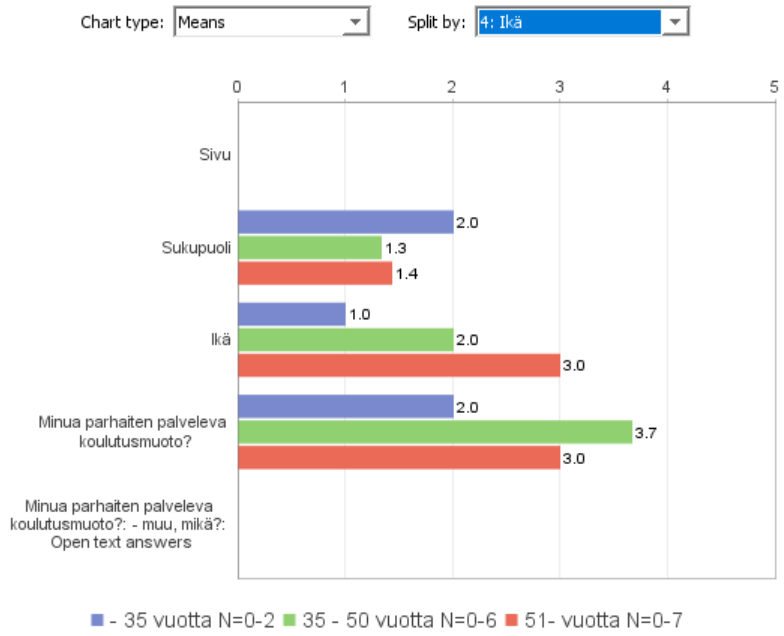
Taulukko 13. Tarvitsenko työssäni lisäkoulusta tietosuoja-asetukseen toimialajakauma



Taulukko 14. Tarvitsenko työssäni lisäkoulutusta sukupuolen mukaan



Taulukko 15. Tarvitsenko työssäni lisäkoulutusta iän mukaan



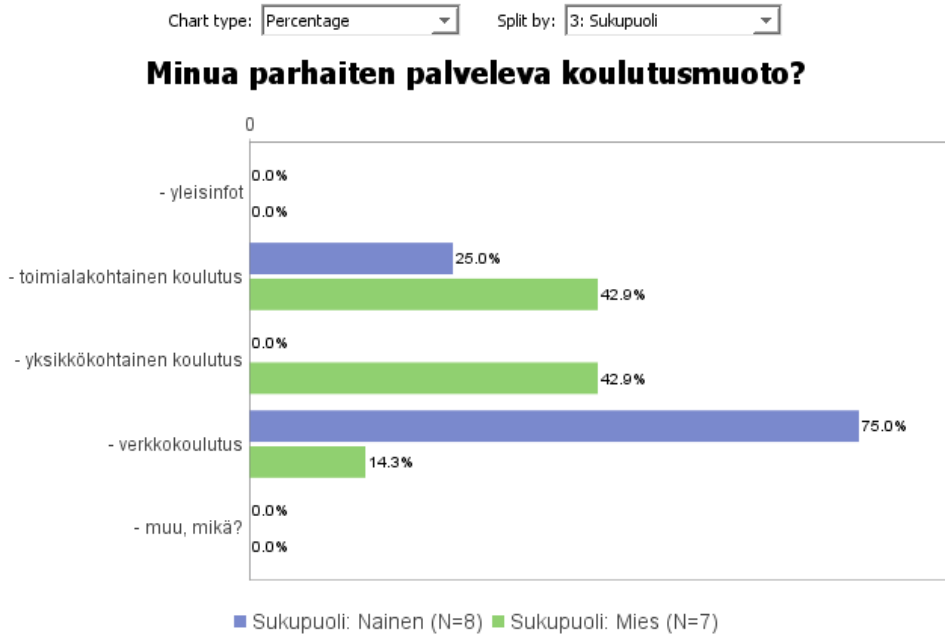
7.2.7 Minua parhaiten palveleva koulutusmuoto

Vastaajien määrä: 15

Vastaajien mukaan verkkokoulutus on naisille paras koulutusmuoto 75%. Miehillä taas toimialakohtainen ja yksikkökohtainen koulutus sai 42,9%.

	n	Prosentti
- yleisinfot	0	0%
- toimialakohtainen koulutus	5	33,33%
- yksikkökohtainen koulutus	3	20%
- verkkokoulutus	7	46,67%
- muu, mikä?	0	0%

Taulukko 16. Vastaajien määrät



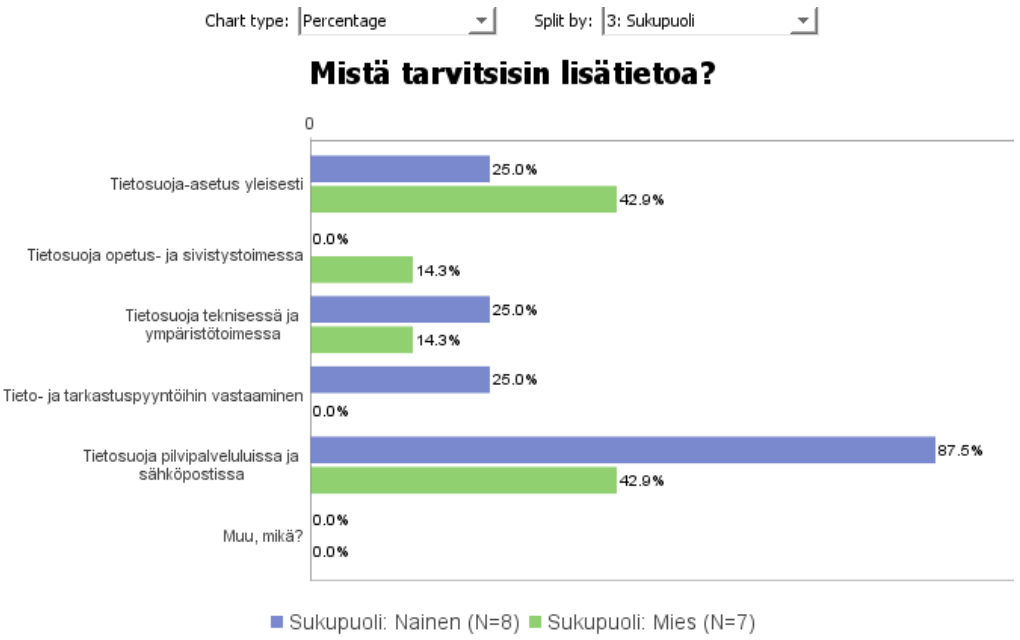
Taulukko 17. Sukupuolijakauma

7.2.8 Mistä tarvitsisin lisätietoa

Vastaajien määrä: 15, valittujen vastausten lukumäärä: n= **21**

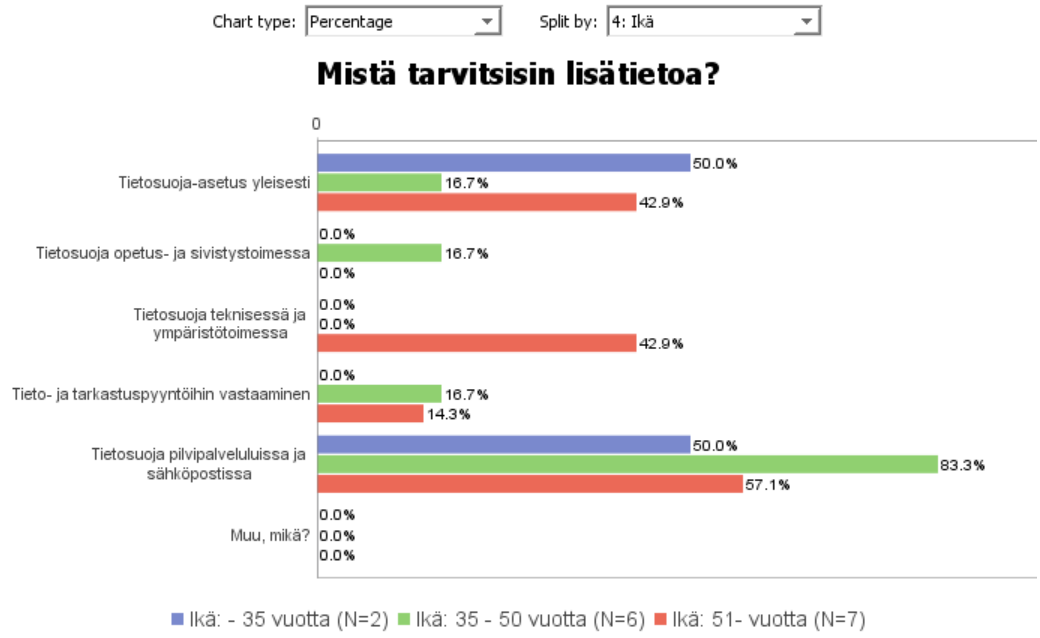
Lisäkoulutuksen tarve on tietosuoja-asioissa vastausten mukaan suurin liittyen pilvipalveluissa ja sähköpostissa 48%, jonka lisäksi tietosuoja-asetuksesta yleisesti 24%. Tutkimuksen kannalta tämän kysymyksen osalta mielenkiintoinen seikka on vaikka kokonaisuudessaan vastasi 15 henkilöä, tähän kysymykseen vastasi 21 henkilöä. Tämän perusteella voidaan olettaa, että tarvittavan lisätiedon saaminen koetaan tärkeäksi. Kyselyyn vastaajat kokivat tähän kysymykseen vastaamisen tärkeäksi, vaikka heillä ei ollut aikaa/mielenkiintoa vastata koko kyselyyn. Alla olevassa prosenttiluvut on laskettu n=21.

Selite	**n**	**%**
Tietosuoja-asetus yleisesti	5	24%
Tietosuoja opetus- ja sivistystoimessa	1	5%
Tietosuoja teknisessä ja ympäristötoimessa	3	14%
Tieto- ja tarkastuspyyntöihin vastaaminen	2	9%
Tietosuoja pilvipalveluissa ja sähköpostissa	10	48%
Muu, mikä?	0	0%



Taulukko 18. Sukupuolijakauma n=15

Webropol laskee nämä prosentit viidentoista vastaajan mukaan, kun itse laskin yllä valittujen vastausten lukumäärän perusteella 21.



Taulukko 19. Ikäjakauman mukaan

Taulukko 20. Mistä tarvitsisin lisätietoa yhteenveto

Taulukon 20:sta mukaan eniten koulutustarvetta on tietosuoja pilvipalveluissa ja sähköpostissa.

7.3 Muuta palautetta ja parannusehdotuksia, Sanapilvi

Vastaajien määrä: 1

	Vastaukset
▼	Tiedetään mitä pitäisi ytehdä, mutta ei ole aikaa, resursseja ja halua tehdä asioita niin vaikeasti. Pitäisi keksiä jokin helppo ja turvallinen tapa toimia yhtenäisesti.

Vapaan palautteen osioon tuli varsinaisesti vain yhden henkilön vapaa palaute ja siinä todetaan, että kyllä tiedetään mitä pitäisi tehdä mutta pitäisi olla resursseja enemmän. Toivotaan helpompaa tapaa tehdä asioita yhdessä sekä turvallista tapaa toimia yhdessä.

Kyselylomakkeen viimeinen kohta oli: ”Muuta palautetta ja parannusehdotuksia” Tutkimuksen tähän kohtaan saatiin kahden henkilön vastaukset. Toinen vastaajista oli tietosuojavastaaja, joka kokeili kyselyn toimivuutta. Tämä tarkoittaa sitä, että tässä tutkimuksessa voidaan hyödyntää tässä kysymyksessä vain yhtä vastausta:

- ”Tiedetään mitä pitäisi tehdä, mutta ei ole aikaa, resursseja ja halua tehdä asioita niin vaikeasti. Pitäisi keksiä jokin helppo ja turvallinen tapa toimia yhtenäisesti.”

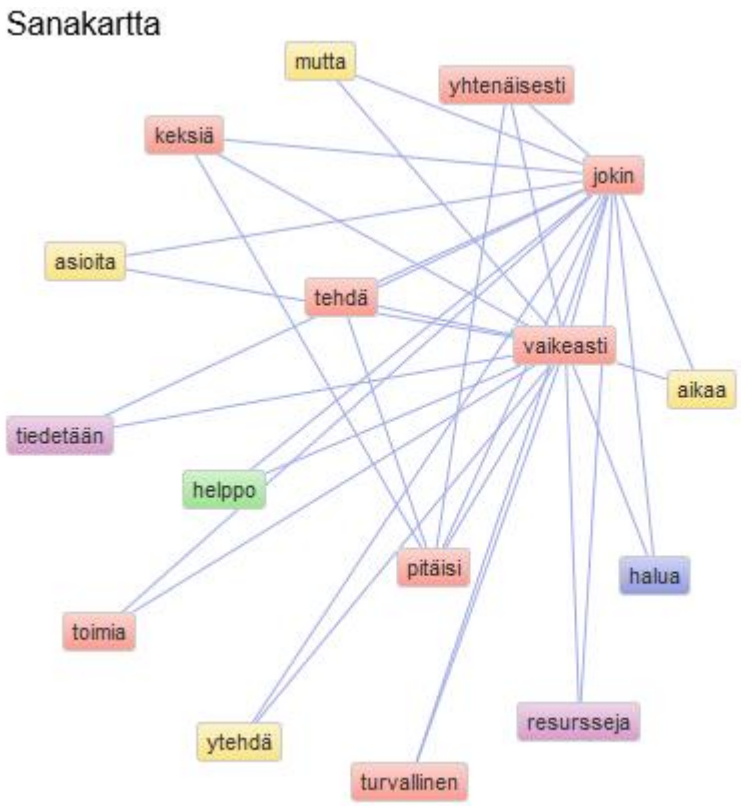
Yllä mainittu vastaus on kuitenkin hyödynnettävissä, sillä se on yleisluontoinen ja voidaan olettaa muidenkin vastaajien kokevan samalla tavalla. Vastauksessa tuodaan esille huoli, siitä kuinka aika ei riitä oppimaan uusia asioita, ei ole aikaa kuunnella kunnan järjestämiä

infoja tai ei ole mahdollista työn ohessa katsoa videolähetystä koulutuksista. Järjestetyissä koulutuksissa kuultiin, kuinka koulujen opettajien ja päiväkotien varhaiskasvattajien on erittäin hankala järjestää aikaa osallistua koulutuksiin. Tämä johtuu siitä, että sijaisten saanti on hankalaa ja aiheuttaa kustannuksia kunnalle. Koulutuksissa saadun palautteen mukaan kyseiset henkilöt toivoisivat kuitenkin saavansa lisäkoulutusta tietosuoja-asetukseen liittyvissä asioissa.

Sanapilvi

aikaa asioita halua helppo jokin keksiä kokeilen linkin mutta pitäisi resursseja samalla tehdä tiedetään tietosuojavastaava toimia toimivuutta turvallinen vaikeasti vastaan yhtenäisesti tehdä

Yleisimmin esiintyvät sanat



Taulukko 21. Sanapilvi

Kaikki

- ”Tiedetään mitä pitäisi ytehdä, mutta ei ole aikaa, resursseja ja halua tehdä asioita niin vaikeasti. Pitäisi keksiä jokin helppo ja turvallinen tapa toimia yhtenäisesti.”

Sanapilvessä nähdään useimmin toistuvat sanat ja ne ovat siinä suurennettuina mitä useampi vastaus, mutta tässä siis vain yhden vastaajan tiedot.

8 Johtopäätökset

Opinnäytetyön tavoitteena oli tutkia kyselytutkimuksen kautta, mitä hyötyä henkilöstö oli saanut jo pidetyistä koulutuksista ja millaisia tulevaisuuden koulutukset pitäisivät olla. Tietosuoja-asetus on jo ehtinyt olla voimassa yli vuoden, joten haluttiin selvittää siitä syntynyttä koulutustarvetta ja sitä mitä henkilöt olivat jo oppineet.

8.1 Tutkimuskysymykset ja niihin saadut vastaukset

Alla yhteen vedettyinä tutkimuskysymykset sekä niihin saadut vastaukset analysoituina.

1. Tarvitseeko henkilö työssään lisäkoulutusta liittyen tietosuoja-asetukseen?

   Saadun tiedon mukaisesti vastaukset jakaantuvat lähes tasan lisäkoulutuksen tarpeenmukaisesti. Voitiin kuitenkin nähdä, että talous- ja hallintopalvelut toimialueilla lisäkoulutuksen tarve oli huomattava.

   Tutkimustuloksissa tulee selvästi esille tarve lisäkoulutuksille ja yleensäkin tarve lisätä henkilöstön tietoisuuttaa tietosuoja-asetuksesta. Tämän lisäksi tulee lisätä säännöllisesti toimialapalavereiden ns. esimiespäivien yhteydessä tietosuoja-asetuksen tietoiskuja, kulloinkin ajankohtaisena olevavasta aiheesta. Koulutustarpeen kautta voi päätellä, että kunnan uusille verkkosivuille on hyvä lisätä oma tietosuojaosio. Tähän tulee päivittää kaikki tietosuojaselosteet ja yleinen ohjeistus tietosuojasta.

   Kunnan viranomaistoiminnan vuoksi tietosuoja-asiat voitiin nähdä olevan jo melko korkealla tasolla. Tämä sen vuoksi, että lainsäädäntö oli jo aiemmin ohjannut kunnan toimintaa. Näin ollen hyvinvointipuolella oli jo laadittu kattavat tietosuojaselosteet, toimintatavat tietosuoja-asioihin sekä henkilötietojen käsittelyyn. Myös kunnan muussa toiminnassa oli jo olemassa tietosuojaselosteet, joita vain tarvitsi päivittää ja lisätä uuden asetuksen muutama kohta selosteeseen mukaan. Työpajoissa oli kartoitettu henkilörekistereitä ja tietojärjestelmiä ja näin tehty tietotason nostaminen oli koettu onnistuneeksi.

2. Minkä koulutusmuodon henkilöt katsovat parhaiten palvelevan heitä?

   Parhaimpina koulutusmuotoina koettiin verkkokoulutus, toimialakohtainen koulutus sekä yksikkökohtainen koulutus. Verkkokoulutuksen hyvinä puolina voidaan nähdä ajasta ja paikasta riippumaton koulutukseen osallistuminen. Tämä tukee hyvin tutkimuksessakin ilmi tullutta koulutukseen osallistumisajan löytämisen haastetta. Nurmijärven kunta 367,3 km2, joka tarkoittaa sitä, että välimatkat eri toimipisteiden välillä ovat pitkät. Näin ollen esimerkiksi koulujen ja päiväkotien työntekijöiden siirtyminen päiväsaikaan vaatisi sijaisen järjestämistä, joka taas nähtiin erittäin kalliina järjestää. Tätä helpottamaan verkkokurssit ovatkin erinomainen apu. Toisena hyväksi koettuna koulutuksena toivottiin toimialakohtaista koulutusta, tästä selkeänä esimerkkinä voi-

daan mainita erilaiset synergia edut saman toimialan tarpeisiin. Kolmantena koulutuksena haluttiin yksikkökohtaista koulutusta. Tämä taas tuo etuja samanlaisten tarpeiden toteuttamiseen eri yksikköjen sisällä. Yksikköjen välisten tietosuojatarpeiden ero saattaa vaihdella huomattavasti.

3. Mitkä ovat tietosuoja-asetuksen osa-alueet, joissa lisätietoa tarvitaan?

   Koulutukset ovat selkeästi lisänneet henkilöstön tietoisuutta ja kiinnostusta tietosuoja-asetusta kohtaan. Lisätietoja koettiin tarvittavan eniten tietosuojapilvipalveluissa, tietosuoja-asetuksessa yleisesti sekä tietosuoja teknisessä ympäristötoimessa.

   Pilvipalveluissa sekä sähköposteissa välitettävä henkilötieto onkin erityisesti kunnassa suuren huomion kohteena. Tämä johtuu siitä, että esimerkiksi sosiaalipuolen kaikki henkilötietoa sisältävä tieto tulee lähettää ainoastaan salatussa sähköpostissa. Uuden tavan toimia omaksuminen jokapäiväisessä työssä saatettiin kokea haastavaksi, mutta koska kunnan henkilökunta haluaa luonnollisesti toimia asetuksen vaatimuksen mukaisesti, haluttiin varmistaa lisäkoulutuksella. Kyseinen asia tuli esille jo varsinaisten koulutusten aikana, eikä sitä enää toistettu kyselyn vastauksissa.

8.2 Saadut kokemukset

Tässä opinnäytetyössä on kuvattu Nurmijärven kunnassa toteutetun tietosuojaprojektin kulkua syksystä 2017 tietosuoja-asetuksen voimaantuloon saakka. Toimin projektityöntekijänä Nurmijärven kunnassa tietosuojaprojektissa. Projekti eteni hyvin suunnitellusti aikataulun mukaan ja asiat saatiin tehtyä asetuksen voimaanastumiseen mennessä.

Kunnan toiminta perustuu hyvin pitkälle erilaisten henkilötietojen käyttöön. Projektissa tuli ilmi, että asiat oli jo valmiiksi melko hyvin hoidettu ja useimmat järjestelmät olivat jo valmiiksi soveltuvia tietosuoja-asetukseen. Tietoturvaryhmän rinnalle kunta perusti tietosuojaryhmän.

Esimerkkinä hyvästä projektin aikana tehdystä investoinnista voidaan mainita Arc-tietosuojatyökaluohjelmiston hankinta. Arc-ohjelman käyttöönoton yhteydessä järjestettiin järjestelmäkoulutus sen käyttäjille. Koulutus mahdollisti jo tehtyjen Excel kaavioiden siirtämisen Arc-tietosuojanhallintaohjelmaan. Ohjelman perusteiden tunteminen mahdollisti yhteyskaavioiden luomisen, kerättyjen tietojen järjestykseen saattamisen. Samalla ohjelmalla voitiin piirtää kaavioita esimerkiksi seuraavista prosesseista:

- Asiakkaan tietojen oikaiseminen

- Asiakkaan tietojen poistaminen
- Asiakkaan tietojen toimittaminen pyynnöstä
- Henkilötietojen tietoturvaloukkauksesta ilmoittaminen
- Tarkastuspyyntöprosessi
- Tietojärjestelmäkaavio jne.

Kyseisessä ohjelmassa on myös hyvä piirtoeditori ja piirrosmerkit, joilla voi tehdä kattavia prosessikaavioita. Järjestelmä mahdollistaa myös kaavioiden linkittämisen muihin tietoihin. Nurmijärven kunnassa suunnitteilla ollut esimerkkikaavio Liite 5. Projektin aikana päätettiin, että Arc-ohjelma on jatkossa ainoa paikka, jossa tietoja ylläpidetään.

Yhteenvetona saaduista vastauksista voi päätellä, että henkilökunta suhtautuu positiivisesti kyselyyn. Alhaisen vastausmäärän voi osittain selittää, että esimerkiksi sivistyspuolella olevat henkilöt ovat opetusverkossa ja opettajilla ei ole välttämättä hallintoverkon koneita. Tämä tarkoittaa sitä, että eivät huomanneet vastata kyselyyn. Mikäli vastaavanlainen tutkimus tehtäisiin tulevaisuudessa, kannattaisi kysely julkaista myös EDU-opetusverkossa. Vastaavalla tavalla kannattaisi keskittyä tutkimuskysymyksiin niin, että valittaisiin muutama henkilö, joiden keskuudessa tehtäisiin haastattelukierros ja näin saadut vastaukset litteroitaisiin. Viitekehyksenä kannattaisi käyttää edelleen tietosuoja-asetusta ja siinä oleellisimmat artiklat.

KUUMA-kuntien tietosuojavastaavien tietosuojan hallintaryhmässä on keskusteltu yleisellä tasolla, kuinka muut kunnat tekivät tietosuojaprojektin. Kokouksissa käsiteltiin tietosuojaan liittyviä asioita. Kyseiset asiat olivat kunnille ja kaupungeille tärkeitä ratkaista, jonka vuoksi ryhmän toiminnasta tiedotettiin kaikkien kaupunkien ja kuntien johtoryhmiä. Yhdessä pohdittiin mm. seuraavia asioita:

- millainen tietosuojaseloste laaditaan
- rekisteröidyn informoiminen
- turvakiellot
- rekisteröidyn oikeudet
- tarkastuspyynnöt
- tietosuojapolitiikka
- koulutukset
- Arc-ohjelman käyttö.

KUUMA-yhteistyötä koordinoi Järvenpään tietosuojavastaava.

Mikäli nyt tehty tutkimus aloitettaisiin alusta, voisi parannusehdotuksena laittaa enemmän tarkentavia kysymyksiä, joiden avulla olisi voitu saada vastaaja pohtimaan asiaa syvällisemmin ja laajemmin. Näin tutkimustuloksista olisi voitu saada tehtyä enemmän päättelyä. Nyt saadun melko alhaisen vastaajamäärän perusteella pystytään päättelemään tuloksia pääosin ainoastaan prosentuaalisesti. Tutkimuskysymyksiä olisi ehkä voinut suunnitella tarkemmin raportoinnin näkökulmasta.

8.3 Jatkotoimenpiteet

Yhteenvetona saatujen vastausten perusteella lisäkoulutusta tarvitaan. Tämän mukaisesti jatkotoimenpiteenä tulee muodostaa kattava jatkokoulutussuunnitelma erityisesti talous- ja hallintopalvelut osastoille. Koulutukset tulee räätälöidä näiden osastojen erityistarpeiden mukaan. Koulutukset tulee toteuttaa pääsääntöisesti tallennettuna verkkokoulutuksena. Tämä koulutusmuoto mahdollistaa ajasta ja paikasta riippumattoman kouluttautumisen. Verkkokoulutus tukee kunnan henkilöstö resurssipulaa, jolloin henkilön ei tarvitse siirtyä toiseen koulutuspaikkaan eikä tarvita sijaisia. Verkkokoulutus mahdollistaa uuden henkilökunnan yksittäisopetuksen, jolloin uuden henkilön aloittaessa voidaan kouluttaa hänet välittömästi, eikä tarvitse odottaa, että useampi henkilö osallistuu koulutukseen. Nurmijärven kunnan tietosuojavastaavan kanssa on alustavasti keskusteltu kyseisen tietosuojakoulutuksen järjestämisestä vuoden 2020 alussa.

Henkilökunta on jo ohjeistettu tekemään vuosittain Navisec tietosuoja- ja tietoturvatestit. Toimenpide-ehdotuksena voidaan mainita, kehityskeskustelujen yhteydessä:

- muistutetaan henkilökuntaa testin tekemisestä
- Prima-henkilöstöhallinto-ohjelmaan lisättävä kenttä, joka tulee pakollisena täyttää, kun henkilö on suorittanut testin

Muiden koulutusten osalta voidaan suositella jatkamaan jo aloitettuja koulutuksia yhteistyössä KUUMA-kuntien kanssa, vuonna 2020. Ulkopuolisia konsultteja kannattaa käyttää varsinkin, jos tietosuoja-asetukseen tulee muutoksia. Tämän lisäksi tulee jatkaa, esimiehille suunnattujen tietoiskujen pitämistä säännöllisesti esimiespäivillä sekä kunnan sisäisissä intotilaisuuksissa. Näin varmistetaan henkilökunnan riittävä korkea tietosuojaosaamistaso.

Lähteet

Alamäki, A., Aunimo, L., Ketamo, H. & Parvinen, L. 2019. Interactive Machine Learning: Managing Information Richness in Highly Anonymized Conversation Data. Teoksessa L.M. Camarinha-Matos, H. Afsarmanesh & D. Antonelli (Toim.), *Collaborative Networks and Digital Transformation.* The Proceeding of 20th IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2019, s. 173-183

Alamäki, A. & Mäki, M. 2019. Data Privacy Concerns Throughout the Customer Journey and Different Service Industries. Teoksessa L.M., Camarinha-Matos, H., Afsarmanesh & D. Antonelli (Toim.), *Collaborative Networks and Digital Transformation*. The Proceeding of 20th IFIP WG 5.5 Working Conference on Virtual Enterprises, PRO-VE 2019, s. 516-526.

Andreasson, A., Riikonen J. & Ylipartanen, A. 2019. Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus. Tietosanoma Oy, Tallinna.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2013. Tietosuojavastaavan käsikirja. Tietosanoma Oy, Helsinki.

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2015. Tietosuojakäsikirja johdolle. Tietosanoma Oy, Tallinna.

Arter Oy 2019. Yhteyskaavio. Luettavissa: https://www.arter.fi/tuotteet/arc/. Luettu: 10.12.2018.

Calder A. 2018. It Governance Publishing. EU GDPR: A Pocket Guide.

Euroopan Unioni 2019. Luettavissa: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm. Luettu: 19.9.2019.

Euroopan unionin virallinen lehti, Euroopan Parlamentin ja Neuvoston asetus EU 2016/679. Tietosuoja-asetus. Luettavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI. Luettu: 2018.

Facebook. Yle uutiset 11.4.2018.

https://www.fsd.uta.fi/menetelmaopetus/ Luettu: 2.10.2019.

Heikkilä, T. Tilastollinen tutkimus. 2014. Edita Publishing Oy, Helsinki.

Hanninen, M., Laine, E., Rantala, K., Rusi, M., & Varhela, M. 2017. Henkilötietojen käsittely: EU-tietosuoja-asetuksen vaatimukset. Kauppakamari.

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. 2018. Uusi Tietosuojalainsäädäntö. Alma Talent, Helsinki.

Nurmijärven kunnan organisaatiokaavio 1.1.2019. Luettavissa: https://www.nurmijarvi.fi/filebank/21848-organisaatiokaavio_2019.pdf. Luettu: 10.7.2019.

Nurmijärven kunta tietosuojapolitiikka. Luettavissa https://www.nurmijarvi.fi/filebank/20012-Tietosuojapolitiikka_11_6_2018.pdf. Luettu: 10.7.2019.

Nurmijärven kunta 2018. Tietosuojaosio. Luettavissa: https://www.nurmijarvi.fi/kunta-tieto_ja_paatoksenteko/tietosuoja. Luettu: 25.5.2018.

https://opitietosuojaa.fi/fi/ Luettu: 12.9.2019.

Ojasalo, K., Moilanen, T. & Ritalahti J. 2015. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Sanoma Pro, Helsinki.

Palautetta GDPR:stä ja kansallisesta tietosuojalaista? Sähköpostiviesti www.asml.fi 11.9.2019.

Susanna I. 2018. Lakimaa Oy. Tietosuojapäivä Sipoo 23.4.2018 materiaali.

Taanila A. 17.4.2019. Akin menetelmäblogi, 10 korrelaatio ja merkitsevyys. Luettavissa: https://tilastoapu.wordpress.com/2011/11/01/10-korrelaatio-ja-sen-merkitsevyys/. Luettu: 3.10.2019.

Tekniikka & Talous. Karkimo, A. Luettavissa: https://www.tekniikkatalous.fi/uutiset/hollannin-tietosuojaviranomaiset-kehottavat-windows-10-kayttajia-olemaan-valppaina-tiedonkeruussa-epaillaan-gdpr-epakohtia/06299c74-2473-4528-9b3b-efbb5d949f3c. Luettu: 29.8.2019.

Tietosuojavaltuutetun toimisto 2019. Luettavissa: www.tietosuoja.fi Luettu: 10.7.2019.

Tietosuojalaki 1050/2018. Luettavissa: https://www.finlex.fi/fi/laki/alkup/2018/20181050. Luettu: 10.12.2018.

Tivi. Luettavissa: https://www.tekniikkatalous.fi/uutiset/verohallinnon-kirjesekaannuksen-syy-selvisi-pyydamme-tietosuojaloukkausta-anteeksi/3fa32b5d-3053-4900-9590-9fd324dfcc48. Luettu: 13.8.2019.
Valtiovarainministeriö 2018. Taistoharjoitus 2018. Luettavissa: www.vrk.fi/taisto.

Vilkka H. 2015. Tutki ja kehitä. PS-kustannus, Jyväskylä.

Webropol 3.0 ohjelmasta tilastoanalyysin ohjeet.

Liitteet

Liite1. Kysely

Tietosuoja-asetus Nurmijärven kunta

Hyvä Nurmijärven kunnan työntekijä!

Euroopan tietosuoja-asetus vaikuttaa kaikkien Nurmijärven kunnan työntekijöiden henkilötietojen käsittelyyn.

Nurmijärven kunnan hallintopalvelut yhdessä eri kunnan toimialojen kanssa suunnitteli ja toteutti eri muotoisia koulutuksia tietosuoja-asetuksen voimaantullessa 25.5.2018 ennen ja jälkeen.

Tämän kyselyn tarkoituksena on kartoittaa ne lisäkoulutustarpeet, joiden avulla voimme auttaa sinua jokapäiväisissä tietosuoja-asetuksen vaatimissa tilanteissa.

Jotta tulevat koulutukset ovat mahdollisimman hyvin arkitilanteita tukevia antamasi palaute on ensiarvoisen tärkeää.

Kyselyn tulosten perusteella tullaan järjestämään tietosuoja-asetukseen liittyviä lisäkoulutuksia alkuvuodesta 2020.

Vastaathan kyselyyn viimeistään 20.9.2019 mennessä.

Kiitos vastauksistasi!

1. Toimialue *

Toimiala

Valitse ▼

Yksikkö

Valitse ▼

.

2. Sukupuoli *

- ○ Nainen
- ○ Mies

3. Ikä *

Valitse ▼

4. Osallistumiseni jo aiemmin järjestettyihin koulutuksiin? *

- ☐ Yleisinfot
- ☐ Toimialakohtaiset infot
- ☐ Kuuma-kuntien yhteisinfo videolähetykset
- ☐ Navisecin EU-GDPR ja tietosuojakolutus

5. Käsittelenkö työssäni henkilötietoja / tietosuojaan liittyviä asioita? *

- ☐ Kyllä
- ☐ Ei
- ☐ Kyllä, arkaluontoisia tai erityisiä henkilötietoja

6. Tarvitsenko työssäni lisäkoulutusta liittyen tietosuoja-asetukseen? *

- ○ Kyllä
- ○ Ei

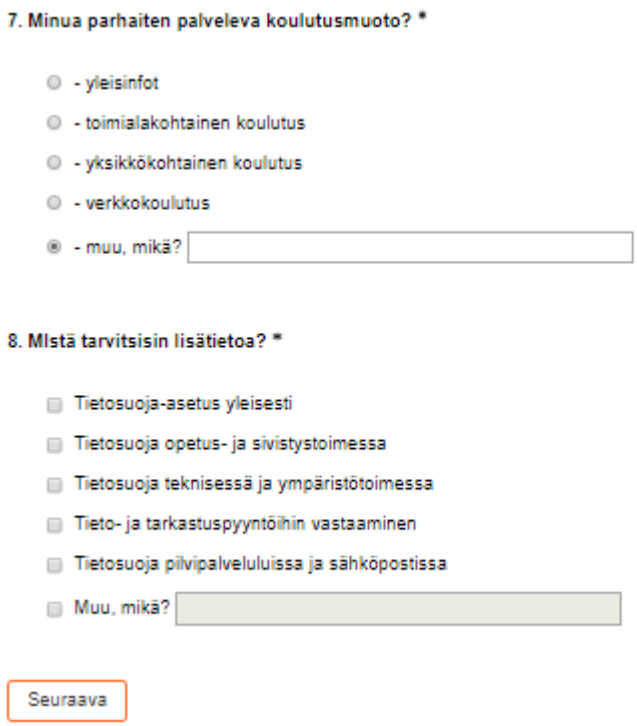
7. Minua parhaiten palveleva koulutusmuoto? *

- ○ - yleisinfot
- ○ - toimialakohtainen koulutus
- ○ - yksikkökohtainen koulutus
- ○ - verkkokoulutus
- ◉ - muu, mikä?

8. Mistä tarvitsisin lisätietoa? *

- ☐ Tietosuoja-asetus yleisesti
- ☐ Tietosuoja opetus- ja sivistystoimessa
- ☐ Tietosuoja teknisessä ja ympäristötoimessa
- ☐ Tieto- ja tarkastuspyyntöihin vastaaminen
- ☐ Tietosuoja pilvipalveluluissa ja sähköpostissa
- ☐ Muu, mikä?

Seuraava



Liite 2. Aloituskysely

Kunnassa on meneillään henkilörekisterilain ja EU:n tietosuoja-asetuksen edellyttämien rekisteriselosteiden/tietosuojaselosteiden kerääminen keskitetysti yhteen paikkaan. Seloste tulisi olla tehtynä kaikista järjestelmistä, joissa käsitellään henkilötietoja. Henkilötiedon käsite on EU:n tietosuoja-asetuksessa laaja, ja se pitää sisällään kaiken mikä sisältää tietoa tunnistettavasta henkilöstä (esim. kiinteistötunnus, puhelinnumero...). Onko teidän järjestelmästänne, järjestelmän nimi olemassa rekisteriselostetta? Jos on, toimittaisitteko sen minulle sähköpostitse, niin kerään kaikki tiedot yhteen.

Jos selostetta ei vielä ole tehtynä, liitteenä on valmis pohja sen laatimiseen ja laatimisohje. Lisätietoa löytyy mm. Myllystä ja tietosuojavaltuutetun sivuilta:

http://nursp3/sites/mylly/tietotekniikka/_layouts/15/start.aspx#/SitePages/Tietoturva.aspx

http://www.tietosuoja.fi/fi/

Tämä viesti lähetetään kaikkien sellaisten järjestelmien pääkäyttäjille ja omistajille, joissa mahdollisesti on henkilötietoja. Jatkossa selosteet on tarkoitus laittaa näkyville kunnan www-sivuille, jossa kuntalaisilla on mahdollisuus tutustua niihin. Toivomme selosteita syyskuun loppuun mennessä, tai jos se tulee liian pikaisesti, niin ilmoitatteko, niin sovitaan jatkosta! Selosteen laatimiseen voi kysellä neuvoja asianhallintapäällikkö Hanna Elomaalta, p. 040 317 2002.

Terveisin,

Tomi Ahonen

Projektityöntekijä
Nurmijärven kunta
PL 37 (Keskustie 2a), 01901 Nurmijärvi
puh. 040 317 4012
tomi.ahonen@nurmijarvi.fi

Liite 3. Rekisteri/järjestelmäkohtainen tarkastuslista

Rekisteri/järjestelmäkohtainen tarkastuslista
-kysymyksiä kartoitustaulukon ulkopuolelta
-tietojärjestelmä voi olla rekisteri, osa rekisteriä tai sisältää useampia rekistereitä

Rekisterin nimi: Kirjoita tekstiä napsauttamalla tätä.
Käytetyt järjestelmät: Kirjoita tekstiä napsauttamalla tätä.
Päivämäärä: Kirjoita päivämäärä napsauttamalla tätä.
Rekisterikohtaiset tiedot
Rekisterikohtaiset tiedot

Onko varmistettu, että rekisteröidyistä kerätään (ja tallennetaan) vain se määrä tietoa, mikä on rekisterin käyttötarkoituksen ja em. laillisen perusteen kannalta tarpeellista? ☐ Kyllä ☐Ei
Onko rekisterin käyttöoikeudet määritelty niin, että tietoja voivat käsitellä (tai edes nähdä) vain ne, jotka siihen rekisterin laillisen käyttötarkoituksen vuoksi ovat oikeutettuja? ☐Kyllä ☐Ei
Onko käyttöoikeuksien myöntämisperiaatteet kuvattu/dokumentoitu? ☐ Kyllä ☐Ei
Onko tunnistettu ja kuvattu tietojen lähteet, että niiden käyttö ja mahdollinen luovutus muille prosesseille tai ulkopuolisille? ☐Kyllä ☐Ei

Onko rekisteriin liittyvistä tietovirroista tehty kirjallinen kuvaus? ☐Kyllä ☐Ei

Jos rekisteri on myös ulkopuolisten *henkilötietojen käsittelijöiden* käytössä (esim. alihankkijoiden), onko varmistettu, että hekin noudattavat käsittelystä annettuja ohjeita? (ks. myös kohta Sopimukset) ☐Kyllä ☐Ei

Onko määritelty ja ohjeistettu menettely, jolla varmistetaan rekisterissä olevien tietojen oikeellisuus ja ajantasaisuus? ☐Kyllä ☐Ei

Onko käytössä menettely tietojen poistamiseksi mahdollisimman pian sen jälkeen, kun niiden pitämiseen ei enää ole oikeutta/tarvetta? (Vrt. rekisterin käyttötarkoitus ja tietojen säilyttämisen tai arkistoimisen säännöt.) ☐Kyllä ☐Ei

Onko tietojen poistamistarpeita varten huomioitu, miten tiedot poistetaan myös varmuuskopioilta? ☐Kyllä ☐Ei

Onko määritelty ja ohjeistettu tapa, jolla rekisteröity voi tarkistaa ja tarvittaessa oikaista häntä koskevat tiedot? ☐Kyllä ☐Ei

Tietojärjestelmän tiedot

Onko järjestelmän tietosisältö kauttaaltaan dokumentoitu (riittävällä tarkkuudella)? ☐Kyllä ☐Ei

Saadaanko järjestelmästä kootuksi (ilman kohtuutonta vaivaa tai lisäkustannuksia) kaikki yksittäistä rekisteröityä koskevat tiedot, jotta hän voi esimerkiksi tarkistaa niiden oikeellisuuden? ☐Kyllä ☐Ei

Onko järjestelmätoimittajalta saatu kattava tekninen dokumentaatio järjestelmän käyttötarkoituksesta, sen mukaisesta käyttötavasta sekä teknisestä toteutustavasta yms.? ☐Kyllä ☐Ei

Sisältääkö toimittajalta saatu dokumentaatio menettelyistä, joilla järjestelmän riittävä tietoturvallisuus ja tietosuojan toteutuminen on varmistettu? ☐Kyllä ☐Ei

Onko suojauksissa huomioitu mahdolliset erityistarpeet alle 16-vuotiaita koskevien tietojen suojaamisesta? ☐Kyllä ☐Ei

Voidaanko järjestelmällä toteuttaa henkilötietojen anonymisointi (tai pseudonymisointi), jos se riskiarvion perusteella on tarpeen? ☐Kyllä ☐Ei

Onko järjestelmän tiedot ja tietoliikenne (riittävästi) salattu? ☐Kyllä ☐Ei

Onko kaikista järjestelmän käyttäjistä (ml. admin-käyttäjät) ja heidän käyttöoikeuksistaan saatavissa ajantasainen erittely? ☐Kyllä ☐Ei

Ovatko kaikki käyttäjätunnukset henkilökohtaisia? ☐Kyllä ☐Ei

Onko järjestelmän varmuuskopiointisuunnitelma tehty ja dokumentoitu (ja rekisterinpitäjän käytettävissä) ☐Kyllä ☐Ei

Onko järjestelmästä saatavissa lokitiedot? ☐Kyllä ☐Ei

Lokitetaanko järjestelmässä henkilötietojen käsittelytoimet? ☐Kyllä ☐Ei

Lokitetaanko järjestelmässä admin-käyttäjien toimet? ☐Kyllä ☐Ei

Onko lokien säilytys, suojaus ja tarkastelukäytännöt määritelty/dokumentoitu? ☐Kyllä ☐Ei

Muulla kuin järjestelmissä sijaitsevat tiedot

Onko selvitetty, onko henkilötietoja muualla kuin tehtävään liittyvissä tietojärjestelmissä (jos ei muualla, ohita seuraavat)? ☐Kyllä ☐Ei

Onko selkeät periaatteet järjestelmien ulkopuolisten henkilötietojen käsittelyyn ja säilyttämiseen? ☐Kyllä ☐Ei

Verkkolevytiedot ☐Kyllä ☐Ei

Paperiasiakirjat ☐Kyllä ☐Ei

Asiakaspalvelutilanteet ☐Kyllä ☐Ei

Muu, mikä? Kirjoita tekstiä napsauttamalla tätä. ☐Kyllä ☐Ei

Tietosuojaseloste

Onko seloste julkaistu niin, että se on rekisteröityjen helposti saatavilla? ☐Kyllä ☐Ei

Sisältääkö seloste rekisterinpitäjän, rekisteristä (ja samalla selosteesta) vastaavan henkilön, tietosuojavastaavan ja muut tarpeelliset yhteystiedot? ☐Kyllä ☐Ei

Ilmaiseeko seloste tietojen käsittelyn tarkoituksen ja oikeusperusteet? ☐Kyllä ☐Ei

Sisältääkö seloste kuvauksen rekisteröityjen ryhmästä/ryhmistä ja vastaavista tietoryhmistä? ☐Kyllä ☐Ei

Ilmoittaako seloste tietojen käyttäjät ja vastaanottajatahot, joille tietoja (mahdollisesti) luovutetaan? ☐Kyllä ☐Ei

Jos tietoja luovutetaan EU:n ulkopuolelle, ilmaiseeko seloste, miten tähän erityisesti kohdistuvat EU:n suojaus ym. vaatimukset tulevat huomioiduksi ja toteutetuksi? ☐Kyllä ☐Ei

Ilmoitetaanko tietojen säilytysaika tai säilytysajan määrittelykriteerit? ☐Kyllä ☐Ei

Ilmoitetaanko rekisterin suojaustapa tai suojauksessa noudatettavat periaatteet? ☐Kyllä ☐Ei

Henkilötietojen käsittelysopimukset

Onko tunnistettu ja määritelty, miten ulkoiseen käsittelyyn liittyvät vaatimukset sopimuksellisesti pitää (vähintään) toteuttaa? ☐Kyllä ☐Ei

Onko käsittelijöille toimitettu riittävät (rekisterinpitäjän hyväksymät) ohjeet? ☐Kyllä ☐Ei

Sisältyvätkö tietosuojaa ja tietoturvaa koskevat seikat palvelu tai alihankintasopimukseen (sopimuslausekkeina tai esim. liitteenä)? ☐Kyllä ☐Ei

Onko toimeksiannossa/sopimuksessa määritelty (ulkopuolisen) henkilötietojen käsittelyn tarkoitus, tavoitteet ja rajoitukset? ☐Kyllä ☐Ei

Onko sopimuskumppani nimennyt osaltaan tietosuojavastaavan tai muun yhteyshenkilön, jonka kanssa tietosuoja-asiat ensisijaisesti käsitellään? ☐Kyllä ☐Ei

Huolehtiiko sopimuskumppani henkilöstönsä tietosuojatietoisuudesta ja osaamisesta riittävästi ja jatkuvasti? ☐Kyllä ☐Ei

Tietosuojasuositukset

O365 Sähköpostiviestintä

NURMIJÄRVI

24.10.2018

1 Tausta

KUUMA-seudun tietosuojan hallintaryhmä on pyrkinyt muodostamaan yhteisen näkökulman sähköpostin käyttämisestä, jota voidaan hyödyntää kaikissa Keski-Uudenmaan kunnissa. Ryhmä arvioi sähköpostin käyttöön liittyviä riskejä yhteistyössä, jotta ohjeistuksen pohjalle saadaan yhteinen näkemys siitä, miten henkilötietoja käsitellään harkitusti.[1]

2 Riskien arviointi: henkilötiedot sähköpostissa

Sähköpostin käyttöön liittyvät tietosuojariskit ovat usein inhimillisiä virheitä:

Lähettäjä voi lähettää tai välittää viestin väärälle ihmiselle tai vastaanottoryhmälle, esim. näppäilyvirhe tai samannimiset henkilöt (Outlookiin voi asettaa viivästyksen, joka mahdollistaa viestin poiston).
Viestin välittäjä ei huomaa, että pitkässä ketjussa on jossain kohdassa henkilötietoja ja välittää sen eteenpäin.
Sähköpostit säilyvät sähköpostilaatikoissa, mikäli niitä ei aktiivisesti poisteta (saapuneet ja lähetetyt).
Vastaanottaja voi lukea sähköpostin muiltakin laitteilta kuin työasemaltaan, esim. mobiililaitteesta missä tahansa tilassa tai tilanteessa, jolloin viestin voi nähdä muutkin henkilöt.
Sähköpostin saapumisilmoitus voi tulla vastaanottajan ruudulle, esim. tilanteessa, kun henkilöllä on jaettu näkymä verkossa tai ruudulla (esitys).
Sähköpostiliitteiden avaaminen, tallentaa liitteet laitteelle, jossa ne avataan.
Sähköpostiin murtautuminen, esim. tietojen kalastelun yhteydessä sähköpostitunnusten ja salasanojen luovuttaminen, voi altistaa koko sähköpostin sisällön vaaraan. Riski on pienempi, jos sähköpostissasi ei ole arkaluontoisia tietoja.
Tietokone on lukitsematta, kun käyttäjä ei ole koneella.
Yhteissähköpostiosoitteet ja yhteiset puhelimet: riskinä että tieto päätyy vahingossa väärälle henkilölle, myös väärinkäytön mahdollisuus. Riskiä pienentää se, että sähköpostinkäytöstä on sovittu.

3 Erityisten henkilötietojen luovuttaminen sähköpostitse on kielletty

[1] Tietosuoja-asetus artikla 32 ja artikla 25

Erityiset (arkaluontoiset) henkilötiedot määritellään tietosuojalainsäädännössä, ja niiden käsittely on lähtökohtaisesti kiellettyä. Mikäli oikeus näiden käsittelyyn on, on niitä erityisesti suojattava päätymästä vääriin käsiin. Lisätietoja: https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely
Lisäksi sähköpostiviestinnässä tuleen huomioida salassa pidettävä tieto (Julkl 24.1).

Salassapitosäännökset ja henkilötietolain mukainen suojaamisvelvoite eivät mahdollista salassa pidettävien päätös- ja muiden tietojen lähettämistä tavallisessa suojaamattomassa sähköpostissa siitäkään huolimatta, että siihen olisi henkilön suostumus tai asiakas itse tätä haluaisi.[2]

Salaista tai arkaluonteista henkilötietoa ei saa käsitellä suojaamattomassa sähköpostissa. Tämä koskee sekä kunnan sisäistä sähköpostia, että kunnasta ulos lähetettävää sähköpostia. Älä lähetä sähköpostitse myöskään henkilötunnuksia. Muista, että suuret henkilötietomäärät, kuten listaukset, aiheuttavat suuremman riskin.

Salaiset ja arkaluonteiset tiedot pyritään käsittelemään niissä järjestelmissä, joissa niiden muodostaminenkin tapahtuu (operatiiviset järjestelmät) mahdollisia viestikanavia/-tapoja käyttäen. **Mikäli sähköposti on kuitenkin ainoa tapa välittää tietoja, henkilötietojen käsittelyn riskiä pienennetään**. Henkilötiedot tulee pseudonymisoida eli käyttää esimerkiksi potilastietojärjestelmästä saatavaa potilasnumeroa, asianhallinnasta saatavaa diaarinumeroa, oppilasnumeroa tai vastaavaa tunnusta, jolloin tunnistettavaa henkilötietoa ei tarvitse lähettää. Näin toimimalla henkilötietoja ei jää pilvipalveluun eikä lähettäjän tai vastaanottajan sähköpostilaatikoihin.

4 Suojatun sähköpostin (turvapostin) käyttäminen

Tietosuojavaltuutetun kannanoton mukaan tietojen suojaamisvelvollisuudesta ja salassapitovelvollisuudesta seuraa, että terveydenhuollon viranomainen voi lähettää asiakkaalle viestejä vain, mikäli hänellä on käytössään sähköposti, jossa on riittävän vahva salaus ja osapuolet voidaan tunnistaa.[3] **KUUMA-seudun tietosuojan hallintaryhmä suosittaa**, että asiakkaan kanssa ei hoideta arkaluontoisia tai salaisia tietoja sisältävää viestintää edes suojatulla sähköpostilla, koska vastaanottajan henkilöllisyydestä ei voida varmistua. Riski on myös siinä, että osoite kirjoitetaan väärin.

Tietosuojasuositukset
O365 SÄHKÖPOSTIVIESTINTÄ

Liite 1

Suojatun sähköpostin käyttäminen voi olla perusteltua esimerkiksi silloin, kun on kyse asioinnista jonkun organisaation tai toisen viranomaisen kanssa. Tällöin sähköpostiosoitteen vastaanottajan voidaan olettaa varmasti olevan organisaation tai viranomaisen edustaja.

Jos suojattua sähköpostia käytetään henkilötietojen lähettämiseen muuhun kuin viranomaisen sähköpostiin tulee käyttää varmaa tunnistuskeinoa (PIN-koodi) siihen, että henkilö itse todella on sähköpostia lukemassa.

Organisaatiossa voidaan käyttää myös turvapostipalvelinta, jolla organisaation ulkopuolinen yksityishenkilö tai viranomainen voi lähettää suojattua sähköpostia organisaatioon, esim. kirjaamon sähköpostiin.

---

[2] https://tietosuoja.fi/rekisteroidyn-suostumus
[3] Tietosuojavaltuutetun kannanotto Dnro 423/49/2009

5 Asiakkaan lähettämät sähköpostit ja niihin vastaaminen

Joskus kuntalaiset lähettävät asiansa hoidettavaksi sähköpostiviestillä. Viesti saattaa sisältää henkilötietoa tai jopa arkaluonteista henkilötietoa (esim. sosiaali- ja terveydenhuollon tietoja).

On hyvä muistaa, että **sähköpostin lähettäjästä ei voida olla täysin varmoja**. Sähköposti on helppo luoda kenen tahansa nimellä. Tämän vuoksi aina, kun sähköpostiin vastataan, tulisi vastata siten, että voidaan olettaa kenen tahansa lukevan saapuneen tiedon. Vastauksen tulee olla sellainen, ettei vastaanottaja voi saada viestillä mitään lisätietoja tai varmistuksia kenenkään henkilön yksityisasioista.

Sähköpostitse tulee tänä päivänä erilaisia **huijaus- ja tietojenkalasteluviestejä**, joita ei kannata avata eikä varsinkaan viesteihin mahdollisesti sisältyviä linkkejä. Viestit on syytä hävittää välittömästi ilman avaamista, sillä viestit ovat rikollisten lähettämiä ja ne voivat sisältää viruksia. Rikollisten tarkoituksena on hyödyntää saatuja tietoja ansaitsemistarkoituksissa.

Viranomaisilla on kuitenkin aina neuvontavelvollisuus, jonka vuoksi sähköpostin lähettäjää tulisi auttaa hoitamaan asiansa. Suojaamattoman sähköpostiyhteyden kautta voidaan kysyä yleistä neuvontaa esimerkiksi siitä, millä edellytyksillä ja miten jotain etuutta tai palvelua voi hakea tai miten voi omaa asiaansa hoitaa. Tällaiseen yleiseen tiedusteluun voi myös vastata sähköpostitse.

Jos henkilö on jo lähettänyt arkaluonteista henkilötietoa tai muuta salaista tietoa viestissään, tulee lähettäjän viestiin vastatessa poistaa tiedot viestistä ennen lähetystä. Viranomaisen on myös kerrottava, ettei asiakkaan ole suositeltavaa lähettää sähköpostin kautta arkaluonteisia henkilötietoja. Muidenkin henkilötietojen osalta tulee aina olla vaihtoehtoinen tietojen antamisen mahdollisuus. Tästä tulee **informoida kuntalaista**. Jos palvelun järjestäjä ilmoittaa www-sivuillaan organisaationsa sähköpostiosoitteen, sen tulee informoida myös siitä, mihin sähköpostia voidaan käyttää ja sen käyttöön liittyvistä tietoturvaongelmista – esim. että kyse on avoimesta sähköpostista, jossa viestin lähettäjää ei voida tunnistaa eikä viestiä salata. Yleensä sähköpostitse tapahtuvat yhteydenotot ovat suositeltavaa ohjata nimenomaan organisaation sähköpostiosoitteeseen eikä yksittäisen työntekijän sähköpostiin.

6 Viestin väärä vastaanottaja

Jos viranomainen saa sähköpostin, joka ei ole tarkoitettu kyseiselle vastaanottajalle, tulee viesti ohjata oikealle henkilölle ja/tai informoida viestin vastaanottajaa asiasta. Viestin/asian voi ohjata myös esimerkiksi esimiehen tai kirjaamon selvitettäväksi organisaation ohjeistuksen mukaisesti, jos ei ole varma siitä, miten tulisi toimia. Viranomainen on vaitiolovelvollinen eikä siten saa tietoa käyttää hyväkseen. Saapunut viesti ja edelleen lähetetty viesti tulee hävittää asianmukaisesti. Ilmoita aina, jos huomaat virheen tapahtuneen.

Jos viranomainen huomaa lähettäneensä viestiä väärälle henkilölle, ilmoitetaan asiasta välittömästi väärälle henkilölle ja pyydetään hävittämään viesti. Viestissä voi pyytää tietojen hävittämistä ja muistuttaa mahdollisesta luottamuksellisuudesta. Jos olet lähettänyt vahingossa henkilötietoja, tietosuojavastaava auttaa arvioimaan, tarvitseeko ryhtyä tietoturvaloukkauksesta ilmoittamiseen.

7 Viestien välittäminen ja säilyttäminen

Kun viestiä välitetään eteenpäin, varmistetaan koko viestiketjun sisältö. Varmistetaan sisältääkö viesti sellaista asiaa, jota ei saa kaikille vastaanottajalle lähettää. Esimerkiksi nimiä tai asioita voi poistaa uudelleen lähetettävästä viestistä.

Lähetyt viestit -kansiostakin tulee poistaa viestit, jotka sisältävät henkilötietoja.

Sähköposti ei ole henkilötietojen säilytyspaikka. Sähköpostissa voidaan käsitellä viestiä, niin kauan kuin se on asian hoitamisen kannalta merkityksellistä. Joissakin tapauksissa sähköpostiviestin voi tallentaa esim. asianhallintajärjestelmään.

Harkitse piilokopion käyttämistä lähettäessäsi sähköpostia suuremmalle ryhmälle, etenkin kunnan ulkopuolisille vastaanottajille, tai kun et halua vastaanottajien näkevän toistensa osoitteita.

SÄHKÖPOSTIOSOITETTA EI SAA KÄYTTÄÄ YKSITYISASIOIDEN HOITAMISEEN.
SÄHKÖPOSTIN SALASANAN LUOVUTTAMINEN ON KIELLETTYÄ!

Tietosuojasuositukset
O365 SÄHKÖPOSTIVIESTINTÄ

Liite 1

Vinkkejä sähköpostiviestiin reagoimiseksi

<u>Mitä kysyjä haluaa viestillään?</u>
Koskeeko asia asiakkaan omia tietoja?
Onko kyseessä hoitoon/asiakkuuteen vaikuttavia lisätietoja?
Haluaako henkilö tehdä valituksen?
Pyytääkö henkilö omia tietojaan?
Muuta?

Tarvittaessa ohjaa viesti kaupungin sisällä oikealle henkilölle tai esimiehellesi, jos et tiedä mitä asia koskee tai miten toimisit asian suhteen.
Vältä asian leviämistä sivullisille.
Epäselvissä tapauksissa neuvoa voi kysyä tietosuojavastaavalta.

<u>Lähetä viestiin yleisluonteinen vastaus, jos haluat informoida miten henkilön tulisi asiaa hoitaa</u>
Viestissä ei saa olla mukana asiakkaan lähettämiä arkaluonteisia tietoja!!
Viesti ei saa paljastaa henkilön asiakkuutta sosiaalihuoltoon tai terveyspalveluihin!
Arkaluonteiset asiat pyydetään toimittamaan joko paperilla tai postitse
Informoi asiakasta sähköpostin suojaamattomuudesta arkaluonteisten asioiden suhteen

<u>Jos asia vaatii välitöntä reagointia, todenna henkilöllisyys</u>
sähköpostilla ei voi todistaa henkilöllisyyttä
pelkkä nimi viestissä ei riitä henkilön tunnistamiseen
soster: varmista henkilöllisyys ennen kuin käytät asiakas/potilastietoja

Soita henkilölle ja toimi kuten on ohjeistettu puhelimessa tunnistamiseen ja ole tässäkin tarkkana
Jos viestissä ei ole numeroa: pyydä puhelinnumeroa, johon voi soittaa tai anna puhelinnumero, johon voi soittaa vastaamalla sähköpostiin (yleisluontoisella vastauksella), ja informoi syy

Jos asiakas/potilas häiriköi tai uhkailee sähköpostin välityksellä

Ilmoita esimiehelle (esimiehellä on perusteet tietojen käsittelylle)
Tee ilmoitus organisaatiossa sovitulla tavalla (poikkeamailmoitus 4Ks-järjestelmässä)
Mahdolliset muut toimenpiteet tapauskohtaisesti

Hävitä henkilötietoja sisältävät viestit sähköpostista!
Sähköpostissa ei saa säilyttää arkaluonteisia henkilötietoja.
Henkilötiedot tulee poistaa, kun asian käsittelyn suhteen ei viestejä enää tarvita.
Oikeusturvan takaamiseksi tietojen tallentaminen on mahdollista asianhallintajärjestelmässä.

Kun epäilet tietojen kalastelua,
vertaa lähettävää osoitetta ja linkin osoitetta.
älä lähetä käyttäjätunnuksiasi ja salasanojasi.
jos lähetät, vaihda välittömästi salasanasi.
ilmoita asiasta organisaatiossa sovitulla tavalla (tietotekniikka/helpdesk)

Liite 5.

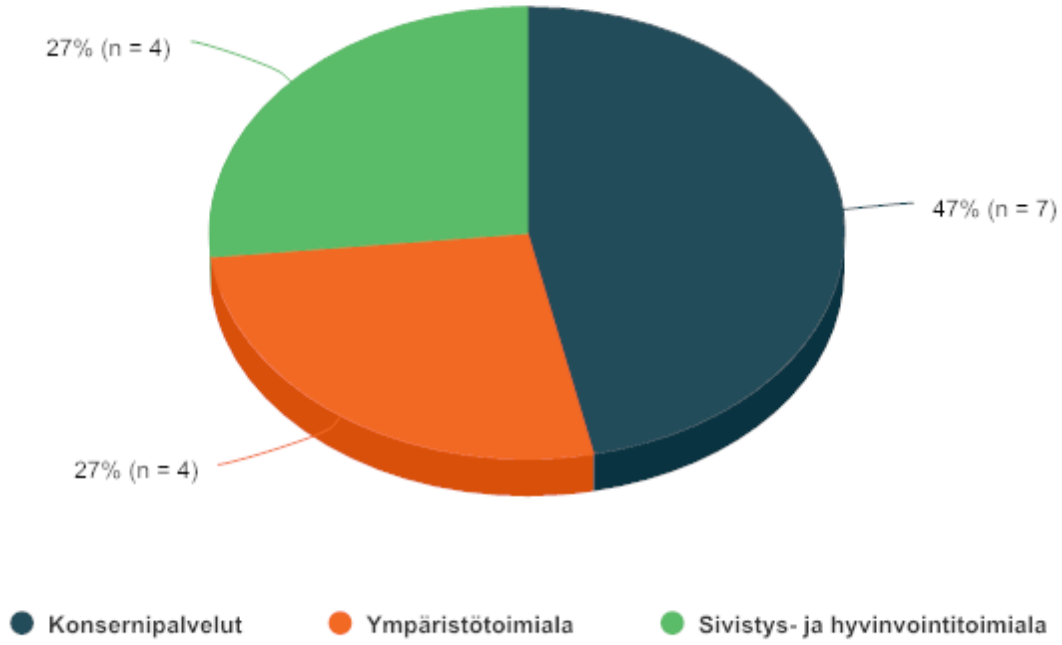
Perusraportti

Tietosuoja-asetus Nurmijärven kunta

Vastaajien kokonaismäärä: 15

1. Toimialue

Vastaajien määrä: 15

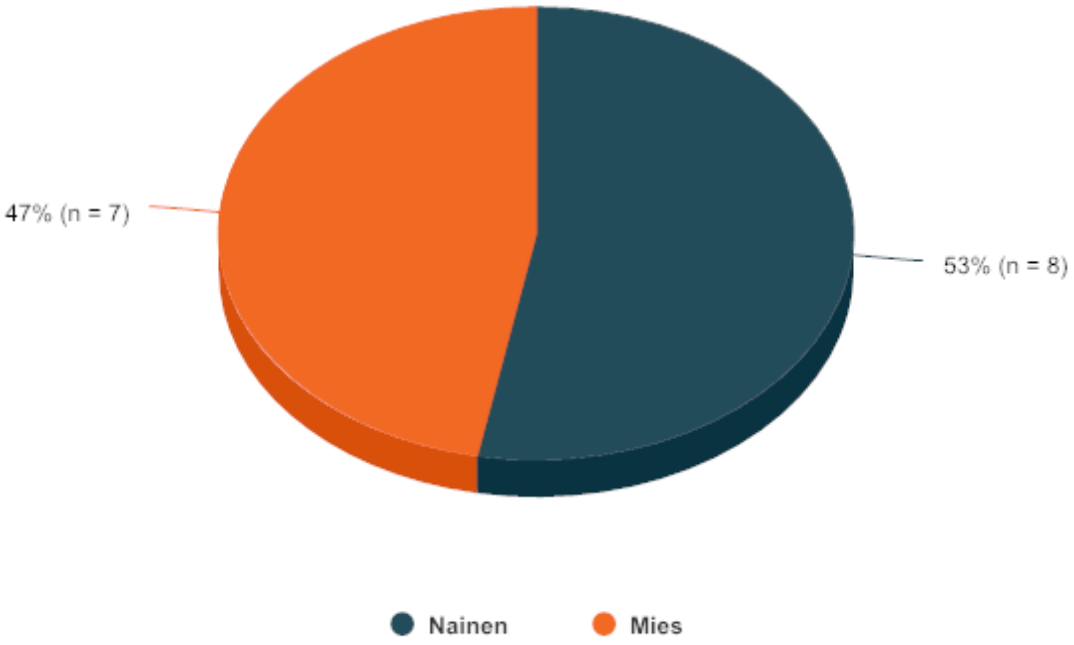


	n	Prosentti	n	Prosentti
Konsernipalvelut	7	46,67%		
Elinvoima- ja kuntakehityspalvelut			0	0%
Viestintä- ja markkinointipalvelut			0	0%
Talouspalvelut			3	42,86%
Hallintopalvelut			3	42,86%
Henkilöstöpalvelut			0	0%
Aleksia-liikelaitos			1	14,29%
TYHJÄ			0	0%
Ympäristötoimiala	4	26,67%		
Hallinto- ja talouspalvelut			0	0%

Maankäyttö ja yleiskaavoitus			1	25%
Rakennusvalvonta			0	0%
Tekninen keskus			1	25%
Asemakaavoitus ja tekninen suunnittelu			1	25%
Tilakeskus			1	25%
Nurmijärven Vesi -liikelaitos			0	0%
Sivistys- ja hyvinvointitoimiala	4	26,67%		
Hallinto- ja talouspalvelut			0	0%
Hyvinvointipalvelut			1	25%
Koulutuspalvelut			0	0%
Varhaiskasvatuspalvelut			1	25%
Kirjasto- ja kulttuuripalvelut			1	25%
Nuorisopalvelut			1	25%
Liikuntapalvelut			0	0%
Yhteensä	15	100%	15	100%

2. Sukupuoli

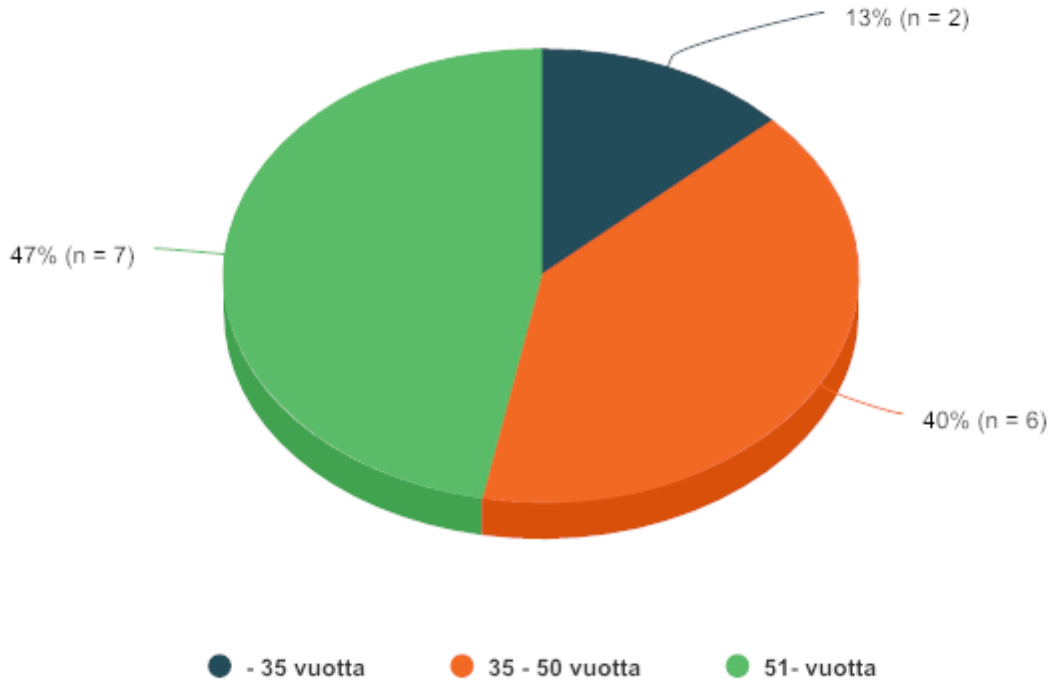
Vastaajien määrä: 15



	n	Prosentti
Nainen	8	53,33%
Mies	7	46,67%

3. Ikä

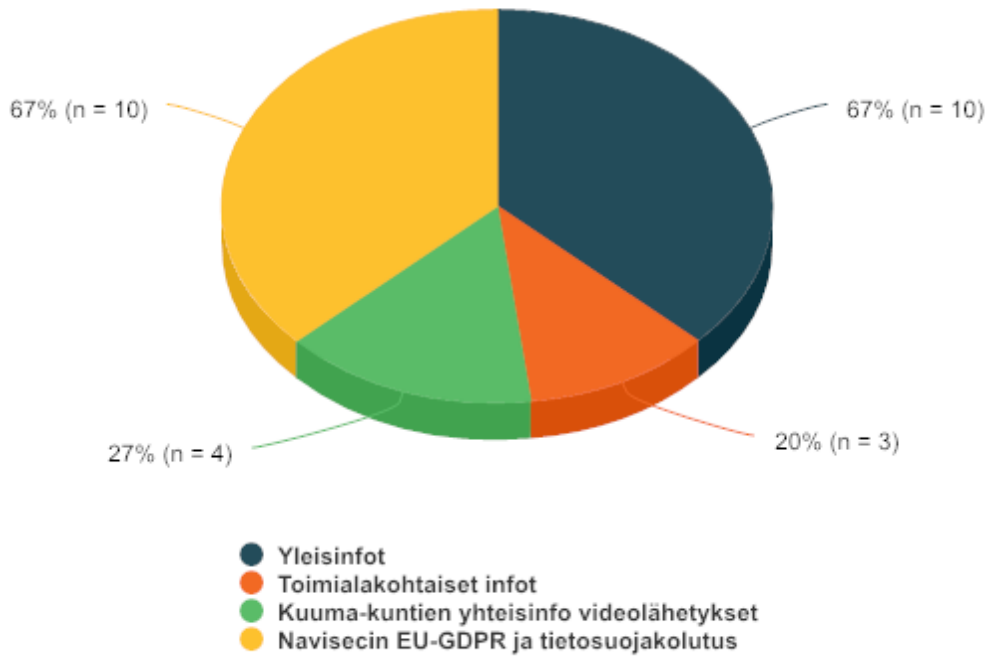
Vastaajien määrä: 15



	n	Prosentti
- 35 vuotta	2	13,33%
35 - 50 vuotta	6	40%
51- vuotta	7	46,67%

4. Osallistumiseni jo aiemmin järjestettyihin koulutuksiin?

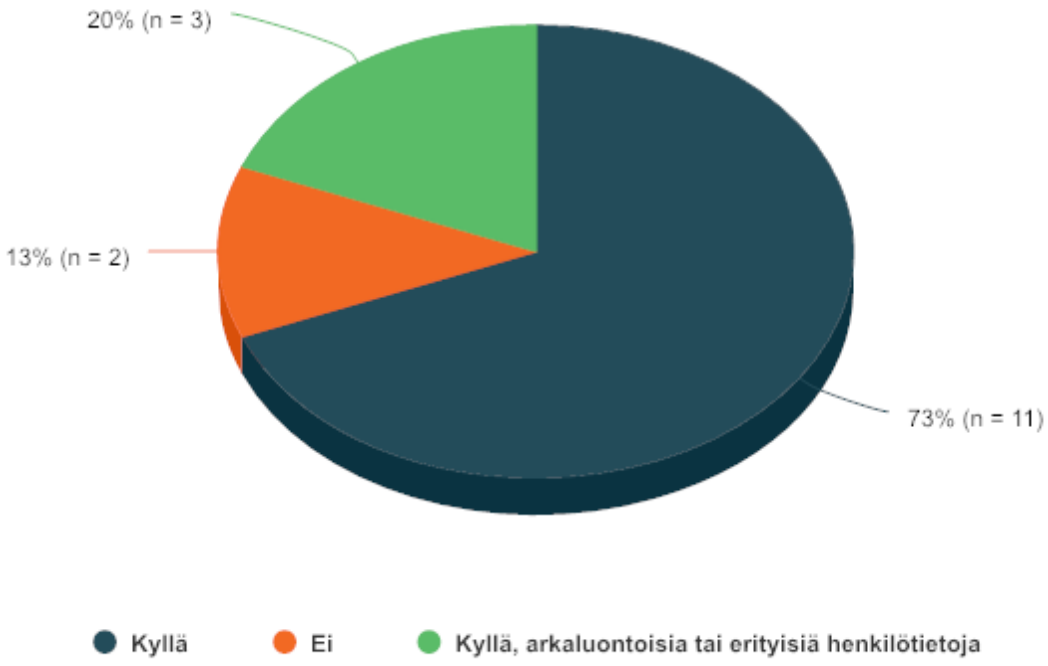
Vastaajien määrä: 15, valittujen vastausten lukumäärä: 27



	n	Prosentti
Yleisinfot	10	66,67%
Toimialakohtaiset infot	3	20%
Kuuma-kuntien yhteisinfo videolähetykset	4	26,67%
Navisecin EU-GDPR ja tietosuojakolutus	10	66,67%

5. Käsittelenkö työssäni henkilötietoja / tietosuojaan liittyviä asioita?

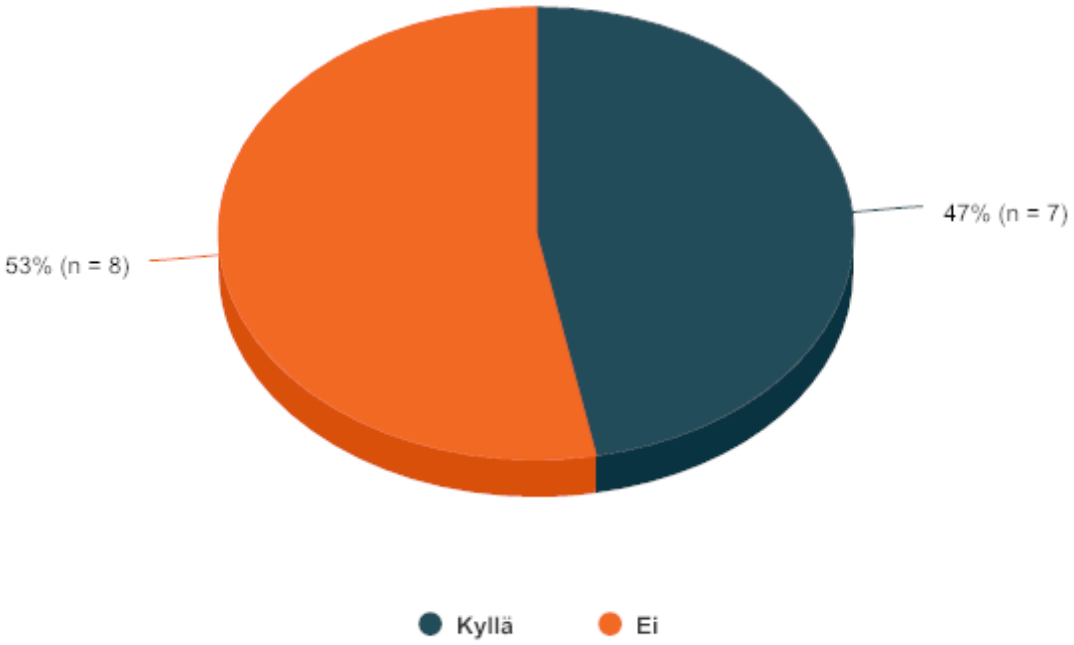
Vastaajien määrä: 15, valittujen vastausten lukumäärä: 16



	n	Prosentti
Kyllä	11	73,33%
Ei	2	13,33%
Kyllä, arkaluontoisia tai erityisiä henkilötietoja	3	20%

6. Tarvitsenko työssäni lisäkoulutusta liittyen tietosuoja-asetukseen?

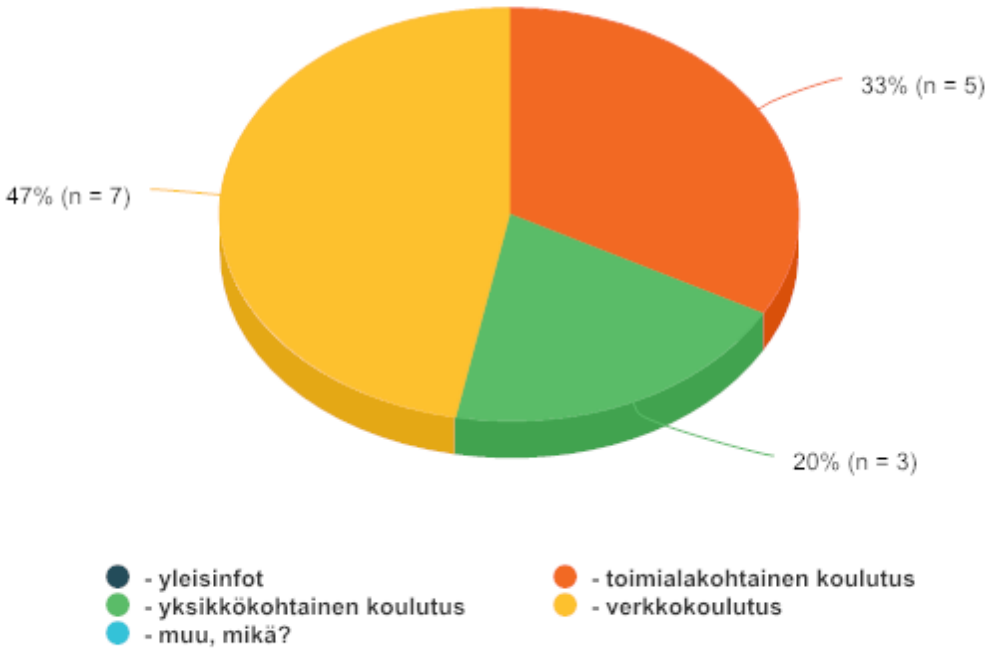
Vastaajien määrä: 15



	n	Prosentti
Kyllä	7	46,67%
Ei	8	53,33%

7. Minua parhaiten palveleva koulutusmuoto?

Vastaajien määrä: 15



	n	Prosentti
- yleisinfot	0	0%
- toimialakohtainen koulutus	5	33,33%
- yksikkökohtainen koulutus	3	20%
- verkkokoulutus	7	46,67%
- muu, mikä?	0	0%

Avoimeen tekstikenttään annetut vastaukset

Vastausvaihtoehdot	Teksti

8. Mistä tarvitsisin lisätietoa?

Vastaajien määrä: 15, valittujen vastausten lukumäärä: 21

	n	Prosentti
Tietosuoja-asetus yleisesti	5	33,33%
Tietosuoja opetus- ja sivistystoimessa	1	6,67%
Tietosuoja teknisessä ja ympäristötoimessa	3	20%
Tieto- ja tarkastuspyyntöihin vastaaminen	2	13,33%
Tietosuoja pilvipalveluluissa ja sähköpostissa	10	66,67%
Muu, mikä?	0	0%

Avoimeen tekstikenttään annetut vastaukset

Vastausvaihtoehdot	Teksti

9. Muuta palautetta ja parannusehdotuksia.

Vastaajien määrä: 1

Vastaukset
Tiedetään mitä pitäisi ytehdä, mutta ei ole aikaa, resursseja ja halua tehdä asioita niin vaikeasti. Pitäisi keksiä jokin helppo ja turvallinen tapa toimia yhtenäisesti.

Liite 6. Malliesimerkki tarkastusprosessikaaviosta, joita suunniteltiin