TIETOSUOJA PALKKAHALLINNON NÄKÖKULMASTA

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Visamäki, Liiketalous

Kevät, 2018

Emma Kivistö

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Liiketalouden koulutusohjelma
Visamäki, Hämeenlinna

Tekijä Emma Kivistö **Vuosi** 2018

Työn nimi Tietosuoja palkkahallinnon näkökulmasta

Työn ohjaaja Kyllikki Valkealahti

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena on perehtyä EU:n yleisen tietosuoja-asetuksen sisältöön (679/2016) sekä selvittää miten palkkahallinnossa tulee valmistautua asetuksen voimaantuloon. Opinnäytetyön toimeksiantaja on KuntaPro Oy ja työtä lähdettiin tekemään toimeksiantajan tarpeesta. KuntaPro tarvitsi selvitystä erityisesti tietosuoja-asetukseen valmistautumisen tasostaan sekä siitä, mitä dokumentteja tulee olla, jotta osoitusvelvollisuus täyttyy. Opinnäytetyössä perehdytään tietosuoja-asetuksen keskeisiin käsitteisiin ja sisältöön sekä palkanlaskennan prosessiin prosessikuvauksen ja palkanlaskennan vuosikellon avulla.

Opinnäytetyö toteutetaan toiminnallisena opinnäytetyönä, jonka konkreettinen tuotos on tarkistuslista (Liite 5) KuntaPron käyttöön. Tarkistuslistan avulla voidaan helposti tarkistaa tietosuoja-asetukseen valmistautumisen tila sekä tarvittavat dokumentit. Teemahaastatteluiden avulla pyritään saamaan kokonaiskuva KuntaPron valmistautumisesta asetuksen voimaantuloon sekä palkanlaskennan prosessista.

Johtopäätöksinä voidaan todeta, että kokonaisuudessaan tietosuojan taso KuntaProlla on tällä hetkellä hyvä eikä tietosuoja-asetuksen voimaantulo aiheuta suuria toimenpiteitä. Tarvittavat dokumentit on listattu tutkimuksen tuloksissa, esimerkiksi tietotilinpäätös on hyvä keino todistaa noudattavansa osoitusvelvollisuutta. Tutkimuksen tulokset ja tarkemmat johtopäätökset löytyvät luvuista viisi ja kuusi sekä liitteestä viisi tarkistuslistan muodossa.

Avainsanat Tietosuoja, EU:n yleinen tietosuoja-asetus, palkkahallinto, palkanlaskennan prosessi

Sivut 45 sivua, joista liitteitä 7 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Business Administration
Visamäki, Hämeenlinna

Author Emma Kivistö **Year** 2018

Subject Data Protection from Payroll Administration Perspective

Supervisor Kyllikki Valkealahti

ABSTRACT

The aim of this thesis is to specialize in the content of the EU's general data protection regulation (679/2016), GDPR, and to clarify how the payroll administration should prepare for the incoming regulation. The commissioner of this thesis was KuntaPro Oy and the thesis was based on the need of the client. KuntaPro needed an account on the level of preparation for the data protection regulation and on what documents would be needed to comply with the regulation. This thesis focuses on the key concepts and contents of the GDPR and the payroll's process through the process description and the payroll´s annual cycle.

This practice-based thesis has a concrete output in the form of a checklist for the use of KuntaPro. The checklist helps to easily check the state of preparation for the GDPR and the necessary documents. The thematic interviews aim to obtain an overall picture of the preparation at KuntaPro for GDPR and the payroll process.

As a conclusion, the level of data protection at KuntaPro is currently good, and the incoming GDPR does not cause any major measures. The required documents are listed in the outcomes of the thesis. For example, the accounting data is a good way of showing compliance with the obligations. The outcomes of the study and more precise conclusions can be found in chapters five and six.

Keywords Data protection, GDPR, payroll administration, payroll process

Pages 45 pages including appendices 7 pages

SISÄLLYS

Liitteet

Liite 1 Palkanlaskennan kokonaisprosessi
Liite 2 Palkanlaskennan kokonaiskuva
Liite 3 Palkka-ajot
Liite 4 Teemahaastattelun runko
Liite 5 Tarkistuslista

1 JOHDANTO

Tämän opinnäytetyön aiheena on EU:n yleinen tietosuoja-asetus ja sen vaikutus palkanlaskentaan. EU:n tietosuojauudistus astuu voimaan toukokuussa 2018 suoraan sellaisenaan osaksi sovellettavaa lainsäädäntöä, joten aihe on ajankohtainen sekä tarpeellinen myös toimeksiantajayritykselle. Tällä hetkellä eletään kahden vuoden siirtymäaikaa, jonka aikana yritysten on valmistauduttava asetuksen voimaantuloon sen vaatimalla tavalla. Tietosuoja-asetuksen keskeisiä tavoitteita on yhdenmukaistaa EU-maiden tietosuojasääntelyä sekä helpottaa palveluiden tarjoamista yli valtioiden rajojen. Asetuksen myötä yksilöillä on enemmän oikeuksia omiin henkilötietoihinsa sekä puolestaan rekisterinpitäjillä enemmän velvollisuuksia, varsinkin henkilötietojen käsittelyn suhteen. (GDPR 679/2016.)

Opinnäytetyö toteutetaan toiminnallisena opinnäytetyönä, jonka lopullinen tuotos on tarkistuslista (Liite 5) toimeksiantajan käyttöön. Teoriapohjan avulla laaditaan alustava tarkistuslista, joka käydään läpi yhdessä tuotantopäällikön kanssa, ja haastattelun avulla pyritään kartoittamaan millä mallilla KuntaPron valmistautuminen tietosuoja-asetuksen suhteen on. Tehtyjen havaintojen perusteella lähdetään työstämään opinnäytetyötä siten, että vastataan mahdollisimman hyvin toimeksiantajan tarpeisiin.

Opinnäytetyön teoriaosuudessa käsitellään EU:n yleistä tietosuoja-asetusta, tuodaan esiin sen keskeinen sisältö, tavoitteet sekä keskeiset muutokset. Tietosuoja-asetuksen lisäksi palkanlaskennan prosessi sekä henkilötietojen käsittely ovat keskeisiä teoriaosuudessa. Teoriaosuus toimii pohjana tarkistuslistan laatimisessa.

Opinnäytetyön tavoitteena on selvittää, miten tietosuoja-asetuksen voimaantuloon tulee valmistautua sekä perehtyä siihen juuri palkanlaskennan ja henkilötietojen käsittelyn kannalta. Lisäksi tavoitteena on tuoda esiin olennaisimmat muutokset ja avata keskeiset käsitteet sekä kartoittaa nimenomaan KuntaPron valmistautumisen nykytila.

1.1 Toimeksiantajan esittely

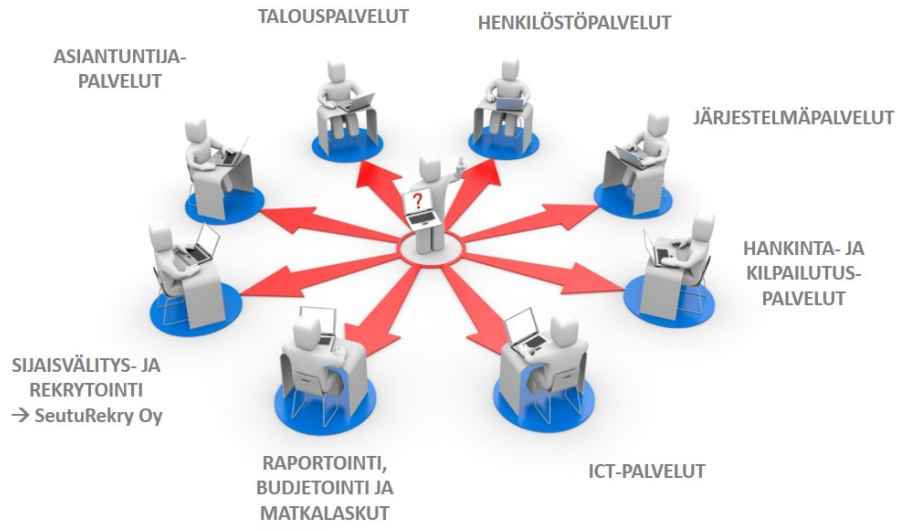
Opinnäytetyön toimeksiantajana toimii KuntaPro Oy. KuntaPro on palvelukeskus, joka tuottaa talous-, henkilöstö-, järjestelmä- ja hankintapalveluita julkiselle sektorille. (KuntaPro 2018 a.)

KuntaPro on perustettu vuonna 2013, jolloin Seutukeskus Oy Häme ja Taloustuki Kuntapalvelut Oy fuusioituivat. Tällä hetkellä KuntaProlla työskentelee noin 300 työntekijää ja yrityksen liikevaihto oli 53 miljoonaa euroa vuonna 2017. KuntaPro on vakavarainen ja kannattava yhtiö. Toimipisteitä

on viisi: Hyvinkäällä, Hämeenlinnassa, Kangasalalla, Porissa ja Tuusulassa. (KuntaPro 2018 a.)

KuntaProlla on 150 asiakasta, joista 92 on omistaja-asiakkaita. KuntaPron omistaja-asiakkaita voivat olla kunnat, kaupungit, kuntayhtymät ja kuntien omistamat yhtiöt. Omistajuuden saa merkitsemällä määrätyn määrän KuntaPron osakkeita. Osakkeen hinta määritellään vuosittain yhtiökokouksessa. (KuntaPro 2018 a.)

KuntaPron palvelukonsepti perustuu pitkäaikaiseen kokemukseen tuottaa keskitettyjä henkilöstöhallinnon tukipalveluita. Asiakas voi halutessaan ulkoistaa hallinnon tukipalvelunsa KuntaProlle kokonaan tai osittain. (KuntaPro n.d.)



Kuva 1. KuntaPron tarjoamat palvelut (KuntaPro 2017 a).

Kuvassa 1 tuodaan tiivistetysti esiin KuntaPron tarjoamia palveluita, joita avataan seuraavissa kappaleissa enemmän. KuntaPron palvelut on jaettu järjestelmäpalveluihin, ulkoistuspalveluihin sekä muutosjohtamisen palveluihin. Kaikki palvelut toimivat pilvessä ja asiakas voi halutessaan ulkoistaa hallinnon tukipalvelunsa KuntaProlle kokonaan, osittain tai vaihtoehtoisesti ottaa käyttöön esimerkiksi pelkät tietojärjestelmät sekä siihen liittyvät tukipalvelut. Ulkoistuspalveluihin lukeutuvat henkilöstö- ja taloushallinnon palvelut, hankinta- ja kilpailutuspalvelut, ICT-palvelut sekä tytäryhtiö Seuturekry Oy:n henkilöstöpalvelut. (KuntaPro n.d.)

Järjestelmäpalvelut muodostavat Kuntax-tuoteperheen, joka sisältää tiedolla johtamisen, taloushallinnon, palkanlaskennan sekä henkilöstöhallinnon ja palveluiden toiminnanohjauksen työkaluja. Käytössä on toiminnanohjausjärjestelmä, jonka avulla pystytään johtamaan sekä seuraamaan reaaliaikaisesti taloutta ja toimintaa eri toimintasektoreilla. (KuntaPro n.d.)

KuntaPro tarjoaa myös muutosjohtamisen palveluita, sillä haluttu muutos vaatii hyvää johtamista. Julkisella sektorilla puhaltaa merkittävien muutosten tuulet ja organisaatioiden on pystyttävä reagoimaan muutoksiin nykyisissä ja tulevissa toimintatavoissaan. Palveluprosessit uudistuvat joustavimmiksi ja kustannustehokkaammiksi. Automatisaatio ja sähköistyminen ovat myös vahvasti mukana palveluiden muutoksessa. Huolelliset järjestelmävalinnat auttavat saavuttamaan hallitun muutosprosessin. (KuntaPro 2018 n.d.)

1.2 **Aiheen rajaus, tutkimusongelmat ja tutkimusmenetelmä**

Opinnäytetyön tietoperusta keskittyy EU:n yleiseen tietosuoja-asetukseen, jota tarkastellaan nimenomaan palkanlaskennan näkökulmasta, joten epäolennaiset asiat palkanlaskennan kannalta rajataan opinnäytetyöstä pois. Tietosuoja-asetuksen lisäksi palkanlaskennan prosessi on olennainen osa tietoperustaa

Palkanlaskennan prosessista kerrotaan hieman myös yleisellä tasolla, mutta pyritään siihen, että teoriaosuus palvelisi mahdollisimman hyvin tarkistuslistan (Liite 5) laatimista, eli tuotettaisiin mahdollisimman vähän ylimääräistä ja turhaa tietoa. Palkanlaskennan prosessissa keskitytään siihen, mitä tietoa palkanlaskennassa tarvitaan, mistä sitä saa ja mitä kaikkea on otettava huomioon tietosuoja-asetuksen kannalta jatkossa.

Tämän opinnäytetyön pääongelma on:

- Miten tietosuoja-asetuksen voimaantuloon tulee valmistautua palkkahallinnon näkökulmasta?

Seuraavien alaongelmien avulla pyritään löytämään vastaus pääongelmaan:

- Mitä EU:n yleinen tietosuoja-asetus tarkoittaa, ja mitä se pitää sisällään?
- Mitä luokitellaan arkaluonteisiksi tiedoiksi, ja mitä niiden käsittelyssä tulee ottaa huomioon?
- Mitä dokumentteja tarvitaan sen osoittamiseksi, että kaikki tarvittava on dokumentoitu sekä mistä asioista pitää olla dokumentti?
- Millainen on palkanlaskennan prosessi?
- Mitä muutoksia uusi EU-tietosuoja-asetus tuo palkkahallinnossa tarvittavien arkaluonteisiksi luokiteltavien tietojen keräämiseen, käsittelyyn, arkistointiin ja tuhoamiseen?
- Miten toimeksiantajayrityksessä on valmistauduttu tietosuoja-asetuksen voimaantuloon?

Opinnäytetyö toteutetaan toiminnallisena opinnäytetyönä, jonka lopullinen tuotos on tarkistuslista. Tarkistuslistan avulla tarkistetaan, kuinka tietosuoja-asetuksen voimaantuloon on valmistauduttu. Tietoperustan

avulla laaditaan alustava tarkistuslista, joka käydään toimeksiantajayrityksen tuotantopäällikön kanssa läpi ja katsotaan, missä vaiheessa valmistautuminen on. Keskustelussa heränneiden havaintojen perusteella lähdetään jatkamaan opinnäytetyön tekemistä tarpeelliseen suuntaan, eli teoriaa ja ohjeistusta niihin asioihin, mihin ei ole vielä toistaiseksi valmistauduttu riittävän hyvin.

Oheisessa kuvassa 2 tuodaan esiin tämän opinnäytetyön runko. Johdannossa tuodaan esiin työn keskeinen idea, tutkimusongelmat sekä käytettävät metodit ja esitellään opinnäytetyön toimeksiantaja. Toisessa pääluvussa käsitellään lähinnä EU:n yleisen tietosuoja-asetuksen sisältöä, keskeisiä käsitteitä sekä omin alaluvuin tarkemmin esimerkiksi henkilötietojen käsittelijän ja rekisterinpitäjän roolia sekä tietojen käsittelyn lainmukaisuutta. Kolmannessa pääluvussa käsitellään palkanlaskennan prosessia sekä palkanlaskennan vuosikelloa ja arkistointia palkkahallinnossa. Toinen ja kolmas luku muodostavat tämän opinnäytetyön tietoperustan. Neljännessä pääluvussa käsitellään tutkimuksen toteutusta ja kerrotaan tutkimusmenetelmistä, joita ovat toimintatutkimus, teemahaastattelu ja osallistava havainnointi. Pääluvussa viisi tuodaan esiin tutkimuksen tulokset, alaluvut käsittelevät KuntaPron valmistautumista, tarvittavaa dokumentaatiota sekä tarkistuslistaa. Tutkimustulosten jälkeen edetään pohdintaan ja johtopäätöksiin, jotka muodostavat kuudennen pääluvun.

Kuva 2. Työn rakenne.

2 EU-TIETOSUOJA-ASETUS

Tässä luvussa käsitellään EU:n yleistä tietosuoja-asetusta, sen keskeistä sisältöä ja tavoitteita, olennaisimpia käsitteitä sekä henkilötietojen käsittelyä. Tekstissä saatetaan käyttää EU:n yleisestä tietosuoja-asetuksesta myös lyhennettä GDPR. Tässä opinnäytetyössä keskitytään erityisesti palkanlaskennan näkökulmaan teoriaosuudessa eli kaikkia asetuksen osia ei käydä läpi, jos ne eivät ole palkanlaskennan kannalta olennaisia.

2.1 Keskeiset käsitteet

Tässä alaluvussa avataan opinnäytetyön keskeiset käsitteet erityisesti tietosuoja-asetuksen pohjalta. Määriteltäviä käsitteitä tietosuoja-asetuksen kannalta ovat henkilötiedot, arkaluonteiset tiedot, rekisteri, rekisteröity ja rekisterinpitäjä sekä osoitusvelvollisuus, henkilötietojen käsittelijä, käsittely ja pseudonymisointi.

Henkilötiedoilla tarkoitetaan kaikkia niitä tietoja, joiden perusteella luonnollinen henkilö voidaan tunnistaa. Tunnistetietoja ovat mm. nimi, henkilötunnus, osoite, verkkotunnistetiedot, fyysinen, kulttuurillinen, geneettinen tai taloudellinen tekijä. Tietosuoja-asetusta ei sovelleta yrityksen tietoihin, mutta esimerkiksi yrityksen yhteyshenkilön nimi ja muut henkilötiedot ovat asetuksen mukaan sovellettavia henkilötietoja. (GDPR 679/2016, 4.artikla 1.luku.)

Arkaluonteisia tietoja ovat tiedot, joista ilmenee henkilön
- rotu tai etninen alkuperä
- poliittinen, uskonnollinen tai yhteiskunnallinen vakaumus
- ammattiliiton jäsenyys
- rikollinen teko, rangaistus tai muu rikoksen seuraamus
- terveyttä koskevat tiedot
- seksuaalinen suuntautuminen
- sosiaalihuollon tarve tai saadut sosiaalihuollon palvelut, tukitoimet ja muut etuudet (HetiL 523/1999 § 11.)

GDPR on EU:n yleisen tietosuoja-asetuksen lyhenne, joka tulee englannin kielisistä sanoista General Data Protection Regulation (679/2016).

”Rekisterillä tarkoitetaan mitä tahansa tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu” (GDPR 679/2016, 4.artikla 1.luku).

Rekisteröity on luonnollinen henkilö eli ihminen, kenen henkilötietoja on rekisteröity. Yritykset eivät siis ole rekisteröityjä tai niiden tiedot eivät ole henkilötietoa, jota tietosuoja-asetus koskettaisi. (GDPR 679/2016, 4.artikla 1.luku.)

Rekisterinpitäjä on useimmiten yritys, joka määrää mitä henkilötietoa kerätään ja miten sekä mihin kerättyjä henkilötietoja käytetään. Rekisterinpitäjä voi olla kuitenkin myös luonnollinen henkilö tai oikeushenkilö, viranomainen tai virasto joka määrittelee henkilötietojen käsittelystä. Rekisterinpitäjää koskee suurin osa asetuksen velvoitteista. (GDPR 679/2016, 4.artikla.)

”Osoitusvelvollisuuden avulla organisaation tulee kyetä osoittamaan, että se on huolehtinut seuraavista henkilötietojen käsittelyn osa-alueista:
- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen ja
- eheys ja luottamuksellisuus” (Valtiovarainministeriö 2016, 11).

Henkilötietojen käsittelijä on luonnollinen -tai oikeushenkilö, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. On muistettava, että käsittelijä ei päätä tietojen keräämisestä vaan toimii ainoastaan rekisterinpitäjän dokumentoitujen ohjeiden mukaan. (GDPR 679/2016, 4.artikla.)

Käsittely voi olla tietojen keräämistä, tallentamista, muokkaamista, yhdistämistä, käyttöä, jäsentämistä, säilyttämistä ja paljon muuta. Käsittelyä on kaikki toiminta, kun henkilötietoja ylipäänsä käytetään mihin tahansa tarkoitukseen. (Hanninen ym. 2017, 20.)

”Tietotilinpäätös on organisaation laatima vapaaehtoinen raportti, joka antaa kokonaiskuvan organisaation tietojenkäsittelyn nykytilasta. Raportti on tarkoitettu johdon työkaluksi ja lisäämään sidosryhmien luottamusta siihen, että organisaatio noudattaa hyvää sääntelyn mukaista tietojenkäsittelytapaa henkilötietojen käsittelyssä. Tietotilinpäätöstä voidaan käyttää yhtenä keinona tietosuoja-asetuksen osoitusvelvollisuuden toteuttamisessa.” (Valtiovarainministeriö 2016, 13.)

Pseudonymisointi tarkoittaa käytännössä tietojen tallennusta eri paikkoihin siten, ettei niitä pystytä yhdistämään rekisteröityyn ilman lisätietoja, jotka on myös säilytettävä erillään. (Hanninen ym. 2017, 21.)

2.2 **Yleistä asetuksesta**

Toukokuun 25.päivänä 2018 astuu voimaan koko EU-alueella sovellettava yleinen tietosuoja-asetus. Tietosuoja-asetuksesta puhutaan myös usein lyhenteellä GDPR, joka tulee englanninkielisistä sanoista General Data Protection Regulation (679/2016). Asetus tulee voimaan sellaisenaan suoraan osaksi sovellettavaa lainsäädäntöä samaan aikaan kaikissa EU-maissa, myös Suomessa. Asetus korvaa vuonna 1995 annetun henkilötietodirektii-

vin (46/1995/EY). Asetuksessa säädetään mm. rekisterinpitäjän ja käsittelijän velvollisuuksista, rekisteröidyn oikeuksista, henkilötietojen käsittelyn periaatteista ja lainmukaisuudesta sekä arkaluonteisten tietojen käsittelystä. (Hanninen, Laine, Rantala, Rusi & Varhela 2017, 13—15; Andreasson & Ylipartanen 2017.)

Tietosuoja-asetuksen tarkoitus on ajantasaistaa ja yhdenmukaistaa tietosuojaa koskevaa sääntelyä EU:n jäsenvaltioissa, vastata teknologian kehitykseen sekä ottaa globaalisti huomioon henkilötietojen käsittelyyn liittyvät haasteet. Asetuksen tavoitteena on parantaa henkilötietojen käsittelyn läpinäkyvyyttä ja avoimuutta sekä lisätä yksilön oikeuksia omiin henkilötietoihinsa. (Oikeusministeriö 2017, 9.)

Parhaillaan eletään kahden vuoden siirtymäaikaa, jonka aikana yritysten on tehtävä tarvittavat toimenpiteet, sillä asetuksen astuessa voimaan henkilötietoja on käsiteltävä asetuksen vaatimalla tavalla. Mikäli yritys ei noudata asetuksen säädöksiä, on asetuksessa säädetty tuntuvista taloudellisista sanktioista, joita valvontaviranomaisilla on oikeus määrätä. Sanktioiden uskotaan kannustavan yrityksiä toimimaan tietosuoja-asetuksen edellyttämällä tavalla ja tämä saattaa tuoda yrityksille myös selvää kilpailuetua. Sanktion suuruus on joko neljä prosenttia tai enintään 20 000 000 euroa yrityksen kokonaisliikevaihdosta. (Hanninen ym. 2017, 13—14, 129.)

Asetusta tulee soveltaa yksityisellä ja julkisella sektorilla, riippumatta siitä kuinka laajasti henkilötietoja käsitellään, mikä käsiteltävien tietojen luonne on tai millaista teknologiaa käytetään. Asetus koskee kaikkia sen soveltamisalaan kuuluvia organisaatioita niin henkilötietojen käsittelijöitä kuin rekisterinpitäjiäkin. (Oikeusministeriö 2017, 9.)

Asetuksessa on säädetty tietosuojaperiaatteista, jotka velvoittavat rekisterinpitäjiä käsittelemään henkilötietoja niin, että rekisteröidyn oikeuksia ja vapauksia kunnioitetaan. Henkilötietolaissa on säädetty periaatteista melko samalla tavalla, mutta asetuksessa on vielä täsmennetty joitakin kohtia. Tietosuoja-periaatteita ovat:

- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- tietojen säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus
- rekisterinpitäjän osoitusvelvollisuus. (Oikeusministeriö 2017, 12.)

Rekisterinpitäjän vastuulla on huolehtia, että tietosuojaperiaatteita noudatetaan aina kun henkilötietoja käsitellään. Rekisterinpitäjän osoitusvelvollisuuden vuoksi on pystyttävä aiempaa tarkemmin todistamaan, että yrityksessä toimitaan asetuksen vaatimalla tavalla. Henkilötietojen käsitte-

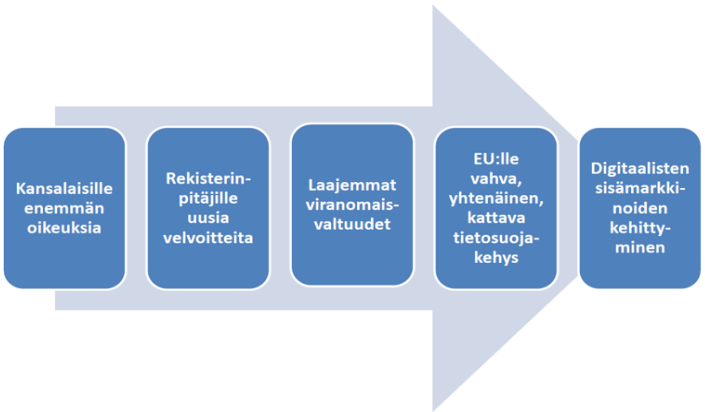
lyn prosesseihin on paneuduttava ja suunniteltava, miten jatkossa toimitaan ja mitä kaikkea on dokumentoitava, jotta osoitusvelvollisuus toteutuu. (Oikeusministeriö 2017, 12.)

Asetukseen valmistautuessaan organisaation on selvitettävä henkilötietojen käsittelyn kokonaisprosessi sillä hetkellä. Nykytilan selvityksen jälkeen olisi hyvä selvittää, mitä konkreettisia muutoksia ja toimenpiteitä tietosuoja-asetus edellyttää tehtävän. Nykytilan selvitykseen hyvä työkalu on tehdä esimerkiksi tietotilinpäätös, joka tiivistää nykytilan valmistautumisen tason. Erityisesti organisaation johdon on oltava hereillä tietosuojalainsäädännön muutoksista ja miten se tulee vaikuttamaan organisaation toimintaan. (Oikeusministeriö 2017, 11.)

2.3 Tietosuoja-asetuksen sisältö ja tavoitteet

Tietosuoja-asetuksen astuessa voimaan, asetuksen sisällön tulisi olla organisaatioille selvä. Tietosuoja-asetuksessa on täsmennyksiä esimerkiksi rekisteröidyn oikeuksista, rekisterinpitäjien sekä henkilötietojen käsittelijöiden tehtävistä ja vastuista. EU:n yleinen tietosuoja-asetus velvoittaa rekisterinpitäjiä ja yrityksiä tekemään kahden vuoden siirtymäajan aikana nykytila-arvion sekä analyysin siitä, vastaako tämänhetkinen henkilötietojen käsittely ja tietosuojakäytänteet kansallisen lainsäädännön ja tietosuoja-asetuksen uusia vaatimuksia. Siirtymäajan päättyessä ei enää riitä, että noudattaa asetusta, vaan rekisterinpitäjien pitää pystyä jatkossa osoittamaan, että tietosuojakäytänteet on huomioitu organisaation toiminnassa. Uuden sääntelyn avulla halutaan ohjata organisaatioita ottamaan tietosuojan huomioon jo toimintansa suunnittelussa. (Andreasson & Ylipartanen 2017.)

”Tietosuoja-asetuksen tarkoituksena on ajantasaistaa tietosuojaa koskevaa sääntelyä, jotta voidaan vastata teknologian kehitykseen ja globalisaatioon liittyviin henkilötietojen suojaa koskeviin haasteisiin.” Asetuksen avulla pyritään tukemaan digitaalisten sisämarkkinoiden kehittymistä yhdenmukaistamalla EU-alueen tietosuojaa koskevaa sääntelyä. (Oikeusministeriö 2017, 9.)



Kuva 3. Asetuksen sisältö ja tavoite (Andreasson & Ylipartanen).

Kuvassa 3 tuodaan esiin tietosuoja-asetuksen keskeinen sisältö sekä tavoite. Keskeistä on lisätä rekisteröityjen oikeuksia sekä luoda EU:lle yhtenäinen ja vahva tietosuojakehys. Asetuksen olennaisimmista osista palkkahallinnon kannalta on omat alalukunsa.

Asetuksessa on 173 johdantokappaletta sekä 99 artiklaa. Koko asetuksen sisältöä ei ole tarpeen osata ulkoa, mutta pääasiat olisi hyvä tietää ja muuttaa toimintojaan sen mukaan. Rekisterinpitäjän ja henkilötietojen käsittelijän on arvioitava henkilötietojen käsittelyyn liittyvät riskit ja tehtävä tarvittavat hallintatoimenpiteet kyseisen riskitason mukaan. Organisaation riskienhallintaprosessiin on hyvä ottaa tietosuojariskien hallinta kiinteäksi osaksi prosesseja. Merkittävän tason riskeistä tulisi raportoida suoraan ylimmälle johdolle asti sekä organisaatioiden tulee riskiarvioinnin avulla selvittää, tarvitseeko heidän nimittää tietosuojavastaava. Jokaisen yrityksen tulee arvioida omaa toimintaansa ja selvitettävä mahdolliset tietosuojaan liittyvät riskit sekä mukautettava henkilötietojen käsittely asetuksen vaatimusten mukaiseksi. (Hanninen ym. 2017, 16—17.)

Hannisen ym. (2017, 16—17) mukaan riskiarviointia seuraava vaikutustenarviointi on asetuksen keskeinen vaatimus. Tietosuojan vaikutustenarviointi on pakollista niille henkilötietojen käsittelytoimijoille, joiden henkilötietojen käsittelytoimiin sisältyy yksilön oikeuksien ja vapauksien kannalta merkittäviä riskejä. Henkilötietojen käsittelyn tulee olla aina suunnitelmallista, mutta jatkossa myös dokumentoitua. Tietoa saa kerätä rekistereihin vain etukäteen laaditun suunnitelman eli tietosuojaselosteen mukaisesti. Tietojen keräämiselle tulee aina olla laillinen peruste.

Oikeusministeriön (2017, 9) mukaan asetuksen velvoitteiden noudattamista valvotaan tehokkaasti, sillä asetuksessa säädetään valvontaviranomaisten lisääntyneistä oikeuksista valvoa organisaatioiden toimintaa ja tarvittaessa määrätä tuntuvistakin sanktioista. Hannisen ym. (2017, 129) mukaan viranomaisten valtuudet kasvavat huomattavasti ja määrättävän sanktion suuruus voikin olla 4 % kokonaisliikevaihdosta tai 20 000 000 euroa. Hallinnollisten sakkojen suuruuteen vaikuttaa esimerkiksi rikkomuksen luonne ja se, mitä velvollisuutta on rikottu sekä haittavaikutuksen alaiseksi joutuneiden rekisteröityjen määrä.

Tietosuoja-asetusta (GDPR 679/2016, 3.artikla) sovelletaan henkilötietojen käsittelyyn, mikäli rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikka sijaitsee unionin alueella ja henkilötietoja käsitellään toiminnan yhteydessä, sillä ei ole merkitystä suoritetaanko käsittely konkreettisesti unionin alueella vai ei. Oikeusministeriön (2017, 9) mukaan henkilötietojen käsittelyn laajuudella, käsiteltävien henkilötietojen luonteella tai käytössä olleella teknologialla ei ole merkitystä siinä, etteikö asetusta sovellettaisi niin julkisella kuin yksityiselläkin puolella.

2.3.1 Rekisteröidyn oikeudet

Rekisteröidyn oikeuksista säädetään melko samalla tavalla myös henkilötietolaissa (523/1999), mutta tietosuoja-asetuksessa oikeuksien toteuttamisesta säädetään entistä tarkemmin. (Oikeusministeriö 2017, 23.) Tavoitteena on vahvistaa luonnollisten henkilöiden oikeuksia omiin henkilötietoihinsa ja niiden käsittelyyn. Rekisteröidyllä on oikeus saada tietoa henkilötietojen käsittelystä läpinäkyvästi, päästä käsiksi tietoihin sekä oikaista virheelliset tiedot. Tietosuoja-asetuksen (679/2016) 17.artiklan mukaan rekisteröidyllä on myös oikeus tulla unohdetuksi, jos joku seuraavista perusteista täyttyy:

- henkilötietoja ei tarvita niihin tarkoituksiin, joihin ne alun perin kerättiin
- rekisteröity peruuttaa suostumuksensa, eikä käsittelylle ole enää laillista perustetta
- rekisteröity vastustaa käsittelyä esimerkiksi sen nojalla, että henkilötietoja käsitellään suoramarkkinointia varten
- henkilötietoja on käsitelty lainvastaisesti
- henkilötiedot tulee poistaa rekisterinpitäjään kohdistuvan lakisääteisen velvoitteen vuoksi
- henkilötiedot on kerätty rekisteröidyn ollessa alle 16-vuotias.

Kuva 4. Rekisteröidyn oikeudet (Privaon 2017).

Kuvassa 4 tuodaan tiivistetysti esiin keskeiset rekisteröidyn oikeudet, joka on keskeinen muutos tietosuoja-asetuksen voimaantullessa, sillä asetuksessa on täsmennetty niitä. Kuva toimii ikään kuin tiivistelmänä ylläolevaan lukuun, jossa rekisteröidyn oikeuksia käsitellään. Rekisteröidyn oikeudet eivät ole kovin merkittävässä osassa opinnäytetyöprosessissa, joten jokaista kuvan kohtaa ei ole lähdetty avaamaan. Kuvasta kuitenkin käy ilmi se, missä asetuksen artiklassa säädetään mistäkin rekisteröidyn oikeudesta, joten kuvan avulla on helppo löytää tarvitsemansa tieto.

Hannisen ym. (2017, 56) mukaan rekisteröidyllä on oikeus rajoittaa tietojen käsittelyä sekä pyytää tieto niistä henkilötietojen vastaanottajista, keille rekisterinpitäjän on ilmoitettava oikaisuista, poistoista ja käsittelyn rajoittamisesta. Rekisteröidyllä on vastustamisoikeus sekä mahdollisuus

siirtää tiedot järjestelmästä toiseen sekä oikeudet profilointiin ja automatisoituihin päätöksiin. Oikeusministeriön (2017, 23) mukaan on kuitenkin huomioitava se, että osa oikeuksista, kuten oikeus siirtää tiedot järjestelmästä toiseen ja vastustamisoikeus ei liity kaikkiin tapauksiin.

2.3.2 Rekisterinpitäjän vastuu ja velvollisuudet

Rekisterinpitäjien vastuu kasvaa ja velvollisuudet lisääntyvät asetuksen voimaantullessa. Rekisterinpitäjän on tehtävä tarvittavat toimenpiteet, jotta pystytään varmistamaan ja osoittamaan, että henkilötietojen käsittelyssä noudatetaan asetusta. Rekisterinpitäjän on pystyttävä osoittamaan jälkikäteen käsittelevänsä henkilötietoja lainmukaisesti. (GDPR 679/2016, artikla 24.)

Oikeusministeriön (2017, 23—24) mukaan rekisterinpitäjän velvollisuuksiin kuuluu pyydettäessä toimittaa henkilötietojen käsittelyä koskevat tiedot rekisteröidylle läpinäkyvästi, helposti ymmärrettävästi sekä muuten asetuksen edellyttämällä tavalla. Tieto toimenpiteistä pitää antaa rekisteröidylle viimeistään kuukauden kuluttua pyynnön vastaanottamisesta. Mikäli rekisterinpitäjä ei aio toteuttaa rekisteröidyn tietojen käsittelyä koskevaa pyyntöä, pitää siitäkin ilmoittaa viimeistään kuukauden kuluessa sekä kertoa muista mahdollisuuksista, kuten oikeudesta tehdä valitus valvontaviranomaiselle.

Rekisterinpitäjällä on ensisijainen vastuu henkilötietojen käsittelyn lainmukaisuudesta sekä siitä, että henkilötietojen käsittelijät toimivat asetuksen edellyttämällä tavalla. Rekisterinpitäjä määrittelee henkilötietojen käsittelyn tarkoituksesta ja keinoista, joten käsittelijä voi käsitellä henkilötietoja ainoastaan rekisterinpitäjän määrittelemien dokumentoitujen ohjeiden mukaisesti. (Hanninen ym. 2017, 24—27.)

Valtiovarainministeriön (2016, 28) mukaan rekisterinpitäjän velvollisuuksiin kuuluu valita ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa sekä pystyvät huolehtimaan siitä, että asetuksen vaatimukset täyttyvät. Rekisterinpitäjällä on oikeus ulkoistaa valitsemansa osa henkilötietojen käsittelystä toimeksisaajalle, toimeksiannosta on oltava aina kirjallinen sopimus.

Kirjallisesta sopimuksesta tulee käydä ilmi henkilötietojen käsittelyn kohde, tarkoitus, kesto sekä sopia käsiteltävistä henkilötiedoista. Lisäksi on huolehdittava siitä, että käsittelijä esimerkiksi noudattaa salassapitovelvollisuutta sekä käsittelee henkilötietoja ainoastaan sopimuksen velvoittamalla tavalla. (Valtiovarainministeriö 2016, 28.)

2.3.3 Tietosuojavastaavan nimittäminen

Tietosuojavastaavan nimittämisvelvollisuudesta säädetään tietosuoja-asetuksen (679/2016) artikloissa 37—39. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee nimetä tietosuojavastaava, mikäli yrityksen ydintehtävät muodostuvat henkilötietojen käsittelyn ympärille, esimerkiksi palkkahallinnon palveluita tarjoavat yritykset ovat täten velvollisia nimittämään tietosuojavastaavan. Tietosuojavastaavan on oltava riippumaton eli henkilö, joka vastaa yrityksen tietojärjestelmistä tai henkilötietojen käsittelystä ei voi olla tietosuojavastaava.

Tietosuojavastaava on sallittua nimittää yrityksen sisältä tai ulkoistaa palvelusopimuksella esimerkiksi asianajotoimistolle. Rekisteröidyillä on oikeus ottaa yhteyttä tietosuojavastaavaan henkilötietojen käsittelyyn liittyvissä kysymyksissä ja tietosuojavastaavan tulee olla valvontaviranomaisten tavoitettavissa. Tietosuojavastaava neuvoo ja ohjeistaa henkilötietoja käsitteleviä yrityksiä sekä työntekijöitä. Tietosuojavastaavan tehtäviin kuuluu myös valvoa tietosuoja-asetuksen mukaisten vaatimusten noudattamista ja raportoida niistä tarvittaessa suoraan ylimmälle johdolle. On kuitenkin muistettava, että tietosuojavastaava ei ole vastuussa tietosuoja-asetuksen velvoitteiden noudattamisesta vaan ensisijaisesti siitä vastaa rekisterinpitäjä sekä henkilötietojen käsittelijä. (Hanninen ym. 2017, 120—123.)

2.3.4 Henkilötietojen käsittelijän rooli ja vastuu

Hannisen ym. (2017, 27) mukaan tietosuoja-asetuksen astuessa voimaan henkilötietojen käsittelijän vastuu kasvaa huomattavasti. Aiemmin henkilötietojen käsittelijän velvollisuudet ovat koostuneet lähinnä sopimusvelvoitteista sekä tietoturvaan liittyvistä velvoitteista. Henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun eli asiakkaan dokumentoidun ohjeistuksen mukaisesti eli käsittelijän on oltava tarkkana, missä oman roolin rajat kulkevat. Mikäli henkilötietojen käsittelijäyritys määrittelee itsenäisesti tietojen käsittelystä ilman rekisterinpitäjän ohjeistusta, käsittelijä tulkitaan rekisterinpitäjäksi. Tällöin myös kaikki rekisterinpitäjän velvollisuudet ovat käsittelijäyrityksen vastuulla.

Rekisterinpitäjän ja henkilötietojen käsittelijän välisestä kirjallisesta sopimuksesta tulee käydä ilmi henkilötietojen käsittelyn kohde, tarkoitus, kesto sekä sopia käsiteltävistä henkilötiedoista. Asetus selkiyttää rekisterinpitäjän ja henkilötietojen käsittelijän välisiä rooleja, sääntelyä sekä osoittaa velvollisuuksia myös suoraan käsittelijälle. (Valtiovarainministeriö 2016, 28.)

Valtiovarainministeriön (2016, 28—29) mukaan henkilötietojen käsittelijän tulee käsitellä henkilötietoja ainoastaan dokumentoidun ohjeen mukaisesti, noudattaa salassapitovelvollisuutta sekä tietosuoja-asetuksen

vaatimuksia tietoturvan kannalta oikein ja auttaa rekisterinpitäjää toteuttamaan rekisteröidyn oikeuksia. Käsittelijä ei saa ulkoistaa henkilötietojen käsittelyä kenellekään ilman rekisterinpitäjän kirjallista ennakkosuostumusta ja käsittelypalvelujen päättyessä henkilötiedot tulee poistaa tai palauttaa rekisterinpitäjälle, myös kaikki kopiot. Käsittelijän tulee ilmoittaa viipymättä mahdollisista tietoturvaloukkauksista rekisterinpitäjälle sekä tuoda esiin sellaiset tiedot, jotka ovat oleellisia osoitusvelvollisuuden todistamisessa. Käsittelijän tulee yhteistyössä rekisterinpitäjän kanssa pyrkiä minimoimaan vahingot, tekemään vaikutustenarviointeja sekä osallistua auditointeihin ja auttaa rekisterinpitäjää noudattamaan hyvää tietoturvallisuutta, sekä puuttua asiaan tarvittaessa, mikäli rekisterinpitäjän ohjeistus on vastoin tietosuoja-asetuksen velvoitteita.

2.3.5 Tietojen käsittelyn yleiset periaatteet

Asetuksessa säädetään tietojen käsittelyn yleisistä periaatteista, jotka tulee ottaa huomioon henkilötietoja käsiteltäessä eli mitä tietoa on sallittua käsitellä ja miten. Suurimmilta osin henkilötietojen käsittelyn periaatteet vastaavat aiempia säädöksiä, mutta joitakin täsmennyksiä asetuksesta löytyy. Rekisterinpitäjän on pystyttävä osoittamaan, että tietosuojaperiaatteita on noudatettu. (Hanninen ym. 2017, 47—51.)

”Tietosuojaperiaatteita ovat:
- käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- tietojen säilytyksen rajoittaminen
- tietojen eheys ja luottamuksellisuus.” (GDPR 679/2016, 5.artikla.)

Henkilötietoja on käsiteltävä lainmukaisesti, kohtuullisesti sekä läpinäkyvästi. (GDPR 2016/679, 5.artikla.) Tietojen käsittelyn lainmukaisuudesta kerrotaan lisää seuraavassa alaluvussa. Läpinäkyvyyden pääperiaate on se, että rekisteröidylle tulisi olla läpinäkyvää, mitä tietoja hänestä kerätään, mihin tarkoitukseen ja miksi. Tämä tulee määritellä tiedonkeruutilanteessa yksiselitteisesti. Rekisteröidyillä on myös oikeus saada tieto siitä, kuka on rekisterinpitäjä ja henkilötietojen käsittelijä. (Hanninen ym. 2017, 48.)

Hannisen ym. (2017, 49) mukaan henkilötietoja ei saa käyttää muuhun tarkoitukseen kuin ne on kerätessä tarkoitettu. Aina on varmistettava, että henkilötietoja todella käytetään vain siihen tarkoitukseen tai tehtävän hoitoon, johon ne on kerätty, kuten työntekijöiden valinta tai asiakassuhteen hoito. Mikäli on mahdollista tehdä toimenpiteitä, niin ettei henkilötietoja käsiteltäisi ollenkaan, sitä parempi.

Tietoja tulee kerätä vain sen verran, mikä on käsittelyn käyttötarkoituksen kannalta välttämätöntä. Yritysten on syytä kiinnittää huomiota siihen, ovatko kaikki kerätyt tiedot todella tarpeellisia. Vaikka rekisteröity antaisi

luvan tietojen keräämiselle, ei suostumus oikeuta tietojen tarpeettomaan keräämiseen. (Hanninen ym. 2017, 49.) Henkilötietojen tulee olla täsmällisiä ja päivitettyjä. Rekisterinpitäjän on tehtävä tarvittavat toimenpiteet virheellisten ja epätarkkojen henkilötietojen oikaisemiseksi tai poistamiseksi viipymättä. (GDPR 679/2016, 5.artikla.)

Hannisen ym. (2017, 50) mukaan henkilötietoja tulisi säilyttää ainoastaan sen aikaa, kun on tarpeen eli säilytysajan tulisi olla mahdollisimman lyhyt. Tasaisin väliajoin on tarkasteltava henkilötietojen tarpeellisuutta, onko niitä vielä säilytettävä vai voisiko henkilötiedot jo tuhota. Usein henkilötietoja säilytetään asiakassuhteen päättymiseen asti, mutta joissakin tapauksissa voi olla tarpeellista säilyttää tietoja päättymisenkin jälkeen, esimerkiksi perinnän, reklamaatioiden tai oikeudellisten toimenpiteiden vuoksi. Jos tietoja on tarpeen säilyttää pidempiä aikoja, kannattaa harkita tiedon säilyttämistä sellaisessa muodossa, mistä rekisteröity ei ole tunnistettavissa eikä tietoja henkilötietojen poiston jälkeen pystytä yhdistämään rekisteröityyn.

”Tietoja 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” (GDPR 679/2016, 5.artikla).

Kuva 5. Tietojen käsittelyn yleiset periaatteet (GDPR 679/2016).

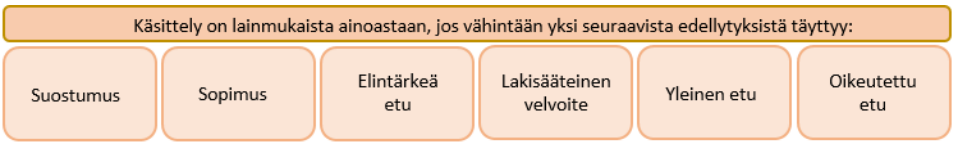
Kuvassa 5 tuodaan esiin tämän alaluvun pääkohdat eli tietosuojan kannalta keskeiset tietojen käsittelyn periaatteet perustuen EU:n yleisen tietosuoja-asetuksen viidenteen artiklaan. Käsittelyn lainmukaisuudesta kerrotaan lisää seuraavassa alaluvussa.

2.3.6 Tietojen käsittelyn lainmukaisuus

Hannisen ym. (2017, 16—17) mukaan henkilötietojen käsittelyn tulee olla aina suunnitelmallista, mutta jatkossa myös dokumentoitua. Tietoa saa kerätä rekistereihin vain etukäteen laaditun suunnitelman eli tietosuojaselosteen mukaisesti sekä tietojen keräämiselle tulee aina olla laillinen peruste.

Hannisen ym. (2017, 29–43) mukaan käsittely on lainmukaista, mikäli vähintään yksi kuudennessa artiklassa säädetyistä käsittelyperusteista täyttyy. Käsittelyperusteita ovat pääsääntöisesti suostumus, sopimus ja oikeutettu etu. Jos kyseessä on kuitenkin erityisten henkilöryhmien eli arkaluon-

teisten henkilötietojen käsittely, säädetään asetuksessa siitä vielä tarkemmin. Pääsääntöisesti arkaluonteisia henkilötietoja koskee käsittelykielto, joten yritysten olisi vältettävä arkaluonteisten tietojen käsittelyä aina, jos se on mahdollista. Rekisteröidyn suostumus on esimerkki erityisestä perusteesta henkilötietojen käsittelylle. Tästä esimerkkinä tapaukset, joissa tietojen käsittely sallitaan työlainsäädännössä tai se on oleellista esimerkiksi oikeusvaateen laatimiseksi.



Kuva 6. Käsittelyn lainmukaisuus (GDPR 679/2016).

Tietosuoja-asetuksen (679/2016) 6.artiklan pohjalta laadittu kuva 6 tuo esiin käsittelyn lainmukaisuuden edellytykset. Vähintään yksi edellytyksistä tulee täyttyä, jotta tietojen käsittely voidaan luokitella lainmukaiseksi. Edellytyksiä ovat: suostumus, sopimus, elintärkeä etu, lakisääteinen velvoite, yleinen etu ja oikeutettu etu. Käsittelyperusteita on pääsääntöisesti suostumus, sopimus ja elintärkeä etu, joista lisää alempana tässä luvussa.

Oikeusministeriön (2017, 20) mukaan mikäli henkilötietoja käsitellään suostumuksen mukaisesti, on yritysten kiinnitettävä erityistä huomiota siihen, miten suostumus pyydetään. Hannisen ym. (2017, 30) mukaan suostumuksen tulee olla vapaaehtoinen, yksilöllinen, tietoinen ja selkeä tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Oikeusministeriön (2017, 20) mukaan suostumus on annettava aktiivisesti, eikä suostumukseksi kelpaa esimerkiksi valmiiksi rastitettu ruutu tai vaikeneminen. Asetuksessa säädetään myös aiempaa tarkemmin lasten henkilötietojen käsittelystä ja alle 16-vuotiaiden henkilötietojen käsittely vaatiikin huoltajan suostumuksen tai valtuutuksen.

”Käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä” (GDPR 679/2016, 6.artikla).

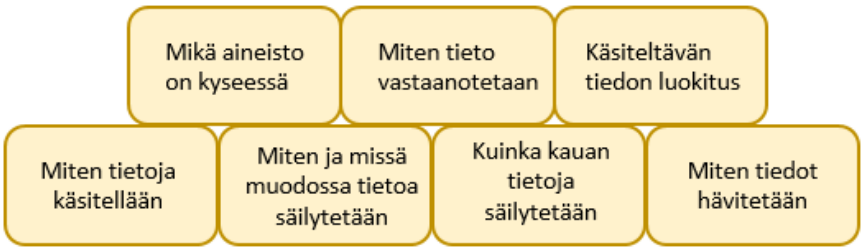
Henkilötietojen käsittely sopimuksen perusteella voi pohjautua esimerkiksi rekisteröidyn osoitteen käsittelyyn verkkokaupassa, jotta tilaus voidaan toimittaa. Työnantajan toimiminen rekisterinpitäjänä ja rekisteröidyn henkilötietojen käsittely työsuhteessa on myös eräs esimerkki, jotta työsopimus saadaan täytäntöön. Tämän perusteella voidaan käsitellä palkka- ja tilitietoja ja sen myötä maksaa rekisteröidylle palkkaa. Työntekijän henkilötietojen käsittely ei perustu kuitenkaan sopimukseen, vaan työnantajan muihin oikeuksiin ja velvoitteisiin. (Hanninen ym. 2017, 30.)

Hannisen ym. (2017, 30) mukaan oikeutettu etu on toinen yleinen tapa käsitellä asiakkaan ja työntekijän tietoja sopimusperusteen lisäksi. Käsittely on lainmukaista, mikäli rekisteröity on esimerkiksi rekisterinpitäjän asiakas tai alainen. Tietosuoja-asetuksessa (679/2016, 6.artikla) säädetään käsittelyn olevan tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi.

Oikeusministeriön (2017, 19—20) mukaan oikeutetun edun mukainen käsittely ei kuitenkaan ole sallittua niissä tilanteissa, missä syrjäytetään rekisteröidyn perusoikeudet sekä -vapaudet, esimerkkinä kun kyseessä on lapsi. Tämän arvioiminen jää rekisterinpitäjien ja kolmansien osapuolien vastuulle, sillä asetuksen myötä tietosuojalautakunnan lupatoimivalta poistuu. Käsittelyn lainmukaisuutta kuitenkin arvioidaan viime kädessä valvontaviranomaisen tai tuomioistuimen toimesta.

2.3.7 Tietojen käsittelyn dokumentointi

Männistön (2017, 21) mukaan on dokumentoitava, miten tietoja käsitellään. Käsittelyn dokumentoinnin tulee sisältää ainakin seuraavat kohdat: miten ne viedään järjestelmään, mitä tietoa tuotetaan, mihin ja miten tietoa luovutetaan sekä mihin tieto arkistoidaan. Dokumentoinnista tulee käydä ilmi myös se, miten ja missä muodossa tietoa säilytetään. Tiedon säilytysajat ja kuvaus siitä, miten tiedot jaetaan vastaanottajille sekä hävitetään, tulee myös sisältyä dokumentointiin. Palkka-aineistossa säilytysajat ovat pääsääntöisesti kirjanpidon säilytysaikojen mukaiset. Kuvassa 7 tiivistetään asiat, jotka tulee käydä läpi ja dokumentoida palkkahallinnon prosesseja kartoitettaessa.



Kuva 7. Tietojen käsittelyn dokumentointi (Männistö 2017, 21).

2.3.8 Prosessien ja ohjelmien kartoitus

Männistön (2017, 20—21) mukaan yrityksen prosessit, joissa käsitellään henkilötietoja, on kartoitettava ja asetusta tulee noudattaa niin automaattisessa, sähköisessä kuin manuaalisessakin käsittelyssä. Kartoituksessa asiaa tulee lähestyä riskiperusteisesti eli arvioida, mikä riskin suuruus on, eli kuinka suurta haittaa vuoto aiheuttaa rekisteröidylle, jos tiedot häviävät tai vuotavat, ja kenen luonnollisen henkilön eli rekisteröidyn tietoja käsitellään. Riskin suuruus määräytyy sen mukaan, ovatko vuotaneet tiedot

esimerkiksi rekisteröidyn yhteystiedot vai esimerkiksi lääkärintodistus tai henkilötunnus.

Prosessit on läpikäytävä ja kuvattava sekä dokumentoitava arkistoitavat aineistot ja niiden säilytysajat. Tietoturvanäkökulma huomioiden on kuvattava, mikä aineisto on kyseessä sekä yksilöitävä prosessissa olevat aineistot. Kuvauksessa tulee käydä läpi, miten tieto vastaanotetaan eli miten se saadaan rekisteröidyltä tai muulta taholta. Käsiteltävät tiedot tulee luokitella joko normaaleiksi henkilötiedoiksi, arkaluonteisiksi tiedoiksi tai tiedoiksi, jotka eivät sisällä henkilötietoja. Erityistä huomiota tulee kiinnittää varsinkin arkaluonteisten henkilötietojen käsittelyyn. Palkka- ja henkilöstöhallinnossa käsitellään paljon terveys- ja ay-jäsenyystietoja, jotka on säilytettävä erillään muista tiedoista erityistä varovaisuutta ja huolellisuutta noudattaen. (Männistö 2017, 21.)

Lisäksi Männistön (2017, 21) mukaan yrityksen tulee selvittää käytettävien ohjelmien ja palvelinten tietoturvallisuuden taso. Prosessikuvaukseen on hyvä lisätä mainինta myös siitä, miten tietoturva on testattu. Nykypäivänä useita järjestelmiä käytetään pilvipalveluja, joten järjestelmän toimittaja on tietosuoja-asetuksen mukaan tietojen käsittelijä, mikäli toimittajan henkilökunnalla on mahdollisuus päästä käsiksi tietoihin. Jos näin on, tulee tietojen käsittelystä tehdä sopimus, johon on hyvä liittää järjestelmän toimittajan selvitys turvatoimista.

Ohjelmia, joiden tietoturva on käytävä läpi ja dokumentoitava toimittajien turvatoimet:
- HR-ohjelma
- palkkaohjelma
- työajanseurantaohjelma
- arkistointijärjestelmät
- muut järjestelmät, joihin tietoja luovutetaan (Männistö 2017, 21).

Seuraavassa luvussa käsitellään palkanlaskennan prosessia, joka muodostaa tietosuoja-asetusta koskevan luvun kanssa tämän opinnäytetyön tietoperustan. Palkanlaskennan prosessia käsitellään aluksi yleisellä tasolla eikä asiaa lähestytä juurikaan tietosuoja-asetuksen pohjalta. Lukujen sisällöissä on kuitenkin pyritty huomioimaan tietosuoja-asetuksen kannalta tarpeelliset asiat, esimerkiksi arkistointiin paneudutaan erillisen luvun (3.3) muodossa.

3 PALKANLASKENNAN PROSESSI

Tässä luvussa perehdytään siihen, miten palkanlaskennan kokonaisprosessi toimii ja mistä saadaan tarvittavat tiedot sen prosessin toteuttamiseksi. Lisäksi pyritään selvittämään, mitä tietoa palkanlaskennassa tarvitaan sekä mitä tietoa missäkin saa näkyä, ja kuka sitä saa käsitellä. Tässä luvussa pyritään sivuamaan sitä, miten tuleva EU:n yleinen tietosuoja-asetus vaikuttaa palkanlaskentaan, tulosten esittelyn kohdassa kuitenkin paneudutaan tähän syvällisemmin. Tavoitteena on saada teoriaosuuksista yhtenäinen ja laadukas pohja tarkistuslistan laatimiselle sekä tutkimuksen loppuun saattamiselle.

Lahden ja Salmisen (2014, 137) mukaan tarve palkanlaskentaprosessille syntyy, kun yrityksessä työskentelee työntekijöitä, joille maksetaan korvaus tehdystä työstä. Palkkausta säädellään lainsäädännön ja erilaisten sopimusten avulla sekä palkanlaskentaan liittyvät verotus, erilaiset vakuutus- ja sosiaaliturvamaksut sekä työ- ja loma-ajan käsittely. Ennakkoperintäasetuksessa (1124/1996) säädetään yritysten velvollisuudesta pitää palkkakirjanpitoa aina, kun palkkoja maksetaan.

Palkanlaskennan perustietojen ylläpitäminen, palkanlaskenta, palkasta perittävien erien tilitys viranomaisille ja palkkakirjanpidon arkistointi ovat esimerkkejä palkkahallinnon työtehtävistä. Todistusten ja hakemusten laatiminen sekä toimittaminen eri sidosryhmille, kuten Kelalle, ulosottovirastolle sekä vakuutusyhtiölle kuuluvat myös palkkahallinnon tehtäviin. (Syvänperä & Turunen 2014, 13.)

Syvänperän ja Turusen (2014, 14—17) mukaan teknisen osaamisen lisäksi palkanlaskijan on tunnettava lait ja säädökset, sekä on osattava käyttää tietokone-ohjelmistoja. Lain ja säädösten muutoksista on oltava selvillä, sillä vanhentuneen lainsäädännön mukaan toimiminen voi vaikuttaa olennaisesti palkan suuruuteen. Palkanlaskennan kannalta keskeisiä säädöksiä ovat lainsäädäntö, työehtosopimukset, työsopimukset, työpaikalla syntyneet käytännöt, muut sopimukset sekä työnantajan määräykset.

Keskeisiä lakeja palkanlaskennassa ovat esimerkiksi työsopimuslaki (55/2001), työaikalaki (605/1996) ja vuosilomalaki (162/2005), sekä laki yksityisyyden suojasta työelämässä (759/2004) ja ulosottolaki (37/1895). EU:n yleinen tietosuoja-asetus (GDPR 679/2016) tulee hyvin todennäköisesti myös olennaiseksi osaksi suoraan sovellettavaa lainsäädäntöä palkanlaskennassa, lainsäädäntö on kuitenkin toistaiseksi kesken, joka vaikeuttaa varsinaista valmistautumista.

Määräykset ja säädökset muodostuvat hierarkkisesti, ja mikäli säännösten välillä on ristiriitoja tai epäselvyyksiä, menetellään etusija- ja edullisemmuusjärjestyksen mukaan. Etusijajärjestys tarkoittaa sitä, ettei hierarkki-

sesti alin säädös voi mennä ylemmän edelle, eli esimerkiksi harvoin työnantajan määräys voi mennä lainsäädännön edelle. Palkanlaskijoiden täytyy kuitenkin tietää, milloin jostakin asiasta on säädetty erityislailla, joka menee yleislain edelle. Esimerkiksi työaikalaki (605/1996) on esimerkki yleislaista, jota kuitenkin täsmennetään lailla nuorista työntekijöistä (998/1993), joka on erityislaki. Edullisemmuusjärjestys puolestaan velvoittaa työnantajan noudattamaan sellaista normia, joka on työntekijälle edullisin ja suotuisin vaihtoehto. (Syvänperä & Turunen 2014, 14—17.)

Palkka määräytyy yleensä alalla vallitsevan yleissitovan työehtosopimuksen mukaan. Palkan suuruuteen vaikuttavat esimerkiksi työtehtävien vaativuus, työntekijän henkilökohtaiset ominaisuudet sekä paikkakuntakohtaiset kalleusluokitukset. Työehtosopimuksissa työtehtävät on luokiteltu erilaisiin vaativuustasoihin, joista jokaiseen on määritelty erisuuruinen palkka. (Hakonen, Eklund & Roos 2016, 183.)

Tyypillisimmin työsopimuksissa sovitaan maksettavan tunti- tai kuukausipalkkaa. Kuukausipalkkaisilla palkkakausi on useimmiten kalenterikuukauden mittainen ja tuntipalkkaisilla puolestaan joko kahden viikon tai kuukauden mittainen. Pääsääntöisesti palkanmaksupäivä on kuun viimeinen päivä, mutta esimerkiksi KuntaPro maksaa palkkoja noin neljä kertaa kuukaudessa. (Hakonen ym. 2016, 184.)

3.1 **Palkanlaskennan prosessikuvaus**

Lahden ja Salmisen (2014, 138) mukaan palkanlaskennan prosessi itsessään on paljon laajempi kokonaisuus kuin pelkkä palkan laskenta ja palkan maksaminen. Kokonaisprosessissa tulee huomioida myös yrityksen ulkopuolelle ulottuvat prosessit, joita ovat esimerkiksi työntekijöiden, esimiesten ja palkkahallinnon toimenpiteet, taloushallinnon raportoinnin tarpeet sekä viranomaisilmoitukset.

KuntaPron palkanlaskennan prosessi on melko yksinkertainen, sillä KuntaPro on ulkoistettua palkkahallintoa hoitava organisaatio. Asiakkaat tallentavat sähköisesti tiedot uuden työsuhteen tiedoista, muutokset palvelussuhteeseen sekä tehdyt tunnit, mikäli kyseessä on tuntipalkkainen työntekijä ja näin on erikseen asiakkaan kanssa sovittu. Aineiston vastaanottamisen jälkeen palkkasihteeri tekee materiaalin teknisen tarkistuksen, jossa tarkistetaan, että kaikki tarvittavat tiedot löytyvät ja kentät on täytetty oikein. Lomakkeelta tulisi löytyä henkilötietojen lisäksi esimerkiksi tiedot tiliöinneistä, kustannuspaikoista, toiminnoista sekä verotustiedoista. Mikäli lomake on virheellinen, palkkasihteeri palauttaa lomakkeen takaisin esimiehille korjattavaksi ennen kuin se siirretään järjestelmään. (Haastattelu 1.)

Periaatteessa palkkasihteeri ei siis ota kantaa tai tee muutoksia lomakkeen sisältöön. Palkat maksetaan sen mukaan, mitä esimies ilmoittaa. Kun pal-

velussuhde etenee, tehdään palveluaikalaskenta. Asiakas tekee päätöksen, ja KuntaPro hoitaa maksatuksen palveluaikalaskennasta aikaisemman työkokemuksen perusteella, tarvittaessa voidaan tehdä takautuva maksatus. Kun muutokset on päivitetty järjestelmään, hyväksyy palkkasihteeri sen palkanlaskentaan ja aloitetaan ajotoimenpiteet. (Haastattelu 1; Liitteet 1 & 2.)

Lahden ja Salmisen (2014, 140) mukaan automatisoidussa palkanlaskennan prosessissa varsinainen palkanlaskenta on ainoastaan palkanlaskentaohjelmistolla tehtävä ajo tai suoritus, jonka perusteella ohjelmisto laskee automaattisesti ennakonpidätyksen, muut tehtävät vähennykset sekä työntekijälle maksettavan nettopalkan. Tarvittavat tarkistusrutiinit ja poikkeustilanteiden käsittelyt pystytään tekemään palkanlaskentaohjelmiston käyttöliittymän kautta, joten paperitulosteita ei useimmiten tarvita.

Haastattelun 1. mukaan jokaisessa palkanlaskennan prosessin osassa käsitellään henkilötietoja, mutta massat ovat niin isoja, etteivät henkilöt ja asiat kohtaa varsinaisessa työssä, sillä palkanlaskennassa toimitaan enimmäkseen kustannuspaikkojen ja henkilönumeroiden avulla, joten tietosuojan toteutumisen kannalta ei pitäisi olla ongelmaa. Ei siis ole tilannetta, jossa henkilön tiedot ja asiat oikeastaan yhdistyisivät.

Kun KuntaProlla palkkasihteeri on tallentanut palkkakauden muutokset järjestelmään, vastuuajaja käynnistää ajon aikataulun mukaisesti. Ajot tehdään pareittain ja kerrallaan on kaksi vastuuajajaa. Valmisteluajo suoritetaan tavallisesti seuraavana aamuna aineistonjättöpäivästä, ja tämän jälkeen vastuuajaja lähettää valmisteluajon virhelistat palkkasihteereille tarkistettavaksi. Virheiden tarkistukseen ja korjaukseen on useimmiten noin kolme päivää aikaa ennen varsinaista palkka-ajoa. Palkkojen tarkistusprosessi toteutetaan tiettyihin tarkistuspisteisiin luotujen raporttien avulla, joista pyritään havaitsemaan virheet, eikä henkilö henkilöltä tarkistuksia enää juurikaan tehdä. Näin pyritään tekemään palkanlaskennasta ”nimetöntä” ja tehokkaampaa. Poikkeuksena tietysti erityistilanteet, jotka vaativat lisäselvitystä, jolloin joudutaan paneutumaan tarkemmin henkilön tietoihin. (Haastattelu 1.)

Palkkoja ajetaan noin neljä kertaa kuukaudessa. Tarkastusten jälkeen voidaan suorittaa lopullinen palkka-ajo, jossa ajetaan palkkalaskelmat toimittajalle, palkat kirjanpitoon sekä palkat pankkiin. Lopullisen palkka-ajon jälkeen luodaan asiakkaalle raportti maksetuista palkoista ja täyttyvistä lisistä sekä välitetään raportti täyttyvistä vuosisidonnaisista lisistä eteenpäin palkkasihteereille. Ajoketjuun kuuluu myös ay-jäsenmaksun, puolueveron ja ulosoton tilitykset. (Liite 3.) Lisäksi palkanlaskennan prosessiin liittyy palkanlaskennan viranomaisvelvoitteita, joita ovat esimerkiksi tilitykset, eläkeilmoitukset ja vuositilitykset (Syvänperä & Turunen 2014, 145).

3.2 Palkanlaskennan vuosikello

Luvun 3 alussa käsitellään lyhyesti palkkavuoden toistuvia rutiineja. Tässä alaluvussa käydään läpi vuosittaisella tasolla palkkavuoden rutiineja nimenomaan palkkasihteerin näkökulmasta.

Tammikuussa tehdään menojäämäajo normaalien palkka-ajojen ja muiden tehtävien lisäksi. Menojäämäajolla tarkoitetaan sitä, että edellisen vuoden puolella aiheutuneet menot tulee saada kirjattua edellisen vuoden kuluksi, esimerkiksi vuorotyölisät. Tammi- ja helmikuussa tulee satoja verokortteja, jotka tallennetaan manuaalisesti ja laitetaan mappiin. Uudet verokortit otetaan helmikuussa käyttöön, ja ne tulevat suorasiirtona verottajalta. Muutosverokortit ja uusien palvelussuhteiden verokortit tulevat postitse. (Haastattelu 2.) Tulevaisuudessa pyritään reaaliaikaisempaan verotukseen, jolloin tieto maksetuista palkoista siirtyisi kuukausittain suoraan verottajalle ja päivittyisi palkansaajan tietoihin (Verohallinto 2017).

Maaliskuun lopussa tehdään vuosilomalaskenta ja tarkistetaan lomalaskenta eli tulevan vuoden lomat. Tarkistusten jälkeen lomaoikeudet toimitetaan vielä asiakkaalle tarkastettavaksi. Lomamääräytymisvuosi vaihtuu huhtikuun alussa, joten silloin alkaa kertyä jälleen seuraavalle vuodelle uutta lomaoikeutta, nämä perustuvat työehtosopimuksiin ja vuosilomalakiin. Touko- ja kesäkuussa vastaanotetaan paljon työsopimuksia, sillä kesätyöntekijät aloittavat työnsä. Sopimusten lisäksi verokortteja tulee paljon ja niitä tallennetaan manuaalisesti. Kesäkuussa maksetaan lomarahat palkansaajille omana palkkapäivänään, vakituisille maksetaan kuun puolivälissä ja määräaikaisille kuun viimeinen päivä. Lomarahat tulevat keskitetysti järjestelmän kautta useimmiten kesäkuun palkkojen mukana. Lomarahan maksupäivä on kuitenkin asiakaskohtainen, joten ne voidaan maksaa myös heinä- tai elokuussa. Heinäkuu on melko hiljaista aikaa eikä mitään erityistä kuukausittaisten rutiinitöiden lisäksi ole. (Haastattelu 2.)

Elo-syyskuu on melko työllistävää aikaa ja tällöin ollaan myös paljon yhteyksissä asiakkaaseen. Elokuussa alkaa koulujen ja päiväkotien toimintavuosi, joten uusia sopimuksia saattaa tulla paljon. KuntaPro ajaa paljon koulujen ja päiväkotien työntekijöiden palkkoja, joten sen vuoksi toimintavuoden alulla on merkityksellinen osuus vuosikellossa. Loppuvuosi marraskuun loppuun asti on melko tasaista aikaa, jolloin ei ole mitään ihmeellistä kuukausittaisten rutiinitöiden lisäksi. Joulukuussa aletaan valmistautumaan jo seuraavaan vuoteen esimerkiksi päivittämällä sivukulut, omaishoidon indeksikorotukset ja tarkastellaan tulevan vuoden aikatauluja. Joulukuun viimeinen päivä tehdään lomapalkkavarauksen tarkastus, jossa katsotaan, paljonko varausta on kertynyt ja paljonko on maksamatta. Lisäksi neljännesvuosittain tehdään tilastoja. Tiedot ilmoitetaan tilastokeskukseen tekemällä sähköinen tilastointilomake tilastokeskuksen nettisivuilla. (Haastattelu 2.)

3.3 **Arkistointi palkkahallinnossa**

Palkkahallinnossa syntyy arkistoitavaa materiaalia, joiden säilytysajat ja–tavat vaihtelevat. Tietojen säilyttämiseen, käsittelyn helppouteen, vaivattomuuteen ja oikea-aikaiseen hävittämiseen tulee kiinnittää huomiota. Aineiston arkistoinnista tulee aina tehdä suunnitelma tai ohje, joka määrittää esimerkiksi arkiston sisällön ja sisältää kuvauksen järjestelmästä, jonka avulla seurataan, milloin mitäkin aineistoa hävitetään sekä dokumentoinnin siitä, miten aineisto hävitetään oikealla tavalla. Arkistointisuunnitelmassa tai -ohjeessa tulee olla kuvaus tavoista, joilla huolehditaan, että tietoihin pääsevät käsiksi ainoastaan ne henkilöt, keillä on siihen tarve ja oikeus sekä tieto siitä, mitä menetelmiä arkistoinnissa käytetään. Lisäksi arkistointisuunnitelmasta tai -ohjeesta tulee käydä ilmi, mitkä tiedot ovat sähköisessä ja paperisessa muodossa sekä aineiston arkistointiajat. (Lehtinen 2013.)

Palkkaluetteloita tulee säilyttää aikajärjestyksessä omien arkistointitapojen mukaisesti kaksi vuotta, palkkaluetteloiden jäljennökset riittävät. Työajan seurantaraportteja tulee säilyttää omien arkistointitapojen mukaisesti aikajärjestyksessä kaksi vuotta riippuen viraston tarpeesta. Perimispalkkio- ja toimenpidepalkkiolaskelmia tulee säilyttää aikajärjestyksessä välilehdillä erotettuina 10 vuotta. Henkilöstöasioita koskevien viranhaltijapäätösten säilytysaika määräytyy sisällön mukaan. Työhakemuksia ja CV:tä tulee säilyttää kahden vuoden ajan. (Finlex n.d.)

Asiakirjat, joita ei ole määrätty pysyvästi säilytettäviksi, tulee hävittää niille määrätyn säilytysajan päättyessä siten, että riittävän tietosuojan taso on varmistettu (Arkistolaki 831/1994 § 13). Arkaluonteiset tiedot tulee poistaa rekisteristä välittömästi sen jälkeen, kun käsittelylle ei ole enää perustetta. Käsittelyn tarvetta ja perustetta tulee arvioida vähintään viiden vuoden välein. (HetiL 523/1999 § 12.)

Lahden ja Salmisen (2014) mukaan tositteiden skannaus sähköiseksi on perusteltua ainoastaan silloin, kun tosite on saatu paperilla. Ainoa asiakirja, jota tulee lakisääteisesti säilyttää paperilla, on tasekirja, joten kaikki muu materiaali voidaan arkistoida sähköisesti. Sähköisen arkistoinnin hyötyjä on muun muassa se, että arkistoon pääsee helposti käsiksi ja tietojen hakeminen on nopeaa. Sähköisesti arkistoitujen tietojen tulee olla helposti hyödynnettävissä erilaista raportointia varten, sillä niitä tulee voida siirtää esimerkiksi sähköisesti tietokantajärjestelmiin, Exceliin sekä tarkastusohjelmiin. Sähköisen arkistoinnin tavoite on se, että tositteet olisivat ymmärrettävässä muodossa jo ilman tulostamista.

Lehtisen (2013) mukaan silloin kun on kyse paperiarkistosta, terveydentilatietojen arkistoinnissa tulee olla erityisen tarkka, sillä tietojen suojaamisvelvoite määrää esimerkiksi lääkärintodistusten säilyttämisestä lukitussa tilassa ja erillisissä kansioissa. Sähköisessä arkistossa aineistosta tulee huo-

lehtia esimerkiksi tietojärjestelmäsuojauksin, käyttäjätunnuksin ja salasanoin niin, että terveydentilaa koskeviin tietoihin pääsee vain nimetyt henkilöt.

Ulkoistettua palkkahallintoa hoitavien organisaatioiden tulee huomioida, ettei asiakkaan aineiston arkistointia tule ottaa hoitaakseen oma-aloitteisesti, vaan aineiston arkistoinnista tulee tehdä aina asiakkaan kanssa kirjallinen sopimus ja asiakkaalle tulee selventää omat velvoitteensa arkistoinnissa. Ulkoistamistapauksissa rekisterinpitäjän lukuun henkilötietoja käsittelevien tulee noudattaa huolellisuusvelvoitetta, suojaamisvelvoitetta sekä erillään säilyttämisen velvoitetta. Huolellisesti tehty ja käytännössä toimiva arkistonhallintajärjestelmä sekä arkistointisuunnitelma ovat tärkeä pohja hyvälle arkistoinnille, joka täyttää kaikki lait niin sähköisessä kuin paperisessakin arkistoinnissa. (Lehtinen 2013.)

Kokonaisuudessaan palkanlaskentaan liittyy monia erilaisia prosesseja, joista jokaisessa käsitellään henkilötietoja. Nykypäivänä palkka-ajoissa ei kuitenkaan yhdisty nimet ja tiedot, sillä palkka-ajo on niin automatisoitu toiminto. Tietosuoja-asetuksen voimaantullessa tulee kuitenkin kiinnittää huomiota jokaisessa prosessin vaiheessa huomiota siihen, onko henkilötietojen käsittely kussakin tilanteessa tarpeellista. Arkistoinnin suhteen tulee myös olla tarkka ja perehtyä jokaisen arkistoitavan tiedon tarpeellisuuteen. Tietojen käsittelystä on kerrottu enemmän luvussa 2, mutta kokonaisuudessaan tietoperusta tutkimuksen toteuttamiselle muodostuu luvuista kaksi ja kolme.

Seuraavassa luvussa perehdytään siihen, mitä tutkimusmenetelmiä tässä opinnäytetyössä on käytetty sekä miten tutkimus on toteutettu. Tietosuoja-asetusta koskevan luvun 2 ja palkanlaskennan prosessia koskevan luvun 3 avulla on laadittu teemahaastattelun runko. Teemahaastattelun rungon muodostuksessa myös tutkimusmenetelmistä kertova luku 4 oli olennainen osa kokonaisuutta.

4 TUTKIMUSMENETELMÄT JA TOTEUTUS

Luvussa neljä kuvataan tutkimuksen toteutus sekä empiirisessä tutkimuksessa käytetyt tutkimus- ja tiedonkeruumenetelmät. Opinnäytetyön toteuttamistavaksi valikoitui toiminnallinen opinnäytetyö, jonka konkreettinen tuotos on tarkistuslista (Liite 5) toimeksiantajan käyttöön. Toimintatutkimuksesta, teemahaastattelusta, osallistavasta havainnoinnista sekä empiirisen tutkimuksen toteutuksesta on omat alalukunsa, jotka muodostavat perustelut tutkimusmenetelmien valinnalle. Opinnäytetyö toteutetaan toimeksiantona KuntaPro Oy:lle ja teemahaastattelut suoritettiin tuotantopäällikölle sekä palkkasihteerille.

4.1 Toimintatutkimus

Toimintatutkimuksessa ollaan kiinnostuneita siitä, miten asioiden pitäisi olla tulevaisuudessa eikä ainoastaan siitä, miten ne ovat tällä hetkellä (Ojasalo, Moilanen, Ritalahti 2014, 58). Keskeistä on toiminnan ja tutkimuksen vuorovaikutus sekä se, että tutkimuksella pyritään saamaan aikaan välitöntä sekä käytännöllistä hyötyä. Teoriaa ja käytäntöä ei useimmiten pidetä erillisinä, vaan saman asian eri puolina. Toimintatutkimuksen päämäärä ei ole ainoastaan tutkiminen, vaan myös toiminnan samanaikainen kehittäminen. (Heikkinen 2007, 196—197.) Toimintatutkimus on yleisnimitys niille toimintatavoille, joiden avulla pyritään tavalla tai toisella vaikuttamaan tutkimuskohteeseen (Eskola & Suoranta 1998, 128).

Toimintatutkimuksen tavoitteena on vahvasti käytännön kautta löytää ratkaisut organisaation ongelmiin, tuottaa uutta tietoa ja luoda ymmärrystä kyseiseen ilmiöön. Tutkimuksen tärkeimpiä kulmakiviä ovat esimerkiksi aktiviinen vuorovaikutus tutkijan ja tutkittavan välillä, käytännönläheisyys sekä ongelmakeskeisyys. Toimintatutkimus soveltuu hyvin esimerkiksi työmenetelmien kehittämistyöhön, sillä sen avulla pyritään uudenlaisen toiminnan ymmärtämiseen. (Ojasalo ym. 2014, 58—59.)

Ojasalon ym. (2014, 60—61) mukaan toimintatutkimuksessa vuorottelee suunnittelun, toiminnan ja toiminnan arvioinnin vaihe. Tutkimuksen alussa valitaan päämäärät tai määritellään tutkimusongelma. Sitten perehdytään alan kirjallisuuteen ja mahdollisiin aiemmin aiheesta tehtyihin tutkimuksiin. Aineistoihin tutustumisen jälkeen voidaan täsmentää tutkimussuunnitelmaa sekä tutkimuksen tavoitteita ja sisältöä. Kun tietämystä aiheesta alkaa olla riittävästi, siirrytään analysoimaan saatuja aineistoja, kehitetään tutkimussuunnitelmaa, muokataan oikeaan suuntaan, tarkennetaan tutkimusongelmia ja päämääriä sekä kokeillaan käytännössä. Kehittäjän roolissa olennainen ero muihin tutkimusmenetelmiin on se, että toimintatutkimuksessa tutkimuksen tekijä on aina ryhmän aktiivinen jäsen.

Toimintatutkimuksessa tutkimusaineistoa on mahdollista kerätä esimerkiksi haastatteluilla, kyselyillä tai havainnoimalla. Usein käytetään myös

toimijoiden yhteisiä keskusteluita. Tärkeää on, että tutkija käyttää osallistavia menetelmiä ja pääsee tällä tavalla todennäköisesti syvemmälle toimeksiantajayritykseen. Tällöin saadaan syvempi ja erilainen näkökulma verrattuna siihen, että tutkimus pohjautuisi ainoastaan teoriatiedon varaan. (Ojasalo ym. 2014, 58—62.)

4.2 **Teemahaastattelu**

Teemahaastattelu on ennalta suunniteltu vuorovaikutustilanne, jossa haastattelu kohdennetaan tiettyihin teemoihin. Haastattelija on perehtynyt etukäteen tutkimuksen kohteeseen niin teoriassa kuin käytännössä. Haastattelutilanteessa haastattelija johtaa tilannetta ja pyrkii saamaan luotettavaa, olennaista ja tarpeellista tietoa tutkimusongelmien kannalta. (Hirsjärvi & Hurme 2001, 42—47.)

Hirsjärven ja Hurmeen (2001, 47—48) mukaan teemahaastattelu on puolistrukturoitu menetelmä, jossa käsiteltävät teemat ovat kaikille samat. Teemahaastattelu etenee useimmiten yksityiskohtaisten kysymysten sijasta keskeisten teemojen avulla. Muutamia kysymyksiä voidaan myös etukäteen laatia ja niiden järjestystä voidaan vaihdella eikä haastateltavan vastaukset ole sidottu vastausvaihtoehtoihin, vaan haastateltava saa vastata omin sanoin. Ominaista on, etteivät kaikki haastattelun näkökulmista ole ennalta määriteltyjä.

Teemahaastattelussa on hyvä keskittyä haastatteluteemojen suunnitteluun. Tutkijan tulee harkita, mitkä aihepiirit ovat olennaisia haastattelussa, jotta saadaan vain tarpeellista tutkimustietoa. Haastattelurunkoa laatiessa tulee tehdä teema-alueluettelo yksityiskohtaisen kysymysluettelon sijaan, sillä ne ovat todellisuudessa tarkempia ja monipuolisempia kuin yksittäiset kysymykset ja ongelmat. Haastattelutilanteessa teema-alueita voidaan kuitenkin tarkentaa kysymyksillä. (Hirsjärvi & Hurme 2001, 66.)

4.3 **Osallistuva havainnointi**

Havainnointi on hyödyllinen kehittämistyön menetelmä, sillä sen avulla päästään tarkkailemaan ihmisten käyttäytymistä luonnollisessa toimintaympäristössään ja päästään selville siitä toimivatko ihmiset siten, miten sanovat toimivansa. Havainnointi on järjestelmällistä ja etukäteen suunniteltua, mihin havainnointi kohdistuu. (Ojasalo ym. 2014, 114—115.)

Tässä tutkimuksessa havainnointia ei käytetä kovinkaan olennaisena osana tutkimusta, sillä havainnoinnin merkitys on lähinnä se, että seurataan työntekijöiden toimintaa tietosuojan kannalta.

4.4 **Empiirisen tutkimuksen toteutus**

Tutkimus toteutetaan aluksi perehtymällä EU:n yleiseen tietosuoja-asetukseen sekä palkanlaskennan prosessiin alan kirjallisuuden ja muiden luotettavien lähteiden pohjalta. Luvut tietosuoja-asetuksesta ja palkanlaskennan prosessista muodostavat opinnäytetyön tietoperustan. Tietoperustan avulla laaditaan alustava tarkistuslista, joka käydään työn alkuvaiheessa läpi toimeksiantajayrityksen tuotantopäällikön kanssa. Tapaamisessa kartoitetaan, vastaako sen hetkinen tarkistuslista sekä opinnäytetyö kokonaisuudessaan toimeksiantajayrityksen tarpeita vai löytyykö jotain muutoksen tarpeita.

Kun työtä on muutettu molempien osapuolien tarpeita vastaavaksi, laaditaan tietoperustan ja menetelmäkirjallisuuden avulla teemahaastatteluille runko. Teemahaastattelun pääteemat ovat EU:n yleinen tietosuoja-asetus sekä palkanlaskennan prosessi. Haastattelut nauhoitetaan ja sen jälkeen litteroidaan kirjalliseen muotoon. Haastattelujen avulla pyritään selvittämään asetukseen valmistautumisen nykytila sekä saamaan lisäinformaatiota palkanlaskennasta ja sen prosesseista. Teemahaastatteluita käytetään lähteinä myös palkanlaskennan prosessin teoriassa sekä tutkimuksen tuloksissa. Haastattelut suoritettiin Kangasalan ja Tuusulan tuotantopäällikölle 22.3.2018 ja Tuusulan palkkasihteerille 28.3.2018.

Teemahaastatteluiden suorittamisen jälkeen opinnäytetyötä työstetään eteenpäin tehtyjen havaintojen ja tulosten pohjalta. Tietyin väliajoin työtä käydään läpi niin opinnäytetyön ohjaajan kuin toimeksiantajayrityksen tuotantopäällikön kanssa. Tällöin tehdään tarvittavia muutoksia, jotta pystytään vastaamaan mahdollisimman hyvin toimeksiantajayrityksen tarpeisiin. Lopullinen tuotos eli tarkistuslista kootaan pohjautuen teoriaan (GDPR 679/2016 ja palkanlaskennan prosessi) sekä tutkimuksen aikana tehtyjen haastatteluiden ja havaintojen pohjalta tehtyihin huomioihin. Tarkistuslista lisätään varsinaisen opinnäytetyön liitteeksi (Liite 5). Seuraavassa luvussa käydään tarkemmin tutkimuksen tuloksia läpi.

5 TUTKIMUSTULOKSET

Tässä luvussa käsitellään KuntaPron tietosuoja-asetukseen valmistautumisen nykytilaa, tarvittavaa dokumentaatiota, mahdollisia parannusehdotuksia sekä tuodaan esiin lopullisen tuotoksen eli tarkistuslistan (Liite 5) sisältö tiivistetysti. Tietosuoja-asetuksen sisältöön, arkaluonteisten tietojen käsittelyyn sekä mahdollisiin tietosuoja-asetuksen tuomiin muutoksiin ja palkanlaskennan prosessiin liittyviin alaongelmiin löytyy vastaukset tietoperustan toisesta ja kolmannesta luvusta, joten niitä ei käsitellä tässä luvussa.

KuntaPron valmistautumisen tasoa arvioidessa on hyödynnetty kahta tehtyä teemahaastattelua sekä esimerkiksi organisaation sisäisiä materiaaleja. Tietoperustaa käytetään myös pohjana tuloksissa, erityisesti tarkistuslistan laatimisessa.

5.1 Tietosuoja-asetukseen valmistautumisen aloitus ja nykytila

KuntaProlla aloitettiin tietosuoja-asetukseen valmistautuminen hyvissä ajoin jo kesällä 2016. Tällöin aloitettiin tiedon hankkiminen sekä erilaiset koulutukset, joista esimerkkinä tietosuojavastaavan koulutukset. Alkuvuodesta 2017 teetettiin vaatimustenmukaisuusanalyysi, joka tuotti tehtävälistan, jota on jalostettu tarkemmiksi tehtäviksi. Tehtävät muodostavat sisällön hankkeen eri kehitysprojekteille. (KuntaPro 2017 b.)

Syksyllä 2017 perustettiin tietosuojaorganisaatio, jossa on edustaja jokaiselta palvelualueelta sekä nimettiin tietosuojavastaava. Tämän jälkeen alettiin tehdä asiakkaiden kanssa tietosuojasopimusliitettä, johon palkattiin avuksi myös konsultteja, sillä asiakkaita on paljon. Työ on edelleen kesken, mutta on henkilöstöhallinnon osalta pisimmällä, joka on hyvä asia, sillä palkkahallinnossa henkilötietoja käsitellään eniten. Henkilöstö on suorittanut aiemmin koulutuksen tietoturvasta, ja henkilöstön koulutussuunnitelmaan tarkennettiin tietoturvakoulutus vuosittaiseksi sekä lisättiin kaksi jatkokoulutusta koskien tietosuojaa. Jokaisen tulee suorittaa tietosuojakoulutukset hyväksytysti maaliskuun loppuun mennessä ja esimies valvoo suoritusten täyttymistä. (Haastattelu 1.)

Helmikuun 2018 alussa johtoryhmä hyväksyi ja julkaisi KuntaPro-konsernin tietosuojapolitiikan ja siihen liittyvän koulutuksen. Tietosuojapolitiikkakoulutuksen avulla pyritään siihen, että jokainen työntekijä saa yleiskuvan KuntaPron tietosuojapolitiikasta ja osaa huomioida tietosuojaan liittyviä asioita päivittäisessä työssään. Kaikkien tulee suorittaa koulutus 25.5.2018 mennessä. Tietosuojapolitiikassa kuvataan henkilöön liittyvien henkilötietojen tai muiden luottamuksellisten tietojen käytön periaatteet ja menetelmät organisaatiossa. (KuntaPro 2018 c.)

Tietosuoja-asetus velvoittaa entistä tarkempaan henkilötietojen käsittelyyn, johon KuntaPro on valmistautunut melko hyvin. Tiedon saanti on rajattu esimerkiksi kulkuluvin eikä tiloihin pääse, sillä ovet ovat aina lukossa. Asiakasta mennään vastaan heti ovelle ja saatetaan takaisin tapaamisen päättyessä. Missään vaiheessa ulkopuoliset vierailijat eivät ole ilman valvontaa tiloissa, joissa on tietoja, jotka eivät kaikille kuulu. Talon sisällä eri osastojen välistä pääsyä tietoihin on myös rajattu erilaisin käyttöoikeuksin. Palkkasihteerit näkevät vain palkkasihteerien tietoja ja siitä tulee huolehtia, ettei avokonttorissa esimerkiksi taloushallinnon puolella ole edes mahdollisuutta nähdä, esimerkiksi ulosottotietoja tai muita arkaluontoisia tietoja. Sen vuoksi tulisikin aina lukita kaapit, joissa arkaluontoista tietoa säilytetään. (Haastattelu 2.)

Kulkulupien, käyttöoikeuksien ja turvatulostuksen lisäksi perehdytyksellä on suuri merkitys tietosuojan toteutumisessa. Työsuhteen alkaessa tehdään sopimus, jossa sitoudutaan käsittelemään henkilötietoja lainmukaisesti, tämän lisäksi on kuitenkin olennaista, että uusi henkilö perehdytetään nopeasti siihen, miten henkilötietoja tulee käsitellä käytännön työtehtävissä ja miten saavutetaan riittävä tietosuojan taso. (Haastattelu 2.)

KuntaProlla on käytössä tiketti-järjestelmä, jonka kautta viestitään asiakkaiden kanssa. Myös puheluista ja soittopyynnöistä tehdään tiketti, joten kaikki viestintä on dokumentoitua, joka helpottaa jälkikäteen käytyjen keskusteluiden todentamista. Tiketti-järjestelmän kautta ei kuitenkaan saa ilmoittaa arkaluonteisia henkilötietoja, vaan se on ainoastaan väline yhteydenpitoon. (Haastattelu 2.) Tietosuoja-asetuksen (679/2016) viidennen artiklan mukaan rekisterinpitäjän tulee pystyä osoittamaan noudattavansa asetusta, johon dokumentointi on hyvä keino. Samaisessa artiklassa säädetään kuitenkin myös siitä, että henkilötietojen tulee olla asianmukaisia, olennaisia, rajoitettuja, sekä niitä tulee kerätä ja arkistoida ainoastaan siihen tarkoitukseen, mikä on tarpeellista. Dokumentoinnin laajuuteen ja säilytysaikoihin olisi hyvä jatkossa kiinnittää huomiota.

KuntaProlla kaikki palkanlaskennan prosessit on kuvattu, sekä niitä on kartoitettu tietosuoja-asetuksen voimaan tulon vuoksi. Kaikki prosessit eivät ole kuitenkaan pysyneet yleisellä tasolla sellaisena kuin aiemmin on kuvattu ja niitä on jo osittain päivitettykin. Eräs löydös kartoituksia tehdessä oli se, ettei prosessikuvauksissa ole kuvattu sitä, millaisia henkilötietoja prosessin eri vaiheissa käsitellään. Sairauspoissaolojen käsittelyn tai ylityölaskentaan liittyvät prosessikuvaukset ovat esimerkkejä pienemmistä prosesseista, jotka eivät ole vielä ajan tasalla. Prosessien kirjallinen avaaminen ja analysointi ovat tarpeellinen toimenpide, jotka tulisi huolehtia kuntoon. (Haastattelu 1.)

KuntaPro on kuvannut ja kartoittanut myös liittymät, mutta kuvaukset ovat tällä hetkellä eri paikkoihin ripoteltuna, vaikka niiden tulisi löytyä helposti samasta paikasta. Toimet on aloitettu, mutta ennen kuin tietosuoja-

asetus astuu voimaan, tulisi huolehtia liittymien kuvausten siirtämisestä samaan paikkaan, josta ne ovat helposti löydettävissä. (Haastattelu 1.)

Tällä hetkellä pitkät sairauspoissaolotodistukset (9+1 sairauslomapäivää) toimitetaan KuntaProlle, jotta tiedetään hakea Kelasta korvausta työnantajalle. Sairauspoissaolotodistus sisältää kuitenkin paljon arkaluontoisia tietoja ja palkanlaskentaan riittää pelkkä poissaoloaika ja syykoodi, joten parempi ratkaisu saattaisi olla se, ettei sairauspoissaolotodistuksia toimitettaisi KuntaProlle ollenkaan, vaan asiakas toimittaisi ne suoraan Kelaan tai työterveyteen ilman välikäsiä. Sairauspoissaolojen syyt tai diagnoosit eivät kuulu palkanlaskentaan, joten siinä mielessä prosessia pyritään kehittämään yksityisyyttä paremmin suojaavaksi. Asiakkaan, esimiehen tai henkilöstöhallinnon tulee ottaa kantaa sairauspoissaolon palkallisuuteen ja yhdenjaksoisuuteen. (Haastattelu 2.)

KuntaPron henkilöstön intranetissä on infopankki-välilehden alla tietosuojaa koskeva osio, josta jokainen henkilöstön jäsen voi helposti etsiä tietosuoja-asetukseen ja ylipäätään tietosuojaan liittyviä tietoja. Etusivulla on kello, josta käy ilmi, kuinka paljon on aikaa tietosuoja-asetuksen voimaantuloon sekä ohjeistusta ja selosteita moniin olennaisiin asioihin. Erityisen hyvää sivustossa on se, että kuka tahansa henkilöstön jäsen pääsee helposti selville esimerkiksi siitä, mikä tietosuoja-asetus on sekä millä mallilla valmistautuminen tietosuoja-asetukseen KuntaProlla on. Etusivulla on myös selkeä kuva tietosuojan vuosikellosta, josta käy kaikki olennaisimmat toimet ilmi aikatauluineen. (KuntaPro 2018 c.)

Vielä on kuitenkin tehtävää ja opinnäytetyöllä on siinä mielessä merkityksellinen rooli, jotta saadaan viitettä siitä, mitä kaikkea tulee dokumentoida ja missä muodossa, jotta asetuksen vaatimukset täyttyvät. Ongelmallisen tilanteesta tekee se, ettei lainsäädäntö ole vielä valmis, vaikka asetus astuu jo 25.5.2018 voimaan. Työnantajia on ohjeistettu toistaiseksi todella vähän ja nyt koulutuksia on vasta alettu järjestää. (Haastattelu 1.)

5.2 **Tarvittava dokumentaatio**

Tietosuoja-asetukseen valmistautuessa tulee laatia käsittelijän seloste. Se on seloste asiakkaan lukuun tehtävistä käsittelytoimista, jossa on yleisluontoinen kuvaus prosesseista sekä asiakaskohtaisuudet. Käytännössä kannattaa tehdä malli, miten yleensä toimitaan sekä malli, miten tämän asiakkaan kohdalla toimitaan. Käsittelijän selosteen tulee sisältää henkilötietojen käsittelijän, alihankkijoiden sekä niiden rekisterinpitäjien nimet ja yhteystiedot, joiden lukuun käsittelijä toimii. Mahdollisuuksien mukaan selosteen olisi hyvä sisältää yleisen kuvauksen teknisistä ja organisatorisista turvatoimista, esimerkiksi maininnat ovien lukitsemisesta, turvatulostamisesta sekä salasanasuojauksista. (Lehtinen 2017)

KuntaProlla on olemassa tilaajan ja KuntaPron välinen henkilötietojen käsittelyohje, joka sisältää kaikki tarvittavat yllä mainitut kriteerit eli käsittelijän seloste on laadittu ja kunnossa. Ohje sisältää kuvauksen myös teknisistä ja organisatorisista turvatoimista ja ohjeessa luokitellaan esimerkiksi käsiteltävät tiedot sekä tuodaan esiin, keillä on pääsy tietoihin. (KuntaPro 2018 b.)

Organisaatioiden on suositeltavaa laatia tietosuojapolitiikka tai muu vastaava asiakirja, jonka johto määrittelee. Tietosuojapolitiikka on ylin tietosuojaa ohjaava dokumentti, joka kuvaa henkilötietojen käsittelyn perusperiaatteet organisaatiossa sekä tietosuojan merkityksen organisaatiolle. Kaikessa henkilötietojen käsittelyssä tulee noudattaa niin lainsäädäntöä kuin tietosuojapolitiikkaa. (Valtiovarainministeriö 2016, 27.) KuntaPro julkaisi johtoryhmän vahvistaman tietosuojapolitiikan helmikuussa 2018, jossa kuvataan henkilöön liittyvien henkilötietojen tai muiden luottamuksellisten tietojen käytön periaatteet ja menetelmät organisaatiossa (KuntaPro 2018).

Valtiovarainministeriön (2016, 28) mukaan käytännössä dokumentaation tulisi sisältää esimerkiksi:

- tietosuojapolitiikka
- roolit ja vastuut tietosuojaorganisaatiossa
- tietosuojaselosteet
- kuvaukset rekisterien tietovirrasta
- kuvaukset rekisteröityjen oikeuksien takaamiseksi määritellyistä prosesseista
- tehdyt tietosuojan riski- ja vaikutustenarvioinnit hallintakeinoineen
- pöytäkirjat tietosuojaa ja tietoturvaa käsitteleviltä foorumeilta ja ohjausryhmistä
- tietoturvatestauksen tulokset
- kuvaukset prosesseista, joilla varmistetaan sisäänrakennetun ja oletusarvoisen tietosuojan toteutuminen
- ohjeet henkilötietoja käsittelevälle henkilöstölle
- dokumentaatio mahdollisista henkilötietojen käsittelyssä tapahtuneista loukkauksista
- tietotilinpäätös (keino toteuttaa osoitusvelvollisuus)
- arkistointisuunnitelma/-ohje

5.3 **Dokumentaatio KuntaProlla**

Tässä luvussa käydään läpi mitä dokumentteja, ohjeistuksia ja politiikoita KuntaProlla on jo laadittu. Lähes kaikki olennaiset dokumentit on laadittu, mutta joitakin toimia on vielä tehtävänä. Tässä koko luvussa on käytetty lähteenä KuntaPron intranettiä (KuntaPro 2018 c), joten kappaleiden perässä ei eritellä lähteitä erikseen.

Laaditut politiikat, joista tietosuojapolitiikka koskettaa koko KuntaPron konsernia ja kolme muuta KuntaPro Oy:ta:
- tietosuojapolitiikka
- riskienhallintapolitiikka
- tietoturvapolitiikka
- salasanapolitiikka.

Muita KuntaPron laatimia dokumentteja tietosuojan toteutumisen kannalta:
- arkistointiohje
- tietosuojaselosteet
- rekisteriselosteet (täyttöohje ja rekisteriselostepohja)
- käyttöoikeuksien hallinnasta ja varmistuksista yleiset dokumentit
- tietosuojasuunnitelma
- tietosuojatehtävien vuosikello
- tietotilinpäätös (kesken).

Tietoturvasta huolehtimista varten on tehty seuraavat dokumentit ja ohjeet:
- KuntaPron ohje salasanojen muodostukseen
- KuntaPron tietoturva tiedon suojaamisen näkökulmasta
- mobiiliturvaohje KuntaPron henkilöstölle
- tietoturvan pikaohje KuntaPron henkilöstölle
- tietoturvaohje KuntaPron henkilöstölle
- tietosuojaohjeistus koskien käyttöoikeuksien hallintaa.

Hannisen ym. (2017, 16) mukaan riskiarviointia seuraava vaikutustenarviointi on asetuksen keskeinen vaatimus. KuntaPro on valmistautunut tähän hyvin ja suorittanut sekä dokumentoinut seuraavat toimet riskien arvioimiseksi:
- OC BIA Vaikutusten analyysi
- Riskikartoitus
- Riskiarviointitaulukko.

Edellä mainittujen dokumenttien lisäksi KuntaPron tietosuojasuunnitelmassa tuodaan esiin dokumentteja, joita tehdään tai päivitetään. Lyhyitä ohjeita ja tiedotteita tullaan tekemään esimerkiksi tietosuojasta ja tietoturvasta huoneentaulun muodossa, hyvästä salasanakäytännöstä, tietosuojasta etätyössä, mobiililaitteiden tietoturvasta sekä esimerkiksi turvakiellon huomioimisesta.

Lisäksi ohjeistusta tarvitaan päätelaitteiden käsittelyohjeiden, tietojärjestelmien käyttöohjeiden ja ostopalvelusopimusten muodossa. Auditointiohje, tietoturvaloukkauksia koskevien asioiden käsittelyohje sekä teknisen valvonnan järjestämistä koskeva ohje ovat myös tarpeellisia dokumentteja, joita on eritelty tietosuojasuunnitelmassa

5.4 **Tarkistuslista**

Tässä luvussa tuodaan esiin tämän opinnäytetyön lopullinen tuotos eli tarkistuslista KuntaPron käyttöön. Tarkistuslistan (Liite 5) avulla voidaan kartoittaa tietosuoja-asetukseen valmistautumisen tilaa ja arvioida toimia, mitä tulisi vielä tehdä. Tarkistuslista koostuu kuudesta osasta, joista ensimmäiset viisi osaa palvelevat pääasiallisesti palkkahallinnon puolta ja kuudes osa koskettaa enemmän ylempää johtoa. Aihealueet ovat muovautuneet tutkimuksen aikana tehtyjen haastattelujen ja havaittujen tarpeiden pohjalta sekä tietoperustan avulla.

Ensimmäisessä osassa käsitellään tarvittavaa dokumentointia palkkahallinnossa. Dokumentoinnin lähteenä on käytetty luvun 5.2 Valtiovarainministeriön tekemää listausta ja jokaiselle tarpeelliselle dokumentille on oma rivinsä ja valintaruutunsa, joka voidaan rastittaa, kun dokumentti tai tehtävä on tehty. Toinen otsikko on prosessikuvat, johon on listattu KuntaPron intranetistä kaikki palkkahallinnon prosessit. Tutkimusta tehdessä ilmeni, etteivät prosessien kuvaukset sisällä ollenkaan kuvausta siitä millaisia henkilötietoja prosesseissa käsitellään. Prosessikuvausten päivittäminen on siis tarpeellinen tehtävä, joka tulee hoitaa kuntoon.

Kolmannessa osuudessa käsitellään asiakkaan kanssa sovittavia toimintaohjeita, joista esimerkkinä henkilötietojen käsittelyohje ja arkistointiohje. Asiakkaan kanssa sovittavia toimintaohjeita olisi varmasti lukematon määrä, mutta opinnäytetyön aiheen rajauksen vuoksi pyritään keskittymään tietosuoja-asetuksen ja palkkahallinnon muodostamaan kokonaisuuteen. Neljäs otsikko koskee palkanlaskentapalveluiden tuottamista, johon sisältyy esimerkiksi tuotannon riskikartoitus sekä käyttö- ja käsittelyoikeudet. Kolmas ja neljäs osio ovat pienempiä sisällöltään, sillä olennaisessa osassa on osion kaksi prosessikuvien päivitys, jonka jälkeen voidaan kasvattaa tarkistuslistaa.

Viidennessä osuudessa käsitellään palkkasihteerien työtapoja ja siinä kartoitetaan suoraan palkkasihteerien tietämystä esimerkiksi tiedustelemalla tietääkö palkkasihteeri, mitkä tiedot luokitellaan arkaluonteisiksi ja miten niitä tulee käsitellä. Kuudennessa kokonaisuudessa käsitellään tietosuojaprosesseja, joka on osuuksista pisin ja laajin. Tietosuojaprosessit osuus sisältää kaikki tarvittavat toimenpiteet tietosuoja-asetuksen valmistautumisen kannalta.

Kokonaisuudessaan tarkistuslista on tämän opinnäytetyön liitteenä (Liite 5) ja siihen on valmiiksi rastitettu toimet, mitä KuntaPro on jo tehnyt. Tarkistuslista toimitetaan myös toimeksiantajan käyttöön, mutta tyhjänä ja muokattavissa olevana versiona. Opinnäytetyön tuloksista ja koko opinnäytetyöprosessista jatketaan seuraavassa luvussa, joka sisältää pohdintaa, johtopäätöksiä sekä arviointia.

6 POHDINTA JA JOHTOPÄÄTÖKSET

Tämän opinnäytetyön tavoitteena oli selvittää, miten tietosuoja-asetuksen voimaantuloon tulee valmistautua palkkahallinnon näkökulmasta. Mielestäni tähän ongelmaan saa melko kokonaisvaltaisen vastauksen lukiessaan koko opinnäytetyön. Omasta mielestäni olen onnistunut melko hyvin saavuttamaan asetetut tavoitteet opinnäytetyöprosessin aikana. Työn tuloksissa pyrittiin palvelemaan mahdollisimman hyvin KuntaPron tarpeita. Suurin esiin noussut tarve oli selvittää, mitä kaikkea tulee dokumentoida ja missä muodossa, jotta kaikki asetuksen vaatimukset täyttyvät, sekä mikä on valmistautumisen tilanne ja tuottaa tarkistuslista. Tarkistuslista (Liite 5) on laadittu opinnäytetyön lopullisena tuotoksena juuri sitä varten, että sen avulla pystytään nopeasti ja helposti tarkistamaan esimerkiksi juuri nämä kyseiset asiat.

Kokonaisuudessaan tietosuojan taso KuntaProlla on tällä hetkellä hyvä eikä tietosuoja-asetuksen voimaantulo aiheuta suuria toimenpiteitä. Prosesseja kartoitettaessa havaittiin, ettei prosessikuvauksissa ole kuvattu ollenkaan sitä, millaisia henkilötietoja prosessin eri vaiheissa käsitellään. Tarpeellinen jatkotoimenpide olisikin prosessien kirjallinen avaaminen ja dokumentointi, josta tulisi huolehtia pikimmiten. Kaikki palkkapalveluiden prosessit on listattu tarkistuslistaan (Liite 5), jonka avulla voidaan huolehtia siitä, että kaikki tulevat läpikäydyiksi. Lisäksi eräs huomio oli se, että liittymät ovat hyvin kuvattu, mutta ne löytyvät ripotellen eri paikoista. Liittymien kuvaukset olisi hyvä siirtää samaan paikkaan, josta ne ovat helposti löydettävissä.

Tietotilinpäätös on hyvä keino toteuttaa osoitusvelvollisuus ja ymmärrykseni mukaan tietotilinpäätös on vielä hieman kesken, joten se kannattaa tehdä huolellisesti loppuun. KuntaPron tavoitteena on jatkaa tietotilinpäätöksen tekemistä vuosittain. Luvussa 5.3 käydään läpi KuntaPron dokumentaatiota, eikä suuria puutteita yllä mainittujen lisäksi ole. Kaikki dokumentit eivät kuitenkaan vielä löydy samasta helposti löydettävästä paikasta. Arkistointiohjeen päivittämistä ja sijoittamista myös tietosuoja-välilehdelle tulisi mahdollisesti harkita, sillä arkistointi on eräs asia, mihin tulee asetuksen voimaantullessa kiinnittää erityistä huomiota.

Kokonaisuudessaan opinnäytetyön tekeminen on ollut oikein opettavainen ja mielenkiintoinen prosessi. On ollut hienoa huomata, miten matkan varrella on oppinut paljon lisää. Alkuun aiheen valinta vähän mietitytti, sillä minulla ei ollut juuri mitään tietämystä tietosuoja-asetuksesta tai palkkahallinnosta. Aluksi oli todella hankala päästä vauhtiin, mutta selkeän rajauksen tekemisen jälkeen työn runko alkoi pikkuhiljaa hahmottua. Tietoperustan kirjoittaminen oli vaikeinta, koska pyrin jatkuvasti muovaamaan tekstiä ja kirjoittamaan vain sellaisista asioista, jotka olisivat olennaisia opinnäytetyön tekemisen kannalta. Mielestäni onnistuin siinä melko hyvin

ja tietoperustan pohjalta oli helppo laatia teemahaastattelun runko sekä tehdä alustava tarkistuslista.

Ilman harjoittelun suorittamista opinnäytetyö olisi jäänyt todennäköisesti paljon pelkistetymmäksi, eikä KuntaPro olisi hyötynyt siitä läheskään yhtä paljon. Harjoittelun kautta pääsin osaksi palkkasihteerien porukkaa ja sain itsekin ymmärrystä palkanlaskennasta sekä sen prosesseista sen sijaan, että työni tekeminen olisi nojannut pelkän kirjallisuuden varaan. Lisäksi sisäisen tiedon saaminen olisi jäänyt vähiin eikä empiiristä osaa olisi ollut kovin helppoa toteuttaa.

Opinnäytetyön tekemisestä on tehnyt mielekästä ja motivoivaa tieto siitä, että opinnäytetyö ja tarkistuslista tulevat tarpeeseen. Lisäksi aiheen ajankohtaisuudella oli suuri vaikutus motivaatioon, koska työstä ei olisi ollut mitään hyötyä KuntaProlle, jos olisin saanut sen valmiiksi vasta tietosuoja-asetuksen voimaatulon jälkeen.

KuntaPron palaute oli kokonaisuudessaan hyvää. Opinnäytetyö valmistui harjoittelun aikana ajallaan asetettujen tavoitteiden mukaisesti. Toimeksiantajan mukaan olin aktiivinen ja oma-aloitteinen sekä osoittanut mielenkiintoa aihetta kohtaan. Työ sisälsi toimeksiantajan mielestä hyviä havaintoja nykytilanteesta kootusti, ja työssä arvioidaan, miten tällä hetkellä uudistuva tietosuoja on otettu KuntaProlla huomioon. Tietosuoja-asetuksen avaaminen ja analysointi olivat tarpeellista ja ajankohtaista tietoa, jota on mahdollista hyödyntää erilaisten ohjeiden ja dokumenttien laadinnassa.

Opinnäytetyötä tullaan käyttämään KuntaPron palkanlaskentapalveluissa monin eri tavoin, josta esimerkkinä opinnäytetyön antaminen luettavaksi esimiehille sekä käyttö ohjeiden pohjana. Tarkistuslista tulee olemaan apuna esimiehille, kun asioita käydään läpi, joita tulee saada kuntoon ennen tietosuoja-asetuksen voimaantuloa.

LÄHTEET

Aaltola, J. & Valli, R. (2007). *Ikkunoita tutkimusmetodeihin.* Heikkinen, L.T. (2007). *Toimintatutkimus—toiminnan ja ajattelun taitoa.* Jyväskylä: PS-kustannus.

Aaltola, J. & Valli, R. (2015). *Ikkunoita tutkimusmetodeihin 1.* Jyväskylä: PS-kustannus. Tästä kirjasta käytetty: Eskola, J. & Vastamäki, J. *Teemahaastattelu: opit ja opetukset.*

Andreasson, A. & Ylipartanen, A. (2017). Haettu osoitteesta 26.1.2018. https://opitietosuojaa.fi/index.php/fi/oikeus/lait/eu-n-tietosuoja-asetus

Arkistolaki 831/1994. Haettu 5.4.2018 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1994/19940831#L4

Ennakkoperintäasetus 1124/1996. Haettu 11.4.2018 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1996/19961124

Euroopan parlamentin ja neuvoston asetus (EU) GDPR 679/2016. Haettu osoitteesta 2.1.2018. http://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI

Euroopan parlamentin ja neuvoston asetus (EU) GDPR 679/2016. Haettu osoitteesta 2.1.2018. http://www.privacy-regulation.eu/fi/

Eskola, J. & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen.* Jyväskylä: Vastapaino.

Finlex (n.d.) Arkistonmuodostussuunnitelma. Haettu 5.4.2018 osoitteesta https://www.finlex.fi/data/normit/4416/arkmliit.pdf

Hakonen, M., Eklund, I. & Roos, M. (2016). *Taloushallinnon taitajaksi.* Helsinki: Sanoma Pro Oy.

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

Henkilötietolaki 523/1999. Haettu 23.3.2018 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Hirsjärvi, S. & Hurme, H. (2001). Tutkimushaastattelu – teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

KuntaPro Oy (n.d.) Palkanlaskennan kokonaiskuva. Sisäinen materiaali.

KuntaPro Oy (n.d.) Palkanlaskennan prosessi. Sisäinen materiaali.

KuntaPro Oy (n.d.) Palkka-ajot. Sisäinen materiaali.

KuntaPro Oy (2018). Tietosuojapolitiikka. Sisäinen koulutus.

KuntaPro Oy (2018 a). Powerpoint. KuntaPron sisäinen materiaali.

KuntaPro Oy (2018 b). Word. Ohje henkilötietojen käsittelystä. KuntaPron sisäinen materiaali.

KuntaPro Oy (2018 c). KuntaPron intranet.

KuntaPro Oy (2017 a). PowerPoint. Moodle. Hämeen ammattikorkeakoulu. Haettu 25.1.2018 osoitteesta https://moodle.hamk.fi

KuntaPro Oy (2017 b). Powerpoint. *Tietosuoja-asetus käytännössä ja asiakkaan arjessa.* KuntaPron sisäinen materiaali.

KuntaPro Oy (n.d.). Nettisivut. Haettu 25.1.2018 osoitteesta https://kuntapro.fi/kuntapro/

Lahti, S. & Salminen, T. (2014). *Digitaalinen taloushallinto.* Helsinki: Sanoma Pro Oy.

Laki nuorista työntekijöistä 998/1993. Haettu 11.4.2018 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1993/19930998

Laki yksityisyyden suojasta työelämässä 759/2004. Haettu 11.4.2018 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Lehtinen, R. (2017). Tietosuoja-asetus 25.5.2018. Webinaari 19.10.2017, Visma Software Oy.

Lehtinen, R. (2013). *Palkkahallinnon aineistojen arkistointi sähköistymisen aikakaudella.* Haettu 5.4.2018 osoitteesta https://tilisanomat.fi/henkilostohallinto/palkkahallinnon-aineistojen-arkistointi-sahkoistymisen-aikakaudella

Männistö, E. (2017). Miten palkkahallinnossa tulee valmistautua tietosuoja-asetukseen? *Tilisanomat* 37(6), 20-21

Oikeusministeriö. Tietosuojavaltuutetun toimisto. (2017). Miten valmistautua EU:n tietosuoja-asetukseen? Haettu 4.2.2018 osoitteesta http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Ojasalo, K., Moilanen, T. & Ritalahti, J. (2014). *Kehittämistyön menetelmät.* Helsinki: Sanoma Pro Oy

Syvänperä, O. & Turunen, L. (2014). *Palkkavuosi*. Helsinki: Edita.

Tietosuojatieto. (2018). Yleistä tietoa asetuksesta. Haettu 26.1.2018 osoitteesta www.tietosuojatieto.fi (Agendium Oy)

Tietosuojavaltuutetun toimisto (2015). EU:n tietosuojauudistus. Haettu 11.4.2018 osoitteesta http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html

Tietosuojavaltuutetun toimisto (2018). Tietosuoja-asetuksen soveltamisesta uusia ohjeita: aiheina tietoturvaloukkaukset, automatisoitu päätöksenteko ja profilointi. Haettu 11.4.2018 osoitteesta http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/on/02/tietosuoja-asetuksensoveltamisestauusiaohjeitaaiheinatietoturvaloukkauksetautomatisoitupaatoksentekojaprofilointi.html

Työaikalaki 605/1996. Haettu 11.4.2018 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1996/19960605

Työsopimuslaki 55/2001. Haettu 11.4.2018 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2001/20010055

Ulosottolaki 37/1895. Haettu 11.4.2018 osoitteesta https://www.finlex.fi/fi/laki/alkup/1895/18950037001

Valtiovarainministeriö. (2016). EU-tietosuojan kokonaisuudistus. Haettu osoitteesta 21.2.2018 https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Verohallinto. (2017). Tulorekisteri käyttöön 2019—tiesitkö tämän? Haettu 11.4.2018 osoitteesta https://www.vero.fi/tietoa-verohallinnosta/verohallinnon_esittely/uutiset/uutiset/2017/tulorekisteri_kayttoon_2019__tiesitko_t/

Vuosilomalaki 162/2005. Haettu 11.4.2018 osoitteesta https://www.finlex.fi/fi/laki/alkup/2005/20050162

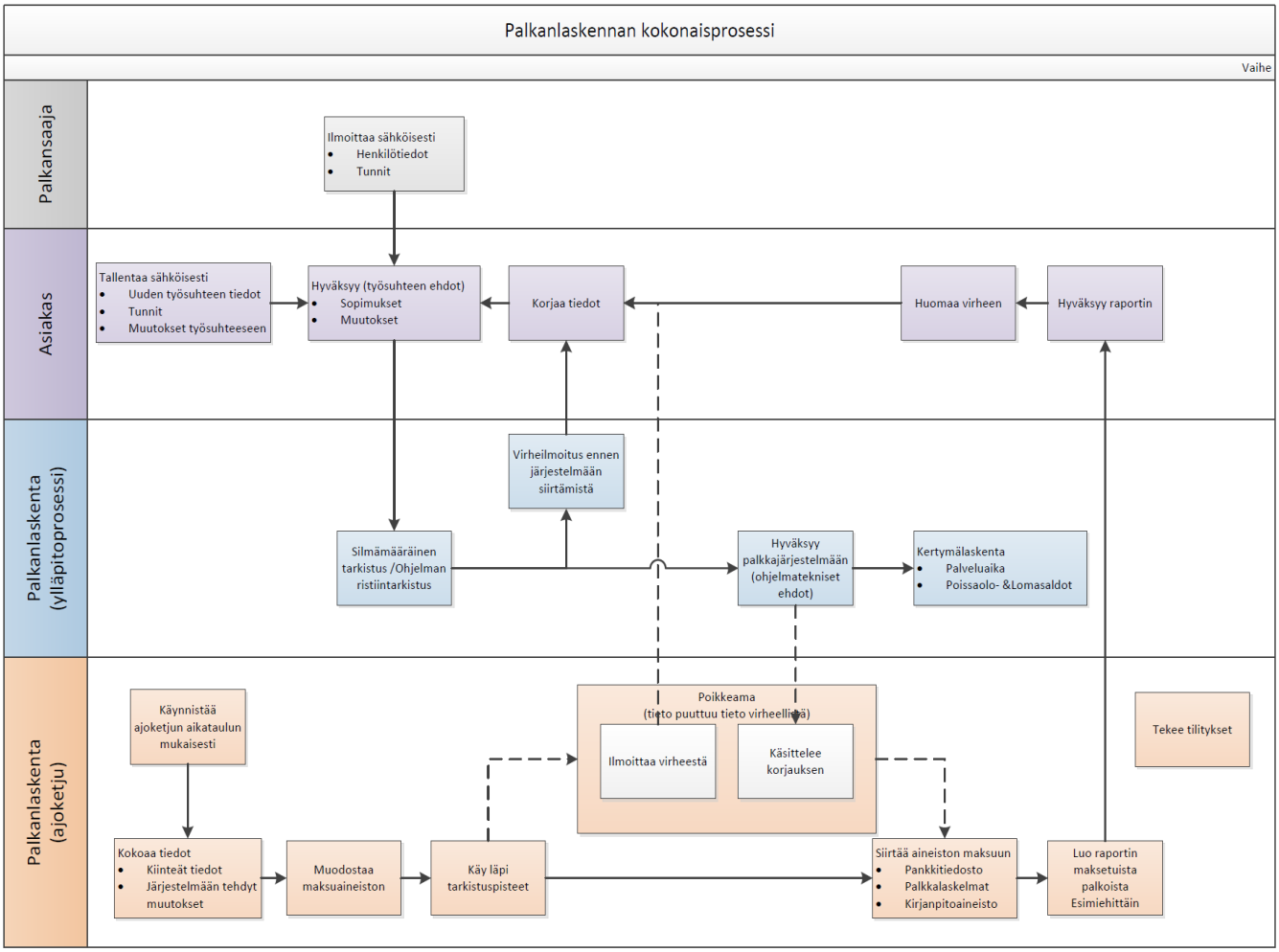
HAASTATTELUT

Haastattelu 1. Tuusulan ja Kangasalan tuotantopäällikkö. (2018). KuntaPro Oy. Haastattelu 22.3.2018, KuntaPro Oy:n toimisto

Haastattelu 2. Tuusulan palkkasihteeri. (2018). KuntaPro Oy. Haastattelu 28.3.2018, Skypen välityksellä

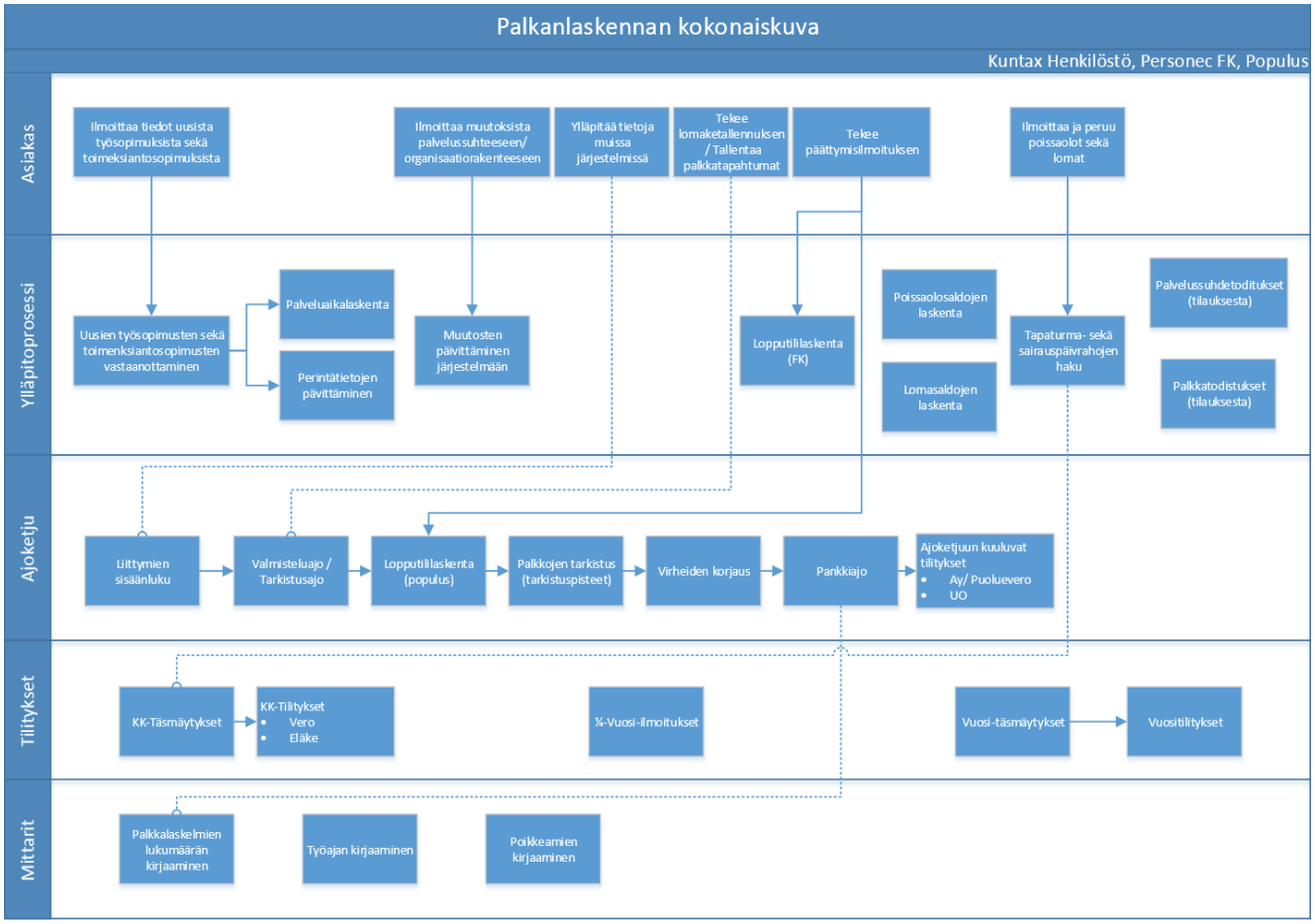
Liite 1

PALKANLASKENNAN KOKONAISPROSESSI



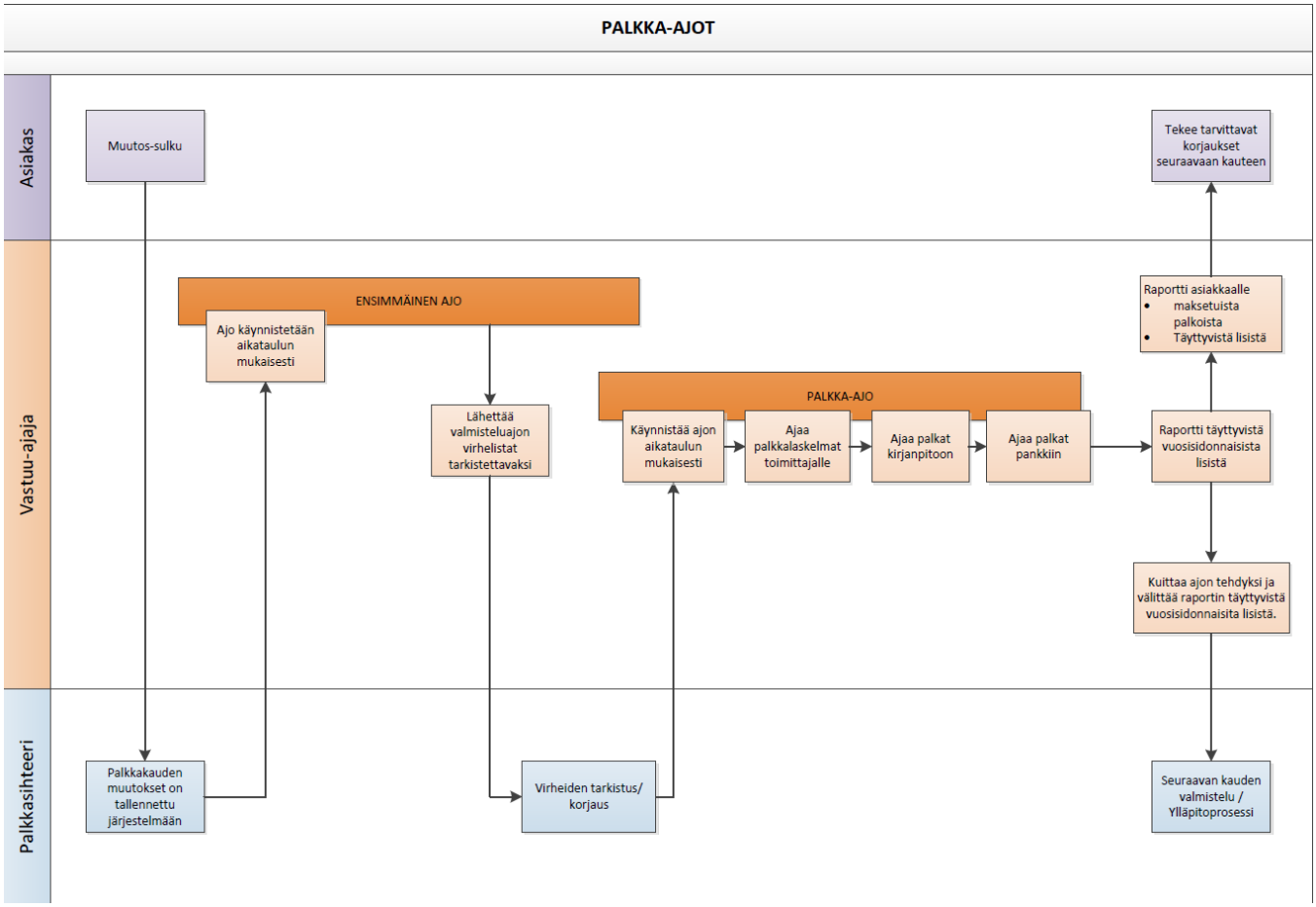
Liite 2

PALKANLASKENNAN KOKONAISKUVA



Liite 3

PALKKA-AJOT



Liite 4

TEEMAHAASTATTELUN RUNKO

Teemahaastattelu suoritettiin

- Kangasalan ja Tuusulan tuotantopäällikölle 22.3.2018
- Tuusulan palkkasihteerille 28.3.2018

Teema 1: EU:n yleinen tietosuoja-asetus

- Miten tietosuoja-asetuksen tuloon on valmistauduttu?
- Onko yrityksen prosessit kartoitettu, joissa käsitellään henkilötietoja?

Teema 2: Palkanlaskennan prosessi

- Millainen on palkanlaskennan prosessi?
- Miten palkanlaskennan prosessi etenee?
- Missä palkanlaskennan prosessin vaiheissa käsitellään henkilötietoja?
- Palkanlaskennan vuosikello?

Liite 5

TARKISTUSLISTA

TIETOSUOJAA KOSKEVA TARKISTUSLISTA

1. TARVITTAVA DOKUMENTOINTI PALKKAHALLINNOSSA

- ☒ Tietosuojapolitiikka
- ☒ Roolit ja vastuut tietosuojaorganisaatiossa
- ☒ Tietosuojaselosteet
- ☐ Kuvaukset rekisterien tietovirrasta
- ☐ Kuvaukset rekisteröityjen oikeuksien takaamiseksi määritellyistä prosesseista
- ☒ Tehdyt tietosuojan riski- ja vaikutustenarvioinnit hallintakeinoineen
- ☒ Pöytäkirjat tietosuojaa ja tietoturvaa käsitteleviltä foorumeilta ja ohjausryhmistä
- ☐ Tietoturvatestausten tulokset
- ☐ Kuvaukset prosesseista, joilla varmistetaan sisäänrakennetun ja oletusarvoisen tietosuojan toteutuminen
- ☐ Ohjeet henkilötietoja käsittelevälle henkilöstölle
- ☐ Dokumentaatio mahdollisista henkilötietojen käsittelyssä tapahtuneista loukkauksista
- ☐ Tietotilinpäätös (keino toteuttaa osoitusvelvollisuus)

  kesken
- ☒ Arkistointiohje

2. PROSESSIKUVAT

- ☒ Palkanlaskennan kokonaiskuva
- ☐ Työsopimuksen vastaanottaminen
- ☐ Toimeksiantosopimus
- ☐ Palveluaikalaskenta
- ☐ Palvelussuhteen muutosten ylläpito
- ☐ Ylityötallennus
- ☐ Poissaolojen tarkistus
- ☐ Lomasaldojen tarkistus
- ☐ Tapaturmat
- ☐ Kela-hakemukset

- ☐ Palkka-ajot
- ☐ KK-Tilitykset
- ☐ Luottamustoimet
- ☐ Liikaa maksettu palkka
- ☐ Populus-Matkalaskut

3. ASIAKKAAN KANSSA SOVITTAVAT TOIMINTAOHJEET

- ☒ Arkistointiohje
- ☒ Tikettien täyttöohje
- ☐ Sairauspoissaolojen toimitus-/käsittelyohje

  Keskustelut asiakkaan kanssa toimintatavan muuttamisesta on aloitettu.
- ☒ Henkilötietojen käsittelyohje
- ☐ Liittymien sisällön kuvaus asiakkaalle (KuntaPron järjestelmien)

4. PALKANLASKENTAPALVELUIDEN TUOTTAMINEN

- ☒ Tuotannon riskikartoitus henkilötietojen käsittelyn näkökulmasta
- ☒ Työnkuvien kartoitus henkilötietojen käsittelyn näkökulmasta
- ☒ Käyttö- ja käsittelyoikeuksien dokumentointi
- ☒ Turvatulostus ja henkilötietoja sisältävien paperien käsittelyohje

5. PALKKASIHTEERIEN TYÖTAVAT

- ☐ Tiedän mitä EU:n yleinen tietosuoja-asetus pitää sisällään
- ☐ Olen käynyt vaaditut Graniten tietosuojakoulutukset
- ☐ Tiedän, mitkä tiedot luokitellaan arkaluontoisiksi
- ☐ Tiedän, miten arkaluontoisia tietoja tulisi käsitellä, kerätä, arkistoida ja tuhota
- ☐ Säilytän arkaluontoisia tietoja muiden ulottumattomissa, esim. lukitsen kaapit lähtiessäni
- ☐ Tiedän, miten toimia tietomurron sattuessa

Edellä esitettyjen vuositarkastelu…X

6. TIETOSUOJAPROSESSIT

- ☒ Tietosuoja-asetuksen mukaiset roolit ja vastuut tunnistettu
- ☒ Nimetty tietosuojavastaava
- ☒ Määritelty ja dokumentoitu työntekijät, joilla on oikeus käsitellä henkilötietoja
- ☒ Kartoitettu kolmannet osapuolet, jotka käsittelevät henkilötietoja
- ☒ Henkilöstön käyttöoikeudet järjestelmiin on rajattu ja dokumentoitu riittävän tarkasti
- ☒ Ohjelmien ja palvelinten tietoturvallisuuden taso on selvitetty
- ☒ Kartoitettu ja tunnistettu järjestelmät, joissa käsitellään henkilötietoja
- ☒ Tehty suunnitelma siitä, miten henkilötietoja käsitellään jatkossa
- ☒ Määritelty käsittelyn kannalta olennaiset henkilötiedot
- ☒ Poistettu vanhentuneet ja tarpeettomat henkilötiedot
- ☒ Määritelty säilytysaika kerättäville tiedoille
- ☒ Kerromme, miksi keräämme henkilötietoja ja mihin ne tallennetaan
- ☒ Kysymme luvan henkilötietojen keräämiselle ja tallentamiselle
- ☒ Laadittu ohjeistus rekisteröidylle, miten ja mistä saada itseään koskevia tietoja
- ☒ Henkilötietojen käsittelystä on tehty kirjallinen sopimus, joka sisältää liitteenä järjestelmätoimittajan selvityksen suojatoimista
- ☒ Henkilöstö on käynyt tarvittavat tietosuojakoulutukset
- ☒ Henkilökunta tietää miten toimia tietomurron sattuessa
- ☒ Aineiston arkistoinnista on tehty ohje
- ☒ Arkistoinnista on tehty asiakkaan kanssa kirjallinen sopimus ja asiakkaalle on selvennetty omat velvoitteensa arkistoinnissa
- ☐ Liittymien kuvaukset on siirretty samaan paikkaan, josta ne ovat helposti löydettävissä
- ☐ Prosessikuvaukset on päivitetty niin, että niissä kuvataan, millaisia henkilötietoja prosessin eri vaiheissa käsitellään