Hanna Salo

Tietosuojariskien hallinta rekrytointiprosessissa

Laskentatoimen ja rahoituksen akateeminen yksikkö
Talousoikeuden pro gradu -tutkielma
Talousoikeuden maisteriohjelma

Vaasa 2024

VAASAN YLIOPISTO
Laskentatoimen ja rahoituksen akateeminen yksikkö
Tekijä: Hanna Salo
Tutkielman nimi: Tietosuojariskien hallinta rekrytointiprosessissa
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Talousoikeus
Työn ohjaaja: Pekka Vainio
Valmistumisvuosi: 2024 **Sivumäärä:** 112

TIIVISTELMÄ:
Jokaisella on oikeus henkilötietojensa suojaan. Henkilötietojen moninaistuneet käyttötarkoitukset sekä kehitys kohti verkostoitunutta tietoyhteiskuntaa uhkaavat kuitenkin tätä oikeutta. Lain ja liiketoiminnan välillä piileekin jatkuva jännite siitä, miten henkilötietoja tulisi käsitellä. Tutkielmassa yksityishenkilön oikeutta henkilötietojensa suojaan käsitellään rekrytointiprosessin viitekehyksessä: päätavoitteena tutkielmassa on luoda lainsäädännön vaatimusten mukaisia ja liikeelämän tarpeet täyttäviä toimintaehdotuksia rekrytointiprosessin tietosuojariskien hallintaan.

Oikeustieteellisen tutkimuksen metodinen pluralismi, tutkielman aihe, sekä talousoikeudelliselle tutkimukselle ominainen juridiikan ja liiketoiminnan yhdistäminen antavat tutkielmalle perustellun lähtökohdan hyödyntää tutkimusmetodeina sekä lainoppia että kvalitatiivista tutkimusmenetelmää. Lainoppia hyödynnetään rekrytointiprosessin tietosuojariskien tunnistamiseen ja riskienhallintakeinojen oikeudelliseen analysointiin. Oikeuslähteinä tutkielmassa toimii ensisijaisesti yleinen tietosuoja-asetus 2016/679 sekä toissijaisesti myös kansalliset säädökset ja oikeustapaukset. Puolistrukturoitujen haastatteluiden avulla tutkielmassa esitellään puolestaan kymmenen HR-alan ammattilaisen näkökulmia rekrytointiprosessin tietosuojariskeistä. Haastattelut tuovat tutkielmaan liike-elämän perspektiivejä: ne havainnollistavat, miten tietosuojariskit ja niiden hallintakeinot näyttäytyvät nykypäivänä organisaatioiden arjessa.

Tutkimustulokset ovat uutuusarvoltaan merkittäviä, sillä aikaisempi tutkimus on keskittynyt lähinnä tulkitsemaan ja systematisoimaan vaikeaselkoista tietosuojalainsäädäntöä ja sen asettamia velvollisuuksia. Tutkielmassa on sen sijaan pyritty pelkän lainopillisen tulkinnan ja systematisoinnin ohella myös ohjeistamaan liiketoimintaa – eli rekrytointiprosessin tietosuojariskien hallintaa – oikeudellisesta näkökulmasta. Tutkimustulokset osoittavat, että rekrytointiprosessin keskeisiä tietosuojariskejä ovat rekisteröidyn puutteellinen suostumus, henkilötietojen liiallinen keräys, sekä henkilötietojen poistamattomuus. Yhteensä kahdeksan keskeistä tietosuojariskiä tuodaan esille. Lisäksi tutkielmassa esitellään tietosuojariskeihin ajavaa tekijöitä, jotka on jaettu inhimillisiin, operatiivisiin, vilpillisiin ja strategisiin tekijöihin. Myös riskienhallintakeinoja rekrytointiprosessin tietosuojariskien hallintaan on tunnistettu kahdeksan kappaletta, ja niistä keskeisimpiä ovat muun muassa työntekijöiden tiedottaminen ja ohjaus, henkilötietojen johdonmukainen minimointi, sisäinen ja ulkoinen valvonta, sekä rekrytointijärjestelmän käyttöönotto.

Tietosuojariskien hallintakeinojen implementoinnin tueksi tutkielmassa esitellään lopuksi kansainvälisen ISO 31000 -riskienhallintastandardin mukaisia ohjeita siihen, kuinka organisaatiot voivat räätälöidä tietosuojariskien hallintakeinoja itselleen sopiviksi. Tässä yhteydessä esitellään myös riskienhallinnan vuosikello, joka voi auttaa organisaatioita tehostamaan ja keskittämään tietosuojariskiensä hallintaa. Tutkielman tulokset voivatkin olla jokaisen organisaation apuna rekrytointiprosessin tietosuojariskien tunnistamisessa ja hallitsemisessa.

AVAINSANAT: henkilötieto, tietosuoja, tietosuojariski, rekrytointiprosessi, riskienhallinta

Alkusanat

Kiitollisuus – tunne, joka kuvastaa tätä hetkeä parhaiten. Edessä kuultaa ekonomin titteli ja takapeilistä näkyy vielä kirkkaana unohtumattomien kokemusten täyttämä tie. Käsipallo ja vahva palo asua ulkomailla veivät tieni Oslon urheiluyliopistoon, ja siellä viettämäni vuodet muokkasivat minua varmasti enemmän kuin osaan vielä tässä vaiheessa elämäntaivaltani käsittää. Urheilujohtamisen tutkinnon kera oli kuitenkin aika jättää Norja taakse ja suunnata kohti Suomen aurinkoisinta kaupunkia.

Vaasa – rakas ja tärkeä opintojen aikainen kotikaupunki. Täällä sain viettää yliopisto-opintojeni toisen puolikkaan, onneksi niin. Hienoja kohtaamisia, pitkiä päiviä kampuksen kirjastolla, sekä revontulia Lapissa ja vaihtokokemus Tukholmassa. Tätä kaikkea on opintojeni tie sisältänyt. Kiitos Vaasan yliopisto, sekä laskentatoimen ja rahoituksen yksikkö saamastani laadukkaasta opetuksesta. Syvä kiitos kuuluu myös pro gradu -tutkielmani ohjaajalle Pekka Vainiolle, jonka ammattitaito yhdistettynä loistavaan huumorintajuun mahdollistivat talousoikeudellisten lakikiemuroiden opin inspiroivassa ympäristössä.

Lämmin kiitos kuuluu myös Vaasan kaupungille järjestämästänne mentoriohjelmasta. Sieltä sain elämääni innostavan ja sydämellisen mentorin. Kiitos Kaija mentoroinnistasi ja HR-maailman lukemattomien mielenkiintoisten tematiikkojen avaamisesta. Avullasi olen saanut varmuutta ja mahdollisuuksia sekä omaan orastavaan uraani, että pro gradu -tutkielmaani. Haluan lisäksi kiittää kaikkia teitä HR-alan ammattilaisia, jotka halusitte antaa panoksenne ja osallistua tutkielmaani haastattelujen muodossa. Ilman teidän ajatuksianne ja kannanottojanne ei tutkimuksen teko olisi ollut yhtä opettavaista ja inspiroivaa. Uskon tämän näkyvän myös tekstini sisällössä.

Osoitan huomioni myös teille tärkeille ystäville, sekä opintojen aikaisille että teille, jotka olette pysyneet matkassa mukana hyvin pitkään. Tiedätte kyllä, keitä olette. Ilman teitä ei opinnoistakaan olisi jäänyt käteen kuin tutkintotodistus. Tärkeä toki sekin, mutta ihmisiä varten täällä ollaan – aivan niin kuin olette minullekin esimerkillänne opettaneet.

Rakkaimmat kiitokset kuuluvat perheelleni. Kiitos lukemattomista tsempeistä ja useista arkisista avustuksista. Kiitos myös lamppujen asennuksista, sekä kaikista niistä muuttoavuista. Yksi tutkielmatyöskentelyn parhaista puolista on ollut ehdottomasti se, että olen saanut viettää kanssanne enemmän aikaa. Sen laitan arvoasteikossani todella korkealle. Ilman teitä en olisi saanut elämääni eväitä, joilla ponnistaa maisteriksi asti. Lopuksi haluan sanoa kiitoksen puolisolleni Robinille. Sinun rakkautesi ja elämänilosi ovat saaneet minut jaksamaan läpi tämänkin projektin. Omistan työni teille.

Vaasassa vappuaattona 2024,
Hanna

Sisällys

Kuviot

Lukijan on hyvä tiedostaa, että tutkielmassa kuvioiden värit havainnollistavat aihetta seuraavasti: rekrytointiprosessi itsessään on kuvattu vihrein sävyin, rekrytointiprosessiin kohdistuvat tietosuojariskit lilalla, tietosuojariskeihin ajavat tekijät keltaisella, ja tietosuojariskien hallintakeinot sinisellä värillä.

Lyhenteet

EIS	Euroopan ihmisoikeussopimus
ETN	Euroopan tietosuojaneuvosto
EUT	Euroopan unionin tuomioistuin
OECD	Organization for Economic Cooperation and Development
SEUT	Euroopan unionin toiminnasta tehty sopimus
SopS	Euroopan ihmisoikeussopimus
TSA	Yleinen tietosuoja-asetus, Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta
YksTL	Laki yksityisyyden suojasta työelämässä

1 Johdanto

1.1 Aiheen kuvaus ja tutkimuskysymykset

''Jokaisella on oikeus henkilötietojensa suojaan.''[1]

Työnhakijoiden henkilötiedot muodostavat hakijadatan, jota voidaan pitää rekrytoinnin valuuttana. Oikein käsiteltynä valuutta voi moninkertaistaa arvonsa ja työnhakijasta tulla organisaatiolle arvokas työntekijä. Valuutan käyttö sisältää kuitenkin myös riskejä ja riskienhallintaa: työnhakijan henkilötietojen suojan rikkoutuminen ei ainoastaan loukkaa ihmisoikeuksia vaan voi lisäksi näkyä suoraan organisaation tuloksessa ja maineessa[2]. Samaan aikaan yritykset kansainvälistyvät ja työelämän prosessit digitalisoituvat[3]. Väistämätön seuraus on, että yhä useampi rekrytointiprosessi tapahtuu verkossa. Rekrytointiprosessien digitaalisuus, tietosuojalainsäädännön tiukentuminen[4] sekä sääntelyn sirpaleisuus[5] ovat aiheuttaneet sen, että Suomessa on lukuisia yrityksiä, joiden tulisi kehittää toimintaansa tietosuojalainsäädännön vaatimusten saavuttamiseksi[6].

Ympärillämme esiintyy lukuisia syitä sille, miksi on ajankohtaista ja olennaista tutkia rekrytointiprosessin tietosuojariskejä. Ensinnäkin, rekrytointiprosessi on tapahtuma, jonka lähes jokainen kohtaa elämänsä aikana ja työnhakijana ihmisellä on oikeus henkilötietojensa suojaan[7]. Toiseksi, aiheen merkityksellisyyttä korostaa se, että vaikka tietosuoja-asetus 2016/679 ainakin lähtökohtaisesti tunnetaan, on organisaatioilla yhä vaikeuksia soveltaa sen vaatimuksia käytännössä: asetusta pidetään vaikeaselkoisena ja tulkinnanvaraisena[8]. Myös Euroopan unioni on vuosina 2020–2022 rahoittanut kaksivuotista

[1] Euroopan unionin perusoikeuskirja 2000/C 364/01, 8 artikla.
[2] Ks. esim. Evans, 2019, s.24.
[3] Alasoini, 2015, s.26–27; Brunila, 2014, s.56.
[4] Ks. esim. KHO 1992-A-10; KHO 1993-A-12; KHO 2018:171.
[5] Korpisaari, Pitkänen & Warma-Lehtinen, 2022, s.3.
[6] Andreasson & Ylipartanen, 2022, s. 30; Tiedeyhteiskunnan kehittämiskeskus, 2022.
[7] Euroopan ihmisoikeussopimus 19/1990; tietosuoja-asetus 2016/679; Suomen perustuslaki 731/1999.
[8] Tietosuoja-asetuksen vaatimukset koetaan erittäin vaativiksi pienissä ja keskisuurissa yrityksissä, ks. esim. Edilex, 2021. Lisäksi organisaatioiden kannalta haitallisinta on vähäinen viranomaisohjaus tietosuojasta, ks. Oikeusministeriö, 2020, s.18.

GDPR2DSM-ohjelmaa, jonka tavoitteeksi oli asetettu yritysten tietosuojaosaamisen lisääminen[9]. Kolmanneksi, tietosuojaongelmien kustannuksista osa valuu yhteiskunnan maksettavaksi esimerkiksi tukipalveluiden ja -neuvojen muodossa[10]. Huomionarvoista on edelleen se, että tietosuoja-asetuksessa on nostettu esille globalisaation ja teknologian nopean kehityksen aiheuttamat uudet haasteet henkilötietojen suojelussa[11]. Näiden ohella tietosuoja-asetuksen yhtenä keskeisenä periaatteena on henkilötietojen käsittelyn riskiperustainen lähestymistapa, johon kuuluu keskeisesti riskien arviointi[12].

Idea tutkielmaan on syntynyt liike-elämässä havaitusta tarpeesta löytää keinoja henkilötietojen suojan kehittämiseen rekrytointiprosessissa. Lisäksi rekrytointiprosessin tietosuojariskien hallinta tulisi olla jokaisen organisaation minimivaatimuksena: henkilöstö on yksi organisaation tärkeimmistä voimavaroista[13] ja rekrytointiprosessin myötä organisaation toimintatavat tulevat ilmi joko julkisesti tai vähintään rekrytoinnissa mukana olleille hakijoille. Hakijoiden kokiessa puutteita henkilötietojen käsittelyssä voivat he levittää tietoa omassa vaikutusympäristössään. Lisäksi rekrytointiprosessissa käsitellään suuri määrä henkilötietoja, jolloin tietosuojariskien todennäköisyys kasvaa. Tämän ohella organisaation toimialasta ja koosta riippuen rekrytointiprosessi voi olla organisaatiolle yksi eniten tietosuojariskejä sisältävä toiminto. Tällöin rekrytointiprosessin tietosuojariskeistä tietoiseksi tuleminen ja niiden hallinta voi auttaa organisaatiota kehittämään myös yrityksen muita tietosuojariskejä sisältäviä toimintoja.

Tutkielma on uutuusarvoltaan merkittävä, sillä se nostaa esille liike-elämästä löydettyjä todellisia rekrytointiprosessin tietosuojariskejä. Päätavoitteena on luoda lainsäädännön vaatimusten mukaisia ja liike-elämän tarpeet täyttäviä toimintaehdotuksia siihen, miten rekrytointiprosessin tietosuojariskejä voidaan hallita. Tietosuojariskien hallitsemisen

---

[9] Tietosuojavaltuutetun toimisto, 2022a; Edilex, 2021. GDPR2DSM-ohjelma on Tietosuojavaltuutetun toimiston ja Tietoyhteiskunnan kehittämiskeskuksen (TIEKE) yhteishanke pk-yrityksille ja sen tavoitteena on ollut vahvistaa yritysten tietojenkäsittelyn käytäntöjä vastaamaan lainsäädännön vaatimuksia.
[10] Valtioneuvosto, 2021, s.21.
[11] TSA 1 artikla.
[12] TSA 25 artikla; TSA 32 artikla; TSA 34 artikla; Korpisaari ja muut, 2022, s.30; Voigt & Bussche, 2017, s.40.
[13] Hyttinen, 2014, s.121.

toimintaohjeet perustuvat tutkielman kvalitatiivisista haastatteluista saatuun empiiriseen datamateriaaliin sekä lähdekirjallisuuteen. Toimintaohjeet on luotu vastaamaan tietosuojalainsäädännön asettamia vaatimuksia. Lisäksi apuna on käytetty ISO 31000 -standardia, joka on yksi keskeisimmistä organisaatioiden riskienhallintatyökaluista[14]. Tutkielma auttaa lukijaansa ymmärtämään, mitä yrityksen tulee huomioida rekrytointiprosessin tietosuojaa edistävien liiketoimintapäätösten suunnittelussa ja miksi rekrytointiprosessin tietosuojariskien hallinta on organisaatioille olennaista. Tutkielman toimintaohjeistuksen ei ole tarkoitus olla tyhjentävä, vaan pikemminkin korostaa yleisimpiä rekrytointiprosessin tietosuojariskejä ja antaa niiden hallintaan ratkaisuehdotuksia.

Tutkielma keskittyy tarkastelemaan organisaation itse toteuttaman rekrytoinnin tietosuojariskejä. Sen sijaan tutkielmasta rajataan pois palveluorganisaatioilta ostettava suorahaku. Lisäksi tutkielma rajautuu käsittelemään vain rekrytointiprosessin tietosuojariskejä, eikä tutkielma ota kantaa organisaatioiden muihin tietosuojariskeihin. Huomionarvoista on myös se, että tutkielman toimintaohjeisto on pääasiallisesti suunnattu suomalaisille yrityksille. Lukijan on lisäksi hyvä tiedostaa, että tutkielmassa käsiteltävät tietosuojariskit edustavat liike-elämän nykytilaa. Henkilötietolainsäädännön muuttuessa sekä henkilötietojen käytön moninaistuessa myös rekrytointiprosessin tietosuojariskien voidaan olettaa muuntuvan.

Tutkielman tavoitteiden ja rajausten pohjalta muodostettu päätutkimuskysymys on:

Miten henkilötietojen suojan tietosuojariskejä voidaan hallita rekrytointiprosessissa?

Kokonaisvaltaisen ja perustellun vastauksen luomiseksi päätutkimuskysymykseen, on tutkielmalla neljä alatutkimuskysymystä:

1) *Miksi rekrytointiprosessissa on tarpeenmukaista kerätä henkilötietoja?*
2) *Miten oikeudellinen sääntely suojaa työnhakijan henkilötietoja rekrytointiprosessissa?*
3) *Miksi rekrytointiprosessin tietosuojariskien hallinta on organisaatioille olennaista?*
4) *Mitä tietosuojariskejä työnhakijan henkilötietoihin kohdistuu rekrytointiprosessissa?*

[14] Kansainvälisen standardoimisjärjestön (International Organization for Standardization) luoma ISO 31000 -standardi on yksi keskeisimmistä riskienhallinannan standardeista. Siihen on koottu organisaation kokonaisvaltaiseen riskienhallintaan yleisesti hyväksytty sanasto, viitekehys ja toimintatapa, ks. Purdy, 2010, s. 881; Ilmonen, Kallio, Koskinen ja Rajamäki, 2016, s.31.

1.2 Tutkimusmetodit ja lähdeaineisto

Oikeustieteellisen tutkimuksen metodinen pluralismi[15], tutkielman aihe, sekä talousoikeudelliselle tutkimukselle ominainen juridiikan ja liiketoiminnan yhdistäminen antavat tutkielmalle perustellun lähtökohdan hyödyntää tutkimusmetodeina sekä lainoppia että kvalitatiivista tutkimusmenetelmää[16]. Lainoppia (*oikeusdogmatiikkaa*)[17], joka toimii tutkielman päämetodina, on tyypillisesti luonnehdittu lain tulkinnaksi ja systematisoinniksi. Lisäksi lainoppi tutkii, mikä merkitys voimassa olevalla oikeudella on kulloinkin käsiteltävään oikeusongelmaan.[18] Koska tutkielmassa tutkimuskohteen ja oikeusongelman muodostavat rekrytointiprosessin tietosuojariskit ja niiden hallinta, on perusteltua hyödyntää käytännöllistä lainoppia eli tulkintaa ja teoreettista lainoppia eli systematisointia[19]. Käytännöllisen lainopin avulla syvennyn tietosuojalainsäädännön *merkityksen* selvittämiseen rekrytointiprosessin näkökulmasta. Toisaalta teoreettisen lainopin keinoilla *analysoin ja jäsennän* sirpaleisen tietosuojalainsäädännön asettamia vaatimuksia.

Kuten Aarnio tähdentää, painotetaan oikeustieteessä harkintaa ja punnintaa, jonka vuoksi oikeustieteellinen metodi voidaan nähdä pikemminkin näkökulmana[20]. Tutkielmani näkökulma kohdistuu tietosuojalainsäädännön tulkitsemiseen, systematisointiin ja soveltamiseen: rekrytointiprosessiin kohdistuvat tietosuojariskit ja riskienhallinta toimii oikeudellisen arvioinnin kohteena. Näkökulman syventämiseksi kvalitatiivinen

---

[15] Ks. esim. Sajama, 2015, s.15; Hirvonen (2011, s.9). Määtän (2015, s.135) mukaan perinteisen oikeustieteen keskeiset suuntaukset (lainoppi, oikeushistoria, oikeussosiologia, oikeuspolitiikka, oikeusteoria, oikeusfilosofia ja vertaileva oikeustiede) eivät enää riitä edustamaan oikeustieteellisen tutkimuksen menetelmiä, vaan menetelmät ovat monipuolistuneet ja muuttuneet avoimemmiksi sekä moniarvoisemmiksi.
[16] Esimerkiksi Siltala (2003, s.137) painottaa oikeustieteellisen tutkimusmetodin määräytyvän tieteenalan, tutkimuskohteen ja valitun tiedonintressin mukaisesti.
[17] Lainoppi on Aarnion (2011, s.1) mukaan oikeudellisen tutkimuksen keskeinen suuntaus ja Timonen (1998, s.1) tähdentää lainopin olevan oikeustieteessä käytettävien metodien ytimessä. Myös Kaisto (2005, s.162) painottaa, että lainoppia on kaikkialla, missä syntyy kysymys oikeusjärjestyksen sisällöstä.
[18] Aarnio, 1975, s.262–268; Aarnio, 1978, s.74–115; Hirvonen, 2011, s.36; Husa, Mutanen & Pohjolainen, 2008,s.20;Nieminen,Lähteenmäki&Aaltonen, 2021, luku 2; Määttä &Paso, 2022,s.3–4;Nykänen,2013, s.50.
[19] Sajama, 2015, s.26–40. Käytännöllinen lainoppi keskittyy lain tulkintaan ja tekstin merkityksen selvittämiseen, kun taas teoreettinen lainoppi syventyy lain systematisointiin, joka on *''epäjärjestyksessä olevan aineiston järjestämistä järkevään* järjestykseen''.
[20] Aarnio, 2006, s.237.

tutkimusmetodi soveltuu avustavaksi tutkimusmetodiksi, sillä laadullisilla tutkimusmetodeilla kyetään havainnollistamaan ihmisten vuorovaikutuksessa syntyneitä, tulkinnallisia, sekä aikaan sidottuja ilmiöitä[21]. Tietosuojariskien hallinta on nimenomaisesti *voimassa olevien* lakien tulkintaa ja riskienhallinta perustuu *ihmisen* toimintaan. Tutkielmassa nostan esille rekrytointiprosessin keskeisiä tietosuojariskejä luodakseni lainsäädännön vaatimusten pohjalta toimintaohjeistuksia niiden hallintaan. Tämä on nimenomaisesti talousoikeuden ydintä: tutkin liiketoimintaa ja ohjeistan sen päätöksentekoa oikeudellisesta näkökulmasta. Tutkielman talousoikeudellisen tieteenalan lainalaisuuksien sekä rajallisen sivumäärän vuoksi yksityiskohtainen seloste kvalitatiivisesta tutkimusosuudesta löytyy tutkimuksen liitteistä (liite 1).

Tutkielmassani on tietyissä määrin kriittinen ote rekrytointiprosessin tietosuojariskien lopullisesta vastuusta, jonka vuoksi tutkielmassa on mukana myös *de lege ferenda* -suosituksia[22]. Suositukset on osoitettu siihen, kuinka tietosuojalainsäädäntöä voisi kehittää, jotta se pystyisi tehokkaammin reagoimaan rekrytointiprosessin tietosuojariskeihin. *De lege ferenda* -näkökulma ei ole tutkimukseni keskeisin lähestymistapa. Näkökulma on kuitenkin aiheellinen ottaen huomioon Euroopan komission tekeillä olevat arvioinnit tietosuoja-asetuksen kansallisesta kehittämisestä[23].

Tutkimuksen lähdeaineisto koostuu kvalitatiivisten haastattelujen aineiston ohella oikeuslähteistä, kuten lainsäädännöstä, lain esitöistä, sekä oikeuskirjallisuudesta[24]. Tutkielmassani tulkitsen ja systematisoin etenkin Euroopan unionin yleistä tietosuoja-asetusta: henkilötietojen käsittelyn periaatteita, rekisteröidyn oikeuksia sekä rekisterinpitäjän

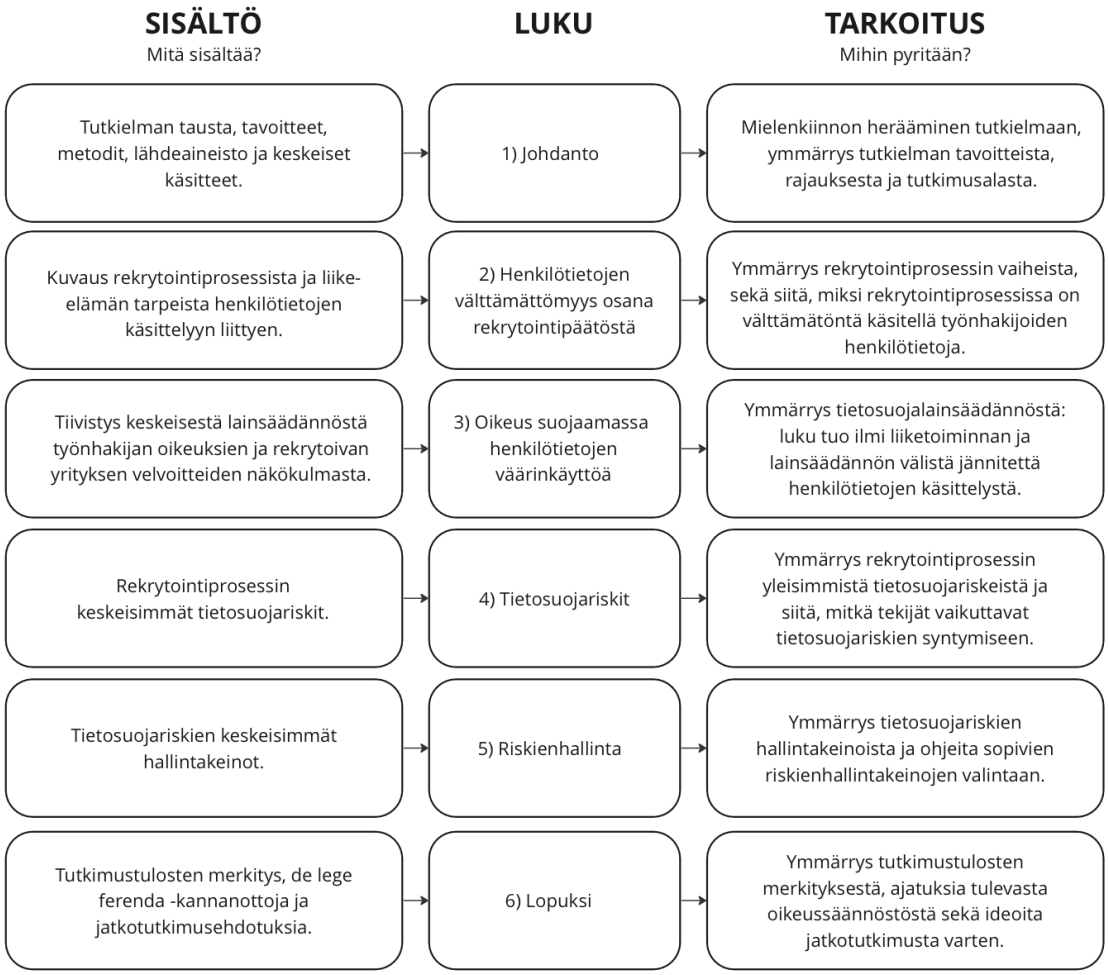
---

[21] Hirsjärvi, Remes & Sajavaara, 2012, s. 162; Tuomi & Sarajärvi, 2018, s.33; Puusa & Juuti, 2020, luku 3–4.
[22] Kolehmainen, 2016, s.128. De lege ferenda -termillä viitataan tulevaan oikeussäännöstöön, ja niissä ehdotetaan uusia ratkaisuehdotuksia siihen, kuinka *tulevaa* lainsäädäntöä voisi kehittää.
[23] Edilex, 2023. Euroopan komissio suorittaa tietosuoja-asetuksen 2016/679 arviointia ja uudelleentarkastelua myös Suomessa. Arvioinnissa on tarkoitus selvittää muun muassa tarvetta kansalliseen lainsäädäntökehitykseen ja Euroopan komission kertomus on määrä julkaista kesällä 2024.
[24] Aarnio, 2014, s.230–232; Aarnio teoksessa Tolonen, 2003, s. 22–27; Oker-Blom, 2009, s.181. Tutkielmassa käytetyt oikeuslähteet voidaan perinteisesti jakaa kolmeen kategoriaan, jotka havainnollistavat oikeuslähteiden välistä hierarkiaa: *vahvasti velvoittavia* oikeuslähteitä tutkielmassa ovat yleinen tietosuoja-asetus sekä tietosuojalaki, *heikosti velvoittavia* oikeuslähteitä ovat lain esityöt sekä oikeuskäytäntö ja *sallittuja* oikeuslähteitä ovat puolestaan tutkielmassa hyödynnetty oikeuskirjallisuus sekä oikeusperiaatteet.

velvollisuuksia. Koska tietosuoja-asetus antaa jäsenvaltioille *kansallista liikkumavaraa*, otan huomioin tutkielmassa myös Suomen kansallista lainsäädäntöä ja oikeustapauksia.

1.3 Rakenne

Tutkielma jakautuu kuuteen päälukuun. Pääluvut, sekä lukujen sisältö on havainnollistettu oheiseen kuvioon (kuvio 1).



Kuvio 1. Tutkielman rakenne.

Ensimmäinen luku toimii tutkielman esittelynä, ja siinä käsitellään aiheen taustaa ja ajankohtaisuutta, tutkimusmetodeja, lähdekirjallisuutta, sekä tutkielman rakennetta. Myös tutkielman kannalta keskeisimmät käsitteet on spesifioitu.

Tutkielman luvut kaksi ja kolme tuovat ilmi liiketoiminnan tarpeiden ja lainsäädännön vaatimusten välistä jännitettä henkilötietojen käsittelystä rekrytointiprosessissa: luku kaksi analysoi, miksi työnhakijoiden henkilötiedot ovat rekrytointiprosessin kannalta välttämättömiä. Lisäksi toinen luku havainnollistaa rekrytointiprosessin päävaiheita ja työtehtäviä. Rekrytointiprosessin vaiheiden käsittelyssä esiin tuodaan myös kannanottoja siitä, mitä tietyissä työtehtävissä tulee huomioida rekisteröidyn oikeuksien näkökulmasta. Luku vastaa tutkielman ensimmäiseen alatutkimuskysymykseen eli siihen, miksi rekrytointiprosessissa on tarpeenmukaista kerätä työnhakijoiden henkilötietoja.

Luvussa kolme puolestaan syvennytään yksityiskohtaisesti siihen, kuinka lainsäädäntö pyrkii edistämään heikommassa asemassa olevan työnhakijan oikeuksia omiin henkilötietoihinsa: luku tuo esiin lainsäädännön keskeisimpiä vaatimuksia henkilötietojen käsittelystä. Tällaisia keskeisiä vaatimuksia ovat rekisteröidyn oikeudet, rekisterinpitäjän velvollisuudet sekä yleiset tietosuojaperiaatteet. Täten luku kolme vastaa tutkielman toiseen alatutkimuskysymykseen eli siihen, miten oikeudellinen sääntely pyrkii suojaamaan työnhakijan henkilötietoja rekrytointiprosessissa. Luvun lopussa tuodaan lisäksi ilmi, kuinka oikeusperiaatetta edustava hyvä liiketapa voi pienentää liiketoiminnan tarpeiden ja lainsäädännön vaatimusten välistä jännitettä henkilötietojen käsittelyssä. Nämä tiedot tuovat esille, kuinka tietosuojariskien hallinta voi hyödyntää organisaatioita, joten luku vastaa myös tutkielman kolmanteen alatutkimuskysymykseen eli siihen, miksi tietosuojariskien hallinta on organisaatioille olennaista.

Rekrytointiprosessin yleisimpiä tietosuojariskejä tuodaan esille luvussa neljä. Tämä on tarpeenmukaista, jotta tutkielmassa voidaan käsitellä rekrytointiprosessin tietosuojariskien hallintaa. Löydettyjä tietosuojariskejä analysoidaan laintulkinnan keinoin: luku tuo esille, miksi kyseiset tietosuojariskit rikkovat tietosuojalainsäädännön vaatimuksia. Lisäksi luku havainnollistaa, miten rekrytointiprosessin tietosuojariskit saavat alkunsa, sekä mitkä tekijät lisäävät riskien todennäköisyyttä. Täten neljäs luku vastaa tutkielman neljänteen alatutkimuskysymykseen eli siihen, mitä tietosuojariskejä työnhakijan henkilötietoihin kohdistuu rekrytointiprosessissa.

Luku viisi tuo esiin rekrytoinnin tietosuojariskien hallintakeinoja. Lisäksi luku havainnollistaa, miten räätälöidä riskienhallintakeinoja omalle yritykselle sopiviksi, sekä kuinka ottaa tietosuojariskien hallinta osaksi riskienhallinnan vuosikelloa. Riskienhallinnan vuosikello -ajattelun tukena tutkielmassa käytetään tietosuojariskien hallintaan keskittyvää ISO 31000 -standardia. Luku vastaakin täten tutkielman päätutkimuskysymykseen eli siihen, miten henkilötietojen suojan tietosuojariskejä voidaan rekrytointiprosessissa hallita.

Kuudes luku toimii tutkielman päätöslukuna, ja siinä käydään läpi tutkimustulosten merkitystä, pohditaan tulevaa lainsäädäntöä *de lege ferenda* -kannanottojen avulla, sekä nostetaan esille jatkotutkimusehdotuksia.

1.4 Keskeiset käsitteet

Yleinen tietosuoja-asetus (*General Data Protection Regulation, GDPR*)[25] jäljempänä tietosuoja-asetus, käsittelee yksilöiden suojelua henkilötietojen käsittelyn osalta. Sen tavoite on ollut antaa yksilöille paremmat mahdollisuudet kontrolloida henkilötietojansa ja helpottaa yksilöiden varmistumista heidän tietojensa asianmukaisesta käsittelystä[26]. Lisäksi tietosuoja-asetuksella on haluttu lisätä oikeusvarmuutta yhdenmukaistamalla jäsenvaltioiden tietosuojalainsäädäntöä[27].

Tietosuoja (*data protection*)[28] on kansainvälisesti vakiintunut ilmaisu, jolla kuvaillaan henkilötietojen suojan oikeudellista sääntelyä. Tietosuojalainsäädännön avulla pyritään

[25] Yleinen tietosuoja-asetus (TSA) on Euroopan parlamentin ja neuvoston antama asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä. Siinä korostuu yksilön tiedollinen itsemääräämisoikeus. Asetusta on sovellettu 25.5.2018 lähtien ja se on voimassa olevaa sekundaarista EU-oikeutta. Muiden EU:n asetusten tapaan tietosuoja-asetus on voimassa automaattisesti ja yhtäaikaisesti kaikissa EU-maissa. Lisäksi se sitoo kaikkia EU-maita koko laajuudessaan, eikä sitä ole tarvinnut saattaa erikseen oksaksi kansallista lainsäädäntöä, ks. Oikeusministeriö, 2016; EPNAs 2016/679; HE 9/2018 vp; Euroopan komissio, 2022b.
[26] Glon, 2014, s.480; KOM (2012) 11, s.4–6; Andreasson & Ylipartanen, 2022, s.30.
[27] Vaikka Euroopan unionia on kuvailtu tietosuojasääntelyn pioneeriksi (Mouzakiti, 2015, s.39), oli ennen tietosuoja-asetusta käytössä ollut henkilötietosuojadirektiivi 95/46/EY vanhentunut, eikä se enää pysynyt teknisen kehityksen ja muuttuvan digitalisaation perässä, ks. Burri ja Schär, 2016, s.480.
[28] Tietosuoja on käsite, jonka tavoitteena ei niinkään ole tiedon suojaaminen itsessään, vaan rekisterinpitäjien ohjaaminen hyviin henkilötietojen käsittelykäytäntöihin lainsäädännön keinoin. Lakiteksteissä käsitettä ei ole määritelty Suomessa, mutta termillä on määritelty henkilötietojen käsittelyyn kuuluvia oikeuksia ja velvollisuuksia, ks. henkilörekisterilaki 471/1987 (kumottu) ja henkilötietolaki 523/1999 (kumottu).

kasvattamaan tiedon kohteen (*data subject*) henkilötietojen suojaa. **Henkilötietojen suojalla** viitataan yksilön yksityisyyteen ja tietojen itsemääräämisoikeuteen.[29] Tutkielmassa viittaan tietosuojalla tietosuojalainsäädäntöön ja henkilötietojen suojalla henkilön yksityisyyden ja tiedollisen itsemääräämisoikeuden suojaan. **Tietoturvalla** tarkoitetaan puolestaan teknisiä ja hallinnollisia toimenpiteitä, joiden avulla pyritään varmistamaan henkilötietojen asianmukainen käsittely. Tietosuoja kattaa vain henkilötietojen oikeudellisen sääntelyn, mutta tietoturvalla viitataan organisaation kaikkien erityyppisten tietojen turvatoimenpiteisiin[30]. Käsitteet elävät rinnakkain, kuitenkin merkiten eri asioita[31]. Seuraavassa kuviossa (kuvio 2) havainnollistan tietosuojan ja tietoturvan yhteyttä.

Kuvio 2. Tietosuojan ja tietoturvan kiinnittyminen toisiinsa.

Henkilötieto (*personal data*)[32] tarkoittaa tunnistetietoa, jonka perusteella on mahdollista tietää tai saada selville luonnollinen henkilö *suoraan* tai *epäsuorasti.* Henkilötiedon

[29] Euroopan unionin perusoikeuskirja, 8 artikla; Alapuranen, Lehtonen, Koskinen & Wiberg, 2020, s.37–38.
[30] Keller, 2023, s. 54.
[31] Andreasson & Ylipartanen, 2022, s.23.
[32] TSA 4 artiklan 1 kohta määrittää henkilötiedon tarkoittavan *''kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä 'rekisteröity', liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa* ***erityisesti*** *tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.''* Listauksesta on hyvä huomioida sana 'erityisesti', sillä se osoittaa, ettei 4 artiklan tunnistetietojen listaus ole tyhjentävä, vaan suuntaa antava. Henkilötiedon käsite on täten hyvin laaja.

käsitettä ei ole mahdollista säätää kansallisesti tietosuoja-asetuksesta poikkeavaksi.[33] Tutkielmassa työnhakijan henkilötieto on määritelty tietosuoja-asetuksen määritelmän mukaisesti. Täten esimerkiksi työnhakijan yhteystiedot, osoite, ikä, harrastukset, motivaatio, kielitaito, sekä työ- ja opiskelutausta luokitellaan tutkielmassa henkilötiedoiksi.

Henkilötietojen käsittely (*data processing*)[34] sisältää kaikki henkilötietoihin kohdistuvat toiminnot henkilötiedon keräämisen suunnittelusta tietojen tuhoamiseen saakka[35]. Rekrytointiprosessin osalta henkilötietojen käsittelyllä tarkoitetaan jokaista työtehtävää aina prosessin suunnittelusta työnhakijoiden henkilötietojen poistamiseen asti.

Rekisterinpitäjällä (*controller*) tarkoitetaan luonnollista henkilöä, oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. **Henkilötietojen käsittelijä** (*processor*) on voi puolestaan olla edellä mainitun listan mukainen taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. **Rekisteröity** (*data subject*) on puolestaan luonnollinen henkilö, jonka henkilötietoja käsitellään.[36] Tutkielmassa rekrytoivat organisaatiot ovat rekisterinpitäjiä ja mahdolliset HR-palveluja tuottavat tahot henkilötietojen käsittelijöitä. Työnhakijat ovat rekisteröityjä, koska rekrytointiprosessissa käsitellään heidän henkilötietojansa.

Rekrytointiprosessi (*recruitment process*) [37] eli rekrytointi on projekti, jonka tavoitteena on saada tarvittava osaaminen ja työvoima kustannustehokkaasti ja ajallaan[38]. Tutkielma

---

[33] Korpisaari ja muut, 2022, s.57–58; Hanninen, Laine, Rantala, Rusi & Varhela, 2017, s.20.
[34] TSA 4 artiklan mukaisesti henkilötietojen käsittelyllä tarkoitetaan *''…tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.''* Henkilötiedon käsittelyksi on lisäksi katsottu henkilötietojen keräämisen suunnittelu, ks. Neuvonen, 2019, s.233.
[35] Alapuranen ja muut, 2020, s.41.
[36] TSA 4 artikla. Tietosuoja-asetuksen suomennettu termi ''rekisteröity'' on käsitteenä suppeampi kuin englanninkielinen vastine ''data subject''. Suomennosta voidaan pitää epäonnistuneena ja harhaanjohtavana, koska asetuksen velvoitteet tulevat sovellettavaksi huolimatta siitä, ovatko henkilötiedot jossakin rekisterissä. Täten luonnollisen henkilön – eli ihmisen – voi olla vaikea ymmärtää, milloin rekisteröityä koskevat säännökset tulevat sovellettaviksi hänen osaltaan, ks. esim. Korpisaari ja muut, 2022, s.34.
[37] Koivisto, 2004, s.23; Phillips & Gully, 2015, s.46–47; Viitala, 2021, s.71; Joki, 2021, s.65–66.
[38] Phillips & Gully, 2017, s.32–35; Kaijala & Tolvanen, 2020, s.130; Hoppe, 2014, s.93; Coverdill & Finlay, 2017, s.135–154. Rekrytointi voi toisinaan tapahtua myös spontaanisti ilman varsinaista hakuprosessia.

tarkastelee organisaation ulkopuolisen työnhakijan henkilötietojen käsittelyä organisaation itse toteuttamassa rekrytoinnissa, jolloin muun muassa palveluorganisaatioilta ostetut suorahakupalvelut rajautuvat tutkielman ulkopuolelle.

Tietosuojariski voidaan käsittää tarkastelemalla ensin sitä, mitä riski tarkoittaa. Riski käsitetään usein tapahtumaksi tai tapahtumatta jäämiseksi, jolla on toteutuessaan negatiivisia vaikutuksia.[39] Käsitys riskistä on kuitenkin laajentunut vahinkonäkökulmaa moninaisemmaksi ja riskin seuraus voi asianmukaisesti hallittuna olla positiivinen[40]. Tutkielmassa tietosuojariski viittaa tapahtumaan, joka toteutuessaan loukkaa henkilötietojen suojaa.

Riskienhallinta (*risk management*)[41] on prosessi, jossa riskit tunnistetaan, analysoidaan sekä kontrolloidaan hyväksyttävälle tasolle hyväksyttävillä kustannuksilla[42]. Näin pyritään varmistamaan toiminnan jatkuvuus. Hyvän riskienhallinnan tunnusmerkkejä ovat toiminnan suunnitelmallisuus, järjestelmällisyys, sekä dynaamisuus.[43] Tutkielman tietosuojariskien hallinnan toimintaohjeisto perustuu osittain ISO 31000 -standardiin, koska standardi perustuu hyvän riskienhallinnan periaatteisiin ja on yksi riskienhallinnan keskeisimmistä standardeista[44].

---

[39] Luonteeltaan riski käsitetään lähtökohtaisesti negatiiviseksi, ks. Kurkela, 2014, s.3. Riskiksi voidaan katsoa myös sellainen käyttämättä jätetty tapahtuma, jolla olisi voitu saavuttaa organisaation tavoitteita, ks. Kupi, Keränen & Lanne, 2009, s.9.

[40] Riskin määritelmä on laajentunut ja riski voi myös auttaa organisaatiota saavuttamaan tavoitteitaan, ks. Alftan ja muut, 2008, s.33. Riski ei aina ole luonteeltaan negatiivinen tai positiivinen vaan siitä aiheutuvat seuraukset voivat vaihdella voiton ja menetyksen välillä, ks. Purdyn, 2010, s.882. ISO 31000 -standardissa korostuu, että riskillä voi olla joko negatiivinen tai positiivinen vaikutus *''the effect on uncertainty on objectives – epävarmuuden vaikutus tavoitteisiin.''* Ks. Ilmonen, Kallio, Koskinen & Rajamäki, 2016, s.32–34. Riskille on myös kvantitatiivinen määritelmä: 1) Mitä voi tapahtua? eli s=scenario, 2) Mikä on tapahtuman todennäköisyys? eli p=probability, sekä 3) Jos tapahtuma toteutuu, mikä on seuraus? eli c=consequence, ks. Kaplan ja muut, 1981, s.944.

[41] International Organization for Standardization -järjestön luoman ISO 31000 -standardin mukaan riskienhallinta on koordinoitua toimintaa, jolla organisaatiota johdetaan riskien osalta, ks. SFS–ISO 31000, 2018, s.12. Yleisin virhe riskienhallinnassa on ajattelu siitä, että riskienhallinta on *jo tapahtuneiden* virheiden korjaamista tai toisaalta täysin riskivapaan toimintaympäristön luomista, ks. Louisot & Ketcham, 2014, s.15.

[42] Roper, 1999, s.13; Thun & Hoenig, 2011, s.243.

[43] Riskienhallinta ei saisi olla staattinen prosessi, sillä riskit muuntuvat, ks. Viscelli ja muut, 2017, s.70.

[44] Ilmonen ja muut, 2016, s. 31.

2 Henkilötietojen välttämättömyys osana rekrytointipäätöstä

2.1 Liiketoiminnan tarpeet ja yksilön oikeudet vastakkain

Liiketoiminnan tarpeiden ja yksilöin oikeuksien välinen jännite rekrytointiprosessissa muodostuu, kun yritykset tarvitsevat henkilötietoja rekrytointiprosessien läpivientiin. Henkilötietojen käsittelyyn kohdistuukin velvoitteita, sillä työnhakijalla on oikeuksia henkilötietojansa kohtaan. Samanaikaisesti tietosuoja-asetuksen mukaan henkilötietojen määritelmä on laaja[45]. Lähtökohtaisesti kaikista työnhakijasta kerättävistä tiedoista työnhakija voidaan tunnistaa *suoraan* tai *epäsuorasti*. Siksi kaikki rekrytoinnin aikana työnhakijasta tiedusteltavat tiedot on tutkielmassa määritelty henkilötiedoiksi. Rekrytoinnin aikana ei kuitenkaan ole tarpeenmukaista kerätä työnhakijan henkilötietoja kaikenkattavasti[46]. Tarpeenmukaisia henkilötietoja voivat olla muun muassa: koulutus, kertynyt osaaminen, kyvyt kuten kielitaito tai matemaattinen lahjakkuus, persoonallisuuden piirteet kuten määrätietoisuus ja luovuus, kiinnostuksen kohteet tai sosiaaliset taidot[47]. Lisäksi toisinaan valintapäätöksen tueksi selvitykset hakijan luottotiedoista, huumausaineiden käytöstä ja rikosrekisteristä ovat tarpeenmukaisia henkilötietoja[48].

Käsittelen seuraavaksi haastatteluissa esiin nousseita kannanottoja siihen, mitä henkilötietoja onnistuneeseen rekrytointiprosessiin tarvitaan ja miksi. Haastatteluissa korostettiin etenkin opiskelu- ja työtaustan tarpeellisuutta:

> *''Haettavaan positioon ja työn tekemiseen vaikuttavia asioita on tarpeen arvioida. Siks avoinna olevan position kannalta relevantti opiskelu- ja työtausta on välttämätöntä kerätä. Tällä varmistetaan myös se, että hakija todistaa olevansa aito henkilö eikä robotti.''*
>
> *-Haastateltava 1*

---

[45] TSA 4 artikla kohta 1. Katso lisäksi tutkielman määritelmä henkilötiedosta sivuilta 13–14.

[46] Tutkielma kannustaa kerättävien henkilötietojen minimointiin. Esimerkiksi nimeä ei automaattisesti tule pitää välttämättömänä henkilötietona rekrytointiprosessin alun työvaiheissa, katso tarkemmin luvusta 5.

[47] Viitala, 2021, luku 3.3; Robles, 2018, s.12; Alapuranen ja muut, 2020, s.174; Saarinen, 2013, s.560.

[48] Laki yksityisyyden suojasta työelämässä 5a§ sekä 7§ luottotietolaki 527/2014 kertovat tarkemmin työnhakijan luottotietojen sekä huumausainetestiä koskevan todistuksen toimittamisen edellytyksistä. Turvallisuusselvityslaki 726/2014 puolestaan kertoo edellytykset, jolloin työnantajalla on työhönoton yhteydessä oikeus hakea henkilöturvallisuusselvitystä, johon sisältyy tietoja rikosrekisteristä. Rekrytoinnissa on huomioitava, että henkilötiedot tulee lähtökohtaisesti kerätä työnhakijalta, ks. Neuvonen, 2019, s.259.

Osa tutkimuksen haastateltavista kuitenkin kyseenalaisti työtaustan merkitystä uudessa työssä menestymisen kannalta. Samalla yhteystietojen välttämättömyyttä korostettiin:

> *''Yhteystiedot kuten puhelinnumero ja sähköposti tarvii kerätä siltä hakijalta sen takia, että voidaan prosessin aikana olla yhteyksissä ja ilmoittaa prosessin etenemisestä.''*
>
> *-Haastateltava 2*

Yksi haastateltavista korosti myös rekrytoivaan yritykseen mahdollisesti kohdistuvia oikeusvaateita[49], joiden vuoksi tiettyjä henkilötietoja on kysyttävä ja säilytettävä:

> *''Tietoja henkilön osaamisesta ja työtaustasta tarvitaan, jotta voidaan jo hakuvaiheessa erottaa, että onko just sillä hakijalla tehtävään vaadittavaa osaamista ja taitoja. Hakijasta täytyy olla tallessa näitä tietoja, jotta mahdollisen oikeusprosessin kohdalla me voidaan todistaa meidän toiminta lainmukaiseks. Oikeusprosessit saattaa esimerkiks liittyä siihen valintapäätökseen, että miks ei just häntä otettu työtehtävään. ''*
>
> *-Haastateltava 3*

Haastatteluissa korostui lisäksi se, että työnhakijan asuinpaikka voi olla rekrytoinnin onnistumisen kannalta ratkaiseva henkilötieto:

> *''Esimerkiks asuinpaikka on osalle tehtäviä hyvin relevantti tieto. Koska on tehtäviä, joita ei voi tehdä etänä, ni se on ilmiselvää et pitää tietää, missä päin ne hakijat asuu. ''*
>
> *-Haastateltava 4*

Haastatteluissa esiin nousseet näkökulmat edustavat rekrytoinnin nykypäiväistä tilaa ja kuvastavat, millaisia henkilötietoja työnhakijoista kerätään rekrytointiprosessin aikana. Lukijan on hyvä tiedostaa, ettei kuitenkaan ole mahdollista laatia täysin tyhjentävää listausta siitä, mitkä henkilötiedot ovat tarpeenmukaisia rekrytointiprosessin onnistumisen näkökulmasta: sen määrittää aina avoinna oleva työnkuva sekä organisaation ominaispiirteet[50]. Myös lainsäädäntö rajoittaa osaltaan sitä, mitä henkilötietoja voidaan pitää tarpeenmukaisina. Tutkielman viidennessä luvussa syvennyn analysoimaan tarkemmin, ovatko tämän luvun haastatteluissa välttämättömiksi koetut henkilötiedot tulevaisuudessa rekrytointiprosessin onnistumisen kannalta tarpeenmukaisia henkilötietoja.

---

[49] Työnhakijoiden henkilötietojen säilytyksellä varmistetaan paitsi työnhakijoiden myös yritysten oikeusturva ja maine: henkilötietoihin perustuvien valintapäätösten avulla organisaatiot voivat osoittaa, ettei rekrytointi ole perustunut esimerkiksi syrjiviin tai yhdenvertaisuutta heikentäviin tekijöihin.

[50] Hallituksen esityksessä (HE 75/2000 vp, s.15–16) on tuotu ilmi, kuinka työelämän monimuotoisuuden vuoksi on mahdotonta luetella tyhjentävästi työsuhteeseen liittyviä tarpeellisia henkilötietoja.

2.2 Rekrytointiprosessin vaiheet ja henkilötietojen kuljetus prosessissa

Rekrytointiprosessi[51] voidaan jakaa osiin yksityiskohtaisesti työtehtävien mukaan tai laveammin teemoittain. Tutkielmassa rekrytointiprosessin vaiheet on määritelty seuraavasti: kirjallisuudesta on mukailtu teemakohtaista jaottelua, ja yksittäiset työtehtävät on nimetty päävaiheiden alle kirjallisuuden ja tutkielman haastatteluiden pohjalta. Hyvässä rekrytointiprosessissa on näin määritelty olevan neljä päävaihetta: suunnittelu-, hakijahankinta-, hakijavalinta-, sekä sopimus- ja perehdytysvaihe. Oheinen kuvio (kuvio 3) havainnollistaa hyvän rekrytointiprosessin päävaiheita ja työtehtäviä.

Kuvio 3. Havainnollistus rekrytointiprosessin päävaiheista ja työtehtävistä[52].

Kuvion (kuvio 3) mukainen määritelmä rekrytointiprosessin eri vaiheista on yksityiskohtainen ja monia työtehtäviä sisältävä. Rekrytointiprosessi lähtee kuitenkin aina liikkeelle yrityksen tarpeesta ja muodostuu siten organisaationsa näköiseksi[53]. Siksi rekrytointiprosessien täsmälliset työtehtävät vaihtelevat. Organisaatioiden välisten erojen lisäksi

[51] Katso rekrytointiprosessin tarkka määritelmä tutkielman sivulta 14. Rekrytointiprosessi voidaan jakaa vaiheisiin yksittäisten työtehtävien mukaisesti, ks. esim. Viitala, 2014, luku 4; Salli & Takatalo, 2014, s.10. Toiset rekrytointeihin syventyneet asiantuntijat jakavat rekrytointiprosessin kattavampiin ja monia työtehtäviä sisältäviin kokonaisuuksiin, ks. esim. Helsilä & Salojärvi, 2009, s.127–136; Kaijala, 2016, s.58–67. Osa asiantuntijoista käsittää prosessin sisältävän teemoja, joiden pohjalta rekrytointiprosessi voidaan jakaa vaiheisiin teemakohtaisesti, ks. esim. Joki, 2021,s.65; Viitala, 2021, s.75.

[52] Joki, 2021, s.65, Helsilä & Salojärvi, 2009, s.136; Viitala, 2014; Viitala, 2021; Kaijala, 2016, s.26; Rötkin, 2015; Salli & Takatalo, 2014 s.10; tutkielman kvalitatiiviset haastattelut. Huomioi, että tutkielmassa rekrytointiprosessista on rajattu pois ulkoistettu suorahaku, ks. tutkielman sivut 8 ja 14–15.

[53] Vaahtio, 2005, s.56–57.

rekrytointiprosessit voivat näyttäytyä erilaisina myös saman organisaation sisällä riippuen siitä, millä resursseilla, aikataululla ja osaamistarpeella työnhakijaa kussakin hetkessä haetaan[54]. Lähdekirjallisuuden lisäksi rekrytointiprosessin eri vaiheiden jaottelu tuli ilmi myös tutkielman haastatteluissa:

> *''Siinä [rekrytoinnissa] on kolme aika yksinkertasta vaihetta. Nää vaiheet on tarpeen määrittely, hakijahankinta ja hakijavalinta. Eli miten hankitaan henkilöt ja miten valitaan heistä sopivin. Sit näistä vaiheista voidaan pilkkoo eri työtehtävät.''*
>
> *-Haastateltava 4*

Kuten edellisestä lainauksestakin käy ilmi, ei perehdytyksen aina katsota olevan osa rekrytointiprosessia. Tutkielman haastateltavista viisi ei maininnut perehdytystä, kun heitä pyydettiin määrittämään rekrytointiprosessin vaiheet. Toiset viisi haastateltavaa puolestaan koki perehdytyksen olevan olennainen osa rekrytointia:

> *''No rekrytointiprosessissa voidaan tietysti nähdä olevan eri työvaiheita ja eri organisaatioissa ne vaiheet voi olla tosi erinäkösiäkin. Mutta ehkä ne tärkeimmät on, että tiedetään mitä haetaan, mistä haetaan, ja sitte koitetaan hankkia niitä hakijoita. Sit tehään valinta ja lopuks keskitytään perehdyttämiseen. Tää vika vaihe on vähintäänki yhtä tärkee ku noi muut osat ihan jo senki takia, että pyrittäs perehdytyksellä sitouttamaan uudet työntekijät siihe organisaatioon. Vältyttäs näin turhilta rekrykierroksilta.''*
>
> *-Haastateltava 10*

Asiantuntijoiden keskuudessa perehdytys määritellään usein osaksi rekrytointia, mutta toisinaan sen katsotaan olevan jatkumo itsenäisiä työtehtäviä, jotka liittyvät läheisesti rekrytointiprosessiin olematta kuitenkaan osa sitä[55]. Se, kuuluuko perehdytys osaksi rekrytointia, määrittyy usein organisaation rakenteen ja koon pohjalta. Henkilötietojen suojan näkökulmasta työnhakijan henkilötietojen käsittely ei rajoitu vain rekrytointiprosessiin, vaan jatkuu perehdytykseen asti. Vasta perehdytyksen viimeisissä työtehtävissä työnhakijasta tulee työntekijä. Siksi tutkielmassa perehdytys on määritelty osaksi rekrytointiprosessia. Seuraavissa kappaleissa käyn rekrytointiprosessia tarkemmin läpi.

---

[54] Joki (2021, s.69) painottaa, että rekrytointiprosessi muovautuu sen mukaisesti, minkälaiseen tehtävään, millä aikataululla ja minkä kokoisella budjetilla työvoimaa haetaan.

[55] Salli ja Takatalo (2014) määrittävät rekrytointiprosessin loppuvan valintapäätökseen. Toisaalta Kaijala (2016), Helsilä ja Salojärvi (2009), Joki (2021), sekä Rötkin (2015) liittävät perehdytyksen olennaiseksi osaksi rekrytointiprosessia. Viitala (2021) esittelee uuden näkökannan: perehdytyksen ensimmäiset vaiheet ovat osa rekrytointiprosessia, ja rekrytoinnin päätyttyä perehdytyksen viimeiset vaiheet ovat itsenäisiä kokonaisuuksia rekrytoinnin ulkopuolella.

2.3 Vaihe 1: Prosessin suunnittelu

Rekrytointiprosessin tulisi aina alkaa suunnittelusta[56]. Suunnitteluvaiheen keskeisin tehtävä on osaamismäärittely eli tiedostus siitä, millaista osaamista organisaatio on vailla[57]. Henkilötietojen käsittelyn näkökulmasta osaamistarpeen ja työtehtävän tarkka määrittely ratkaisee myös sen, mitä henkilötietoja työnhakijasta on tarpeenmukaista kerätä[58]. Työtehtävän määrityksen lisäksi tulee määritellä prosessiin osallistuvat työntekijät[59]. Usein rekrytointiin osallistuvia työntekijöitä ovat muun muassa rekrytoiva esihenkilö, HR:n edustaja sekä uuden työntekijän kollega. Johtotehtävien osalta myös hallitus saattaa osallistua prosessiin.[60] Tutkielman haastatteluissa korostui kollegan osallistamisen tärkeys: koettiin, että tiimiläiset osaavat kertoa parhaiten työarjesta käytännön tasolla. Toisaalta haastateltavat kokivat, että HR Business Partner tai rekrytoivan esihenkilön johtaja ovat toisinaan välttämättömiä prosessin onnistumisen kannalta. Perusteltu valinta rekrytoivalle tiimille riippuu täten täysin haettavan työtehtävän luonteesta.

Tärkeää hallitun rekrytointiprosessin kannalta on, että rekrytointia hoitava tiimi määritellään ennakkoon, eikä rekrytointiin osallisteta tämän tiimin ulkopuolisia työntekijöitä kesken prosessin[61]. Tämä ei kuitenkaan ole aina käytännössä mahdollista:

> *''Tietysti välillä joudutaan tuurailemaan, jos joku rekrytointitiimistä joutuu saikulle tai on pois vaikka kipeen lapsen vuoks. Tai jos kesälomien aikaan joku irtisanoutuu ja tulee nopee rekrytoinnin tarve. Sit on mentävä sillä kokoonpanolla, mikä käsiin saadaan. Et kylhän ne haasteet myllertää sitä prosessia.''*
>
> *-Haastateltava 10*

---

[56] Ennen rekrytointiprosessin käynnistystä on tarpeenmukaista miettiä, onko uuden työntekijän tarve todellinen vai voitaisiinko esimerkiksi poislähteneen työntekijän työtehtävät jakaa nykyisten työntekijöiden kesken tai työmenetelmiä kehittämällä parantaa työn tehokkuutta. Joki, 2021, s.66.
[57] Salli & Takatalo, 2014, s.15–24; Rötkin, 2015, s.47 & 57; Österberg, 2015, s.91.
[58] Organisaation rekrytointiprosessissa kerättävien henkilötietojen tarpeellisuutta voidaan arvioida esimerkiksi yhteystoimintamenettelyiden yhteydessä, kun laaditaan työhönoton ja siihen liittyvien henkilöarviointien periaatteita, ks. Neuvonen, 2014, s.95–96.
[59] Viitala, 2021, luku 3.3.
[60] Kaijala, 2016, s.61–63. Prosessin onnistumisen kannalta olisi hyvä, että rekrytoiva tiimi on hallittu ja tarkkaan valittu, sillä liian suuri valitsijakunta luistaa herkästi rekrytoinnille asetetuista tavoitteista.
[61] Kaijala, 2016, s.63.

Suunnitteluvaiheeseen kuuluu myös rekrytointimuodon valitseminen, sillä rekrytointi on mahdollista toteuttaa monella tapaa[62]. Koska tutkielma on rajattu analysoimaan organisaation ulkopuolisten työnhakijoiden henkilötietojen käsittelyä yrityksen itse toteuttamassa rekrytoinnissa, käsitellään tutkielmassa vain tätä rekrytointimuotoa. Suunnitteluvaiheeseen kuuluu olennaisesti myös rekrytointi-ilmoituksen teko ja päätökset siitä, missä hakukanavissa ilmoitus avoinna olevasta työpaikasta julkaistaan[63]. Myös rekrytointiluvan haku koettiin haastatteluissa osaksi rekrytointiprosessin ensimmäisiä työtehtäviä. Toisissa organisaatioissa rekrytointilupa ei käytännössä edellytä toimenpiteitä. Isommissa organisaatioissa rekrytointilupa saattaa puolestaan vaatia kirjallista suostumusta, jonka saaminen voi edellyttää hierarkkisen toimintaketjun läpikäyntiä:

> *''Elikkä rekrytointi alkaa siitä, että saadan rekrylupahakemus läpi. Sen luvan saamiseen on meijän organisaatiossa tietyt stepit ja se lupa tulee hyväksymiskierroksen kautta. Vasta luvan jälkeen voidaan alkaa etsiä hakijoita.''*
>
> *-Haastateltava 8*

2.4 Vaihe 2: Hakijahankinta

Rekrytointiprosessin toisessa päävaiheessa keskitytään hakijoiden houkutteluun: avoinna olevan työpaikan hakuilmoitus julkaistaan valitussa hakukanavassa, jo hakeneiden ehdokkaiden kanssa panostetaan laadukkaaseen hakijaviestintään, ja potentiaalisia muita ehdokkaita lähestytään[64]. Etenkin asiantuntijarekrytoinneissa pelkkä ilmoitus avoinna olevasta paikasta ei riitä, tai sitä ei imagovaikutusten vuoksi välttämättä haluta

---

[62] Rekrytointi voi olla sisäistä (*internal recruitment*), jolloin työntekijä palkataan organisaatiosta. Tämä tunnetaan myös nimellä *sisäinen siirto*. Yrityksen ulkopuolinen rekrytointi on puolestaan ulkoista rekrytointia (*external recruitment*) ks. O'Meara & Petzall 2013, s. 75–78; Phillips & Gully, 2017, s.32–35; Kaijala & Tolvanen, 2020, s.130. Rekrytointi voi myös olla luonteeltaan joko perinteistä rekrytointia tai suorahakua (*headhunting*). Perinteisessä rekrytoinnissa työnhakijat hakevat organisaatioon, ja suorahaussa organisaation edustajat tai ostettu palveluntarjoaja lähestyy potentiaalisia työntekijöitä, ks. Hoppe, 2014, s.93; Coverdill & Finlay, 2017, s.135–154.

[63] Pelkkä selostus siitä, mitä työtehtäviä uusi työntekijä tulisi organisaatiossa tekemään ei riitä. Tämän lisäksi työpaikkailmoituksessa tulee perustella, miksi organisaatio tarvitsee kyseistä työntekijää eli mikä on työtehtävän olemassaolon perimmäinen tarkoitus, Rötkin, 2015, s.47–50. Ilmoituskanavan valinnassa kannattaa puolestaan pohtia, mitä kanavaa työtehtävään sopivat ehdokkaat seuraavat, Salli & Takatalo, 2014, s.25–30. Ilmoituskanavan valinnassa voi olla myös luova: rekrytointimessuja, korkeakoulujen ja oppilaitosten rekrytointipalveluita, sekä asiakkaiden, alihankkijoiden tai kilpailijoiden sidosryhmiä voi hyödyntää, Viitala, 2021, luku 3.3. Kriittistä on huomioida, että hakukanavan valinta vaikuttaa yrityksen työnantajamielikuvaan, Österberg, 2015, s.94.

[64] Salli & Takatalo, 2014, s.31–35.

edes tehdä[65]. Siksi organisaatioilta vaaditaan myös proaktiivista lähestymistapaa, jossa yrityksen arvoja, strategiaa ja avoinna olevaa työpaikkaa pyritään myymään potentiaalisille ehdokkaille henkilökohtaisesti[66]. Tätä kutsutaan hybridirekrytoinniksi: perinteisen ilmoitteluhaun ohella organisaatio on itse aktiivinen. Työnhakijoiden proaktiivinen lähestyminen korostui myös tutkielman haastatteluissa:

> *''Kyllähän tavote on se, että meillä on organisaatiossa jo valmiiks rakennetut talentpoolit, joiden avulla voidaan ottaa yhteyttä sellasiin ihmisiin, joilla tiedetään olevan potentiaalia menestyä meillä. Sit tietty voidaan kans ite lähestyä esim. Linkkarissa [LinkedIn – applikaatiossa] potentiaalisen olosia tyyppejä, ja kertoa meidän avoimesta paikasta heille.''*
>
> *-Haastateltava 2*

Hakijahankintavaiheessa henkilötietoja saatetaan vastaanottaa esimerkiksi työhakemuksista tai puhelimitse suorahakupuheluiden yhteydessä. Työnhakijasta tulisi kerätä vain sellaisia henkilötietoja, jotka on rekrytointiprosessin suunnitteluvaiheessa kirjattu rekrytoinnin onnistumisen näkökulmasta tarpeenmukaisiksi. Toisinaan organisaatiot saattavat kuitenkin ymmärtää vasta kesken prosessin, millaista työntekijää he todellisuudessa tarvitsisivat. Siksi työnhakijoista saatetaan kerätä toisistaan poikkeavia henkilötietoja. Lisäksi rekrytoiva tiimi ei voi aina vaikuttaa siihen, mitä henkilötietoja hakijasta käsitellään rekrytointiprosessin aikana: työnhakija päättää itse, mitä henkilötietoja hän itsestään kertoo esimerkiksi CV:ssä, työhakemuksessa tai muussa viestinnässä.

2.5 Vaihe 3: Hakijavalinta

Seuraavaksi rekrytointiprosessi etenee potentiaalisten ehdokkaiden luokitteluun ja karsintaan[67]. Hakijavalinta perustuu usein henkilöarviointiin, jossa analysoidaan muun muassa työnhakijan pätevyyttä, motivaatiota sekä persoonallista yhteensopivuutta organisaatioon [68] . Lähtökohtaisesti valintaprosessiin kuuluu vähintään haastattelut ja

---

[65] Rekrytointiprosessi, jossa julkaistaan työpaikkailmoitus, soveltuu nykypäivänä pääosin vain suoritettavien tehtävien käyttöön. Nykyaikaiset asiantuntijat tietävät osaamisensa ja hintansa sille, ks. esim. Kaijala, 2016, s.15. Lisäksi esimerkiksi toimitusjohtajan rekrytointi hoidetaan usein julkisuudelta piilossa, ks. esim. Miles & Larcker, 2010, s.11–15. Tällöin rekrytointiprosessiin ei kuulu ollenkaan hakuilmoituksen käyttö.

[66] Kaijala, 2016, s.64.

[67] Rötkin, 2015, s.57–63. Työnhakijoiden luokittelusta rekrytointiprosessissa käytetään myös nimitystä shortlistaus, ks. esim. Viitala, 2021, luku 3.3.

[68] Syrjänen, 2006, s.161; Honkanen, 2005, s.12–15; Honkaniemi, 2007, s.20.

suosittelijoiden tarkastus[69]. Rekrytoivan tiimin tulee muistaa, että hakijalta on ehdottoman tärkeää saada lupa suosittelujen selvitykseen. Tämä perustuu työelämän tietosuojalain 4 §:n edellytykseen siitä, että työnantajan on hankittava työnhakijaa koskevat tiedot lähtökohtaisesti työnhakijalta itseltään. Lisäksi osa organisaatioista hyödyntää ennalta nauhoitettuja videoita, joissa työnhakija nauhoittaa vastauksensa rekrytointitiimin asettamiin kysymyksiin. Myös soveltuvuusarviointeja, portfolioita ja koetehtäviä käytetään toisinaan valintapäätöksen tukena[70]. Lopullinen päätös on syytä pohjautua suunnitteluvaiheessa asetettuihin kriteereihin ja se tulee tehdä ripeästi, kuitenkaan hosumatta[71].

Tyypillisesti HR:n edustajat esittelevät valintavaiheessa potentiaaliset hakijat rekrytoivalle esihenkilölle ja mahdollisesti tiimiläisille. Toisinaan HR-yksikön puuttuessa hoitaa esihenkilö itsenäisesti tämänkin työvaiheen. Valintavaiheessa yritysten tulisi kerätä työnhakijoista henkilötietoja, jotka eivät ole vielä tulleet ilmi, ja jotka ovat valinnan kannalta tarpeenmukaisia. Tällaisia henkilötietoja voivat olla muun muassa hakijan asenne, tarkentavat tiedot työ- tai koulutustaustasta, sekä tulevaisuuden uratavoitteet. Henkilötietojen suojan näkökulmasta on kriittistä noudattaa rekrytointisuunnitelmaa, jossa on määritelty, ketkä käsittelevät työnhakijoiden henkilötietoja. Esimerkiksi rekrytointiin osallistuvan kollegan ei tarvitse saada tietoonsa työnhakijan kaikkia henkilötietoja.

2.6 Vaihe 4: Työsopimus ja perehdytyksen aloitus

Rekrytointiprosessin viimeinen päävaihe sisältää työsopimukseen ja perehdytykseen liittyviä työtehtäviä[72]. Valitulle työnhakijalle tehdään työtarjous, minkä jälkeen tarjousta

---

[69] Kaijala, 2016, s.65–66. Suosittelijoihinkin kannattaa suhtautua kriittisesti, ks. Salli & Takatalo, 2013, s.87

[70] Soveltuvuusarviointien koetaan nostavan rekrytointipäätöksen luotettavuutta, ja niitä kannattakin hyödyntää erityisesti työtehtävissä, joissa palkkakustannukset tai mahdolliset imagohaitat rekrytoinnin epäonnistumisesta olisivat suuret, ks. Salli & Takatalo, 2014, s.79–84. Joki korostaa, että soveltuvuusarviointeja tulisi käyttää ainoastaan valintapäätöksen tukena, eikä päätös saisi koskaan perustua ainoastaan soveltuvuusarvion antamaan tulokseen, ks. Joki, 2021, s.79–80. Koetehtävät voivat olla apuna etenkin ICT-puolen rekrytoinneissa. Rekrytointiprosessin soveltuvuustestien teko vaatii aina työnhakijan suostumuksen. Samanaikaisesti työnantajan ei tarvitse valita hakijaa, joka ei suostu testeihin, ks. Parnila, 2017, s.40.

[71] Salli & Takatalo, 2014, s.85: Mikäli prosessissa ei löydy sopivan oloista hakijaa, ei tule rekrytoida ketään.

[72] Viitala, 2021, luku 3.3. Perehdytys tulisi aloittaa jo rekrytointiprosessin aikana: työnhakijalle tulisi antaa tietoja organisaatiosta, sekä työhön liittyvistä yksityiskohdista ennen ensimmäistä varsinaista työpäivää.

hiotaan osapuolten toiveiden mukaisesti. Sitten luodaan työsopimus, jonka molemmat osapuolet allekirjoittavat. Tähän työvaiheeseen sisältyy myös henkilötietojen käsittelyä:

> *''Rekrytointiprosessin kannalta viimeiset henkilötiedot hakijasta kerätään sopimusvaiheessa. Silloin pitää olla tiedossa tilinumero, hetu, osote ja yleensä myös lähiomaisen yhteystiedot. Mut ne tarvitaan vasta sitten ku hän on vastannut myöntävästi työtarjoukseen.''*
> *-Haastateltava 1*

Työsopimuksen luomiseen tarvitaan työnhakijan henkilötunnus ja kotiosoite, jotta ihminen voidaan yksilöidä ja sopimuksesta saadaan sitova[73]. Tilinumero tarvitaan puolestaan palkanmaksua varten. Tiedot lähiomaisista ovat lähtökohtaisesti vapaaehtoisia, mutta esimerkiksi ulkomaankomennuksien yhteydessä työnantajan saattaa olla tarpeellista tietää perhesuhteista tavallista enemmän[74]. Kun työsopimus on allekirjoitettu, jäljellä on perehdytyksen aloitus ja ei-valittujen hakijoiden henkilötietojen poistaminen[75]. Lisäksi työsopimuksen arkistointi sisältää henkilötietojen käsittelyä, kun sekä työsopimus, että osa uuden työntekijän henkilötiedoista siirretään ja tallennetaan organisaation järjestelmiin. Tällaiset työtehtävät sijoittuvat ajallisesti sopimusvaiheen ja perehdytysvaiheen välimaastoon. Kun uusi työntekijä aloittaa työnteon ensimmäisenä työpäivänään, voidaan rekrytointiprosessi katsoa päättyneeksi, jolloin myös henkilötietojen käsittely rekrytointiprosessissa päättyy, ja työntekijän henkilötietojen käsittely työsuhteessa alkaa.

---

[73] TSA:n artiklojen 87:n ja 88:n mukaisesti jäsenvaltiot voivat määritellä henkilötunnuksen käsittelyn edellytykset, sekä säätää kansallisesti yksityiskohtaisemmin henkilötietojen käsittelystä työsuhteessa. Henkilötunnusta saa käsitellä tilanteissa, joissa yksiselitteinen yksilöiminen on tärkeää. Tämä kriteeri täyttyy työsuhteen ja sen etuja koskevissa asioissa: työsuhteen solmiminen ja julkisella sektorilla virkasuhteeseen nimitys vaativat työntekijän yksilöinnin, ks., tietosuojalaki 29§; Järvinen, 2022, s.25; Parnila, 2017, s. 43; Neuvonen, 2014, s.98.

[74] HE 75/2000, s.15–16. On hyvä huomioida, ettei työnantajalla ole yleistä velvollisuutta onnettomuustilanteessa ilmoittaa lähiomaisille: se on viranomaisten tehtävä, ks. Tietosuojavaltuutetun toimisto, Työelämän tietosuojan käsikirja, s.20. Käytännössä kuitenkin työntekijä saa halutessaan jakaa lähiomaistensa tietoja työnantajalle lähiomaisten suostumuksella esimerkiksi juuri työtapaturmien tai työntekijän pitkäaikaissairauden vuoksi.

[75] Rekrytointiprosessissa hylätyille hakijoille tulee hyvän liiketavan hengessä viestiä hylkäyksestä mahdollisimman nopeasti. Lisäksi rekisterinpitäjän tulee poistaa ei-valittujen hakijoiden henkilötiedot, kun henkilötietoja ei enää tarvita niiden alkuperäiseen tarkoitukseensa, TSA 17 artikla, kohta 1 ja TSA, 5 artikla kohta 1. Jos työnhakija koetaan potentiaaliseksi yrityksen muihin tulevaisuudessa mahdollisesti avattaviin rooleihin, tulee hakijalta pyytää suostumusta säästää hänen henkilötietojansa tällaista menettelyä varten, ks. Korpisaari ja muut, 2022, s.249. Korpisaaren ja muiden (2022, s.249) tulkinnan perusteella ei-valittujen työnhakijoiden henkilötiedot voi poistaa jo silloin, kun työhön palkatun työntekijän koeaika päättyy. Otan tutkielmassa kuitenkin laajemman tulkinnan henkilötietojen poistamisesta, katso tutkielman sivu 32–33.

3 Oikeus suojaamassa henkilötietojen väärinkäyttöä rekrytoinnissa

3.1 Henkilötietojen käsittely ja sen oikeusperusta

Tutkielman tietosuojariskien oikeudellisen arvioinnin lähtökohtana on, että koko rekrytointiprosessin elinkaari aina rekrytoinnin suunnittelusta henkilötietojen poistamiseen saakka on rekisteröidyn henkilötietojen käsittelyä[76]. Tietosuoja-asetuksessa luetellaan henkilötietojen käsittelyn tunnuspiirteitä, ja voidaankin havaita, että henkilötietojen käsittely voi kohdistua joko pelkkiin henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin ja se voi olla luonteeltaan sekä automaattista että manuaalista[77]. Rekrytointi-prosessissa työnhakijasta kerättävät tiedot ovat lähes poikkeuksetta pelkkiä henkilötietoja, mutta toisinaan esimeriksi työhakemuksen motivaatiokirjeessä saattaa olla muitakin kuin pelkkiä henkilötietoja. Koska hakemus sisältää myös henkilötietoja, luetaan työhakemuksen käsittely henkilötietojen käsittelyksi. Rekrytointiprosessin henkilötietojen manuaalisella ja automaattisella käsittelyllä tarkoitetaan puolestaan sitä, miten henkilötietoja käsitellään. Analysoin henkilötietojen automaattista käsittelyä myöhemmin tutkielmassa rekisteröidyn oikeuksien yhteydessä.

Koska rekisteröity – eli rekrytointiprosessissa työnhakija – on lähtökohtaisesti heikommassa asemassa rekisterinpitäjää kohtaan, on rekisteröidyn oikeuksien varmistamiseksi henkilötietojen käsittelyä säännelty lainsäädännön keinoin[78]. Henkilötietojen suojasta

---

[76] Katso tietosuoja-asetuksen ja tutkielman tarkka määritelmä henkilötietojen käsittelylle tutkielman sivulta 14, sekä tutkielman määritelmä rekrytointiprosessille sivulta 18.

[77] TSA 4 artiklan 2 kohdan mukaisesti henkilötietojen käsittelyllä tarkoitetaan *''toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti''*.

[78] Rekisteröidyn oikeudet perustuvat sekä ihmisoikeuksiin että niin kutsuttuun heikomman suojaan. *Heikomman suoja* on sopimusoikeuteen keskeisesti liittyvä oikeusperiaate, jolla pyritään varmistamaan sopimussuhteen olevan vastavuoroinen, eikä alisteinen tai pakkoon pohjautuva. Esimerkiksi osapuolten kokemus, taloudellinen asema, juridinen osaaminen tai muu epätasavertaisuutta aiheuttava tekijä johtaa lähtökohtaisesti heikomman suojan soveltamiseen sopijakumppaneiden välillä. Heikomman suojan periaate rajoittaa sopimusvapautta myös työsuhteen solmimisessa, ks. Karhu, Tolonen ja Ämmälä, 2012, s.101–102.

on säädetty sekä eurooppaoikeudellisella, että kansallisella tasolla[79]. Aihetta on sivuttu ensimmäisiä kertoja jo vuonna 1948, kun Yhdistyneiden kansakuntien ihmisoikeuksien yleismaailmallisessa julistuksessa käsiteltiin yksityiselämän suojaa ja siihen liittyviä oikeuksia[80]. Myös Euroopan ihmisoikeussopimuksessa käsitellään oikeutta nauttia yksityis- ja perhe-elämän kunnioituksesta[81]. Näiden ohella Euroopan unionin perusoikeuskirjan 8 artiklan ja Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 16 artiklan mukaisesti jokaisella EU:n kansalaisella on oikeus henkilötietojensa suojaan[82].

Lukijan on hyvä havaita, että edellä mainitut säädökset ovat kaikki kansainvälisiä oikeuslähteitä. Kansalliset ja kansainväliset oikeuslähteet elävät ja vaikuttavat vuorovaikutuksessa[83]. Lisäksi kansainvälistyminen on vaikuttanut viimeisten vuosikymmenten aikana voimakkaasti Suomen oikeusjärjestyksen lähdepohjaan. Sovellettavasta normistokokonaisuudesta on siten tullut myös pirstaleinen.[84]. EU-oikeus on toisinaan hierarkkisesti korkeammassa asemassa kansallisiin oikeuslähteisiin nähden, minkä vuoksi esimerkiksi tietosuoja-asetusta sovelletaan EU:n jäsenmaissa *yli* kansallisten lakien[85]. Tämä tarkoittaa, että tietosuojalain ja tietosuoja-asetuksen ristiriitatilanteissa tietosuoja-asetuksen säännöksiä tulee noudattaa[86].

---

[79] Ks. esim. Euroopan unionin perusoikeuskirja 2000/C 364/01, 8 artikla; tietosuoja-asetus 769/2016; Euroopan ihmisoikeussopimus 19/1990, artikla 8; Suomen perustuslaki 731/1999, 10§; tietosuojalaki 1050/2018. Lisäksi aikanaan tietosuojalainsäädännön asemaa vakiinnuttivat jo kumoutuneet henkilötietodirektiivi 95/46/EY, henkilörekisterilaki (471/1987), sekä henkilötietolaki (523/1999).

[80] Korpisaari ja muut, 2022, s.4–5; Kuopus, 1985, s.122. Yhdistyneiden kansakuntien lisäksi OECD (Organization for Economic Cooperation and Development) on ollut merkittävä toimija myöhemmin 1980- ja 1990-luvuilla tietoverkkojen ja tietojärjestelmien turvallisuusperiaatteiden kehittäjänä, ks. Saarenpää & Wiatrowski, 2016, s.224.

[81] SopS 19/1990, artikla 8.

[82] Euroopan unionin perusoikeuskirja 2000/C 364/01, artikla 8; SEUT 16 artikla.

[83] Pääpiirteiltään Suomen oikeus kuuluu länsimaalaisen romaanisgermaanisen oikeusjärjestyksen ryhmään. Suomessa ensisijaisesti etenkin eduskunnan tehtävänä on varmistua siitä, että maamme oikeusolot ovat Suomea sitovien kansainvälisten sopimusjärjestelyiden, kuten Euroopan ihmisoikeussopimusten, vaatimalla tasolla, ks. Hyvärinen, Hulkko & Ohvo, 2002, s.25–26.

[84] Oikeuslähdepohjan laajentuessa voimme huomata säädöshierarkian samalla monimutkaistuvan, ks. Kanninen, 2009, s.175–176; Tala, 2000, s.390–392. Kansallisia oikeusnormeja ovat muun muassa kansalliset lait, asetukset, yleiset oikeusperiaatteet sekä suomalaisten tuomioistuinten ratkaisut. Lisäksi Suomea sitoo kaikki EU:n sisällä solmitut sopimukset, joihin kuuluvat muun muassa Euroopan unionin perussopimukset, asetukset, direktiivit ja päätökset, ks. Nykänen, 2013, s.28–29 & 68.

[85] Ojanen, 2016, s.43–45. Euroopan unionin asetus on oikeuslähteenä velvoittavampi kuin kansallinen laki.

[86] SEUT 288.2 artikla: Asetus *''pätee yleisesti''*, *''on kaikilta osin velvoittava''* ja *''sitä sovelletaan sellaisenaan kaikissa jäsenvaltioissa''.*

Vuonna 2018 voimaan astunut tietosuoja-asetus heijastelee niitä periaatteita, oikeuksia ja velvollisuuksia, jotka ovat edeltäneiden vuosikymmenten aikana muotoutuneet henkilötietojen käsittelyn viitekehyksessä. Tietosuoja-asetus on ollut yksi 2000-luvun merkittävimmistä askelista kohti yksityishenkilöiden perusoikeuksien vahvistamista.[87] Asetuksessa on korostettu erityisesti rekisteröityjen asemaa vahvistamalla uusia ja tarkentamalla aiempia oikeuksia[88]. Lisäksi oikeuksien käyttöä on pyritty helpottamaan.[89] Rekrytointiprosessin tietosuojariskien hallinnassa yritysten tulee tiedostaa näkökulma, jonka valossa asetus on luotu: rekisterinpitäjällä on osoitusvelvollisuus asetuksen noudattamisesta[90]. Tutkielman toimintaohjeistus rekrytointiprosessin tietosuojariskien hallintaan pohjautuu vahvasti tietosuoja-asetukseen, sillä se on Suomen kannalta tärkein henkilötietoja koskeva säädös. Lisäksi sitä sovelletaan aina, kun on kyse henkilötietojen käsittelystä tilanteesta riippumatta.[91] Tämän vuoksi tietosuoja-asetuksen vaatimuksilla on keskeinen vaikutus henkilötietojen suojaamiseen myös rekrytointiprosessissa.

Henkilötietojen käsittelyllä on tietosuoja-asetuksen mukaisesti oltava oikeusperuste[92]. Oikeusperusteet asettavat raamit sille, milloin henkilötietojen käsittely on lainmukaista.

---

[87] Euroopan komissio, 2022a. Tietosuoja-asetuksen myötä myös Suomessa lainsäädäntöä uudistettiin: henkilötietolaki 523/1999 kumottiin, ja tietosuojalaki 1050/2018 säädettiin täydentämään yleisen tietosuoja-asetuksen vaatimuksia, ks. HE 9/2018 vp. Euroopan parlamentti ja neuvosto katsoi 2010-luvun alkupuolella, että tietosuojadirektiivi 95/46/EY ei enää riittänyt turvaamaan tietosuojaa esimerkiksi tiedon lisääntyneen jakamisen sekä teknologian kehityksen vuoksi, ks. esim. KOM (2012) 11, s.1–4; KOM (2010) 609 lopullinen, s.2. Erityisesti teknologian kehitys ja globalisaatio ovat muokanneet kansainvälistä liiketoimintaympäristöä niin merkittävästi, että tietosuojalakien yhdenmukaistamista ja uudistamista pidettiin välttämättömänä, ks. Burri ja Schär, 2016, s.480; Korpisaari ja muut, 2022, s.19–20.

[88] Korpisaari ja muut, 2022, s. 20 & s.40–41. Luonnollisten henkilöiden perusoikeuksien ja -vapauksien suojelu on ollut tietosuoja-asetuksen keskeisin tavoite. Asetuksella on pyritty myös edesauttamaan digitaalitalouden kasvua. Tarkoituksena ei siis ole ollut estää henkilötietoihin perustuvaa liiketoimintaa, vaan asettaa sille lailliset raamit, ja määritellä millainen henkilötietojen hyödyntäminen on sallittua.

[89] Tietosuoja-asetuksen 15 artikla: rekisteröidyn oikeus saada pääsy tietoihin; 16 artikla: oikeus tietojensa oikaisemiseen; 17 artikla: oikeus tietojensa poistamiseen; 18 artikla: oikeus käsittelyn rajoittamiseen; 20 artikla: oikeus siirtää tiedot järjestelmästä toiseen; 21 artikla: henkilötietojen käsittelyn vastustamisoikeus. Rekisteröidyn oikeuksista kattavasti on kirjoittanut esimerkiksi Hanninen ja muut, 2017, s.56–72.

[90] Pelkkä tietosuoja-asetuksen vaatimusten noudattaminen ei enää riitä: vuonna 2018 voimaan astuneen tietosuoja-asetuksen myötä organisaatioiden tulee myös kyetä todistamaan vaatimusten mukainen toiminta, ks. Hanninen ja muut, 2017, s.56.

[91] Tietosuoja-asetus on voimassa olevaa EU-oikeutta, minkä vuoksi Suomen tulee EU:n jäsenvaltiona noudattaa sen vaatimuksia. Lisäksi asetus on oikeuslähteenä hierarkkisesti kansallista oikeutta korkeammassa asemassa, ks. tutkielman sivu s.12, sekä Aalto-Setälä & Viitaila, 2018, s.5.

[92] Tietosuoja-asetuksen lähtökohta on se, että henkilötietojen käsittely on lainmukaista ainoastaan silloin, kun yksi lainmukaisuuden edellytyksistä täyttyy, ks. TSA 6 artikla; TSA johdanto kohta 40.

Tämä on yksi lainsäädännön keinoista, joilla työnhakijan henkilötietoja pyritään suojaamaan rekrytointiprosessissa. Henkilötietojen käsittely voi perustua joko rekisteröidyn suostumukseen, sopimukseen, lakisääteiseen velvoitteeseen, elintärkeään etuun, yleiseen etuun tai rekisterinpitäjän sekä kolmannen oikeutettuun etuun[93]. Rekrytointiprosessissa henkilötietojen käsittelyn oikeusperusteita on lähtökohtaisesti kaksi. Ensimmäinen oikeusperuste on rekisteröidyn *suostumus*. Jotta rekisteröidyn henkilötietojen käsittely on lainmukaista – ja mikäli muut asetuksen asettamat oikeusperusteet eivät täyty – tulee rekisterinpitäjän saada työnhakijalta vapaaehtoinen, yksilöity sekä yksiselitteinen tahdonilmaisu siitä, että työnhakija on hyväksynyt henkilötietojensa käsittelyn.[94] Rekrytoivan yrityksen on huomioitava, että suostumuksen vapaaehtoisuus tulee kyetä osoittamaan. Lisäksi rekisteröidyn tulee voida kieltäytyä suostumuksen antamisesta ilman haitallisia seuraamuksia.[95]

Toinen henkilötietojen käsittelyyn oikeuttava oikeusperuste esiintyy rekrytointiprosessin loppupuolella, kun työsopimusvaiheessa muodostuu *tarve luoda sitova työsopimus* rekisteröidyn ja rekisterinpitäjän välille[96]. Tietosuoja-asetuksen vaatimusten mukaisesti työnhakijan henkilötietoja ei saa tässäkään vaiheessa rekrytointia kerätä tarpeettoman laajasti, ja henkilötietojen käsittelyn laajuus tulee olla työnhakijan kannalta ennalta arvattavaa[97]. Lähtökohtaisesti henkilötietojen käsittely sopimusta varten on sallittua silloin, kun sopimusta ei olisi mahdollista luoda ilman henkilötietojen käsittelyä. Lisäksi henkilötietojen tarpeellisuutta tulee arvioida tapauskohtaisesti ja suppeasti[98].

---

[93] TSA 6 artikla kohdat a–f; TSA 85 artikla. Henkilötietojen käsittelyn oikeusperusteiden englanninkieliset vastineet ovat: rekisteröidyn suostumus (*consent of the data subject)*, sopimus (*contract*), lakisääteinen velvoite (*legal obligation*), elintärkeä etu (*vital interests*), yleinen etu (*a task carried out in the public interest*) sekä rekisterinpitäjän tai kolmannen oikeutettu etu (*legimitate interests*).

[94] TSA 4 artikla kohta 11; Tietosuojavaltuutetun toimisto, n.d., Rekisteröidyn suostumus.

[95] TSA 7 artikla kohdat 1–4; Korpisaari ja muut, 2022, s.146.

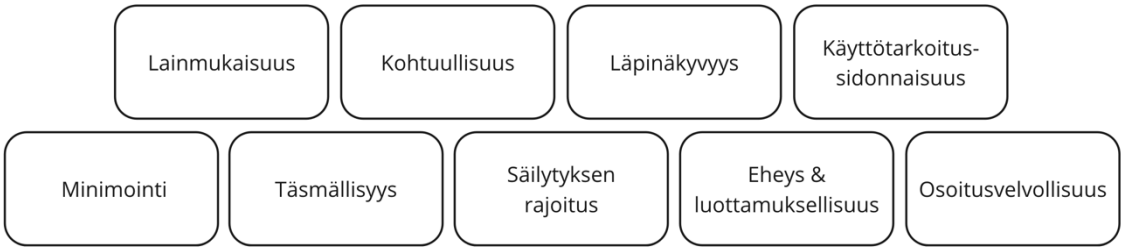
[96] TSA 6 artikla kohta a: *''käsittely on lainmukaista, kun rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten*'' sekä TSA 6 artikla kohta b: *''käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä''*. Henkilötietojen käsittely työsopimuksen vuoksi ei siten perustu *sopimukseen*, vaan pikemminkin sopimuksen *täytäntöönpanoon*.

[97] TSA 5 artikla, yleiset tietosuojaperiaatteet.

[98] Voigt & Bussche, 2017, s. 102; Korpisaari ja muut, 2022, s.119; Hanninen ja muut, 2017, s. 47.

3.2 Tietosuojaperiaatteet ohjaamassa henkilötietojen käsittelyä

Tietosuoja-asetuksen 5 artikla määrittää yleiset periaatteet, joita henkilötietojen käsittelyssä on noudatettava. Periaatteita kutsutaan yleisiksi tietosuojaperiaatteiksi ja ne suojaavat rekisteröidyn henkilötietoihin kohdistuvia oikeuksia myös rekrytoinnin aikana.[99] Tietosuojaperiaatteet on havainnollistettu oheiseen kuvioon (kuvio 4).



Kuvio 4. Yleiset tietosuojaperiaatteet[100].

Kuvion (kuvio 4) mukaisesti tietosuojaperiaatteet ovat: lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, sekä eheys ja luottamuksellisuus. Lähtökohtaisesti tietosuojaperiaatteet eivät ole uusia: ne muistuttavat asetuksen edeltäjän, tietosuojadirektiivin 95/46/EY artiklan 6 mukaisia tietosuojaperiaatteita. Uutta asetuksessa oli kuitenkin se, että rekisterinpitäjällä on osoitusvelvollisuus periaatteiden noudattamisesta.[101] Rekrytoivalle organisaatiolle tämä tarkoittaa sitä, että pelkkä asetuksen vaatimusten noudattaminen ei enää riitä, vaan se on kyettävä todistamaan sekä rekisteröidylle että viranomaisille.

Tarkastelen seuraavaksi tietosuojaperiaatteiden merkitystä rekrytointiprosessin osalta. Ensimmäiseksi analysoitavana ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys. Tietosuoja-asetuksen mukaan henkilötietojen käsittely on lainmukaista sen pohjautuessa

---

[99] Korpisaari ja muut, 2022, s. 99 & 112. Englanninkielinen ilmaisu tietosuojaperiaatteille on *Data Protection Principles* sekä *Data Quality Principles*, ks. Lambert, 2017.

[100] TSA 5 artikla.

[101] TSA 5 artikla kohdat a–f; Korpisaari ja muut, 2022, s. 99. Tietosuojaperiaatteiden englanninkieliset vastineet ovat: lainmukaisuus (*lawfulness*), kohtuullisuus (*fairness*), läpinäkyvyys (*transparency*), käyttötarkoitussidonnaisuus (*purpose limitation*), tietojen minimointi (*data minimisation*), täsmällisyys (a*ccuracy*), säilytyksen rajoittaminen (*storage limitation*) sekä eheys ja luottamuksellisuus (*integrity and confidentiality*), ks. TSA englanninkielinen versio.

oikeusperusteeseen[102]. Kohtuullisuudella viitataan yleiseen reiluuteen. Rekrytointiprosessin kannalta tämä tarkoittaa, että rekrytoiva yritys ottaa henkilötietojen käsittelyssä huomioon työnhakijan edut ja odotukset. Tämän ohella kohtuullisuuden periaatteella on pyritty varmistamaan, että rekisteröity on tietoinen käsittelyn luonteesta ja tarkoituksesta.[103] Läpinäkyvyyden periaate pyrkii puolestaan tasapainottamaan rekisterinpitäjän ja rekisteröidyn välistä tiedollista epätasapainoa: rekisterinpitäjä nimittäin tietää rekrytoinnin edetessä rekisteröidystä yhä enemmän, vaikkei rekisteröity välttämättä tiedä, mihin ja kuinka laajalle hänen tietojansa saatetaan hyödyntää[104]. Henkilötietojen käsittely voidaan katsoa rekrytointiprosessissa kohtuulliseksi ja läpinäkyväksi, kun työnhakijalle viestitään selkeää ja ymmärrettävää kieltä käyttäen, millä laajuudella sekä kuinka kauan henkilötietoja käytetään. Lisäksi työnhakijalle tulee viestiä, millaisia oikeuksia hänellä on henkilötietoihinsa.[105] Kuvaus henkilötietojen käsittelystä rekrytoinnin aikana voidaan viestiä esimerkiksi vakiomuotoisilla kaavakkeilla tai tietosuojaselosteella[106].

Yksinkertaistettuna käyttötarkoitussidonnaisuus, tietojen minimointi sekä täsmällisyys tarkoittaa, että henkilötietoja tulee käsitellä vain rekrytointiprosessin tehtävien hoitamiseksi ja tietojen keräys tulee rajautua siihen, mikä on henkilötietojen käsittelyn tarkoituksen – eli rekrytoinnin valintapäätöksen – kannalta välttämätöntä. Lisäksi työnhakijoiden henkilötietoja tulee täsmällisyyden periaatteen mukaisesti päivittää tarvittaessa.[107]

---

[102] Katso oikeusperusteista tarkemmin Korpisaari ja muut, 2022, s.99–100 sekä tutkielman sivuilta 29–30. Oikeusperusteet eivät olet toisiaan poissulkevia: useampi oikeusperuste voi olla yhtäaikaisesti käsillä, ks. Hanninen ja muut, 2017 s.29. Rekrytoinnin osalta tämä voi tarkoittaa esimerkiksi sitä, että rekisteröidyn henkilötietoja käsitellään sekä hänen suostumukseensa perustuen, että työsopimuksen luomista varten.

[103] Korpisaari ja muut, 2022, s.97–101. Kohtuullisuuden periaate liittyy läheisesti käyttösidonnaisuusperiaatteen ydinsisältöön.

[104] Korpisaari ja muut, 2022, s.102.

[105] TSA 12 artikla; Hanninen ja muut, 2017, s.48; Voigt ja Bussche, 2017, s.143–144.

[106] Tietosuoja-asetus ei määrittele tarkasti, miten henkilötietojen käsittelystä tulisi informoida rekisteröityä. Asetusta tulkittaessa voidaan ajatella, että esimerkiksi informointivideo, virtuaalitodellisuuden toteutus tai kuvat käyvät myös tavoiksi tiedottaa rekisteröityä hänen henkilötietojensa käsittelystä, katso tarkemmin Hanninen ja muut 2017, s.48 & s.73–78. Tietosuojaseloste ei ole tietosuoja-asetuksen mukainen virallinen termi: se on yksi toteuttamistapa, jolla rekisterinpitäjä voi toteuttaa niin kutsuttua informointivelvollisuuttaan läpinäkyvästä toiminnasta henkilötietojen käsittelyssä. Tietosuojaselosteesta käytetään myös nimitystä tietosuojailmoitus, ks. Korpisaari ja muut, 2022, s.195.

[107] Hanninen ja muut (2018, s.49–50) korostavat, että rekrytoinnin yhteydessä työnhakijalta tulee kerätä vain valintapäätöksen kannalta tarpeenmukaisia henkilötietoja. Lisäksi käyttötarkoitussidonnaisuuden

Säilytyksen rajoittamisen periaatteella pyritään puolestaan siihen, että henkilötietojen säilytysaika on rekrytoinnissakin mahdollisimman lyhyt. Se, miten kauan työnhakijoidensa henkilötietoja tulee säilyttää, on puolestaan tulkinnallisempi kysymys. Tietosuoja-asetuksessa ei nimittäin ole täsmällisiä vaatimuksia säilytysajasta. Kuitenkin työnhakijan oikeusturva edellyttää vähintään jopa kahden vuoden määräaikaa henkilötietojen säilytykselle rekrytoinnin päätyttyä.[108] Siksi rekrytoivan organisaation kannattanee säilyttää työnhakijoidensa henkilötietoja kaksi vuotta rekrytointivalinnasta.

Rekrytointiprosessin kannalta eheyden ja luottamuksellisuuden tietosuojaperiaatteilla pyritään varmistamaan, että työnhakija tietäisi jo ennen henkilötietojensa lähettämistä, että tietoja tullaan rekrytoinnin aikana käsittelemään asianmukaisesti. Luottamuksellisuudella viitataan tietosuoja-asetuksen mukaisesti siihen, että henkilötietoja tulee käsitellä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus[109]. Rekrytoinnin yhteydessä tämä tarkoittaa esimerkiksi sitä, että organisaation on varmistettava asianmukaisin teknisin toimin, ettei työnhakijan henkilötiedot häviä, tuhoudu tai vahingoitu, eikä asiattomilla ole pääsyä henkilötietoihin[110].

---

periaatteella voidaan katsoa rajoittavan työnhakijoiden henkilötietojen käsittelyä esimerkiksi niin, ettei hakijoiden henkilötietoja, kuten sähköpostiosoitetta, saa hyödyntää vaikkapa suoramarkkinointiin ilman työnhakijan erillistä suostumusta.

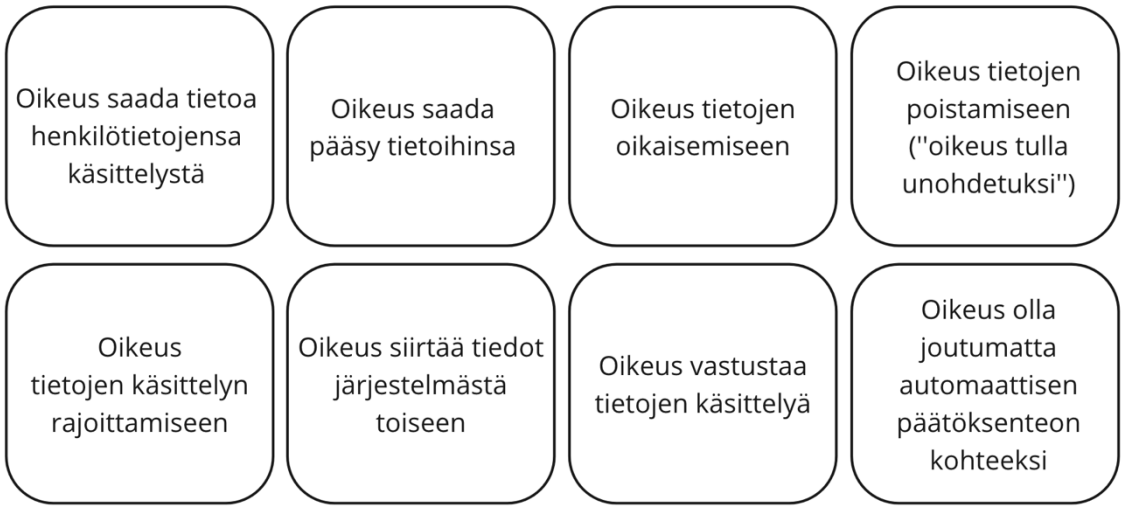
[108] Kahden vuoden määräaika kohdistuu laittoman työhönoton syrjintäkanteen nostamisen määräaikaan, ks. Neuvonen, 2014, s.97. TSA 13 artiklan mukaan henkilötietojen säilytysaika täytyy ilmoittaa rekisteröidylle jo tietoja kerättäessä. Henkilötiedot, joita ei enää tarvita rekrytoinnin suorittamiseen tulee poistaa tai anonymisoida, ks. Korpisaari ja muut, 2022, s.107. Tämä tarkoittaa sitä, että yritys voi tilastoida esimerkiksi vuositasolla työnhakijoiden lukumääriä, kunhan työnhakijoiden henkilötiedot on anonymisoitu.

[109] TSA 5 artikla kohta f. Tietosuojavaltuutetun toimisto käyttää tietosuoja-asetuksen suomennoksesta ’’eheys’’ termiä ’’turvallisuus’’, minkä voidaan nähdä olevan osuvampi suomennos, ks. Tietosuojavaltuutetun toimisto, n.d., Luottamuksellisuus ja turvallisuus. Termi oli käytössä myös henkilötietodirektiivissä, katso henkilötietodirektiivin 16 artikla sekä 17 artikla.

[110] Korpisaari ja muut, 2022, s.108. Luottamuksen periaatteen vaatimiin teknisiin toimenpiteisiin lasketaan muun muassa henkilötietojen suojaaminen salasanoilla, sekä riittävän tietoturvallisilla järjestelmillä. Lisäksi on varmistettava, ettei rekrytointijärjestelmään pääse käsiksi esimerkiksi pelkän matkapuhelimen salasanan avulla, vaan järjestelmän tulee vaatia puhelimen avauduttua vielä erillinen salasana.

3.3 Rekisteröidyn oikeudet rekrytointiprosessissa

Rekisteröidyn henkilötietoja on pyritty suojaamaan myös luomalla oikeudet, jotka rekisteröidyllä on omiin henkilötietoihinsa. Nämä oikeudet mukailevat tietosuojaperiaatteita ja niiden taustalla piilee ajatus suojata henkilötietoja oikeudetonta ja vahingollista käyttöä vastaan.[111] Tietosuoja-asetuksen mukaisesti rekisteröidyllä on oikeus saada tietoa henkilötietojensa käsittelystä, sekä saada tutustua näihin tietoihin ja oikaista tietoja. Lisäksi rekisteröity voi halutessaan rajoittaa henkilötietojensa käsittelyä, sekä pyytää henkilötietojensa poistamista. Näiden ohella rekisteröidyllä on oikeus pyytää henkilötietojensa siirtämistä järjestelmästä toiseen, sekä oikeus vastustaa henkilötietojensa käsittelyä. Digitaalisen valtakauden aikana huomionarvoista on myös se, että rekisteröidyllä on oikeus olla joutumatta automaattisen päätöksenteon kohteeksi.[112] Rekisteröidyn oikeudet on havainnollistettu oheiseen kuvioon (kuvio 5).



Kuvio 5. Rekisteröidyn oikeudet[113].

Rekisteröidyn halutessa käyttää henkilötietoihinsa kohdistuvia oikeuksiaan, on rekisterinpitäjän toimitettava tietosuoja-asetuksen 12 artiklan mukaisesti rekisteröidylle tiedot

[111] Aalto-Setälä & Viitaila, 2018, s.19.
[112] TSA artiklat 12–22. Rekisteröidyn oikeuksiin liittyy samalla rajoituksia, eivätkä kaikki rekisteröidyn oikeudet ole kaikissa tilanteissa rekisteröidyn käytettävissä, katso rajoituksista tarkemmin Tietosuojavaltuutetun toimisto, n.d., Rekisteröidyn oikeudet.
[113] TSA 12–22 artiklat.

toimenpiteistä, joihin rekisterinpitäjä on ryhtynyt oikeuksien toteuttamiseksi. Tiedot on toimitettava ilman aiheetonta viivytystä, sekä kuitenkin viimeistään kuukauden kuluessa pyynnön vastaanottamisesta.[114] Lisäksi tämän tulee lähtökohtaisesti olla rekisteröidylle maksutonta[115]. Mikäli rekisteröity haluaa saada pääsyn omiin henkilötietoihinsa, tulee rekrytoivan organisaation toimittaa työnhakijalle jäljennös käsiteltävistä henkilötiedoista[116]. Koska rekisteröidyllä on myös oikeus tietojensa oikaisemiseen, on rekrytoivan yrityksen muokattava työnhakijan henkilötiedot pyydettäessä ajantasaisiksi.

Rekisteröidyn oikeutta tulla unohdetuksi ja pyytää henkilötietojensa poistamista voidaan puolestaan pitää tulkinnallisena ja haasteellisena tehtävänä rekrytoivan yrityksen kannalta. Mikäli rekisteröity pyytää henkilötietojensa poistamista tai henkilötietojen alkuperäinen käsittelyperuste päättyy, on yrityksen ilman aiheetonta viivytystä poistettava häntä koskevat henkilötiedot. Tietosuoja-asetuksessa ei kuitenkaan määritellä, kuinka tiedot tulee teknisesti poistaa. Riittäväksi poistamiseksi ei ole katsottu tietojen ’’siirtämistä roskakoriin’’. Sen sijaan tietojen varsinaisella poistamistekniikalla ei ole väliä, kunhan rekisterinpitäjä, käsittelijä tai kolmas osapuoli ei pääse niihin käsiksi.[117] Osa tietosuojaoikeuteen perehtyneistä asiantuntijoista kokee, että mikäli yrityksen käyttämässä järjestelmässä ei ole mahdollista poistaa tietoja kokonaan, riittäisi tietojen aktiivisen käsittelyn estäminen rajaamalla käyttäjien pääsyä henkilötietoihin[118].

---

[114] Jos työnhakija esittää pyyntönsä henkilötietojansa kohtaan sähköisesti, on tiedot toimitettava yleisesti käytetyssä sähköisessä muodossa, ellei rekisteröity pyydä toisin.

[115] TSA artiklojen 13–22 nojalla toimitetut tiedot ovat rekisteröidylle maksuttomia, ellei rekisteröidyn pyynnöt ole ilmeisen kohtuuttomia ja perusteettomia. Tällöin rekisterinpitäjä voi joko periä kohtuullisen maksun tai kieltäytyä suorittamasta pyydettä toimea, ks. TSA 12 artikla 5 kohta. Ensimmäisen jäljennöksen tulisi aina lähtökohtaisesti olla ilmainen, ks. Voigt & Bussche, 2017, s.152.

[116] Rekrytoivan organisaation on toimitettava rekisteröidylle TSA:n 15 artiklan 1 kohdan a–h alakohtien mukaiset tiedot.

[117] Tietojen poistaminen näennäisesti siirtämällä ne vain roskakoriin, ei ole tarpeeksi riittävä toiminto tietojen poistamiseksi, sillä tällöin ne on helppo hakea takaisin käsiteltäväksi. Varsinaisten välttämättömien poistotoimenpiteiden edellytykset riippuvat sekä tietojen muodosta (paperinen vai sähköinen) sekä mahdollisten poistotoimenpiteiden olemassaolosta, ks. Korpisaari ja muut 2022, s.248.

[118] Hanninen ja muut (2017, s.63) katsovat, että henkilötietojen aktiivisen käsittelyn estäminen esimerkiksi käyttäjärajoituksilla, sekä muilla toimilla riittäisi täyttämään rekisteröidyn oikeuden tulla unohdetuksi.

Myöskään varmuuskopioiden poistamiseen ei ole tietosuoja-asetuksessa otettu täsmällistä kantaa. Rohkein kanta varmuuskopioiden poistamisesta lienee Hannisen ja muiden päätelmä siitä, että varmuuskopioita ei tarvitse poistaa tai kyetä poistamaan rekisteröidyn halutessa käyttää oikeuttaan tulla unohdetuksi. Kirjailijat kuitenkin jatkavat, että yrityksen on varmistettava, ettei varmuuskopiot palaudu käyttöön.[119] Tämä on myös realistisin päätelmä siitä, että varmuuskopioiden täydellinen poistaminen on lähtökohtaisesti myös rekrytoinnin yhteydessä mahdotonta. Siksi aktiivisen rekrytointiprosessin sulkemista ja poistamista rekrytointijärjestelmästä – edellytyksenä, että rekrytointitiimin jäseniltä poistuu pääsy kyseiseen rekrytointiprojektiin – voidaan pitää riittävänä toimena työnhakijoiden henkilötietojen sekä näiden tietojen varmuuskopioiden poistamiseksi.

Lain tarkempaa tulkintaa vaatii myös se, mitä rekisteröidyn oikeus olla joutumatta automaattisen päätöksenteon kohteeksi tarkoittaa rekrytoinnin osalta. Tietosuoja-asetuksen 22 artiklan mukaan automatisoidut päätökset sekä profiloinnit ovat lähtökohtaisesti kiellettyjä[120]. Tietodatan keräämisestä ja rikastamisesta on kuitenkin tullut tietokoneiden laskentatehon sekä tekoälyjärjestelmien kehityksen myötä yhä helpompaa. Uuden tietotekniikan hyödyntäminen on yrityksille houkuttelevaa, sillä automatisoidut päätökset tehostavat prosesseja.[121] Tämä vaikuttaa automatisoidun päätöksenteon määrään myös rekrytointiprosesseissa: automaattinen päätöksenteko mahdollistaa esimerkiksi työnhakijoiden profiloinnin ammatillisten kykyjen perusteella. Varsinaisesta automatisoidusta päätöksenteosta on kyse silloin, kun automaattinen käsittely – kuten profilointi[122] –

---

[119] Hanninen ja muut (2017, s.63). Mikäli varmuuskopioiden poistaminen vaarantaisi muiden ihmisten henkilötietojen varmuuskopiot, ei varmuuskopioita tule lähteä poistamaan yhden ihmisen unohdetuksi tulemisen -oikeuden vuoksi, ks. Korpisaari ja muut, 2022, s.248. Tästä esimerkistä voimme nähdä, että myös tietosuojaoikeudessa lähdetään siitä lähtökohdasta, että henkilötietojen suoja tulee käsittää kokonaisuuden kannalta. Organisaatioiden ja yksittäisten ihmisten tulee suosia toimia, jotka lisäävät henkilötietojen oikeuksien toteutumista suuressa mittakaavassa.

[120] TSA 22 artikla, kohta 1. Vaikka automatisoitu päätöksenteko on lähtökohtaisesti tietosuoja-asetuksessa kiellettyä, on se kuitenkin käytännössä usein sallittua sen perustuessa esimerkiksi rekisteröidyn ja rekisterinpitäjän välisen sopimuksen välttämättömyyteen, rekisteröidyn antamaan nimenomaiseen suostumukseen tai unionin oikeuden tai jäsenvaltion lainsäädännön hyväksyntään, ks. Korpisaari ja muut, 2022, s.289.

[121] Korpisaari ja muut, 2022, s.279–289.

[122] Profiloinnilla tarkoitetaan jonkin henkilötiedon analysointia tai ennakointia. Profilointi on luonteeltaan automaattista tai osittain automaattista, se kohdistuu henkilötietoihin ja se arvioi henkilökohtaisia ominaisuuksia, ks. Tietosuojavaltuutetun toimisto, Automaattinen päätöksenteko ja profilointi. Tämä

perustuu *ainoastaan* tietojärjestelmän itsenäiseen päätökseen ilman *merkityksellistä* inhimillistä myötävaikutusta. Tietosuoja-asetus tulee puolestaan sovellettavaksi, kun automaattinen päätöksenteko kohdistuu henkilötietoihin, ja sillä on rekisteröidylle oikeusvaikutuksia tai se vaikuttaa rekisteröityyn vastaavalla tavalla merkittävästi. Sähköinen rekrytointivalinta voidaan nähdä tällaisena merkittävänä vaikutuksena.[123]

Tulkinnanvaraista on täten se, mitä *merkityksellinen* inhimillinen myötävaikutus tarkoittaa. Korpisaaren ja muiden mukaan päätöstä voidaan nimittäin pitää automatisoituna, kun ihminen osallistuu päätöksentekoon muodollisesti ja ihmisen myötävaikutus ei tosiasiassa vaikuta päätöksen sisältöön[124]. Katson, että rekrytointiprosessin osalta automatisoidun päätöksen tunnusmerkistö ei täyty, mikäli valintapäätös pohjautuu rekrytointijärjestelmän ehdotusten lisäksi ihmisen tekemiin arvioihin. Toisin sanoen, vaikka rekrytoija saisi rekrytointijärjestelmältä apua työnhakijoiden luokitteluun, mutta päätyisi itse lopulta samaan ratkaisuun – ja vaikka ratkaisu olisi rekrytointijärjestelmän kanssa yhtenevä – ei rekisteröity ole joutunut automaattisen päätöksenteon kohteeksi.

Huomionarvoista on myös se, että tietosuoja-asetuksessa sallitaan automaattinen päätöksenteko muun muassa rekisteröidyn suostumuksella[125]. Rekrytoinnin kannalta tämä tarkoittaa, että organisaatiot voivat hyödyntää automatisoitua päätöksentekoa, kunhan rekisteröity on sen *erikseen* sallinut ja rekisteröityä on informoitu kyseisestä menettelystä *ennen* hänen suostumuksensa antamista[126]. Lisäksi työnhakijalla on oikeus pyytäessään saada merkitykselliset tiedot automaattisen päätöksenteon – kuten profiloinnin – logiikasta ja seurauksista[127]. Työnhakijalla on lisäksi oikeus vaatia ihmisen osallistamista

---

tarkoittaa esimerkiksi sitä, että työnhakijoiden kyvykkyyttä ja tulevia työsuorituksia arvioidaan henkilökohtaisten ominaisuuksien perusteella. Korpisaaren ja muiden (2020, s.177) tulkinnan mukaan profilointia tulisi välttää, sillä se aiheuttaa työhönotossa suuria riskejä työnhakijan yksityisyyden suojan loukkaamisesta.

[123] Korpisaari ja muut, 2022, s.279–289; Voigt & Bussche, 2017, s.181.

[124] Korpisaari ja muut, 2022, s.289.

[125] TSA 22 artikla 1 kohta c.

[126] Voigt & Bussche, 2017, s.184.

[127] TSA 15 artikla 1 kohta h. Tietosuoja-asetus rajoittaa tietyissä määrin tekoälyn hyödyntämistä rekrytointiprosessin yhteydessä, sillä rekrytoivan organisaation tulee kyetä yksinkertaisessa muodossa selittämään

henkilötietojensa käsittelyyn[128]. Tämä tarkoittaa, että työnhakijan pyytäessä hänen hakemuksensa ja henkilötietonsa tulee käsitellä ihmisen toimesta.

3.4 Rekisterinpitäjän velvollisuudet rekrytoinnin yhteydessä

Rekisteröidyn oikeuksia pyritään suojaamaan rekrytointiprosessissa myös rekisterinpitäjän velvollisuuksien kautta. Nämä velvollisuudet ovat rekisteröidyn tehokkaan suojan peruspilareita, ja siksi rekisterinpitäjän velvollisuuksista voidaan nähdä viitteitä myös tietosuojaperiaatteiden ja rekisteröidyn oikeuksien sisällön ja sanamuotojen taustalla. Rekisterinpitäjän velvollisuuksia on käsitelty tietosuoja-asetuksen artikloissa 24–39[129]. Otan tarkasteluun tutkielman kannalta merkityksellisiä rekisterinpitäjän velvollisuuksia. Voimme lähteä liikkeelle siitä, että rekrytoiva organisaatio on velvollinen käsittelemään työnhakijoiden henkilötietoja tietosuojaperiaatteiden vaatimukset huomioiden. Rekisterinpitäjällä on täten vastuu niin kutsutusta sisäänrakennetusta ja oletusarvoisesta tietosuojasta. Tällä tarkoitetaan sitä, että organisaatioiden ei tulisi vain jälkikäteen pyrkiä ’’liimaamaan’’ tietosuoja-asetuksen vaatimuksia osaksi henkilötietojen käsittelyä. Sen sijaan rekrytoivien yritysten tulisi jo rekrytointiprosesseja suunnitellessa huomioida ennakoivasti rekrytoinnin mahdollisia tietosuojariskejä ja niiden hallintakeinoja[130].

Rekrytointiprosessin osalta tämä tarkoittaa muun muassa sen suunnittelua, keiden on tarpeenmukaista olla osa rekrytointitiimiä, millaiset oikeudet rekrytoivan tiimin jäsenillä on oltava esimerkiksi rekrytointijärjestelmään, sekä miten yritys varmistaa

---

käyttämänsä tekoälyjärjestelmän päätöksenteon logiikkaa. Tekoälyjärjestelmän käyttämän logiikan selittäminen sellaisessa muodossa, että ihminen sen ymmärtää ei kuitenkaan ole aina niin yksinkertaista, ks. Korpisaari ja muut, 2022, s.290.

[128] Korpisaari ja muut, 2022, s.289.

[129] TSA artikla 24: rekisterinpitäjän vastuu, artikla 25: sisäänrakennettu ja oletusarvoinen tietosuoja, artikla 26: yhteisrekisterinpitäjät, artikla 27: unionin ulkopuolelle sijoittuneiden rekisterinpitäjien tai henkilötietojen käsittelijöiden edustajat, artikla 28: henkilötietojen käsittelijä, artikla 29: tietojenkäsittely reksiterinpitäjän tai henkilötietojen käsittelijän alaisuudessa, artikla 30: seloste käsittelytoiminnasta, artikla 31: yhteistyö valvontaviranomaisen kanssa, artikla 32: käsittelyn turvallisuus, artikla 33 ja 34: tietoturvaloukkauksista ilmoittaminen valvontaviranomaiselle ja rekisteröidylle, artikla 35: vaikutustenarviointi, artikla 36: ennakkokuuleminen, artiklat 37–39: tietosuojavastaavan nimittäminen, asema ja tehtävät.

[130] Tutustuaksesi tarkemmin sisäänrakennettuun ja oletusarvoiseen tietosuojaan lue Korpisaari ja muut 2022, s.311 sekä Aalto-Setälä ja Viitaila, 2018, s.26.

tietosuojaperiaatteiden integroinnin osaksi rekrytointiprosessia. Apuna voivat toimia Euroopan tietosuojaneuvoston (ETN) ohjeet tietosuojaperiaatteiden sekä sisäänrakennetun ja oletusarvoisen tietosuojan täytäntöönpanosta käytännössä[131]. Sisäänrakennetun tietosuojan vaatimukseen kuuluu myös, että rekrytoivan yrityksen tulee tarkastella henkilötietojen käsittelytapojansa, sekä varmistaa teknisin ja organisatorisin toimenpitein henkilötietojen käsittelyn turvallisuus.[132] Tarkastelussa voidaan käyttää apuna ulkoisia auditointeja: esimerkiksi rekrytointiprosessin turvallisuuden tasoa voidaan kartoittaa ulkoisen auditoijan avulla, joka pyrkii henkilöstön haastatteluiden, dokumenttien katselmoinnin, sekä teknisten järjestelmien arvioinneilla tunnistamaan ja raportoimaan tietoturvariskejä[133].

Lisäksi rekrytoivan organisaation tulee rekisterinpitäjän roolissa luoda *seloste* työnhakijoiden henkilötietojen käsittelytoimista[134]. Selosteen on tarkoitus auttaa organisaatiota hahmottamaan käsittelytoimien laajuus ja sillä edesautetaan myös rekisterinpitäjän osoitusvelvollisuutta: rekisterinpitäjän tulee esittää seloste valvontaviranomaiselle pyydettäessä.[135] Tämän vuoksi seloste on osa rekisterinpitäjän vastuuta tehdä yhteistyötä valvontaviranomaisen kanssa[136]. Seloste on lähtökohtaisesti tarkoitettu organisaation sisäiseen käyttöön, eikä sitä ole tarkoitus jakaa rekisteröidyille[137]. Kyseessä on siksi eri seloste kuin rekisteröidyille jaettava niin kutsuttu tietosuojaseloste. Näiden velvoitteiden

---

[131] ETN ohjeet 4/2019. Näissä Euroopan tietosuojaneuvoston luomissa ohjeissa käydään yksityiskohtaisesti ja esimerkkien avulla läpi, kuinka tietosuoja-asetuksen yleiset tietosuojaperiaatteet pannaan organisaatiossa tehokkaasti täytäntöön samalla huomioiden sisäänrakennettu ja oletusarvoinen tietosuoja.

[132] TSA 24 artiklan 1 kohtaan on kirjattu, että *''ottaen huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset … on rekisterinpitäjän toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Näitä toimenpiteitä on tarkistettava ja päivitettävä tarvittaessa.''* Asetuksen 25 artiklassa on puolestaan korostettu tietosuojaperiaatteiden asianmukaista noudattamista kaikessa henkilötietojen käsittelyssä. Artiklassa 32 käydään puolestaan läpi rekisterinpitäjän velvollisuudet henkilötietojen käsittelyn turvallisuuden varmistamisesta, katso erityisesti TSA artikla 31 kohta 1 d.

[133] Jackson, 2010.

[134] TSA artikla 30. Katso tarkemmin, mitä tietoja selosteessa on oltava TSA:n artiklan 30 kohdista a–g.

[135] Korpisaari ja muut, 2022, s.363.

[136] TSA artikla 31: *''rekisterinpitäjän … on pyynnöstä tehtävä yhteistyötä valvontaviranomaisen kanssa sen tehtävien suorittamiseksi.''*

[137] Korpisaari ja muut, 2022, s.362–368. Koska tietosuoja-asetuksen 30 artiklan mukaisessa selosteessa on paljon samaa kuin asetuksen artiklojen 12–14 edellyttämässä rekisteröidyn informoinnissa, on organisaatioiden joissain tilanteissa järkevää miettiä, tulisiko nämä kaksi vaatimusta yhdistää yhteen dokumenttiin.

ohella rekrytoivan organisaation tulee tietoturvaloukkauksen yhteydessä ilmoittaa tapahtumasta sekä valvontaviranomaiselle että rekisteröidylle eli työnhakijalle[138].

Rekisterinpitäjän täytyy lisäksi tietyissä tilanteissa nimetä tietosuojavastaava sekä tehdä vaikutustenarviointeja henkilötietojen käsittelytavoista[139]. Tietosuojavastaavan nimittämisen pakollisuus riippuu pitkälti organisaation ydintehtävistä[140]. Vaikutustenarviointi tulee puolestaan tehdä, kun rekisteröidyn työsuoritusta, henkilökohtaisia mieltymyksiä, luotettavuutta tai käyttäytymistä arvioidaan tai pisteytetään. Lisäksi uusien teknisten innovaatioiden – etenkin automaattisen käsittelyn – hyödyntäminen lisää todennäköisyyttä vaikutustenarvioinnin välttämättömyydestä.[141] Siksi vaikutustenarviointi tulee toteuttaa, mikäli rekrytoinnissa käytetään uutta teknologiaa tai automatisoitua käsittelyä esimerkiksi työnhakijoiden profiloinnin ja luokittelun yhteydessä.

3.5 Hyvä liiketapa lain vaatimusten ja liiketoiminnan tarpeiden yhdistäjänä

Kuten tutkielman aiemmista kappaleista havaitaan, on lain ja liiketoiminnan välillä jatkuva jännite siitä, kuinka paljon ja miten henkilötietoja tulee rekrytointiprosessin aikana käsitellä. Hyvä liiketapa[142], tunnettu myös nimellä hyvä tapa, on oikeusperiaate, joka parhaimmillaan minimoi tätä jännitettä. Oikeusperiaatetta edustava hyvä liiketapa on

---

[138] TSA artiklat 33 ja 34. Tämä on niin kutsuttu rekisterinpitäjän *ilmoitusvelvollisuus.*

[139] TSA artiklat 35–39. Jos organisaatioon on nimetty tietosuojavastaava, tulee hänet osallistaa rekrytoinnin tietosuojariskien hallintaan ja vaikutustenarviointiin. Huomioi artiklan 37 mukainen ennakkokuuleminen, joka rekisterinpitäjän tulee tehdä, kun *''tietosuojaa koskeva vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin, jos rekisterinpitäjä ei ole toteuttanut toimenpiteitä riskin pienentämiseksi''.*

[140] Hanninen ja muut, 2017, s. 120–123; Korpisaari ja muut, 2022, s.420–432.

[141] Tietosuojatyöryhmän [WP 248 rev. 01] ohjeet tietosuojaa koskevasta vaikutustenarvioinnista, 2017, s.10–12; Tietosuojavaltuutetun toimisto, Vaikutustenarviointi.

[142] Hyvä liiketapa määritellään juridisessa yhteydessä usein kielteisen muodon kautta: jokin toiminta tai menettely määritellään hyvän tavan vastaiseksi, jolloin tällaista toimintaa tulee välttää, ks. Pöyhönen, 1999, s.198. Esimerkiksi SopMenL:n 1 §:ssä käydään läpi vain hyvän liiketavan vastaisen toiminnan kielto. Poikkeuksiakin toki on, vrt. tekijänoikeuslaki § 22. Hyvä tapa käsitetään tietyissä juridisissa tilanteissa hyvän liiketavan synonyymiksi, ks. Hoppu, 2021, s.60. Oikeusperiaatteen käsite, jota myös hyvä tapa edustaa, on moniulotteinen ja osittain myös täsmentymätön. Tuki oikeusperiaatteille löytyy usein lainsäädännöstä, lain esitöistä, oikeuskäytännöstä tai oikeustieteestä, ks. esim. Aarnio, 1989, s.79; Hirvonen, 2012, s.72–75.

nimittäin oikeuslähteiden hierarkian näkökulmasta sallittu oikeuslähde[143]. Tämä tarkoittaa, että tuomiovaltaa käyttävät elimet voivat käyttää oikeusperiaatetta päätöksiensä tukena. Koska hyvä liiketapa on täten osa oikeutta ja lainsäädäntöä, pyrkii se johdattamaan elinkeinotoimintaa kohti rehellisyyttä ja tasapuolisuutta lainsäädännön keinoin[144].

Samanaikaisesti hyvä liiketapa peilaa yhteiskunnan arvomaailmaa, ja toimii oikeuden sekä arvojen leikkauskohtana[145]. Tällainen lainsäädännön ja yhteiskunnallisten arvojen sulautuminen voidaan nähdä positiivisena ilmiönä, sillä oikeudellinen sääntely ei ole kaikkivoipaa. Sääntelyä on jopa neljänlaista: lainsäädäntöä, sosiaalisia normeja, markkinavoimia ja teknologiaa. Markkinavoimat vaikuttavat kaupalliseen toimintaan toisinaan jopa enemmän kuin lainsäädäntö. [146] Koska valvontaviranomaisten mahdollisuuksia puuttua yritysten tietosuojaongelmiin on pidetty vajavaisina, on markkinavoimilla vaikutusta siihen, toimivatko yritykset tietosuojalainsäädännön mukaisesti[147]. Mikäli markkinavoimat – kuten sidosryhmät – vaativat henkilötietojen asianmukaista käsittelyä, on todennäköisempää, että organisaatiot pyrkivät kohti tällaisia toimintatapoja.

Tietosuojalainsäädännön tiukentuneiden vaatimusten noudattaminen liitetäänkin vahvasti compliance-ajatteluun ja vastuullisuuteen. Lisäksi tietosuojariskit luetaan nykypäivänä merkittävien complicance-riskien joukkoon.[148] Saavuttaakseen menestystä ja välttääkseen mainehaittoja, tulee organisaatioiden panostaa eettisyyteen yhä enenevissä

---

[143] Oikeuslähteet on Aarnion (2014) oikeuslähdeopin mukaisesti jaettu kolmeen kategoriaan: vahvasti velvoittaviin oikeuslähteisiin, heikosti velvoittaviin oikeuslähteisiin, sekä sallittuihin oikeuslähteisiin.
[144] Huhtamäki, S., Saarnilehto, Huhtamäki, A. & Tähti, 1992, s.27.
[145] Oikeusperiaatteilla voidaan viitata oikeusjärjestyksen perustana oleviin arvoihin, ks. Laakso, 1990, s.121–122. Positiiviset oikeusperiaatteet voidaan jakaa arvoa edistäviin arvoperiaatteisiin ja tietyn päämäärän toteuttamista tavoitteleviin periaatteisiin, ks. Pöyhönen, 1988, s.54 ja Aarnio, 1989, s.81. Hyvä liiketapa on aikaan ja paikkaan sidottua. Se, mitä emme voi käsittää Pohjoismaissa, voi toisaalla olla maan tapa. Myös oma aiempi toimintamme voi tänä päivänä näyttäytyä kestämättömältä, ks.Ratsula,2016a, s.14.
[146] Korpisaari ja muut, 2022, s.22–24.
[147] Vaikka Euroopan komission kesällä 2020 julkaisemassa arviossa todettiin, että valvontaviranomaisten keinovalikoima puuttua tietosuojaongelmiin on parantunut, koettiin siinä olevan yhä puutteita, ks. Korpisaari ja muut, 2022, s.21–22.
[148] Termillä *compliance* viitataan vaatimustenmukaisuuteen eli lakien, säännösten ja määräysten noudattamiseen, sekä organisaation ulkopuolisten tahojen asettamien eettisten vaatimusten mukailuun, ks. Ratsula, 2016a, s.131. Liike-elämässä on havaittu viitteitä siitä, että tietosuoja-asetus on lisännyt yritysten vastuullista toimintaa, ks. Redondo ja Mariz, 2022, s.11

määrin sidosryhmien asenteiden ja arvojen mukaisesti[149]. Yritysvastuuta pidetään nykypäivänä jopa liiketoiminnan edellytyksenä[150]. Lisäksi työntekijät ovat entistä kiinnostuneempia siitä, kuinka heidän henkilötietojansa käsitellään[151]. Henkilötietojen käsittely rekrytoinnin yhteydessä tulee siksi olla organisaation sidosryhmien asettamien eettisten vaatimusten mukaista. Myös haastatteluissa nousi esille tietosuojalainsäädännön noudattamisen tärkeys:

> *''Varmaan suurin ongelma siinä, ettei noudata tietosuojalakeja on mainehaitta, mikä voi vaikuttaa siihen, uskaltaako ihmiset enää hakea sinne ja miten yrityksen kokonaisluotettavuutta sen jälkeen arvioitais. Ne kaikista pätevimmät hakijat saattaa jättää hakematta.''*
> *-Haastateltava 2*

Voidaan todeta, että hyvän liiketavan mukaisella toiminnalla voi olla aitoja, organisaation toimintaa eteenpäin vieviä vaikutuksia: tietosuojariskien asianmukaisella hallinnalla voidaan saavuttaa kilpailuetua[152]. Lisäksi väitän, että tulevaisuudessa parhaiten menestyvät yritykset, jotka noudattavat tietosuojaa koskevaa lainsäädäntöä ja pystyvät saavuttamaan luottamuksen sidosryhmiensä silmissä[153]. Sidosryhmien luottamuksen ohella tietosuojalainsäädännön noudattaminen hyvän liiketavan hengessä vähentää yrityksen taloudellisia menetyksiä. Tietosuojavuodosta johtuvat taloudelliset menetykset voivat

---

[149] Viitala & Järlström, 2014, s.3. Esimerkkejä mainehaittojen syntymisestä henkilötietojen käsittelyn yhteydessä ovat muun muassa korkeimman hallinto-oikeuden tapaukset KHO 2023:81 ja KHO 2023:82, joissa Posti Oy:tä syytettiin tietosuoja-asetuksen vastaisesta toiminnasta. Tapauksessa KHO 2023:81 Posti Oy:lle määrättiin 100 000 euron maksuvaatimus. Kuitenkin maksuvaatimusta merkittävämpänä haittana voidaan pitää tapauksen KHO 2023:82 esiin tuomia väitteitä Posti Oy:n työhönottoprosessin työnhakijoiden henkilötietojen suojan laiminlyönnistä. Vaikka vaatimukset hallinnollisesta 12 000 euron seuraamusmaksusta hylätään korkeimmassa hallinto-oikeudessa, ovat mainehaitat ilmeisiä ja voivat vaikuttaa muun muassa Posti Oy:n työnantajamielikuvaan.

[150] Liappis, Pentikäinen & Vanhala, 2019, s.28; Pentikäinen, 2019, s.568.

[151] Aalto-Setälä & Viitaila, 2018, s.4.

[152] Tietosuoja-asetuksen vastaisesta toiminnasta määräytyviä taloudellisia seuraamuksia on pidetty kannustimena asianmukaiselle henkilötietojen käsittelylle. Lisäksi oikeaoppisesta henkilötietojen käsittelystä on ajateltu olevan organisaatioille jopa kilpailuetua, ks. Hanninen ja muut, 2017, s.14.

[153] Sidosryhmien luottamuksen lunastaminen henkilötietojen asianmukaisesta käsittelystä edellyttää, että rekrytoiva yritys sisäistää henkilötietojen käsittelyyn liittyvän paradoksin: tietosuojalainsäädännön tiukentumisesta huolimatta yksilöt ovat nykypäivän verkostoituneessa yhteiskunnassa yhä valmiimpia jakamaan omia henkilötietojansa toisilleen. Silti rekrytoivien organisaatioiden on ymmärrettävä, ettei heidän ole kannattavaa hyödyntää näitä yksilöiden julkaisemia tai kertomia henkilötietoja ilman yksilöiden tietoisuutta ja suostumusta. Esimerkki yksilön itse jakamasta henkilötiedosta on LinkedIn -sivustolle päivitetyt tiedot omasta työhistoriasta, katso lisää omien henkilötietojen omistamisesta Korpisaari ja muut, 2022, s.25–28.

nimittäin olla hyvin moninaisia: hallinnollisia seuraamusmaksuja[154], oikeudenkäyntikuluja, liikevaihdon pienentymistä asiakkaiden kaikotessa, immateriaalioikeuksien menetyksiä sekä henkilöstökuluja esimerkiksi uusrekrytoinnin vaikeutuessa[155].

Kilpailuedun ohella hyvän liiketavan mukainen toiminta voi edesauttaa työviihtyvyyttä ja vähentää henkilöstön vaihtuvuutta. Perustelu tähän löytyy siitä, että jatkuva tasapainoilu organisaation epäeettisyyden ja työntekijän henkilökohtaisen moraalikäsityksen välillä lisää turhautumista, pettymystä, sekä henkistä uupumusta. Lisäksi se voi lisätä halua irtisanoutua.[156] Yleisen moraalikäsityksen vastainen toiminta henkilötietojen käsittelyssä voidaan nähdä myös hyvän liiketavan vastaisena toimintana. Henkilöstön vaihtuvuuden hallinta ja sitouttaminen auttaa organisaatiota puolestaan saavuttamaan tavoitteitaan[157].

Näiden argumenttien nojalla totean, että rekrytointiprosessin tietosuojariskien hallinta on yrityksille olennaista, sillä siten organisaatiot voivat välttää juridisia ongelmia, edesauttaa vastuullista mielikuvaa, saavuttaa kilpailuetua, sekä välttää taloudellisia menetyksiä. Täten hyvä liiketapa yhdistää lain vaatimuksia ja liiketoiminnan tarpeita. Kuitenkin, niin kauan kuin yritykset tarvitsevat rekrytoinnissa henkilötietoja, ei lainsäädännön vaatimusten ja yritysten tarpeiden välinen jännite poistu kokonaan: henkilötietojen käsittely aiheuttaa riskejä henkilötietojen suojan loukkauksista ja yritysten on otettava näitä riskejä. Siksi käsittelen seuraavaksi rekrytointiprosessin tietosuojariskejä ja niiden hallintaa.

---

[154] EU:n kansallisilla tietosuojavalvontaviranomaisilla on toimivalta määrätä tietosuoja-asetuksen noudattamattomuudesta hallinnollisia sakkoja, ks. TSA 58 artikla; tietosuojalaki §18 & §24. Isoimmat tietosuojalainsäädännön vaatimusten laiminlyönnistä annetut sakot on suunnattu amerikkalaisten teknologiayritysten eurooppalaisille tytäryhtiöille. Suomessa tietosuojaloukkausten perusteella annetut sakot ovat lähtökohtaisesti olleet maltillisempia ja niitä on myös määrätty vähemmän, ks. Keller, 2023, s.222–223.

[155] Evans, 2019, s.16–24.

[156] Kreitzer, Brintnell, Sharon & Austin, 2020, s.1951–1952; Jaskela, Guichon, Page & Mitchell, 2018, s.100; Ulrich, O'donnell, Taylor, Farrar, Danis & Grady, 2007, s.1715–1717; Oliver, 2013, s.205–206.

[157] Henkilökunnan tiheä vaihtuvuus lisää inhimillisen pääoman menettämiseen liittyviä riskejä, ks. Talvio & Välimaa, 2004, s. 142–143. Inhimillisen pääoman menetys puolestaan vaikeuttaa yrityksen menestystä.

4 Rekrytointiprosessin tietosuojariskeistä

4.1 Tietosuojalainsäädännön näkökulmasta merkittäviä tietosuojariskejä

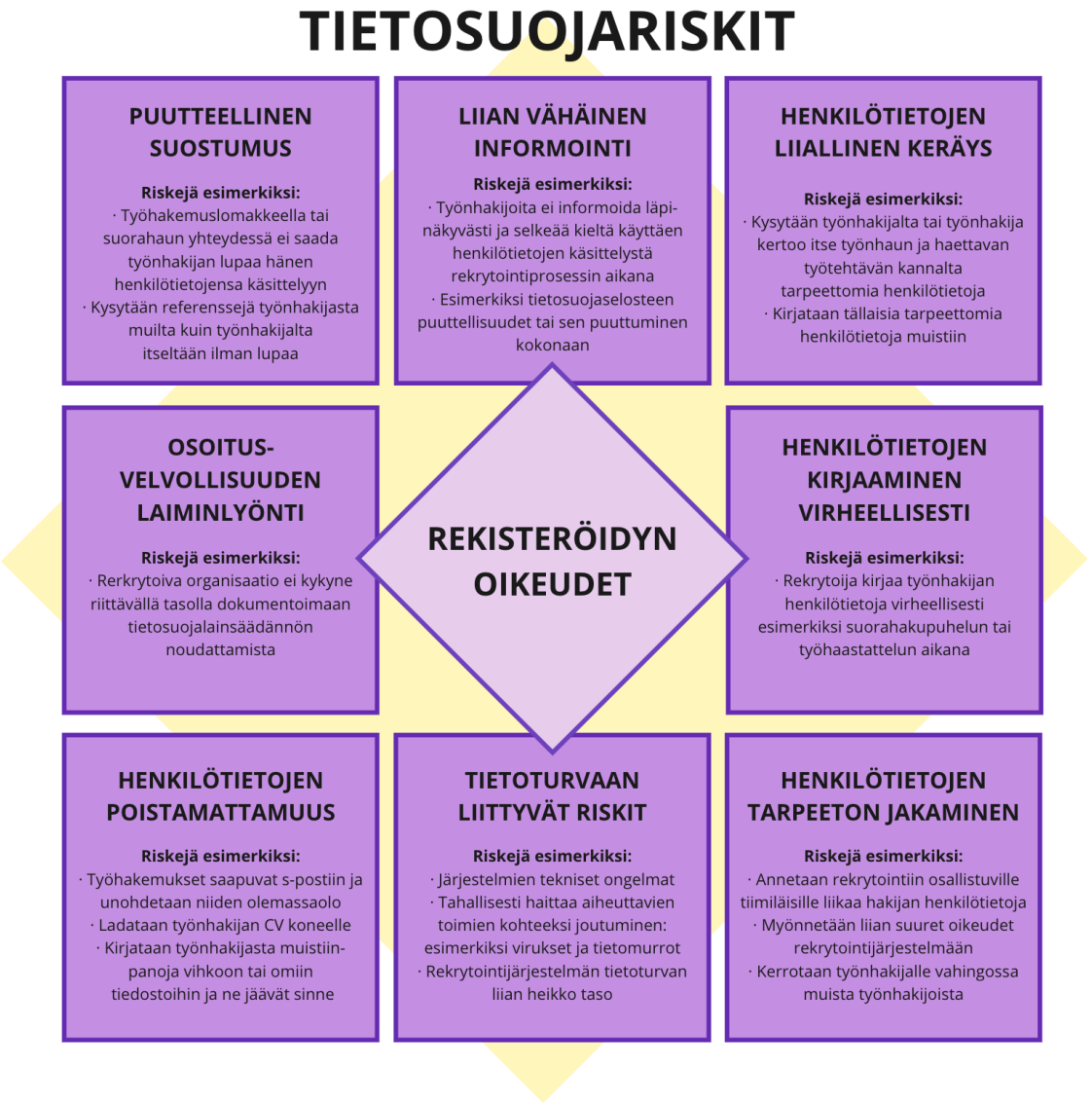
Jotta rekrytointiprosessin tietosuojariskien tulkinta on mahdollista, palataan ensin tietosuojariskin määritelmään[158]. Tietosuoja-asetuksen mukaan tietosuojariskiä arvioitaessa henkilötietojen käsittelyä olisi tarkasteltava rekisteröidyn näkökulmasta. Asetus määrittää riskiksi kaikki sellaiset tapahtumat, joissa käsitteillä olevat henkilötiedot voivat tuhoutua laittomasti, hävitä, muuttua tai luvattomasti tulla luovutetuiksi eteenpäin. Myös luvaton pääsy henkilötietoihin on asetuksessa määritelty tietosuojariskiksi. Huomionarvoista on se, että asetuksen mukaisesti edellä mainituista tapahtumista muodostuu riski jo silloin, kun niistä *voi* aiheutua fyysisiä, aineellisia tai aineettomia vahinkoja rekisteröidylle. Asetus ei siis vaadi sitä, että esimerkiksi tietovuoto aiheuttaa rekisteröidylle todellisen aineellisen vahingon, mutta jo tieto siitä, että tapahtumasta *voisi* aiheutua rekisteröidylle vahinkoa tekee siitä riskin.[159] Tämän vuoksi tutkielmassa tietosuojariski on määritelty tapahtumaksi, joka loukkaa työnhakijan henkilötietojen suojaa[160].

Täten rekrytointiprosessissa voidaan nähdä olevan kahdeksan merkittävää tietosuojariskiä: työnhakijan puutteellinen suostumus henkilötietojen käsittelystä, työnhakijan liian vähäinen informointi, henkilötietojen liiallinen keräys, henkilötietojen virheellinen kirjaaminen, henkilötietojen tarpeeton jakaminen, tietoturvaan liittyvät riskit, henkilötietojen poistamattomuus, sekä rekisterinpitäjän eli rekrytoivan organisaation

---

[158] Tutkielman määritelmää tietosuojariskistä on käsitelty alustavasti johdannossa sivulla 16.
[159] TSA johdanto kohta 83.
[160] Tutkielmassani tietosuojariskin määritelmässä painottuu tulkinta siitä, että jo pelkkä henkilötietojen suojan loukkaus aiheuttaa tietosuojariskin, sillä tällöin rekisteröidylle *voi aiheutua* fyysisiä, aineellisia tai aineettomia vahinkoja. Kaikki tutkielman tietosuojariskit on määritelty rekisteröidyn näkökulmasta. Myös ne tietosuojariskit, jotka laiminlyövät rekisterinpitäjän velvollisuuksia tai jotka ovat tietosuojaperiaatteiden vastaisia loukkaavat rekisteröidyn oikeuksia: tietosuoja-asetuksen lähtökohtana nimittäin on, että rekisterinpitäjän velvollisuuksien ja yleisten tietosuojaperiaatteiden avulla pyritään vahvistamaan rekisteröidyn oikeuksia. Tällöin myös rekisterinpitäjän velvollisuuksien laiminlyönti ja tietosuojaperiaatteiden vastainen toiminta heikentää rekisteröidyn oikeusasemaa ja on sen vuoksi selvä tietosuojariski.

osoitusvelvollisuuden laiminlyönti. Nämä tutkielmassa havaitut rekrytointiprosessin tietosuojariskit on havainnollistettu oheiseen kuvioon (kuvio 6).



Kuvio 6. Rekrytointiprosessin tietosuojariskejä.

Oheisen kuvion (kuvio 6) mukaisesti tietosuojariskien jako kahdeksaan kategoriaan mukailee henkilötietojen käsittelyn elinkaarta lähtien liikkeelle henkilötietojen keräyksestä ja päättyen henkilötietojen poistamiseen. Tämä ohjaa myös järjestystä, jossa käyn rekrytoinnin tietosuojariskejä läpi seuraavien kappaleiden aikana: lähden liikkeelle työnhakijan puutteellisesta suostumuksesta ja päätän tietosuojariskien käsittelyn

rekisterinpitäjän osoitusvelvollisuuden laiminlyöntiin. Tutkielmassa määritellyistä rekrytointiprosessin tietosuojariskeistä viisi korostui haastatteluiden aikana ja kolme nousi esille tietosuojalainsäädäntöä tulkitsemalla. Haastatteluissa alleviivattuja tietosuojariskejä olivat työnhakijan puutteellinen suostumus, henkilötietojen liiallinen keräys, henkilötietojen tarpeeton jakaminen, tietoturvaan liittyvät riskit sekä henkilötietojen poistamattomuus. Työnhakijoiden liian vähäinen informointi, henkilötietojen kirjaaminen virheellisesti sekä rekisteröidyn osoitusvelvollisuuden laiminlyönti ovat puolestaan tietosuojariskejä, joiden olemassaolo on tutkielmassa havaittu lainsäädännön tulkinnan keinoin. Seuraavaksi analysoin näitä kahdeksaa rekrytointiprosessin tietosuojariskiä.

4.2 Puutteellinen suostumus

Yksi rekisteröidyn oikeuksia loukkaava sekä rekrytointiprosessissa usein toistuva tietosuojariski on rekisteröidyn eli työnhakijan puutteellinen suostumus hänen henkilötietojensa käsittelystä rekrytoinnin aikana. Tutkielman haastatteluissa seitsemän HR-alan ammattilaista nimesi työnhakijan puutteellisen suostumuksen yhdeksi rekrytoinnin tietosuojariskiksi. Työnhakijan puutteellinen suostumus henkilötietojen käsittelyyn rekrytointiprosessissa on lähtökohtaisesti aina tietosuojariski, sillä tietosuoja-asetuksen mukaisesti henkilötietojen käsittelyn tulee olla lainmukaista ja täyttää lainmukaisuusperiaate. Lainmukaista henkilötietojen käsittelystä tekee puolestaan se, että käsittelyn on perustuttava tietosuoja-asetuksen erikseen asettamille oikeusperusteille.[161] Kuten tutkielmassa on aiemmin todettu, on rekrytointiprosessissa henkilötietojen käsittelyn oikeusperusteita lähtökohtaisesti kaksi: työnhakijan suostumus ja sitovan työsopimuksen teko. Koska työnhakijoiden henkilötietoja tarvitaan rekrytointipäätöksen tueksi jo ennen

[161] TSA 5 artikla kohta 1a: TSA 6 artikla kohdat 1a–f; Korpisaari ja muut, 2022, s.113–114. Tietosuoja-asetuksen 6 artiklassa on listattu henkilötietojen käsittelyn olevan lainmukaista, jos ja vain siltä osin kuin yksi näistä edellytyksistä täyttyy: henkilötietojen käsittely perustuu joko rekisteröidyn suostumukseen, sopimukseen, rekisterinpitäjän tai kolmannen oikeutettuun etuun, lakisääteiseen velvoitteeseen, elintärkeään etuun tai yleiseen etuun.

työsopimuksen laadintaa, on henkilötietojen käsittely laitonta ilman työnhakijan suostumusta – edellyttäen, ettei muut henkilötietojen käsittelyn oikeusperusteista täyty[162].

Vaikka työnhakija olisi antanut suostumuksen henkilötietojensa käsittelyyn, voi suostumus olla puutteellinen myös siltä osin, ettei sen antaminen ole tapahtunut tietosuoja-asetuksen vaatimusten mukaisesti[163]. Suostumus ei ole tapahtunut tietosuoja-asetuksen mukaisesti esimerkiksi silloin, kun sitä ei voida yhdistää työnhakijaan tai se on annettu vain vaikenemalla tai valmiiksi rastitetulla ruudulla jonkin lomakkeen yhteydessä[164]. Työnhakijan suostumus on puutteellinen myös silloin, kun rekisterinpitäjä ei jälkikäteen pysty osoittamaan rekisteröidyn suostumuksen antoa[165]. Huomionarvoista on edelleen se, että työnhakijan puutteellinen suostumus saattaa kohdistua joko kaikkiin hänestä kerättyihin henkilötietoihin tai pelkästään osaan niistä.

Työnhakijan suostumus henkilötietojen käsittelyyn saattaa puuttua kokonaan esimerkiksi silloin, kun rekrytoiva organisaatio pyytää työnhakijoita täyttämään CV:n ja työhakemuksen nettisivuillaan. Mikäli työnhakijalta ei pyydetä suostumusta hänen henkilötietojensa käsittelyyn työhakemuksen lähetyksen yhteydessä, lähestytään tilannetta, jossa

---

[162] Työsopimuksen laatimista voidaan pitää tietosuoja-asetuksen 6 artiklan 1b kohdan tarkoittamana sopimuksen täytäntöönpanona, joka muodostaa laillisen oikeusperusteen työnhakijan henkilötietojen käsittelylle. Työsopimuksen laatiminen ei kuitenkaan lähtökohtaisesti tapahdu ennen rekrytointipäätöstä, mikä usein edellyttää työnhakijoiden karsintaa ja luokittelua henkilötietojen pohjalta. Tämän vuoksi työnhakijan suostumus tarvitaan lähtökohtaisesti aina, jotta työnhakijan henkilötietojen käsittely on lainmukaista. Teorian tasolla on toki mahdollista, että työnhakijalle tarjotaan suoraan työsopimusta, jolloin varsinaista suostumusta henkilötietojen käsittelyyn ei tarvita, vaan pelkkä tarve sitovan työsopimuksen tekoon riittää työsopimukseen tarvittavien henkilötietojen käsittelylle. Tällaista tapahtumaketjua voidaan toki pitää mahdollisena esimerkiksi senioritason rekrytoinnin yhteydessä, joskin vähintäänkin harvinaisena.

[163] TSA:n 7 artiklan kohdat 1–4 määrittävät rekisteröidyn suostumuksen edellytykset.

[164] Tietosuoja-asetuksen johdannossa (kohta32) on maininta, että rekisteröidyn suostumuksen tulee olla vapaaehtoinen, yksiselitteinen, tietoinen sekä yksilöity ja sitä ei saa antaa vaikenemalla tai *valmiiksi* rastitetulla ruudulla taikka esimerkiksi jättämällä jokin toimi tekemättä. Esimerkiksi Euroopan unionin tuomioistuin (EUT) katsoi, ettei suostumusta oltu annettu tapauksessa Planet49 (C-673/17) pätevästi, kun käyttäjän olisi itse pitänyt ymmärtää poistaa valmiiksi rastitettu ruutu evätäkseen suostumuksensa tietojen käyttämiseen evästeiden avulla.

[165] Rekrytoivan organisaation tulisi aina dokumentoida rekisteröidyn suostumus, jotta rekisterinpitäjänä toimiva rekrytoiva yritys voi täyttää osoitusvelvollisuutensa. Suostumuksen peruutuksesta voidaan puolestaan lisätä ohjeet esimerkiksi organisaation nettisivuille tietosuojalomakkeeseen ja suostumuksen peruutuksen on oltava yhtä vaivatonta kuin suostumuksen antamisen, ks. esim. Korpisaari ja muut, 2022, s.146.

työnhakijalta ei ole saatu riittävää suostumusta hänen henkilötietojensa käsittelyyn. Tällaiset tapahtumaketjut ilmenivät myös tutkielman haastatteluissa:

> *''Kyllä sitä on toisinaan tullut todistettua tilanteita, joissa yleensä ne pienet organisaatiot tai startupit ei vaan tajua kysyä sitä lupaa työnhakijoiden henkilötietojen käsittelyyn. Sitä ollaan vaan yksinkertasesti niin innoissaan painamassa omaa duunia ja ettimässä uusia talentteja, ettei edes tajuta – että ainiin – tälle kandidaattien henkilötietojen pyörittelylle pitäis olla myös se suostumus.''*
>
> *-Haastateltava 10*

Tutkielman haastatteluissa nousi esille myös tilanteita, joissa työnhakijoilta ymmärretään pyytää suostumus henkilötietojen käsittelyyn vain perinteisen ilmoitteluhaun yhteydessä. Haastatteluissa korostui, että tämä johtuu toisinaan siitä, että perinteisen ilmoitteluhaun yhteydessä suostumus henkilötietojen käsittelyyn rekrytoinnin aikana kysytään automaattisesti lomakkeella, jota työnhakijat käyttävät lähettäessään työhakemuksen nettisivujen kautta. Kuitenkin esimerkiksi suorahaun yhteydessä potentiaaliselta kandidaatilta ei välttämättä muistetakaan kysyä suostumusta henkilötietojen käsittelyyn:

> *''Se suurin riski piilee niillä lakia suht hyvin noudattavillakin firmoilla siinä, et sit kun mennään sinne suorahaun puolelle, niin ei muisteta samalla tavalla sen suostumuksen pyytämistä enää. Se johtuu siitä, et nettisivujen puolella se homma on jo niin automatisoitu ja sitä suostumusta kysytään usein automaattisesti lomakkeen kautta. Suorahaussa suostumuksen pyytäminen jää usein muistin varaan.''*
>
> *-Haastateltava 10*

Suorahaun yhteydessä työnhakijan puutteellinen suostumus voi johtua inhimillisen unohduksen lisäksi siitä, että julkisen ja yksityisen tiedon raja hämärtyy[166]. Kun perinteisessä ilmoitteluhaussa on selvää, että työnhakijan henkilötiedot ovat yksityisiä, ja työnhakija antaa näitä yksityisiä tietojaan rekrytointiprosessin käyttöön, on inhimillisesti helpompi hahmottaa, että työnhakijan antamat tiedot ovat luottamuksellisia ja niitä tulee käsitellä tietosuojalainsäädännön vaatimusten mukaisesti. Sosiaalinen media yleisestikin ja esimerkiksi etenkin työnhakuun sekä työlliseen verkostoitumiseen tarkoitettu LinkedIn

[166] Ratkaisussa KHO 1992-A-10 korkein hallinto oikeus katsoi, että työnhakijoiden henkilötietoja voitiin kerätä *julkaisuista tiedoista,* kuten vuosikertomuksista ja aikakausijulkaisuista, ilman työnhakijoiden nimenomaista suostumusta. Tulkitsen, että KHO:n linjauksen mukainen lopputulema on se, että LinkedIn -sivustolla olevia työnhakijan itse julkaisemia henkilötietoja voitaisiin pitää julkaistuina, mutta sivuston kautta käytävät chat-viestit ovat puolestaan yksityisiä viestejä, jolloin yksityisviestein saatujen henkilötietojen käsittelyyn tulisi saada työnhakijalta nimenomainen suostumus.

-sivusto[167] muodostaa puolestaan eräänlaisen harmaan katvealueen tietosuojalainsäädännön näkökulmasta. Tämä sen vuoksi, että työnhakija on kyseisellä sivustolla lähtökohtaisesti itse julkaissut itsestään henkilötietoja omalle sivulleen. Tällöin tällaisia tietoja voidaan pitää julkisempina tietoina. Mikäli rekrytoiva yritys löytäisi tällaisia tietoja, voitaisineen katsoa, että tiedot on saatu työnhakijalta itseltään.[168] Tällöin erillistä lupaa työnhakijalta henkilötietojen käsittelyyn ei tarvittaisi.

Toisaalta pelkkä henkilötietojen julkaiseminen esimerkiksi edellä mainitulle LinkedIn -sivustolle ei vielä osoita sitä, että työnhakija olisi toivonut kyseisiä henkilötietoja käytettävän kyseiseen työnhakuun. Tämän ohella huomioon tulisi ottaa sosiaalisen median palvelun luonne: esimerkin mukaisen työlliseen verkostoitumiseen suunnatun LinkedIn -sivuston tarkastelua – uusien työntekijöiden löytämiseksi – voidaan pitää hyväksyttävämpänä kuin esimerkiksi henkilökohtaisempaan käyttöön tarkoitetun Facebook -sivuston tarkastelua. On kuitenkin huomioitava, että joissakin sosiaalisen median palveluissa työnhakija saattaa olla rajannut profiiliaan siten, ettei kaikilla ole sinne pääsyä. Samanaikaisesti työnhakijan LinkedIn -sivustolla voi olla hänestä julkaistuja kuvia, videoita tai tekstejä, jotka ovat muiden kuin työnhakijan julkaisemia. Tällöin työnhakija on pyrkinyt asettamaan henkilötietojansa yksityisemmiksi ja henkilötietoja ei voitaisi myöskään katsoa saaduiksi työnhakijalta itseltään.[169] Tämä myös tarkoittaisi sitä, että tällaisten tietojen käyttö rekrytoinnin aikana edellyttää työnhakijan nimenomaista suostumusta.

Edellä mainitut esimerkit edustavat riskitilanteita, joissa työnhakijan suostumus puuttuu kokonaan. Rekrytointiprosessin aikana työnhakijan suostumus henkilötietojen käsittelyyn voi puuttua myös osittain. Suostumuksen osittainen puuttuminen ilmenee

---

[167] LinkedIn-sivusto on määritelty Microsoftin omistamaksi verkostoitumisvälineeksi ja verkkoyhteistöpalveluksi, joka toimii ammattilaisten käyntikorttina ja CV:nä. Sitä on myös luonnehdittu ammatilliseksi verkostoitumispaikaksi, jonka avulla ihmiset voivat laajentaa omaa verkostoaan, ja sitä voidaan käyttää myös työnhaussa vaikkei se ole varsinaisesti pelkkä työnhakusivusto, ks. lisää esimerkiksi Nieminen, 2022.

[168] Lähtökohtana henkilötietojen keruussa on, että tiedot on saatava työnhakijalta itseltään, katso tutkielman sivu 24 sekä YksTL 4§. Alapurasen ja muiden (2020, s.232) mukaan sosiaaliseen mediaan lisättyjen tietojen käyttäminen työhönoton yhteydessä muodostaa tulkinnallisia ongelmia siitä, onko sosiaalisesta mediasta kerätyt tiedot saatu työnhakijalta itseltään vai tulisiko ne laskea tiedoiksi, jotka on kerätty muualta kuin työnhakijalta, jolloin niiden kerääminen vaatisi työnhakijan erillisen suostumuksen.

[169] Katso aiheesta tarkemmin Alapuranen ja muut, 2020, s.232–233.

esimerkiksi siten, että työnhakijalta on saatu lupa hänen henkilötietojensa käsittelyyn, mutta suosittelupuheluiden tekoon ei pyydetä työnhakijalta erikseen lupaa. Tällöin tietosuojariskin muodostaa se, että työnhakijasta selvitetään henkilötietoja muilta kuin häneltä itseltään ilman hänen suostumustansa. Vaikka joitakin henkilötietoja voidaan lain sallimissa rajoissa kysyä myös muualta ilman työnhakijan suostumusta, ei referenssipuheluiden teko lähtökohtaisesti kuulu tällaisen sallitun toiminnan alle[170]. Tämän vuoksi suosittelupuheluiden tekoon tarvitaan ensin työnhakijan suostumus. Referenssipuheluiden suorittaminen lainvastaisesti korostui myös haastatteluissa ongelmalliseksi:

> *''Kyllä konsulttiuran aikana on usein tullu vastaan tilanteita, ettei tehdä referenssisoittoja ammattimaisesti. Esimerkiks että soitetaan Penan kaverille Erkille, että Pena on hakemassa meille töihin, että kerros vähän meille tästä Penasta. Ja taustalla tilanne on se, et Pena ei oo meille todellakaan antanut lupaa soittaa Erkille.''*
>
> *-Haastateltava 2*

Suosittelupuheluiden ohella puutteellinen suostumus työnhakijan henkilötietojen käsittelyyn korostui haastatteluissa myös siten, että kokemattomat esihenkilöt saattavat etsiä työnhakijasta henkilötietoja esimerkiksi internetin hakukoneiden avulla:

> *''Tossa just viimeviikolla meillä oli rekry päällä ja esihenkilö heitti ohimennen et hän käy vielä googlaamassa hakijan, ettei vaan sieltä löydy mitään mikä muuttais tän meijän rekryn valintapäätöksen. Et kyllä näitä tilanteita ihan oikeesti sattuu ja ihan koko ajan.''*
>
> *-Haastateltava 9*

Henkilötietojen kerääminen internetin välityksellä ilman työnhakijan suostumusta on erityisen ongelmallista jo senkin vuoksi, että se on lainsäädännön esitöissä erikseen kiellettyä. Hallituksen esityksessä (HE 75/2000)[171] on nimittäin kielletty tietoverkoista eli internetistä hakukoneen avulla kerätyn tiedon käyttöä ilman työnhakijan suostumusta. Lisäksi Tietosuojavaltuutettu on katsonut ratkaisussaan (626/452/2006) [172] , että

---

[170] Rekrytoivan organisaation kerätessä henkilötietoja muualta kuin työnhakijalta itseltään, tulee työnhakijalta saada tähän lupa YksTL:n 4§:n mukaisesti. Työnhakijan suostumusta ei kuitenkaan tarvita silloin, kun viranomainen luovuttaa työnantajalle tietoja laissa säädetyn tehtävän suorittamiseksi tai työnantajan hankkiessa henkilöluottotietoja tai rikosrekisteritietoja työntekijän luotettavuuden selvittämiseksi. Tässäkin tapauksessa työnhakijaa on joka tapauksessa kuultava ennen kuin tällaisia tietoja käytetään häntä koskevassa päätöksenteossa, ks. tarkemmin Alapuranen ja muut, 2020, s.229.

[171] Katso tarkemmin HE 75/2000, etenkin sivut 17–18.

[172] Tietosuojavaltuutettu on ratkaisussa 626/452/2006 katsonut, että erityisesti hakukoneen avulla saatavia tietoja tulee lähtökohtaisesti pitää epäluotettavina. Lisäksi googlaamalla löydetyn tiedon käyttämistä

työnantajan kerätessä työnhakijan henkilötietoja internetistä, tulee rekrytoivan organisaation ilmoittaa tästä työnhakijalle ennakkoon. Rekrytoivan yrityksen tulee myös kertoa, mitä tietoja se on työnhakijasta saanut ennen tietojen käyttämistä työnhakijaa koskevaan päätöksentekoon. Riski puutteellisesta suostumuksesta kasvaa siksi aina, kun työnhakijasta käsitellään tai etsitään mitä tahansa henkilötietoja ilman tämän tietoisuutta.

4.3 Liian vähäinen informointi

Toinen rekrytointiprosessista löytyvä tietosuojariski on havaittu tulkitsemalla tietosuoja-asetusta. Rekisterinpitäjän eli rekrytoivan organisaation tulee nimittäin informoida työnhakijoitaan läpinäkyvästi ja selkeää kieltä käyttäen, kuinka työnhakijoiden henkilötietoja kerätään ja käsitellään rekrytoinnin aikana. Lisäksi rekisteröidyn eli työnhakijan tulee rekrytoivan organisaation toimesta saada tietoa omista henkilötietojen suojaan liittyvistä oikeuksistaan.[173] Yksi merkittävä tietosuojariski on täten se, että rekrytoiva organisaatio laiminlyö velvoitettaan toimia läpinäkyvästi henkilötietojen käsittelyn tiedottamisen osalta. Tämä riski on tutkielmassa nimetty liian vähäisen informoinnin riskiksi ja se rikkoo etenkin henkilötietojen käsittelyn läpinäkyvyyden tietosuojaperiaatetta[174]. Lisäksi liian vähäinen informointi voi rikkoa myös rekisteröidyn oikeutta saada tietoa henkilötietojensa käsittelystä[175] sekä rekisterinpitäjän osoitusvelvollisuutta[176]. Riski liian vähäisestä

---

ja käsittelyä voidaan pitää erittäin kyseenalaisena toimintana, eikä tällä tavoin kerätty tieto täytä YksTL:n tarpeellisuusvaatimusta – googlaamalla saadaan tietoon myös työn kannalta epäolennaisia henkilötietoja.

[173] TSA johdanto etenkin kohdat 39, 58 ja 60; TSA 5 artikla kohta 1a; TSA 12 artikla.

[174] Katso tietosuoja-asetuksen 12 artikla, jossa määritellään, että rekisterinpitäjän tulee ilmoittaa rekisteröidylle henkilötietojen käsittelyä koskevat tiedot ’’tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä’’.

[175] Tietosuoja-asetuksen 13:sta artiklassa käsitellään tarkemmin rekisteröidyn oikeutta saada tietoa henkilötietojensa käsittelystä.

[176] Kokonaan puuttuva tai puutteellinen seloste henkilötietojen käsittelystä rikkoo rekisterinpitäjän osoitusvelvollisuutta, mikäli organisaatiolla ei ole muutakaan osoitusta siitä, että työnhakijoita on informoitu läpinäkyvästi ja selkeästi henkilötietojen käsittelystä. Tietosuoja-asetuksen 12 artiklassa mainitaan, että tiedot henkilötietojen käsittelystä tulee ilmoittaa rekisteröidylle kirjallisesti tai muulla tavoin ja tapauksen mukaan sähköisessä muodossa. Lisäksi rekisteröidyn pyytäessä tiedot voidaan antaa suullisesti. Tulkitsen, että tietosuoja-asetus kehottaa suosimaan kirjallista tai videomateriaalista toteutettua tapaa. Siksi rekrytoivan organisaation tulisi olla erityisen kriittinen pelkkää suullista tiedottamista kohtaan. Mikäli suulliseen tiedottamiseen päädytään, olisi suositeltavaa, että joku organisaation työntekijöistä pystyy todistamaan tämän henkilökohtaisesti, jolloin rekisterinpitäjä kykenisi täyttämään osoitusvelvollisuutensa.

informoinnista on erityisen suuri etenkin silloin, kun yritys ei ole luonut minkäänlaista tietosuojaselostetta tai tietosuojailmoitusta[177] henkilötietojen käsittelystä.

Toisaalta liian vähäisen informoinnin riski on olemassa myös silloin, kun seloste henkilötietojen käsittelystä on olemassa ja julkaistu työnhakijoille esimerkiksi nettisivujen kautta. Tietosuojaseloste saattaa nimittäin olla virheellinen tai puutteellinen: se voi sisältää esimerkiksi väärää tietoa tai siitä voi puuttua olennaisia tietoja työnhakijan oikeuksista, henkilötietojen käsittelyyn liittyvistä riskeistä tai tietoja siitä, kuinka rekisteröidyt voivat käyttää henkilötietojensa suojaan liittyviä oikeuksiaan kyseisen organisaation rekrytointiprosessien yhteydessä[178]. Tietosuojaseloste voi lisäksi olla sekava tai harhaanjohtava. Nämä kaikki edellä mainitut piirteet lisäävät riskiä liian vähäisestä rekisteröidyn informoinnista ja riski on sitä suurempi, mitä epätarkemmin tietosuojaseloste on laadittu. Käsittelen tietosuojariskien hallinnan yhteydessä, mitä rekrytoivan organisaation tulisi kertoa työnhakijalle, jotta riski rekisteröidyn liian vähäisestä informoinnista laskisi[179].

4.4 Henkilötietojen liiallinen keräys

Kolmas tutkielmassa esiin nousseista tietosuojariskeistä on henkilötietojen liiallinen keräys. Tutkielmassa tällä tarkoitetaan tilannetta, jossa työnhakijasta kerätään avoinna olevan työnkuvan kannalta tarpeettomia henkilötietoja. Tietosuojalainsäädännön näkökulmasta henkilötietojen liiallinen keräys muodostaa tietosuojariskin, sillä se loukkaa ainakin käyttötarkoitussidonnaisuuden sekä tietojen minimoinnin tietosuojaperiaatteita[180].

---

[177] Huomautus termeistä *tietosuojaseloste* ja *tietosuojailmoitus*: tietosuojaseloste on terminä yleisesti vakiintunut, muttei kuitenkaan tietosuoja-asetuksen mukainen virallinen termi. Siksi tietosuojaseloste on vain yksi niistä toteuttamistavoista, joilla rekisterinpitäjä voi toteuttaa niin kutsuttua informointivelvollisuuttaan läpinäkyvästä toiminnasta henkilötietojen käsittelyssä. Tietosuojaselosteesta käytetään myös nimitystä tietosuojailmoitus, ks. Korpisaari ja muut, 2022, s.195.

[178] Tietosuoja-asetuksen johdannon kohdan 39 mukaisesti luonnolliselle henkilölle (eli tässä tapauksessa työnhakijalle) tulisi olla selvää ja läpinäkyvää, kuinka häntä koskevia henkilötietoja kerätään ja käytetään. Lisäksi asetus selventää, että tällaiset tiedot tulisi olla helposti saatavilla. Myös käsittelyyn liittyvät riskit, säännöt, suojatoimet sekä se, kuinka rekisteröidyt voivat käyttää oikeuksiaan tulisi olla selvästi kerrottu.

[179] Katso tarkemmin tutkielman sivuilta 69–71.

[180] Rekrytointiprosessin kannalta käyttötarkoitussidonnaisuuden periaatteen mukaisesti työnhakijasta kerättävien henkilötietojen tulee olla tarpeenmukaisia ja perusteltuja. Lisäksi tietojen minimoinnin

Lisäksi henkilötietojen liiallinen keräys rikkoo YksTL:n 3 §:n tarpeellisuusvaatimusta, jonka mukaan työnhakijasta saa kerätä vain tarpeellisia henkilötietoja[181]. Työnhakijan näkökulmasta riski on todellinen, sillä työnhakija ei usein tiedä tarkkaa kuvaa mahdollisista tulevista työtehtävistään ja suostuu siksi työpaikan lunastamisen toivossa kertomaan itseään koskevia asioita laajasti rekrytoinnin yhteydessä[182]. Tällöin työnhakija voi herkästi kertoa pyydettäessä myös työnkuvan ja rekrytoinnin kannalta tarpeettomia henkilötietoja – millä voi puolestaan olla työnhakijalle negatiivisia vaikutuksia.

Haastateltavista seitsemän HR-alan ammattilaista nosti esille tämän tietosuojariskin. Esille nousi ajatuksia siitä, että työnhakulomakkeella kysytään toisinaan liikaa henkilötietoja. Eräs haastateltavista korosti sitä, kuinka ihmisten välinen henkilökemia saattaa aiheuttaa sen, että unohdetaan varsinainen haastattelutilanne. Tällöin riskit tarpeettomien henkilötietojen kysymisestä ja keräämisestä kasvaa, kun työnhakija alkaa tuntua tutulta ja luotettavaltakin henkilöltä:

> *''Yks tietosuojariskeistä on varmasti se, että hakulomakkeella saatetaan kysyä vähän liikaa tietoja – siis sellasia henkilötietoja, joita ei oikeesti tarvittais sen paikan täyttämiseen. Tän lisäks oon valitettavasti joskus joutunut istumaan vieressä, kun esihenkilö on kysyny hakijalta turhia henkilötietoja. Siinä on sit nopeesti vähän naurahdeltu ja huudeltu väliin, et joo hei, ei tarvi vastata tohon! Tää on usein tapahtunu esimerkiksi tokalla haastattelukierroksella, kun se hakija on jo alkanu tuntua ikään kuin uudelta työkaverilta, jonka kanssa vaihdellaan kuulumisia.''*
>
> *-Haastateltava 5*

Oikeuskäytäntö vahvistaa, että henkilötietojen liiallinen keräys on loukkaus henkilötietojen suojaa kohtaan. Esimerkiksi tuomiossa KKO 2015:41 korkein oikeus katsoi, että työnhakijan ei olisi tarvinnut vastata kysymykseen, jossa pyrittiin selvittämään puolison

---

periaatteen mukaisesti rekrytoinnin aikana kerättävien ja käsiteltävien henkilötietojen tulee rajautua siihen, mikä on rekrytointiprosessin kannalta välttämätöntä. Huomionarvoista on myös se, että edes työnhakijan suostumuksella työnhakijasta ei saa kerätä määrätyn käyttötarkoituksen kannalta epäolennaisia henkilötietoja, katso tarkemmin Hanninen ja muut, 2017, s.49.

[181] YksTL:n 3§:n mukaisesti ''työnantaja saa käsitellä vain välittömästi *työntekijän* työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitamiseen tai työnantajan työntekijöille tarjoamiin etuuksiin taikka johtuvat työtehtävien erityisluonteesta. Tarpeellisuusvaatimuksesta ei voida poiketa työntekijän suostumuksella.'' Lisäksi huomionarvoista on, että YksTL:n 2§:n toisen kohdan mukaisesti kyseistä lakia sovelletaan soveltuvin osin myös *työnhakijaan*. Siksi tarpeellisuusvaatimus henkilötietojen keräämisestä koskee työntekijän ohella myös työnhakijaa.

[182] Alapuranen ja muut, 2020, s.195.

poliittinen suuntaus[183]. Perusteluissaan korkein oikeus katsoi, että työhönoton yhteydessä liiallisten henkilötietojen keräys rikkoo nimenomaisesti YksTL:n 3 §:n tarpeellisuusvaatimusta.[184] Ratkaisussa KHO 1993-A-12[185] korkein hallinto-oikeus puolestaan katsoi, että yhtiötä voitiin sakon uhalla velvoittaa kertomaan, millaisia tietoja se keräsi työnhakijoistaan. Tällä pyrittiin nimenomaisesti valvomaan, toteutuiko työnhakijoiden henkilötietojen keräys lainmukaisesti ja tarpeellisuusvaatimusta noudattaen. Myös Tietosuojavaltuutetun toimisto on päätöksessään dnro 137/161/20 katsonut, että rekrytoiva yritys oli työnhakulomakkeellaan kysynyt työnhakijoista tietosuoja-asetuksen ja tietosuojalain vastaisia henkilötietoja[186]. Työnhakulomakkeella pyydetyistä henkilötiedoista tarpeettomiksi henkilötiedoiksi oli katsottu muun muassa työnhakijan syntymäkunta, seurakunta, asunto, puolison nimi, puolison ammatti, lasten syntymävuodet sekä terveydentila.

Täten on selvää, että henkilötietojen liiallinen keräys on tietosuojalainsäädännön näkökulmasta tietosuojariski. Tulkinnallisempaa on puolestaan, millaiset henkilötiedot ovat avoinna olevan työnkuvan kannalta tarpeettomia. Edellisen kappaleen listaus antaa ensiymmärryksen siitä, millaiset henkilötiedot ovat lähtökohtaisesti työnhaun kannalta tarpeettomia. Listaus ei kuitenkaan ole täydellinen, eivätkä listauksen henkilötiedot ole aina rekrytointiprosessin kannalta tarpeettomia, sillä poikkeustilanteitakin on[187]. Myös

---

[183] Huomionarvoista tuomion KKO 2015:41 perusteluissa on se, että puutteellisen tai jopa valheellisen vastauksen antaminen tarpeettoman henkilötiedon kysymykseen ei saisi korkeimman oikeuden mukaan johtaa työnhakijan kannalta kielteisiin seuraamuksiin.

[184] Tuomiossa KKO 2015:41 korkein oikeus on katsonut, että YksTL:n säätämiseen johtaneessa hallituksen esityksessä 75/2000 on todettu seuraavaa: ''työnantajan oikeutta kerätä työnhakijan henkilötietoja tulisi tarkastella siitä työtehtävästä lähtien, johon työnhakijaksi ilmoittautunut halusi. Tarpeellisia olisivat silloin lähinnä ne tiedot, jotka osoittavat hakijan pätevyyttä ja sopivuutta kyseiseen tehtävään. Työnhakija voisi jättää vastaamatta sellaiseen kysymykseen, joka ei ollut työsuhteen kannalta tarpeellinen. Puutteellisen tai epätäydellisen vastauksen antaminen ei saisi johtaa työnhakijan kannalta kielteisiin seuraamuksiin.''

[185] Tämän korkeimman hallinto-oikeuden ratkaisun aikaan henkilörekisterilaki (nyttemmin jo kumottu laki) oli yhä voimassa olevaa oikeutta. Lisäksi tietosuoja-asetusta edeltänyt henkilötietodirektiivi oli vasta vireillä. Kuitenkin, näissäkin säädöksissä ideologia tarpeellisuusvaatimuksesta oli jo olemassa, ks. esim. henkilörekisterilaki 5§ ja henkilötietodirektiivi 6 artikla kohta 1(b).

[186] Tietosuojavaltuutetun toimiston päätös perustui tietosuoja-asetuksen 5 artiklan 1 (a) ja (c) kohtien, 6 artiklan 1 kohdan, 9 artiklan 1 kohdan sekä asetusta täydentävän työelämän tietosuojalain 3 ja 5 §:n säännöksiin. Päätöksessä korostettiin etenkin tarpeellisten henkilötietojen termiä. Katso tarkemmin Tietosuojavaltuutetun toimiston päätös 137/161/20, etenkin sivut 2–5.

[187] Ajatuksia työhönoton poikkeustapauksista, joissa lähtökohtaisesti tarpeettomiksi luokitellut henkilötiedot voivatkin olla rekrytoinnin kannalta tarpeellisia: perhesuhdetta koskevat tiedot voivat olla tarpeellisia,

henkilötiedot, jotka saattavat alkusilmäyksellä tuntua tarpeettomilta työnhaun kannalta, voivatkin osoittautua työnhaun onnistumisen näkökulmasta tarpeellisiksi[188]. Tarpeellisten henkilötietojen kokonaisuus muodostuu siksi aina rekrytointiprosessin ja avoinna olevan työtehtävän mukaan. Tämän vuoksi avoinna oleva työnkuva määrittää myös sen, millaisten henkilötietojen keräys aiheuttaa riskin liiallisesta henkilötietojen keräämisestä.

Alapurasen ja muiden (2020) tulkinnan mukaisesti myös rekrytointiprosessin vaihe vaikuttaa siihen, onko jokin työnhakijan henkilötieto tarpeellinen: prosessin alkuvaiheessa kerättävät tiedot ovat yleensä yleisluontoisempia kuin prosessin loppuvaiheen kannalta tarpeelliset henkilötiedot. Lisäksi rekrytoinnin loppuvaiheessa on lähtökohtaisesti vain muutama hakija.[189] Esimerkiksi tiedot pankkitilistä tai veroprosentista ovat henkilötietoja, joita rekrytoiva organisaatio ei hallituksen esityksen 75/2000 mukaisesti tarvitse vielä valintapäätöstä tehtäessä[190]. Täten riski henkilötietojen liiallisesta keräämisestä ja käsittelystä on myös riippuvainen rekrytointiprosessin työvaiheesta. Tiivistetysti voidaan todeta, että riski henkilötietojen liialliseen keräämiseen kasvaa, kun rekrytointiprosessissa ei ole ennakkoon suunniteltu, millaisia tietoja hakijoista on tarpeen kerätä, sekä missä vaiheessa prosessia mitäkin henkilötietoja todella tarvitaan.

4.5 Virheelliset kirjaukset

Seuraava rekrytointiprosessista löytyvä tietosuojariski on havainnollistettu tietosuoja-asetusta tulkitsemalla. Tämä rekrytointiprosessin tietosuojariski liittyy työnhakijan henkilötietojen virheellisiin kirjauksiin. Tutkielmassa tällä tarkoitetaan tilannetta, jossa työnhakijan henkilötiedot on rekrytoivan organisaation toimesta kirjattu virheellisesti

---

kun arvioidaan työnantajan mahdollisia tulevia velvoitteita esimerkiksi ulkomailla työskentelyn osalta. Toisinaan myös työaikalain tarkoittaman hätätyön yhteydessä tiedot perhesuhteista voivat olla ajankohtaisia henkilön päästyä palvelussuhteeseen. Lue lisää Alapuranen ja muut, s.199.

[188] Yhtenä esimerkkinä voidaan pitää lemmikkieläinten omistusta: tavallista rekrytointiprosessia ajatellen tällainen henkilötieto tuntuu tarpeettomalta. Hallituksen esityksessä 75/2000 on kuitenkin määritelty, että esimerkiksi perhepäivähoitajan rekrytoinnin yhteydessä tällainen henkilötieto voi olla tarpeellinen. Tämä sen vuoksi, että tuolloin saatetaan tarvita tietoa siitä, voitaisiinko mahdollisesti rooliin valittavalle uudelle perhepäivähoitajalle osoittaa hoidettavaksi allergisia lapsia, ks. HE 75/2000, s.16.

[189] Alapuranen ja muut, 2020, s.197; Nyyssölä, 2018, s.66–69.

[190] HE 75/2000, s.16.

esimerkiksi suorahakupuhelun tai työhaastattelun yhteydessä. Virheellisesti kirjattavia henkilötietoja saattavat olla esimerkiksi tietyn alan ammattivuosien määrä, koulutuksen taso tai kielitaidon syvyys. Rekrytoija saattaa myös toisinaan sekoittaa työnhakijoita toisiinsa hoitaessaan useita suorahakupuheluita samanaikaisesti. Tällöin osa työnhakijoiden henkilötiedoista saattaa tulla kirjatuiksi väärälle työnhakijalle. Tällaiset virheelliset kirjaukset henkilötiedoista loukkaavat rekisteröidyn oikeutta henkilötietojensa täsmällisyydestä, sekä laiminlyövät täsmällisyyden tietosuojaperiaatetta.[191]

Erityisen ongelmallista tällaisista tilanteista tekee se, että mikäli rekrytoiva organisaatio on kirjannut työnhakijan henkilötietoja virheellisesti, on riski, että työnhakijan oikeus oikaista häntä koskevia tietojaan ei toteudu. Tämä sen vuoksi, että työnhakija ei tällöin voi tietää tai edes olettaa, että hänestä kirjatut henkilötiedot olisivat virheellisiä. Siksi työnhakijalla ei ole tällöin realistisia mahdollisuuksia toteuttaa oikeuttaan oikaista henkilötietojansa: työnhakijan ei voida nimittäin vaatia epäilevän kaikkia häntä koskevia rekrytointiprosesseja sen suhteen, että häntä koskevat henkilötiedot olisi kirjattu virheellisesti. Tämän vuoksi rekrytoivan organisaation toimesta tehdyt virheelliset kirjaukset työnhakijan henkilötiedoista muodostavat tietosuojariskin rekisteröidyn henkilötietojen suojan näkökulmasta[192]. Työnhakijan henkilötietojen epätäsmällisyys on työnhakijan kannalta epäoikeudenmukaista myös sen vuoksi, että joissakin tapauksissa virheellisesti merkityt henkilötiedot voivat johtaa työnhakijan kannalta negatiivisiin rekrytointivalintoihin.

4.6 Henkilötietojen tarpeeton jakaminen

Viides rekrytointiprosessin tietosuojariski liittyy työnhakijan henkilötietojen tarpeettomaan jakamiseen. Tutkielmassa tällä tarkoitetaan tilannetta, jossa rekrytoiva

[191] TSA 5 artikla määrittää, että ’’henkilötietojen on oltava täsmällisiä’’. Tätä kutsutaan niin sanotuksi täsmällisyyden tietosuojaperiaatteeksi. Lisäksi asetuksen 16:sta artiklassa tuodaan esille rekisteröidyn oikeus vaatia, että rekisterinpitäjä oikaisee ilman aiheetonta viivytystä rekisteröityä koskevat epätarkat ja virheelliset henkilötiedot.

[192] Voidaan ajatella, että myös työnhakijan itse kirjaamat tai antamat virheelliset henkilötiedot voivat johtaa työnhakijan kannalta negatiivisiin seurauksiin. Tällöin vastuussa on kuitenkin työnhakija itse, eikä työnhakijaan negatiivisesti vaikuttavia seuraamuksia voida pitää henkilötietojen suojan tietosuojariskeinä.

organisaatio jakaa työnhakijan henkilötietoja tarpeettomasti rekrytoivan tiimin ulkopuolisille henkilöille. Samanaikaisesti tähän tietosuojariskiin lasketaan mukaan myös tapahtumaketjut, joissa työnhakijasta kerrotaan rekrytoivaan tiimiin kuuluvalle jäsenelle tarpeettoman paljon henkilötietoja: esimerkiksi rekrytointiin osallistuvalle tiimiläiselle jaetaan työnhakijan edellisen työsuhteen palkkatietoja[193]. Henkilötietojen tarpeeton jakaminen on tietosuojalainsäädännön vastaista, sillä esimerkiksi tietosuoja-asetuksen mukaan rekisterinpitäjän tulee käsitellä rekisteröityjen henkilötietoja luottamuksellisesti ja asianmukaisesti[194]. Henkilötietojen tarpeettoman jakamisen voidaankin katsoa rikkovan tietosuojaperiaatteita: se rikkoo ainakin luottamuksellisuuden ja eheyden periaatetta, käyttötarkoitussidonnaisuuden periaatetta, sekä kohtuullisuuden periaatetta.

Henkilötietojen tarpeettoman jakamisen voidaan nähdä rikkovan kohtuullisuuden periaatetta, sillä kuten tutkielmassa on aiemmin tuotu ilmi, tarkoittaa kohtuullisuus eräänlaista sisäänrakennettua reiluutta. Lisäksi rekisterinpitäjän on otettava henkilötietoja käsitellessään huomioon työnhakijan edut ja odotukset[195]. Siksi työnhakijan henkilötietojen tarpeetonta jakamista ei voida pitää toimintana, joka olisi rekisteröidyn edun mukaista tai jota rekisteröity voisi olettaa tapahtuvan. Tämän ohella henkilötietojen tarpeeton jakaminen on käyttötarkoitussidonnaisuuden periaatteen vastaista, sillä tällä tietosuojaperiaatteella on nimenomaisesti tarkoitus rajoittaa sitä, mihin tarkoitukseen rekrytoiva organisaatio voi käyttää työnhakijoista keräämiään henkilötietoja[196]. Siksi henkilötietojen jakaminen muille kuin rekrytointiin osallistuville henkilöille tai muihin kuin rekrytoinnin suorittamisen kannalta olennaisiin tarkoitusperiin on alkuperäisen

[193] Vaikka rekrytoija saisi tietoonsa tällaisia työnhakijan edellisen työsuhteen palkkatietoja, ei voida pitää tarpeellisena, että hän jakaisi tällaisia henkilötietoja eteenpäin rekrytointiin osallistuvalle tiimiläiselle. Tämän voitaisiin katsoa olevan kohtuullisuuden ja luottamuksellisuuden periaatteen vastaista.
[194] Katso tietosuoja-asetuksen yleiset tietosuojaperiaatteet: TSA 5 artikla.
[195] Korpisaari ja muut (2022, s.101) painottavat, että kohtuullisuuden periaate edellyttää sitä, ettei rekisteröidyn henkilötietoja väärinkäytetä.
[196] Käyttötarkoitussidonnaisuuden periaatteeseen kuuluu kaksi tärkeää näkökulmaa: ensinnäkin henkilötiedot tulee kerätä tiettyä nimenomaista laillista tarkoitusta varten. Lisäksi niitä ei saa myöhemminkään käsitellä näiden tarkoitusten kanssa yhteensopimattomalla tavalla, ks. Korpisaari ja muut, 2022, s.103. Mikäli organisaatio esimerkiksi on kerännyt työnhakijoista henkilötietoja rekrytoinnin läpiviemiseksi, ei näitä kerättyjä henkilötietoja ole luvallista jakaa eteenpäin esimerkiksi tiedoista kiinnostuneelle uteliaalle toimitusjohtajalle, jolla ei muuten olisi mitään asianmukaista tarvetta osallistua rekrytointiin.

käyttötarkoituksen – eli rekrytointiprosessin loppuunsaattamisen – vastaista. Lisäksi henkilötietojen tarpeeton jakaminen on luottamuksellisuuden periaatteen vastaista, sillä tietosuoja-asetuksen mukaisesti henkilötietoja tulee käsitellä niin, ettei asiattomilla ole tietoihin pääsyä[197]. Seuraavaksi tuon ilmi, miten kyseessä oleva tietosuojariski – henkilötietojen tarpeeton jakaminen – näyttäytyy rekrytointiprosessissa.

Tutkielman haastateltavista jopa yhdeksän mainitsi henkilötietojen tarpeettoman jakamisen yhdeksi rekrytointiprosessin tietosuojariskeistä. Seuraavassa esimerkissä korostuu HR-alan ammattilaisen huoli siitä, kuinka esihenkilöt toisinaan keskustelevat työnhakijasta omien verkostojensa kanssa. Nämä verkostot koostuvat usein rekrytointitiimin ulkopuolisista henkilöistä:

> *''Eniten riskinä on kyllä ihmisten välinen keskustelu. Se on mulle HR:n edustajana aina semmonen kauhunhetki, jos esihenkilö tulee sanomaan, että joo mä juttelinkin jo tästä hakijasta mun työkaverin kanssa, että se tiesi tästä hakijasta. Et esihenkilöt ei tuu vaan ajatelleeks, et tämä työkaverin kanssa käyty keskustelu on henkilötietojen jakamista eteenpäin, eikä niitä tietoja tuu luovuttaa kellekkään yli-innokkaalle ja uteliaalle pomon pomolle, jolla ei muuten oo asianmukasta pääsyä siihen rekryyn. Vaik se titteli olis mikä niin se ei vielä välttämättä oikeuta sua saamaan niitä tietoja.''*
>
> *-Haastateltava 8*

Henkilötietojen tarpeetonta jakamista rekrytointitiimin ulkopuolisille henkilöille toistettiin useassa haastattelussa. Yhdessä haastattelussa korostui myös toinen henkilötietojen tarpeettomaan jakamiseen liittyvä näkökanta, nimittäin se, etteivät kaikki työnhakijan henkilötiedot kuulu jaettavaksi kaikille rekrytointiin osallistuville työntekijöille:

> *''Kyllä tietenkin yks tietosuojariski on se, että puhutaan rekrytointiin osallistuvan tiimiläisen läsnä ollessa työnhakijan edellisen työsuhteen aikaisesta palkasta. En näe, että tällaista henkilötietoa tulis jakaa kellekkään tarpeettomasti ilman työnhakijan erikseen antamaa suostumusta. Usein nimittäin sen rekryyn osallistuvan tiimiläisen ei oikeesti tarvis tietää tulevan työntekijän vanhaa palkkaa.''*
>
> *-Haastateltava 9*

Edellä mainitut esimerkit edustavat tilanteita, joissa työnhakijan henkilötietoja jaetaan tarpeettomasti eteenpäin verbaalista kieltä käyttäen. Haastatteluissa nousi esille myös näkökulma siitä, kuinka pelkästään työnhakijan olemassaolo ja huolimattomasti

[197] Hanninen ja muut, 2017, s.51; Korpisaari ja muut, 2022, s.108.

koordinoidut ja toteutetut työhaastattelutilanteet saattavat tuoda ilmi työnhakijan henkilötietoja tarpeettomasti:

> *''Eräänlaisen tietosuojariskin muodostaa päättelyriskit. Tällä tarkotan sitä, että mä en voi työnhakijan päähän vetää paperipussia, et peitetääs tolla noi sun kasvot. Koska kyllä ne kasvotkin on henkilötietoa, ja sitä kautta neukkarin ohi kulkevät rekrytointitiimin ulkopuoliset henkilöt voi päätellä, et hei, nyt toi mun naapuri on hakenu meille töihin, ku se on tuolla palaverissa meijän rekrytoijan kanssa. Nää on semmosta tiedon turhaa jakamista, mikä vois joltain osin olla estettävissä esimerkiks etätyöhaastattelujen avulla.''*
>
> *-Haastateltava 4*

Oheisesta esimerkistä havaitaan, että jopa työhaastattelun käytännön toteutuksella voi olla vaikutusta työnhakijan henkilötietojen suojaan. Työnhakija ei nimittäin uutta työpaikkaa hakiessaan halua välttämättä kertoa tätä vielä vanhalle työpaikalleen. Tiivistetysti voidaan todeta, että riski tarpeettomasta henkilötietojen jakamisesta lisääntyy, mitä vähemmän rekrytointiprosessin käytännöllisiä toimenpiteitä – kuten työhaastattelun sijaintia ja ajankohtaa – on suunniteltu. Lisäksi henkilötietojen tarpeettoman jakamisen riski lisääntyy sitä myötä, mitä useampi ihminen rekrytointiprosessiin osallistuu, sekä mitä enemmän työnhakijoista jaetaan henkilötietoja kaikille rekrytointiin osallistuville työntekijöille. Myös selkeiden roolitusten ja sääntöjen puute[198] voi lisätä riskiä henkilötietojen tarpeettomaan ja rekrytointiprosessin kannalta liian laajaan jakamiseen.

4.7 Tietoturvaan liittyvät riskit

Kuudes rekrytointiprosessin tietosuojariski kattaa sisälleen kaikki sellaiset tietoturvaan liittyvät riskit, jotka asettavat työnhakijoiden henkilötietoja tietovuotoriskin alaiseksi. Tietovuoto[199], joka kohdistuu henkilötietoihin, on nimeltään henkilötietovuoto ja tutkielmassa käsitellään nimenomaisesti *työnhakijoiden* henkilötietoihin kohdistuvia henkilötietovuotoja[200]. Tutkielman määritelmän mukaisesti tietoturvalla pyritään hallinnollisin

---

[198] Selkeiden roolitusten ja sääntöjen puutteella viittaan tilanteeseen, jossa esimerkiksi esihenkilö ei tiedä, kenelle hän saa jakaa työnhakijan henkilötietoja. Tällaiset tilanteet voitaisiin välttää esimerkiksi ohjeistuksilla. Lisää aiheesta tutkielman seuraavassa luvussa, jossa käsitellään tietosuojariskien hallintaa.

[199] Raman, Kaycik & Somayaji, 2011, s.1. Tietovuodolla (*data leak*) tarkoitetaan salassa pidettävän tiedon tahatonta tai tahallista leviämistä ulkopuolisille. Tietovuotoja voi tapahtua myös muiden kuin tietoturvaan liittyvien ongelmien vuoksi ja tutkielmassa aikaisemmin mainitut tietosuojariskit, kuten henkilötietojen liiallinen keräys ja henkilötietojen tarpeeton jakaminen aiheuttavat myös tietovuotoriskejä.

[200] On hyvä huomioida, että henkilötietovuodot voivat organisaatiossa kohdistua myös muiden kuin työnhakijoiden henkilötietoihin. Esimerkiksi nykyisten työntekijöiden henkilötiedot voivat yhtä lailla olla henkilötietovuotojen riskin alaisena. Tällaiset tietosuojariskit ovat kuitenkin tutkielman rajauksen ulkopuolella.

ja teknisin toimenpitein varmistamaan henkilötietojen asianmukainen käsittely[201]. Siksi tietoturvariskien kirjo on laaja, ja rekrytointiprosessin aikana monet eri tekniset tapahtumaketjut ja toimenpiteet voivat aiheuttaa tietoturvariskejä. Lainsäädännön näkökulmasta tietoturvariskit loukkaavat luottamuksellisuuden sekä eheyden tietosuojaperiaatetta, sillä työnhakija ei tietovuotojen yhteydessä voi tietää, kenellä on pääsy hänen henkilötietoihinsa. Tällöin rekisterinpitäjä myös laiminlyö velvoitettaan huolehtia riittävistä toimenpiteistä henkilötietojen asianmukaisen käsittelyn varmistamiseksi.[202] Tietoturvariskit myös vaikeuttavat rekisteröidyn oikeutta henkilötietojen poistamiseen sekä henkilötietojen käsittelyn rajoittamiseen[203].

Haastatteluissa kahdeksan HR-alan ammattilaista mainitsi tietoturvariskit yhdeksi rekrytointiprosessin tietosuojariskeistä. Myös haastatteluissa korostui, että tietoturvariskit voivat näyttäytyä rekrytointiprosessin aikana hyvin monella eri tavalla:

> *''Tietojärjestelmiin voi päästä ulkopuolinen tietosuojaloukkauksen yhteydessä, jos ilmenee esimerkiks hakkerointi, haittaohjelma, kyberhyökkäys tai tietokoneen varastaminen.''*
>
> *-Haastateltava 3*

Lisäksi haastatteluissa korostui näkemys siitä, että tietoturvariskit ovat todellisia, ja niiden olemassaolo tulisi huomioida rekrytointiprosessien yhteydessä:

> *''IT-riskit on aina olemassa, ne etevimmät hakkerit pääsee keskiverron yrityksen sisälle järjestelmään ku järjestelmään. Et jos joku kyvykäs toimija haluaa tietää, kuka hakee johonkin työpaikkaan, ni se pystyy sen tekemään järjestelmästä riippumatta.''*
>
> *-Haastateltava 4*

Rekrytointiprosessin tietoturvariskien todennäköisyys on sitä suurempi, mitä haavoittuvaisempi järjestelmä yrityksellä on käytössä, sekä mitä helpompaa järjestelmään sisäänkirjautuminen on. Myös henkilötietojen pitkät säilytysajat lisäävät tietoturvariskejä.

---

[201] Katso tarkemmin tutkielman sivulta 14.

[202] Tietosuoja-asetuksessa tuodaan useasti esille, kuinka rekisterinpitäjän tulee varmistaa henkilötietojen käsittelyn yhteydessä asianmukainen turvallisuus ja luottamuksellisuus. Lisäksi rekisterinpitäjää velvoitetaan ehkäisemään luvaton pääsy henkilötietoihin tai niiden käsittelyyn käytettyihin laitteistoihin, ks. esim. TSA 5 artikla kohta 1a sekä johdanto kohta 39.

[203] TSA 17 artikla käsittelee rekisteröidyn oikeutta tulla unohdetuksi. TSA 18 artikla käy puolestaan läpi rekisteröidyn oikeutta henkilötietojen käsittelyn rajoittamiseen. Työnhakija ei lähtökohtaisesti pysty vaatimaan omien henkilötietojensa poistamista tai käsittelyn rajoittamista, mikäli hän ei tiedä, kuinka laajalle hänen henkilötietonsa ovat tietovuodon seurauksesta päätyneet.

4.8 Henkilötietojen poistamattomuus

Seitsemäs rekrytointiprosessin tietosuojariski liittyy työnhakijoiden henkilötietojen poistamattomuuteen. Työnhakijan henkilötietojen tarpeettoman pitkä säilyttäminen on sekä tietojen minimoinnin että säilytyksenrajoitusperiaatteiden vastaista[204]. Tutkielman haastatteluissa kahdeksan HR-alan ammattilaista koki tietojen poistamattomuuden olevan yksi rekrytointiprosessin tietosuojariskeistä. Käytännössä tietojen poistamattomuus voi ilmetä rekrytointiprosessin yhteydessä eri tavoin. Yksi haastateltavista kiteytti kolme keskeistä tapaa, jotka lisäävät riskiä työnhakijoiden henkilötietojen poistamattomuuteen:

> *''Esimerkiksi pienissä organisaatioissa on usein sähköpostiosoite, minne laitetaan työhakemukset – niin ihan oikeasti – kukaan ei välttämättä muista poistaa niitä. Toisilla esihenkilöillä on myös semmonen tapa, että mennessään rekrytointihaastatteluun ne tulostaa työhakemukset. Sit ne hakemukset saattaa pyöriä niillä vaikka kuinka kauan. Tai sitten kolmas vaihtoehto on se, että sä kirjoitat niistä [työnhakijoista] muistiinpanoja, niin millon sä poistat ne? Jos se on vaikka sun muistikirja, jossa sulla on bisnesjutut ja rekrytoinnit samassa muistikirjassa niin harva niitä rupee sieltä repimään irti.''*
>
> *-Haastateltava 2*

Vaikka rekrytoiva organisaatio olisi iso ja rekrytointijärjestelmä olisi käytössä, ei sekään estä sitä, etteikö työhakemuksia saapuisi organisaation sähköpostiosoitteisiin:

> *''Vaikka meillä pyydetään kaikki hakemukset rekrytointijärjestelmään hakemuslomakkeen kautta, niin kylhän välillä jengi lähettää meille sähköpostilla niitä hakemuksia. Ja tää on kyllä aika yleistä.''*
>
> *-Haastateltava 3*

Rekrytointiprosessin suorittamiseen käytettävien järjestelmien ohella myös tietokoneen asetukset ja muut taustaohjelmat voivat vaikuttaa tietojen poistamattomuuteen:

> *''Tietosuojariski on se, kun se CV avataan ja ladataan koneelle, tai joillakin on koneessa se, et kun ne avaa PDF:n niin se kone lataa sen automaattisesti. Ja sit ne henkilötiedot jää sen CV:n mukana sinne koneelle.''*
>
> *-Haastateltava 1*

Haastatteluissa esiin nousseiden näkökulmien lisäksi henkilötietojen poistamattomuuden riski voi lisääntyä, mitä vähemmän rekrytointiprosessia on suunniteltu. Mikäli

---

[204] Korpisaari ja muut, 2022, s.104–107. Sekä tietojen minimoinnin että säilytyksen rajoitusperiaatteiden mukaisesti rekisterinpitäjän tulee poistaa tai anonymisoida henkilötiedot heti, kun niiden alkuperäinen käsittelytarkoitus päättyy. Työnhakijoiden henkilötietojen säilytysaika määräytyy laittoman työhönoton valitusajan maksimin mukaisesti, joka on kaksi vuotta, katso lisää tutkielman sivulta 33.

yrityksessä ei esimerkiksi ole käytössä rekrytointijärjestelmää, tai järjestelmä ei automaattisesti poista henkilötietoja tietyn määräajan jälkeen, voivat työnhakijoiden henkilötiedot jäädä poistamatta. Rekrytoinnista vastuussa olevat työntekijät eivät puolestaan välttämättä osaa tai muista poistaa henkilötietoja, tai asettaa järjestelmään automaattista poisto-ominaisuutta, mikäli organisaatiossa ei ole erikseen käsitelty henkilötietojen poistamista. Tämän ohella epäselvät roolitukset voivat lisätä tietojen poistamattomuutta: jaettu vastuu on harvoin kenenkään vastuu.

4.9 Osoitusvelvollisuuden laiminlyönti

Kahdeksas tutkielmassa havaittu rekrytointiprosessin tietosuojariski liittyy rekisterinpitäjän, eli rekrytoivan organisaation, osoitusvelvollisuuden laiminlyöntiin. Nimensä mukaisesti osoitusvelvollisuuden laiminlyönti rikkoo tietosuoja-asetuksen vaatimusta siitä, että rekisterinpitäjän tulee kyetä osoittamaan henkilötietojen käsittely lainmukaiseksi. Tämä tietosuojariski kattaa sisälleen kaikki tapahtumaketjut, joiden aikana tai joiden seurauksena rekrytoiva yritys ei täytä tietosuoja-asetuksen vaatimusta rekisterinpitäjän osoitusvelvollisuudesta[205]. Osoitusvelvollisuuden laiminlyönnin riskiä lisää merkittävästi rekrytointiprosessin aikaisen henkilötietojen käsittelyn dokumentoinnin puute: mikäli yritys ei dokumentoi, kuinka se käsittelee työnhakijoiden henkilötietoja, laskee sen mahdollisuudet osoittaa työnhakijoiden henkilötietojen käsittelyn lainmukaisuus.

Tietosuojalainsäädännön vaatimus osoitusvelvollisuudesta on rekrytoivan yrityksen kannalta jokseenkin ongelmallista, sillä tietosuoja-asetus on laadittu avoimella kielellä: asetus ei selosta, kuinka rekisterinpitäjän tulee toteuttaa osoitusvelvollisuuttaan. Siksi lienee ilmeistä, että rekrytoivan yrityksen on käytettävä harkintavaltaa osoitusvelvollisuuden käytännön toteutustavoissa. Tietosuoja-asetusta tulkitsemalla on kuitenkin havaittavissa joitakin osoitusvelvollisuuden laiminlyönnin riskiä lisääviä tekijöitä. Tutkielmassa

[205] TSA:n 5:n artiklan toisen kohdan sekä 24:n artiklan ensimmäisen kohdan mukaan rekisterinpitäjän on kyettävä osoittamaan toimivansa tietosuojalainsäädännön vaatimusten mukaisesti: rekisterinpitäjän tulee rekrytointiprosessin aikana varmistaa noudattavansa rekisterinpitäjälle määrättyjä velvollisuuksia sekä samalla huolehtia siitä, että rekisteröityjen oikeuksia ei laiminlyödä rekrytointiprosessin yhteydessä.

on aiemmin nostettu esiin tapahtumaketju, jossa rekisterinpitäjän osoitusvelvollisuus ei täyty. Tämä on tietosuojaselosteen laatimatta jättäminen: tietosuoja-asetuksen 12 artiklan mukaisesti tiedot henkilötietojen käsittelystä tulee ilmoittaa rekisteröidylle kirjallisesti ja tapauksen salliessa sähköisesti. Vaikka asetuksessa sallitaan myös suullinen tietojen luovuttaminen rekisteröidyn niin pyytäessä, lähtee asetus olettamuksesta, että tiedot tulisi antaa kirjallisessa muodossa. Siksi selosteen puuttuminen lisää osoitusvelvollisuuden laiminlyönnin riskiä.

Toinen osoitusvelvollisuuden laiminlyönnin riskiä kasvattava tekijä on vaikutustenarvioinnin tekemättä jättäminen. Kuten tutkielmassa on aikaisemmin tuotu esille, tulisi rekrytoinnin yhteydessä tehdä vaikutustenarviointi, kun uutta teknologiaa ja automatisointia otetaan käyttöön etenkin työnhakijoiden profiloinnin yhteydessä. Koska rekisterinpitäjän osoitusvelvollisuus on kuitenkin varsin yleisluontoinen velvoite, jonka toteuttamiskeinoista ei ole säädetty yksityiskohtaisesti, tulee osoitusvelvollisuus käsittää eräänlaisena tavoiteltuna lopputuloksena. Täsmällisiä keinoja tämän velvoitteen täyttämiseksi ei välttämättä ole vielä olemassa, mutta osoitusvelvollisuuden laiminlyönnin riskin voidaan nähdä kasvavan, mitä vähemmän rekrytoiva organisaatio dokumentoi ja kirjaa ylös työnhakijoiden henkilötietoihin liittyviä käytänteitä ja toimintamalleja.

4.10 Tietosuojariskeihin ajavia tekijöitä

Jotta rekrytointiprosessin tietosuojariskien alkuperä voidaan tunnistaa, on analysoitava, millaiset tekijät aiheuttavat tietosuojariskejä. Siksi esittelen seuraavaksi neljä tyypillistä rekrytointiprosessin tietosuojariskejä aiheuttavaa tekijää: inhimilliset, operatiiviset, vilpilliset, sekä strategiset tekijät[206]. Kategoriat eivät ole toisiaan poissulkevia ja toisinaan ne esiintyvät myös päällekkäin. Esimerkiksi operatiivisiin tekijöihin liittyy usein ihmisen toiminnasta johtuvia eli inhimillisiä tekijöitä. Tietosuojariskejä aiheuttavien tekijöiden

[206] Inspiraatio jakaa tietosuojariskejä aiheuttavat tekijät neljään kategoriaan on lähtöisin Suomen riskienhallintayhdistyksen riskitekijöiden jaottelusta, ks. Suomen riskienhallintayhdistys, 2023. Vaikka inhimilliset riskitekijät voidaan luokitella myös operatiivisten tekijöiden alle, on ne tutkielmassa haarautettu täysin omaksi kategoriaksi, sillä inhimillisillä tekijöillä on tässä tutkielmassa nähty olevan merkittävä vaikutus rekrytointiprosessin tietosuojariskien muodostumisessa. Sama pätee vilpillisiin tekijöihin.

kategorisointi auttaa kuitenkin havaitsemaan, kuinka tietosuojariskit syntyvät eri tekijöiden myötävaikutuksessa. Seuraavien kappaleiden esimerkit antavat yrityksille perustan hahmottaa rekrytointiprosessin tietosuojariskeihin ajavia tekijöitä. Oheinen kuvio (kuvio 7) havainnollistaa näitä neljää tekijää.

Kuvio 7. Rekrytointiprosessin tietosuojariskeihin ajavia tekijöitä.

Rekrytointiprosessin tietosuojariskeihin ajavista tekijöistä inhimilliset eli ihmisen aiheuttamat tekijät toistuivat tutkielman haastatteluissa usein. Inhimillisillä tekijöillä tarkoitetaan tässä tutkielmassa kaikkia ihmisen päätökseen ja toimintaan liittyviä tekijöitä, ja

niissä korostuu *yksittäisten* ihmisten tekemät päätökset, jotka liittyvät oman työn suorittamiseen tai omaan käyttäytymiseen työympäristössä. Tämä erottaa tietosuojariskejä aiheuttavat inhimilliset tekijät esimerkiksi strategisista tekijöistä, joissa puolestaan korostuu koko organisaatiota tai organisaation osaa koskeva päätöksenteko. Inhimilliset riskitekijät voivat johtua esimerkiksi ihmisen ajattelemattomuudesta, laiskuudesta, unohduksista tai välinpitämättömyydestä. Tutkielman haastatteluissa korostui, miten herkästi ihmisten ymmärtämättömyys aiheuttaa tietosuojariskejä:

> *''Riskejä aiheuttaa ehkä eniten ihmisten ymmärtämättömyys ja me ihmiset ollaan kyllä käveleviä tietosuojariskejä. Ei me yksinkertasesti aina osata ajatella, että millanen toiminta ois oikeesti suotavaa tai edes sallittua. Esimerkiks esihenkilö ei välttämättä yleensä ymmärrä, että jakaessaan CV:n toiselle henkilölle esimerkis viestintäkanavien kautta, lisääntyy riskit samalla huomattavasti.''*
>
> *-Haastateltava 1*

Myös kirjallisuus tukee ajatusta, että tietosuojariskien synty liittyy toisinaan ihmisen ymmärtämättömyyteen[207]. Seuraava esimerkki havainnollistaa inhimillisten tekijöiden olennaisuutta tietosuojariskien syntymisessä:

> *''Vaikka meillä ois kuinka hyvät ja turvatut järjestelmät, niin kyllä ihmisten toiminta aiheuttaa eniten tietosuojariskejä. Ei mikään järjestelmä pysty suojaamaan niiltä riskeiltä, ellei me, jotka niitä prosesseja suorittaa – eli ihmiset – oikeesti haluta varautua riskeiltä.''*
>
> *-Haastateltava 7*

Haastattelujen esimerkeistä voimme havaita, että inhimillisillä tekijöillä on suuri vaikutus rekrytointiprosessin tietosuojariskien syntymisessä. Tietosuojariskejä aiheuttavat lisäksi operatiiviset tekijät. Tutkielmassa operatiivisilla tekijöillä tarkoitetaan organisaation prosesseja sekä käytössä olevia järjestelmiä. Operatiivisiin tekijöihin luetaan myös yrityksen toimintatavat ja rutiinit, jotka ohjaavat jokapäiväisiä arkisia tapahtumaketjuja. [208]

---

[207] Alapuranen ja muut (2020, s.237) tuovat ilmi, kuinka monille henkilötietojen käsittelyn parissa työskenteleville ihmisille voi tulla yllätyksenä, kuinka paljon henkilötietojen käsittelyä on säännelty ja rajoitettu, sekä miten laajasti rekisteröidyn oikeudet omiin henkilötietoihinsa todellisuudessa vaikuttaa siihen, kuinka rekisteröityjen henkilötietoja on mahdollista kerätä ja käsitellä.

[208] Alhosuon, Nilsenin, Nousiaisen, Pellikan ja Sundbergin (2012, s.86) mukaan operatiiviset riskitekijät aiheutuvat puutteellisista järjestelmistä, prosesseista sekä systeemeistä. Myös henkilöstön toiminta tai ulkoiset hyökkäykset ovat toisinaan luokiteltu operatiivisiksi riskitekijöiksi. Tässä tutkielmassa ne on kuitenkin eritelty omiksi riskitekijöikseen. Jobst (2207, s.4–5) tuo ilmi, ettei operatiivisesta riskitekijästä ole yleistä, vahvistettua määritelmää, mutta se usein ymmärretään riskitekijäksi, joka johtuu virheellisistä prosesseista tai toiminnasta prosessin aikana ja joka johtaa pääoman menetykseen.

Tutkielman haastatteluissa nousi esille, kuinka nimenomaisesti tavat ja rutiinit aiheuttavat tietosuojariskejä rekrytointiprosessien yhteydessä. Yksi haastateltavista kuvaili, miten työnhakijan henkilötietojen poistamattomuuden riski liittyy toisinaan juuri niihin tapoihin ja rutiineihin, joilla olemme tottuneet suorittamaan rekrytointiprosessia:

> *''Se paperirumba on kyl yks iso tietosuojariski. Ihmiset tykkää tehä paperilla asioita ja katella niitä CV:eitä omin silmin sekä kirjottaa ylös haastattelutilanteissa hakijoitten vastauksia. Siihen tulosteluun ja muistiinpanoihin ollaan niin totuttu. Ja sit ne tulosteet ja muistiinpanoja täynnä olevat paperit jää tuhoamatta. Tää riskihän oikeestaan johtuu meijän jokapäiväsistä rutiineista, ja siitä, millä tavalla suoritetaan sitä prosessia.''*
>
> *-Haastateltava 1*

Lisäksi rekrytointijärjestelmä – tai sen puute – voidaan lukea operatiiviseksi riskitekijäksi. Mikäli rekrytointijärjestelmää ei nimittäin ole käytössä, käsittelevät rekrytoivat yritykset usein työnhakijoiden henkilötietoja sähköpostien ja erilaisten viestintäkanavien, kuten Microsoft Teams:in tai Slack:in avulla[209]. Työnhakijoiden henkilötiedot eivät tällöin poistu automaattisesti sähköpostista tai sisäisistä viestintäkanavista, jolloin tietojen poistaminen on täysin inhimillisen toiminnan varassa. Lisäksi etenkin yhteiskäyttöisissä sähköposteissa riskit henkilötietovuodoille ovat aina olemassa. Tämä kävi ilmi myös tutkielman haastatteluissa:

> *''Jos esimerkiks assistenteilla on lukuoikeus osakkaiden sähköpostiin – ja vaikka siinä miten lukis confidential – niin ku sä kirjaudut sinne s-postiin ja se työhakemus sattuu olemaan ensimmäinen sähköposti niin sähän näät sen preview-osion siitä, ja sitä kautta sen työnhakijan henkilötietoja, vaikket sä olis ees mukana siinä rekrytiimissä.''*
>
> *-Haastateltava 7*

Myös rekrytointiprosessin aikana tapahtuva henkilötietojen siirto voidaan laskea operatiiviseksi tietosuojariskejä aiheuttavaksi tekijäksi. Rekrytoivalla yrityksellä saattaa olla käytössään eri rekrytointi- ja HR-järjestelmät. Tämä tarkoittaa, että rekrytointiprosessin loppupuolella työnhakijan henkilötiedot joudutaan siirtämään rekrytointijärjestelmästä HR-järjestelmään. Mikäli tiedonsiirrossa on esimerkiksi hyödynnetty tekoälyä, on tärkeä varmistaa siirtoprosessin tietoturvallisuus, sillä suojaamattomat yhteydet näiden järjestelmien välillä voivat asettaa työnhakijan henkilötiedot alttiiksi henkilötietovuodoille.

---

[209] Kuten tutkielmassa on aiemmin tuotu ilmi, kasvavat tällöin riskit henkilötietojen poistamattomuudesta sekä tietoturvaan liittyvistä henkilötietovuodoista: sähköpostit sekä sisäiset viestintäkanavat ovat nimittäin lähtökohtaisesti haavoittuvaisempia tietoympäristöjä kuin mitä rekrytointijärjestelmät ovat.

Inhimillisten ja operatiivisten tekijöiden ohella rekrytointiprosessin tietosuojariskejä aiheuttavat vilpilliset tekijät. Tutkielmassa vilpillisillä tekijöillä tarkoitetaan kaikkia niitä tekoja ja aikomuksia, joilla halutaan tehdä tahallaan pahaa. Vilpilliset tekijät ovat usein ulkopuolisia: esimerkiksi tutkielmassa aiemmin käsitellyt tietoturvariskit – eli esimerkiksi tietomurrot ja palvelunestohyökkäykset – ovat lähtökohtaisesti organisaation ulkopuolisen vilpillisen mielen aiheuttamia. Tutkielman haastatteluissa kävi kuitenkin ilmi, että toisinaan tietosuojariskejä aiheuttavat vilpilliset tekijät voivat kummuta jopa organisaation sisältä. Täten rekrytoivien yritysten ei tule sulkea silmiään mahdollisuudelta, etteikö yrityksessä jo työskentelevä työntekijä voisi aiheuttaa tahallisesti henkilötietovuotoja.

Viimeiseksi nostan esille strategiset riskitekijät. Tutkielmassa strategisilla tekijöillä tarkoitetaan yrityksen johdon tekemiä ylätason suunnitelmia[210]. Näillä strategisilla tekijöillä voi puolestaan olla suora vaikutus tietosuojariskien esiintymistiheyteen:

> *''Isommat organisaatiot on mielenkiintoisempia kohteita urkinnalle. Lisäks maailman tilanne huomioiden idässä sijaitsevat yritykset ja infrastruktuurin kannalta kriittiset yritykset – kuten sähkölaitokset – on mielenkiintoisempia kohteita tietomurtojen tekijöille. Tällöin myös tiedot, ketä yritykseen on hakemassa töihin, on mielenkiintosempia urkkijoille.''*
>
> *-Haastateltava 4*

Oheisen esimerkin mukaisesti yrityksen koon kasvaessa tietosuojahyökkäysten määrä voi lisääntyä. Toisaalta haastatteluissa kahdeksan HR-alan ammattilaista korosti ison koon suojaavan yritystä tietosuojariskien hallinnan näkökulmasta, sillä isoilla organisaatioilla on usein enemmän tietosuojaosaamista ja resursseja pieniin yrityksiin verrattuna. Myös tietosuoja-asetuksen vaikeaselkoisuus ja tulkinnallisuus[211] on strateginen riskitekijä, sillä rekrytoivat yritykset eivät täten pysty tekemään tietosuojalainsäädännön näkökulmasta asianmukaisia strategisia valintoja. Strategisia riskitekijöitä ei tule sivuuttaa, sillä ne vaikuttavat inhimillisten, operatiivisten ja vilpillisten tekijöiden olemassaoloon[212]. Täten tietosuojariskien synty on monimutkainen kokonaisuus.

---

[210] Strategisia tekijöitä on kahdeksan: kasvupäätökset, päätökset ongelmien siirtämistä, ongelmanratkaisusta ja tavoitteiden tasapainottamisesta, laajenemispäätökset, palkitsemispäätökset, päätökset resurssien allokoinnista, sekä päätökset yhteistyöstä, katso tarkemmin Secudo, Elia, Margherita ja Letner, 2022.
[211] Edilex, 2021.
[212] Esimerkiksi tietosuojakoulutuksen puute lisää inhimillisten riskitekijöiden todennäköisyyttä ja päätös rekrytoida ilman järjestelmää vaikuttaa operatiivisten riskitekijöiden olemassaoloon.

5 Riskienhallinnasta

5.1 Tietosuojariskien hallintakeinoja

Tutkielmassa rekrytointiprosessin tietosuojariskien hallintaan esitetään kahdeksan riskienhallintakeinoa. Nämä riskienhallintakeinot pohjautuvat haastatteluiden näkökulmiin ja niiden olennaisuutta tietosuojariskien hallintaan on arvioitu tietosuojalainsäädännön avulla. Kyseiset tietosuojariskien hallintakeinot on koottu oheiseen kuvioon (kuvio 8).

Kuvio 8. Rekrytointiprosessin tietosuojariskien hallintakeinoja.

Oheisen kuvion (kuvio 8) mukaisesti tutkielmassa käsiteltävät rekrytointiprosessin tietosuojariskien hallintakeinot ovat: työnhakijoiden tiedottaminen ja ohjaus, lainmukaisen suostumuksen varmistaminen, henkilötietojen käsittelyn johdonmukainen minimointi, ulkoinen valvonta, sisäinen valvonta, henkilöstön kouluttaminen, rekrytointijärjestelmän käyttöönotto, sekä organisaation arvoihin ja yrityskulttuuriin panostaminen. Käsittelen seuraavaksi näitä kahdeksaa tietosuojariskien hallintakeinoa yksityiskohtaisemmin.

5.2 Työnhakijoiden tiedottaminen ja ohjaus

Ensimmäinen tapa hallita rekrytointiprosessin tietosuojariskejä liittyy työnhakijoiden informointiin ja ohjaukseen. Tutkielmassa tällä tarkoitetaan esimerkiksi tietosuojaselosteen[213] laadintaa ja sen saattamista rekisteröidyn tietoon. Tietosuojaselosteen on tarkoitus olla julkinen, mutta tietosuoja-asetus ei ole säätänyt tietystä viestintämuodosta, jonka kautta tiedot on rekisteröidylle annettava[214]. Tämä tarkoittaa, että rekrytoiva organisaatio voi hyödyntää työnhakijoiden tiedottamiseen parhaaksi katsomaansa tapaa. Voigt ja Bussche huomauttavat, että rekisterinpitäjän tulisi suosia sitä viestintämuotoa, jota rekisterinpitäjän ja rekisteröidyn välillä on tavanomaista kyseisessä tapauksessa hyödyntää[215]. Rekrytointiprosessin osalta luonnollisina viestintämuotoina voitaisiinkin pitää esimerkiksi sähköpostia, organisaation nettisivuja tai työpaikkailmoitustekstiä.

Jotta tietosuojaseloste on tietosuoja-asetuksen mukainen, tulee siinä käsitellä artiklojen 13, 14, 15–22, sekä 34 vaatimuksia[216]. Käytännössä tämä tarkoittaa, että tietosuojaselosteessa tulee käydä läpi, kuinka rekrytoiva yritys käsittelee sekä työnhakijalta itseltään

---

[213] Tässä esiin tuotu tietosuojaseloste – toiselta nimeltään myös tietosuojailmoitus – on eri asia kuin henkilötietojen käsittelytoimia koskeva *seloste*, katso tarkemmin näiden termien eroista tutkielman sivulta 39 sekä Korpisaaren ja muiden (2022) kirjasta sivulta 195.

[214] TSA:n 12 artiklan mukaan tiedot on toimitettava rekisteröidylle tiiviisti esitetyssä, läpinäkyvässä ja helposti ymmärrettävässä sekä saatavassa muodossa kirjallisesti tai muulla tavoin, sekä mahdollisuuksien mukaan sähköisessä muodossa. Tietosuoja-asetuksen kirjoitustavan muotoilu antaa siis vapautta välittää tietosuojaselosteen tiedot rekisteröidylle myös muussa kuin kirjallisessa muodossa, katso tarkemmin tutkielman sivulta 32. Huomionarvoista on myös se, että tiedot on annettava rekisteröidylle maksutta, ks. WP 260 rev. 01, s.6–7.

[215] Voigt & Bussche, 2017, jaksot 5.1. ja 5.1.2.

[216] Katso lisää Korpisaari ja muut, 2022, s. 192–196.

saatuja henkilötietoja että muualta kuin työnhakijalta kerättyjä henkilötietoja. Lisäksi tietosuojaselosteesta tulee käydä ilmi seuraavat asiat: kuinka rekisteröidyn oikeus päästä käsiksi omiin henkilötietoihin on taattu, millaiset mahdollisuudet rekisteröidyllä on oikaista omia tietojaan, miten rekisteröidyn oikeus tietojen poistamiseen toteutuu rekrytointiprosessin aikana, sekä millaiset mahdollisuudet työnhakijalla on rajoittaa henkilötietojensa käsittelyä. Näiden ohella tietosuojaselosteeseen tulee kirjata rekisterinpitäjän ilmoitusvelvollisuus mahdollisista tietoturvaloukkauksista. Tämä tarkoittaa, että rekrytoivan organisaation on kuvailtava, kuinka se mahdollisen tietoturvaloukkauksen tapahtuessa ilmoittaa asiasta niin valvontaviranomaiselle kuin rekisteröidylle eli työnhakijalle[217]. Tietosuojaselosteessa on myös lueteltava henkilötietojen käsittelyyn liittyvät riskit, rekisteröidyn oikeudet omia henkilötietojansa kohtaan, sekä suojatoimet tietosuojariskien hallintaan[218]. Lisäksi tietosuojaselosteessa on mainittava, että työnhakijan henkilötiedot kerätään nimenomaisesti rekrytointiprosessia varten, ja niiden poisto tapahtuu, kun henkilötietoja ei enää tarvita rekrytoinnin näkökulmasta[219].

Tietosuojaselosteen ohella rekrytoivan yrityksen olisi hyvä ohjata työnhakijoita toimimaan tietosuojalainsäädännön mukaisesti. Koska jokainen yritys on toimintatavoiltaan ja -ympäristöltään erilainen, on luonnollista, että myös henkilötietojen käsittelytavat poikkeavat yritysten kesken. Siksi työnhakija ei välttämättä tiedä, miten juuri kyseinen rekrytoiva yritys käsittelee henkilötietoja. Mikäli yrityksellä on esimerkiksi rekrytointijärjestelmä käytössään, on se hyvä viestiä työnhakijalle ja kehottaa hakijaa välttämään työhakemuksen ja CV:n lähettämistä organisaation sähköpostiosoitteisiin. Yksi tutkielman haastateltavista kuvaili, kuinka tämä on käytännön työelämässä mahdollista toteuttaa:

> *''Meillä on esimerkiks käytössä semmonen rutiini, että jokaseen työpaikkailmotukseen lisätään teksti, joka menee tyyliin näin 'tietosuojaa koskevat oikeutesi löydät täältä, luethan ne ja tiedostat, että sun oikeuksien turvaamiseks me ei käsitellä sähköpostin kautta tulleita hakemuksia lainkaan' … Tästä on kyl ollu meille paljon apua, koska tätä kautta ne hakijat tajuaa, miks me ei käsitellä hakemuksia, jotka ei oo tullu sinne meijän järjestelmään.''*
>
> *-Haastateltava 10*

[217] Rekisterinpitäjän ilmoitusvelvollisuus on kirjattu tietosuoja-asetuksen artikloihin 33 ja 34.
[218] TSA johdanto kohta 39.
[219] Rekrytoiva yritys ei voi poistaa työnhakijan henkilötietoja välittömästi rekrytoinnin päätyttyä, katso tarkemmin tutkielman sivulta 33. Mikäli hakijan henkilötietoja on tarkoitus käyttää myös muihin kuin rekrytointiprosessin tarkoituksiin, on tästä informoitava rekisteröityä ja pyydettävä hänen suostumuksensa.

Tietosuojaselosteen laatimisella ja työnhakijoiden ohjaamisella voidaan saavuttaa ainakin seuraavia hyötyjä: ensinnäkin, rekrytoiva organisaatio voi näin täyttää paremmin velvollisuuttaan informoida rekisteröityä henkilötietojen käsittelytavoista[220]. Lisäksi työnhakijoiden informointi lähtökohtaisesti muokkaa henkilötietojen käsittelyä kohti tietosuojaperiaatteiden vaatimuksia: tällöin rekrytoiva yritys nimittäin toteuttaa paremmin läpinäkyvyyden tietosuojaperiaatetta sekä osoitusvelvollisuuttaan. Voidaan myös ajatella, että työnhakijoiden tiedottamisella ja ohjauksella riski liian vähäisestä informoinnista laskee. Samanaikaisesti työnhakijat tulevat tietoisemmiksi omista oikeuksistaan, sekä suosituksista, jotka edistävät heidän henkilötietojensa suojaa. Tällöin rekisteröidyn heikompi asema työnantajaa kohtaan voi parhaimmillaan madaltua ja riski tarpeettomien henkilötietojen jakamisesta pienenee. Lisäksi riski henkilötietojen poistamattomuudesta laskee, kun organisaatiot vastaanottavat vähemmän työhakemuksia ja CV: eitä sähköpostien kautta[221].

5.3 Rekisteröidyn lainmukaisen suostumuksen varmistaminen

Toinen keskeinen tapa hallita rekrytointiprosessin tietosuojariskejä on varmistaa, että rekisteröidyn eli työnhakijan suostumus hänen henkilötietojensa käsittelystä on lainmukainen. Tämä riskienhallintakeino keskittyy laskemaan rekisteröidyn puutteellisen suostumuksen tietosuojariskiä. Jotta rekisteröidyn suostumus henkilötietojen käsittelystä on lainmukainen, tulee seuraavien ehtojen täyttyä: suostumuksen tulee olla vapaaehtoinen, siitä tulee voida kieltäytyä – maksutta myös sen antamisen jälkeen – suostumuksen antamatta jättämisestä ei saa olla rekisteröidylle negatiivisia seurauksia, eikä suostumuksen varjolla saa käsitellä käyttötarkoituksen kannalta tarpeettomia henkilötietoja[222].

[220] Rekisterinpitäjän informaatiovelvollisuudesta ja henkilötietojen läpinäkyvästä käsittelystä on mainintoja tietosuoja-asetuksen johdannon kohdissa 39, 58 ja 60, sekä artikloissa 5 ja 12.
[221] Henkilötietojen käsittely rekrytointijärjestelmässä edesauttaa tietosuojariskien vähentymistä, tätä käsittelen myöhemmin tutkielmassa sivuilla 82–84.
[222] TSA 7 artikla, kohdat 1–4. Vaatimus siitä, ettei suostumuksen varjolla saa käsitellä rekrytoinnin kannalta tarpeettomia henkilötietoja tarkoittaa esimerkiksi sitä, ettei rekrytoinnin yhteydessä työnhakijasta saa kerätä rekrytoinnin kannalta tarpeettomia henkilötietoja – edes työnhakijan suostumuksesta, ks. TSA 7 artikla kohta 4. Aiheesta tarkemmin esimerkiksi ETN, Suuntaviivat 05/2020, s.8.

Lisäksi mikäli työnhakijan henkilötietoja käytettäisiin myös muihin kuin työhönottoon liittyviin käyttötarkoituksiin, tulee tähän pyytää rekisteröidyltä suostumus erikseen. Lainmukainen suostumus edellyttää myös, että rekrytoiva organisaatio kykenee jälkikäteen osoittamaan, että rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn[223].

Käytännössä rekisteröidyn suostumus voitaisiin kerätä esimerkiksi luomalla digitaaliseen rekrytointilomakkeeseen rastitettava ruutu, jonka tulee olla rekisteröidyn *itse* rastittama. Huomionarvoista on, ettei rasti saa olla *automaattisesti* täytetty, jolloin rekisteröidyn tulisi itse huomata poistaa rasti, mikäli hän ei haluaisi antaa suostumustaan[224]. Huomionarvoista on edelleen, että esimerkiksi suorahaun yhteydessä suostumus tulisi hankkia muuten kuin pelkästään rekrytoijan ja rekisteröidyn välisin yksityisviestein. Tämä sen vuoksi, että mikäli rekrytoija lähtee organisaatiosta, lähtisi samalla myös dokumentoitu suostumus työnhakijan henkilötietojen käsittelystä[225]. Siksi rekrytoivan organisaation tulisi suosia sellaisia kirjallisen suostumuksen muotoja, jotka säilötään tietoturvallisiin sähköisiin arkistoihin. Yksi vaihtoehto rekisteröidyn suostumuksen sähköiseen arkistointiin on markkinoilla olevilta palveluntarjoajilta ostettava rekrytointijärjestelmä[226].

Kun rekrytoiva organisaatio on tietoinen, mitkä ehdot rekisteröidyn suostumuksen on täytettävä, on seuraava askel varmistaa, että rekisteröidyltä muistetaan *aina* pyytää suostumus. Kuten tutkielmassa on nimittäin aiemmin tuotu ilmi, on esimerkiksi suosittelupuheluiden teko ilman työnhakijan suostumusta yksi merkittävistä rekrytointiprosessin aikaisista tietosuojariskeistä[227]. Siksi ei riitä, että rekrytoiva yritys tietää, mitä lainmukainen suostumus henkilötietojen käsittelystä tarkoittaa. Tätä suostumusta on nimittäin aina myös muistettava pyytää rekisteröidyltä – myös suosittelupuheluiden yhteydessä.

---

[223] TSA 7 artikla kohta 1. Myös tässä tietosuoja-asetuksen vaatimuksessa näkyy osoitusvelvollisuuden ydinvaatimuksen toteutuminen sekä tietosuojalainsäädännön tiukentuminen: jotta henkilötietojen käsittely on lainmukaista, ei tietosuojalainsäädännön noudattaminen riitä, vaan se tulee myös kyetä todistamaan.
[224] Korpisaari ja muut, 2022, s.146. Tietosuoja-asetuksen mukaan suostumusta ei myöskään pitäisi voida antaa pelkällä vaikenemisella tai jättämällä jokin toimi tekemättä, katso TSA johdanto kohta 32.
[225] Mikäli rekrytoijan ja työnhakijan välinen keskustelu olisi esimerkiksi pelkästään LinkedIn -sivuston yksityisviesteissä, lähtisivät nämä tiedot rekrytoijan mukana, mikäli hän lähtisi organisaatiosta.
[226] Käsittelen tätä tietosuojariskien hallintakeinoa tarkemmin tutkielman sivulla 82.
[227] Toinen kohta rekrytointiprosessia, jossa työnhakijan suostumus jää toisinaan pyytämättä on internet haun teko työnhakijan nimellä, katso tarkemmin tutkielman sivuilta 50–51.

Kokonaisuudessaan voidaan todeta, että asianmukaisesti hankittu rekisteröidyn suostumus laskee rekrytoinnin tietosuojariskejä huomattavasti, sillä tällöin laskevat sekä riski puutteellisesta suostumuksesta että riski osoitusvelvollisuuden laiminlyönnistä. Asianmukaisesti hankittu suostumus henkilötietojen käsittelystä lisää myös läpinäkyvyyden sekä luottamuksellisuuden ja eheyden tietosuojaperiaatteiden toteutumista.

5.4 Henkilötietojen johdonmukainen minimointi

Kolmas tapa hallita rekrytointiprosessin tietosuojariskejä liittyy henkilötietojen *johdonmukaiseen* minimointiin. Tutkielmassa tällä tarkoitetaan sitä, että huomio tulee keskittää henkilötietojen keräyksen *oikea-aikaisuuteen*, *tarpeellisuuteen* sekä *jakamiseen*. Käsittelen seuraavissa kappaleissa tarkemmin, mitä tarkoitan näillä kolmella termillä. Tämä tapa hallita tietosuojariskejä juontaa juurensa tietosuoja-asetuksen periaatteeseen henkilötietojen minimoinnista[228].

Henkilötietojen keräyksen *oikea-aikaisuus* ja *tarpeellisuus* viittaavat siihen, että rekrytoivan yrityksen tulisi huomioida, *mitä* henkilötietoja se tarvitsee ja *missä vaiheessa* rekrytointia mikäkin henkilötieto on tarpeellinen. Täten rekrytoivan yrityksen tulisi osata kyseenalaistaa tottumuksiaan työnhakijan arviointikriteereihin liittyen. Rekrytointitiimin olisi hyvä esittää itselleen kysymys, mitä henkilötietoja rekrytoinnin läpivientiin todellisuudessa tarvitaan, ja mitä henkilötietoja työnhakijasta kysytään pelkästä tottumuksesta. Lisäksi tutkielmassa on jo aiemmin tuotu ilmi, että esimerkiksi työnhakijan pankki- ja verotiedot eivät ole tarpeellisia vielä valintapäätöksen yhteydessä[229]. Toisaalta tietojen oikea-aikaista keräystä olisi tarkasteltava myös vastakkaisesta näkökulmasta: esimerkiksi työnhakijan palkkatoive kysytään toisinaan vasta haastattelutilanteessa. Mikäli palkkatoive ei kohtaa työnantajan tarpeiden kanssa, on prosessissa tuhlattu aikaa. Siksi

[228] TSA johdanto kohta 78 sekä 5 artikla.
[229] HE 75/2000, s.16. Työnhakijan pankkitietoja voitaisiin pitää tarpeenmukaisina vasta rekrytointiprosessin sopimusvaiheessa.

esimerkiksi palkkatoive olisi tarpeenmukaista selvittää jo rekrytoinnin alkuvaiheessa[230]. Henkilötietojen tarpeellisuuden näkökulmasta koulutuksen ja työtaustan välttämättömyyttä rekrytointivalinnan tekoon olisi hyvä myös osata kyseenalaistaa. Koulutus- ja työtausta ovat nimittäin henkilötietoja, joita kysytään lähtökohtaisesti aina rekrytointiprosessien yhteydessä. Tutkielman haastatteluissa nousi esiin kritiikkiä sisältäviä näkökulmia näiden henkilötietojen välttämättömyyteen liittyen:

> *''Koulutuksen ja työkokemuksen tarpeenmukasuuden rekrytoinnin onnistumisen näkökulmasta voisin kyllä kiistää vahvastikin. Kokemusvuodet ei nimittäin edusta työmenestystä. Koulutus ja osaaminen on oikeesti välillä ihan tosi huonoja seulantatietoja rekryvalinnan tekoon. Etenki jos niiden voimaan luotetaan liikaa.''*
>
> *-Haastateltava 9*

Työ- ja opiskelutaustan lisäksi myös työnhakijan nimen tarpeellisuutta rekrytointiprosessin alkuvaiheessa tulisi tarkastella kriittisesti:

> *''Kyllähän oikeastaan sen hakijan nimenkin voi kyseenalaistaa, että onko se tieto välttämätön. Sen vois kyllä kerätä myös vasta työsopimusvaiheessa, jolloin siinä shortlistausvaiheessa rekrytointiin osallistuvat ei vois vahingossakaan kahvipöydässä puhua, et hei naapurin Minttu haki meille töihin.''*
>
> *-Haastateltava 2*

Edellisten esimerkkien avulla voimme havaita, ettei rekrytointiprosessissa tulisi välttämättä kerätä kaikkia henkilötietoja, joita rekrytointien yhteydessä on totuttu tiedustelemaan. Yksi haastateltavista nosti esille, kuinka rekrytointiprosessissa on mahdollista vähentää kerättävien henkilötietojen määrää laskematta valintapäätöksen arvoa. Esimerkiksi anonyymia rekrytointia[231] voisi hyödyntää prosessin läpiviennissä:

> *''Meillä on ollu käytössä myös rekryprosesseja, joissa hakijan nimi, syntymäaika, yhteystiedot, sukupuoli, äidinkieli, … opintojen sekä työkokemuksen ajankohdat ja oppilaitosten nimet on piilotettu rekryn alkuvaiheessa. Eli käytännössä rekryn alussa sulla on päätöksen tueks käytettävissä hakijan työkokemus ja opintojen tausta, mut sä et saa käyttöös*

---

[230] Palkkatoiveen osalta rekrytoivan yrityksen on hyvä huomioida, että palkkahaitarin luominen ja sen viestiminen työnhakijoille on kannattavaa: se voi herättää kiinnostuksen potentiaalisissa työnhakijoissa ja toimii täten myös kilpailutekijänä, ks. esim. Berthon, Ewing & Hah, 2005. Lisäksi EU:ssa hyväksytty palkka-avoimuusdirektiivi tuo asiaan uudistusta, sillä vuonna 2026 voimaan tuleva direktiivi tulee velvoittamaan rekrytoivia yrityksiä kertomaan palkkatiedot työnhakijalle palkkaneuvotteluja varten, Elinkeinoelämän keskusliitto, 2023.

[231] Anonyymi rekrytointi on menetelmä, jossa työnhakijan hakemuksesta poistetaan henkilötietoja, kuten ikä, nimi, yhteystiedot, sukupuoli, kuva, syntymäpaikka, äidinkieli, kansalaisuus ja siviilisääty. Tämän tyyppisen rekrytoinnin on nähty lisäävään todennäköisyyttä sille, että työhön valitaan tuottavimmat työntekijät, katso lisää Rinne, 2018, s.2 ja Kanninen & Virkola, 2021, s.23.

> *esimerkiks just oppilaitoksen nimeä, koska siitä sä pystysit päätteleen iän. Sitten, jos rekrytiimi päättää ottaa sen hakijan haastatteluun, niin tarkat henkilötiedot – kuten nimi ja yhteystiedot – tulee esille, samoin ku CV tulee vasta tässä vaiheessa näkyville rekryävälle tiimille. Tätä kautta varmistetaan yhdenvertasuutta, mutta samalla myös ei käsitellä tarpeettomia henkilötietoja turhan aikasin sitä prosessia. Ja ollaan saatu tätä kautta töihin aivan yhtä pätevää ja osaavaa porukkaa kuin normirekryillä.''*
>
> *-Haastateltava 10*

Henkilötietojen *jakamisen* johdonmukaisella minimoinnilla tarkoitetaan tässä tutkielmassa puolestaan sitä, ketkä saavat tietoonsa työnhakijan henkilötietoja. Rekrytoivan yrityksen on hyvä luoda selkeät raamit esimerkiksi sille, millä perusteella rekrytointitiimi luodaan, ja kenen on tarpeenmukaista olla osa tätä tiimiä[232]. Lisäksi mikäli yritys ei esimerkiksi hyödynnä anonyymiä rekrytointia, voi huomion keskittää siihen, kuinka moni rekrytointitiimistä saa prosessin alkuvaiheessa tietoon kaikki työnhakijan henkilötiedot:

> *''Oon tullu siihen tulokseen, et sehän riittäis, et nimi ja yhteystiedot näkyis vaan yhelle rekrytointia hoitavalle henkilölle. Mut tällä hetkellä ainakin meillä hakijan kaikki tiedot on rekrytointijärjestelmässä samassa paikassa ja näkyvissä kaikille rekrytointiin osallistuville.''*
>
> *-Haastateltava 3*

Henkilötietojen johdonmukaisella minimoinnilla tiedon määrää ja jakamista pyritään vähentämään, sekä tiedon keräyksen ajankohtaa täsmentämään *johdonmukaisesti* rekrytointiprosessin tarpeiden mukaan[233]. Henkilötietojen johdonmukaisella minimoinnilla voidaan saavuttaa seuraavia hyötyjä: riskit henkilötietojen liiallisesta keräyksestä ja henkilötietojen poistamattomuudesta laskevat. Lisäksi riski henkilötietojen liiallisesta jakamisesta voi laskea ja tietosuojaselosteen laadinta helpottua[234]. Myös tietosuojaperiaatteet – kuten henkilötietojen minimointi ja käyttötarkoitussidonnaisuus – voivat näin toteutua rekrytoinnin yhteydessä tehokkaammin. Tiivistetysti henkilötietojen johdonmukainen minimointi voi vähentää tietosuojariskejä kokonaisvaltaisesti.

---

[232] Kun tiimiläinen otetaan mukaan rekrytointiin, on hyvä tehdä erillinen salassapitosopimus tai sopia muilla tavoin siitä, ettei työnhakijan henkilötietoja saa jakaa eteenpäin. Tämä siksi, että tiimiläiselle rekrytointiin osallistuminen voi olla harvinaista, eikä hän välttämättä tiedä kuinka toimia lain sallimissa rajoissa.
[233] Henkilötietojen johdonmukainen minimointi ei täten tarkoita, että tietosuojalainsäädännön vaatimusten valossa parhaiten toimisivat ne organisaatiot, jotka keräävät työnhakijoistaan vähiten henkilötietoja.
[234] Jotta yritys voi minimoida työnhakijoiden henkilötietojen käsittelyä, on sen käytävä läpi rekrytointiprosessiensa toimintatapoja. Kun toimintatavat ovat tiedossa, on tietosuojaselosteen laadinta helpompaa.

5.5 Ulkoinen valvonta: auditoinneilla tietosuojariskit näkyviksi

Neljäs tapa hallita rekrytointiprosessin tietosuojariskejä on hyödyntää riskienhallinnassa ulkoisia auditointeja. Auditointi[235] on tapahtuma, jossa organisaation toimintatapoja tai prosesseja arvioidaan ennalta asetetun kriteeristön mukaisesti ja sen avulla pyritään varmistamaan määräysten mukaisia vaatimuksia. Luonteeltaan auditoinnit voivat olla joko sisäisiä tai ulkoisia, mutta ulkoisten auditointien etuna on puolueettomuus ja luvattu asiantuntijuus.[236] Auditointi voi koostua esimerkiksi henkilöstön haastatteluista, dokumenttien katselmoinnista sekä järjestelmien arvioinneista. Auditoinnin aikana kaikki havainnot dokumentoidaan ja auditoinnin päättyessä yritykselle laaditaan raportti, josta käy ilmi auditoinnin aikana mahdollisesti havaitut puutteet ja ongelmakohdat.[237] Rekrytointiprosessiin kohdistuvassa tietosuoja-auditoinnissa rekrytoinnin aikaisia työvaiheita tarkastellaan tietosuojalainsäädännön näkökulmasta ja esiin nostetaan toimintatapoja tai työvaiheita, jotka aiheuttavat tai ovat alttiita aiheuttamaan tietosuojariskejä.

Tietosuojariskien hallinnan yhteydessä tulisi suosia ulkoisia auditointeja nimenomaan sen vuoksi, että asiantuntevan kumppanin avulla rekrytoiva yritys voi tunnistaa omien rekrytointiprosessiensa tietosuojariskejä tehokkaammin:

> *''Meillä on käytössä ulkoiset auditoinnit ja se on musta hyvä menetelmä siinä mielessä, että sieltä saadaan evidenssiä eli todistusaineistoa siitä, että miten me todellisuudessa oikein toimitaan. Ja sen evidenssin kautta näytetään meijän toimintatapaa. Tällöin tunnistetaan paremmin, mitä riskejä meijän toimintatavoissa on. Minusta ne [auditoinnit] on erittäin hyviä, koska yritys helposti tottuu tiettyihin toimintatapoihin, eikä itse enää tunnista mahdollisia riskikohtia. Et ne auditoinnit aina vähän skarppaa sitä omaa toimintaa.''*
>
> *-Haastateltava 8*

Kuten edellä kuvatusta haastattelusta voimme havaita, voidaan ulkoisilla auditoinneilla saavuttaa tietosuojariskien hallinnassa useita hyötyjä. Ensinnäkin, rekrytoivat organisaatiot voivat näin paremmin tunnistaa, mitkä toiminnot rekrytoinnin yhteydessä ovat

---

[235] Auditointi on luonteeltaan riippumaton, järjestelmällinen ja dokumentoitu prosessi, jossa määritetään objektiivisesti sovittujen auditointikriteerien täyttyminen, ks. esim. Halpert, 2011. Rekrytointiprosessin tietosuojariskien osalta tietosuojalainsäädäntö muodostaa pohjan sille, millaisiin vaatimuksiin rekrytointiprosessin tulee auditoinnin yhteydessä päästä.

[236] Jackson, 2010; Lecklin, 2006, s.72–73; Pesonen, 2007, s.190–192.

[237] Kansallinen turvallisuusviranomainen, 2020, s.109–111.

erityisen alttiita tietosuojariskien syntymisen kannalta[238]. Täten yrityksellä on paremmat mahdollisuudet saada rekrytointiprosessin tietosuojariskit näkyviksi ja hallintaan. Toisaalta rekrytoiva organisaatio voi myös saada ulkoisesta auditoinnista varmuutta omaan toimintaansa: mikäli yritys nimittäin jo hyödyntää toiminnassaan tietosuojariskejä laskevia työtapoja, voidaan tällaisten toimintatapojen käyttöä lisätä.

Tietosuojaoikeudellisesta näkökulmasta ulkoisten auditointien hyödyntäminen tietosuojariskien hallinnassa voi olla hyödyllistä, mikäli seuraavaksi luetellut ehdot täyttyvät. Ensinnäkin, auditointia tarjoavan tahon tulisi hallita tietosuojalainsäädännön vaatimukset. Toiseksi, auditoinnin tulisi kattaa koko rekrytointiprosessi ja sen kaikki työvaiheet, jotta rekrytoivan organisaation tietosuojariskit ilmenevät. Tällä tarkoitan sitä, ettei auditointi saa olla liian pintapuolinen: auditointia tekevän tahon tulisi esimerkiksi hahmottaa yrityksen sisäisiä henkilökemioita ja byrokraattisia valtasuhteita, jotka voivat esimerkiksi vaikuttaa siihen, toimivatko kaikki rekrytoivan tiimin jäsenet organisaation asettamien sääntöjen ja kehotusten mukaisesti. Lisäksi auditoivan tahon tulisi päästä arvioimaan yrityksen toiminnan todellista tilaa, eikä vain sitä mielikuvaa, jota rekrytoiva organisaatio saattaa pyrkiä luomaan ulkoista auditointia tekevälle taholle.

Asianmukaisesti suoritettu ulkoinen auditointi tukee rekrytointiprosessin tietosuojariskien hallintaa moninaisesti. Kuten mainittua, auditoinnilla voidaan nimittäin paljastaa rekrytointiprosessin tietosuojaoikeudellisia ongelmakohtia. Näihin ongelmakohtiin puuttuminen kehittää puolestaan riskienhallintaa, sillä etenkin tietosuojaperiaatteet eheydestä ja luottamuksesta, sekä lainmukaisuudesta ja kohtuullisuudesta voivat toteutua rekrytointiprosessin aikana paremmin. Lisäksi rekisteröidyn oikeudet voivat toteutua tehokkaammin. Mikäli rekrytoivassa yrityksessä esimerkiksi havaitaan ongelmia henkilötietojen poistamisessa, voidaan tietojen poistoon luoda selkeät toimintatavat, jolloin rekisteröidyn oikeus henkilötietojen poistamisesta toteutuu todennäköisemmin.

[238] Vacca (2009, s.40) tuo esille, kuinka auditoinneilla voidaan havaita järjestelmissä olevia puutteita ja haavoittuvuuksia. Lisäksi auditoinnit voivat paljastaa tietoturvallisuuteen liittyviä kehitystarpeita, jolloin yritys voi parantaa tietoturvallisuuden tasoaan.

5.6 Sisäinen valvonta: prosessikuvaukset, vastuunjako ja rutiinit

Ulkoisen auditoinnin ohella rekrytointiprosessin tietosuojariskejä tulisi hallita myös sisäisen valvonnan keinoin. Tutkielmassa sisäisellä valvonnalla tarkoitetaan kaikkia niitä toimenpiteitä, joita rekrytoiva organisaatio voi tehdä oman henkilöstön voimin tietosuojariskien minimoimiseksi[239]. Kuten Ratsula painottaa, toimii sisäinen valvonta parhaiten, kun se on rakennettu osaksi liiketoimintaprosesseja[240]. Siksi myös tietosuojariskien kannalta tehokkainta on varmistaa, että tietosuojaa koskeva riskienhallinta otetaan osaksi yrityksen strategiaa, eikä sitä eriytetä kokonaan omaksi valvonnaksi. Huomionarvoista on edelleen, ettei sisäisen valvonnan ensisijainen tehtävä ole ongelmakohtien löytäminen, vaan pikemminkin tavoitteisiin pääsyn tukeminen[241]. Siksi sisäinen valvonta tukee ulkoista auditointia: ulkoisella auditoinnilla tietosuojariskit saadaan näkyviksi ja sisäisen valvonnan keinoin havaitut ongelmakohdat pyritään saamaan hallintaan.

Esittelen seuraavaksi kolme sisäisen valvonnan keinoa, joissa rekrytointiprosessin tietosuojariskien hallinta tapahtuu osana liiketoimintaprosessia. Nämä toimintakeinot ovat kattavat prosessikuvaukset, työtehtävien selkeä vastuunjako, sekä rutiinien luominen. Lähdetään liikkeelle rekrytointiprosessin prosessikuvauksesta. Tutkielmassa prosessikuvauksella tarkoitetaan prosessin peräkkäisten työvaiheiden kuvaamista graafisesti ja/tai sanallisesti, jolloin ymmärrys organisaation tavasta rekrytoida selkiytyy[242]. Tutkielman

---

[239] Sisäinen valvonta (*internal control*) muodostuu organisaation eri tasoille rakennetuista toimenpiteistä, joiden tavoite on kolmijakoinen: toiminnalliset tavoitteet, raportoinnin tavoitteet ja vaatimustenmukaisuuden tavoitteet. Sisäisellä valvonnalla pyritään siis varmistaa toiminnan laillisuus ja tuloksellisuus, katso lisää esimerkiksi Ratsula, 2016b, s.13–18; Ahokas, 2012, s.11–12; COSO, 2017. Koska sisäiselle valvonnalle ei ole olemassa kaiken kattavaa määritelmää, on sisäisellä valvonnalla toisinaan viitattu myös strategiseen valvontaan ja johdon valvontaan. Lisäksi sisäisellä valvonnalla on viitattu myös ulkoiseen tarkastukseen, ks. esim. Pfister, 2009, s.15 ja Maijoor, 2000. Yksi tunnetuimmista ja yleisesti käytössä olevista sisäisen valvonnan malleista on nimeltään COSO-malli. Sen kehittäjänä on toiminut yhdysvaltalainen organisaatio: The Committee of Sponsoring Organizations of the Tradeway Commission.

[240] Ratsula, 2016b, s.18.

[241] COSO, 2017; Ratsula, 2016b, s.248.

[242] Prosessiajattelun perusideana on, että prosessi koostuu peräkkäisten toimintojen ketjusta. Rekrytointiprosessin peräkkäiset toiminnot on jaettu neljään päävaiheeseen, jotka ovat rekrytoinnin suunnittelu, hakijahankinta, hakijavalinta sekä rekrytointivalinta ja perehdytyksen aloitus. Nämä rekrytoinnin päävaiheet ja niiden sisällä olevat työtehtävät on esitetty tarkemmin tutkielman sivulla 20.

haastatteluissa korostui prosessien avaamisen ja kirjaamisen keskeisyys osana tietosuojariskien hallintaa:

> *''Rekrytointiprosesssin tulis olla kuvattu niin, että kaikkien roolit on selvät ja rekrytiimin työntekijät tietää, mitä tietoja prosessin aikana liikkuu ja miten niitä tietoja tulee käsitellä. Tän pitää olla kristallinkirkasta kaikille. Tätä kautta riskikohtia on vähempi, koska osataan olettaa, että mitä seuraavaks tapahtuu.''*
>
> *-Haastateltava 6*

Kuten oheisesta esimerkistä käy ilmi, voidaan selkeillä prosessikuvauksilla saavuttaa tilanne, jossa tietosuojariskejä syntyy vähemmän yksinkertaisesti siitä syystä, että rekrytoivan tiimin jäsenet tietävät, mitä rekrytointiprosessin aikana tehdään ja missä vaiheessa. Tällöin tiimin jäsenet osaavat kyseenalaistaa rekrytointiprosessin toimia, mikäli jokin työtehtävä ei tule tehdyksi tai sen suorittaminen ei tapahdu prosessikuvauksen mukaisesti. Pelkät prosessikuvaukset eivät kuitenkaan riitä: lisäksi selvää tulee olla se, kenen vastuulla mikäkin työtehtävä on. Työtehtävien vastuuttaminen nimittäin lisää hallinnantunnetta ja saattaa saada työntekijät huomaamaan tietosuojariskejä tehokkaammin:

> *''Sen lisäks, että kaikkien pitää tietää, mitä rekryn aikana tapahtuu, tulee ne työtehtävät myös vastuuttaa. Eli jokaisen tulee tietää, missä se oma tontti on ja mitä omalla vastuulla oikein on. Tätä kautta osataan sit olla hereillä, jos tiimikaveri ei hoida omia tehtäviään ja toisaalta kans vältetään tuplatekeminen, eli et työkaveri alkais tehä samaa työtehtävää, ku mitä ite on tekemässä. Tietosuojariskeihin tää vaikuttaa myös, nimittäin, jos työkaveri ei sit hoida niitä omia hommiaan, ni tästä voidaan kertoa muulle tiimille ja sitä kautta välttää mahollinen tietosuojariski, ennenku se kerkee sit tapahtua.''*
>
> *-Haastateltava 6*

Prosessikuvausten ja työtehtävien vastuuttamisen ohella myös rutiinien luominen on osa sisäisen valvonnan keinoa hallita rekrytointiprosessin tietosuojariskejä. Rutiineja voidaan luoda esimerkiksi siihen, miten työnhakijalta varmistetaan suorahaun yhteydessä asianmukainen suostumus henkilötietojen käsittelyyn tai kuinka suorahaussa voidaan välttää virheellisten kirjausten teko. Lisäksi rutiineja olisi hyvä luoda siitä, millä tavoin rekrytoivan tiimin tulee dokumentoida rekrytoinnin vaiheita. Kokonaisuudessaan onnistunut sisäinen valvonta parantaa tietosuojariskien hallintaa, sillä rekrytoiva yritys voi näin täyttää paremmin esimerkiksi läpinäkyvyyden tietosuojaperiaatetta sekä osoitusvelvollisuuden vaatimusta. Tämän ohella, sisäinen valvonta voi ikään kuin jatkaa ulkoisen auditoinnin työtä ja saattaa käytäntöön niitä kehitysehdotuksia, joita ulkoisen

auditoinnin raportointi on tuonut ilmi. Parhaimmillaan sisäisen valvonnan ja ulkoisen auditoinnin yhteistyö tekee tietosuojariskien hallinnasta jatkuvaa ja dynaamista.

5.7 Tietosuojakoulutus ja läheltä piti -tilanteiden läpikäynti

Kuudes tapa hallita rekrytointiprosessin tietosuojariskejä liittyy henkilöstön kouluttamiseen. Tässä tutkielmassa tietosuojakoulutuksella tarkoitetaan kaikkia niitä toimenpiteitä, joilla rekrytoiva organisaatio voi kehittää henkilöstönsä tietosuojaosaamista. Tällaisia toimenpiteitä voivat olla esimerkiksi sisäisen tai ulkoisen puhujan pitämät esitykset tai vuorovaikutteiset tehtävät tietosuojaan liittyen. Jotta tietosuojakoulutus tulee varmasti pidettyä, on henkilöstön tietosuojakoulutustarpeet hyvä kirjata ylös. Yksi tapa varmistaa tietosuojakoulutuksen suunnittelu ja läpivienti on kirjata tietosuojaoikeudellisen koulutuksen tarpeet työyhteisön kehittämissuunnitelmaan[243].

Myös tutkielman haastatteluissa korostui näkemys siitä, että tietoisuuden lisääminen tietosuojalainsäädännön vaatimuksia kohtaan liittyy olennaisesti tietosuojariskien hallintaan. Haastateltavat kaipasivat nimenomaan rekrytoivan tiimin tietosuojaoikeudellisen tietoisuuden kehittämistä ja tasaista muistutusta tietosuojahaasteiden olemassaolosta:

> *''Rekrytointikoulutukset – me pidetään niitä kaikille niille, jotka on osa rekrytointitiimiä. Niin me pidetään kerran vuoteen tai kahteen koulutus. Siellä käydään läpi, et hei tällä tavalla meidän firmassa rekrytoidaan ja prosessi menee näin – jotta kaikki tietää, että aa niin meillä on kaks haastattelukierrosta ja sen jälkeen tehdään ehkä työpaikkatarjous tai soitellaan suosittelijat ja muuta. Tätä kautta kukaan ei lähde sooloilemaan jotain omaa. Sit niis koulutuksissa kerrotaan, et älkää kysykö näitä ja näitä tietoja ja älkää soitelko kaverille siitä hakijasta. Ja jos joku tulee teijän luo ja kertoo halusta hakee sitä paikkaa, niin pyydetään et ne hakee järjestelmän kautta. Et kouluttamalla voidaan hallita niitä riskejä.''*
>
> *-Haastateltava 7*

Tietosuojakoulutuksissa keskeistä on, että ne on suunniteltu organisaation tarpeita vastaaviksi. Rekrytoivalta tiimiltä voidaan esimerkiksi koulutusta suunniteltaessa kysyä, millaisiin tietosuojaoikeudellisiin haasteisiin he kaipaisivat apua tai mitä tietosuojariskejä he

[243] Työyhteisön kehittämissuunnitelma on dokumentti, joka jokaisen työnantajan tulisia laatia, mikäli organisaatiossa työsuhteessa olevien työntekijöiden lukumäärä on säännöllisesti vähintään 20, ks. lisää vuoden 2022 alussa uudistuneesta yhteistoimintalaista, etenkin 2 luku 9§.

ovat itse havainneet rekrytointiprosessin yhteydessä. Näiden tietojen pohjalta, sekä yrityksen toimintatavat ja -ympäristö huomioiden tietosuojakoulutuksesta voidaan saada enemmän irti. Jokaisen rekrytoivan yrityksen olisi kuitenkin hyvä käydä tietosuojakoulutuksissa läpi vähintään seuraavat asiat: mitä henkilötietoja työnhakijasta ei lähtökohtaisesti saa selvittää, miten työnhakijan henkilötiedot selvitetään asianmukaisesti, miten työnhakijan suostumus hänen henkilötietojensa käsittelystä tulee saada, kuinka paljon ja miten työnhakijaa tulee informoida hänen oikeuksistaan, mitä tietosuojariskejä kyseisen yrityksen rekrytointiprosessit voivat sisältää, sekä miten näitä tietosuojariskejä on organisaatiossa pyritty hallitsemaan. Myös rekrytoinnissa hyödynnettävien työkalujen – kuten rekrytointijärjestelmän – käytöstä on hyvä kerrata ohjeet. Tämän ohella rekrytoivaa tiimiä on hyvä kouluttaa siitä, mistä rekrytointiprosessit lähtökohtaisesti koostuvat kyseisessä organisaatiossa sekä mitä työvaiheita yrityksen rekrytointiprosessit yleensä sisältävät.[244] Lisäksi tietosuojakoulutuksessa olisi hyvä käydä läpi tietosuojavastaavan velvollisuuksia sekä tehtäviä[245]. Osana tietosuojakoulutusta rekrytoiva organisaatio voisi myös käydä läpi niin kutsuttuja läheltä piti -tilanteita:

> *''Ei olis yhtään huono juttu käydä nimettömästi läpi sellasia läheltä piti -tilanteita. Et ku jossain on melkeen sössitty, ni mitä siitä voitas kaikki oppia, ettei sellasta tapahdu toiste.''*
> *-Haastateltava 10*

Oheisen esimerkin mukaisesti läheltä piti -tilanteiden läpikännillä tutkielmassa tarkoitetaan sitä, että organisaatio kouluttaa rekrytoivaa henkilöstöään siitä, millaisia tietosuojaoikeudellisia riskitilanteita kyseisen yrityksen toimintaympäristössä on ilmennyt rekrytointiprosessien aikana. Lisäksi olennaista olisi, että koulutuksissa esitettäisiin tai löydettäisiin yhdessä keinoja näiden tietosuojariskien hallintaan. Tietosuojariskien hallinnan

---

[244] Tämä listaus perustuu tämän tutkielman löytämiin tietosuojariskeihin, sekä tietosuoja-asetuksen tulkinnan kautta löydettyihin asetuksen keskeisimpiin tavoitteisiin.

[245] TSA:n 37 artikla on määritellyt tilanteet, joissa yrityksen on nimettävä tietosuojavastaava. Asetuksen mukaan tietosuojavastaava on nimitettävä, kun yrityksen *ydintehtävät* muodostuvat henkilötietojen käsittelytoimista, jotka edellyttävät rekisteröityjen säännöllistä ja järjestelmällistä seurantaa, ks. TSA 37 artikla kohta 1b. Mitä yrityksen *ydintehtävillä* sitten tarkoitetaan? Mikäli yrityksen henkilötietojen käsittelytoiminnot ovat kaikille organisaatioille yleisesti yhteisiä, ei tietosuojavastaavan nimittämistä voitaisi katsoa pakolliseksi, esimerkkinä palkanmaksun yhteydessä tapahtuva henkilötietojen käsittely, ks. Korpisaari ja muut, 2022, s.424–425. Voitaisiinkin katsoa, että pelkkä rekrytointiprosessin aikainen henkilötietojen käsittely ei vielä edellytä tietosuojavastaavan nimittämistä, sillä lähes kaikki yritykset tekevät rekrytointia. Mikäli rekrytointia puolestaan tehdään laskutettavana palveluna asiakasorganisaatiolle, on henkilötietojen käsittely osa yrityksen *ydintehtäviä*, jolloin tietosuojavastaavan nimitys voitaisiin jo katsoa pakolliseksi.

kannalta tietosuojakoulutukset voivat auttaa rekrytoivaa yritystä moninaisesti: esimerkiksi riskit henkilötietojen tarpeettomasta jakamisesta, tietojen poistamattomuudesta sekä puutteellisesta suostumuksesta voivat laskea rekrytoivan tiimin osaamisen kasvaessa[246]. Täten myös yleiset tietosuojaperiaatteet, kuten henkilötietojen minimointi, tarpeellisuusvaatimus sekä osoitusvelvollisuus voivat toteutua rekrytointiprosessin aikana tehokkaammin[247].

5.8 Rekrytointijärjestelmä inhimillisen työn tueksi

Rekrytointijärjestelmän käyttöönotto on seitsemäs tutkielmassa esiteltävä riskienhallintakeino. Rekrytointijärjestelmä on nostettu tutkielmassa yhdeksi keskeiseksi rekrytointiprosessin tietosuojariskien hallintakeinoksi, sillä esimerkiksi Tietosuojavaltuutetun ja Tieke Ry:n vuoden 2021 teettämän kyselyn pohjalta tietosuoja-asetuksen vaatimukset on sisäistetty kaikista heikoiten pienissä ja keskisuurissa yrityksissä[248]. Pienet ja keskisuuret yritykset ovat lisäksi juuri niitä yrityksiä, joissa ei usein ole käytössä rekrytointijärjestelmää[249]. Käynkin seuraavaksi läpi, mitä hyötyjä rekrytointijärjestelmästä on rekrytointiprosessin tietosuojariskien hallinnan näkökulmasta.

Lähdetään liikkeelle siitä, että rekrytointijärjestelmän avulla työnhakijoiden kaikki henkilötiedot saadaan koottua saman sähköisen järjestelmän piiriin. Täten työnhakijoiden henkilötietoja ei ole useassa järjestelmässä samanaikaisesti. Toisinaan rekrytoivissa yrityksissä työnhakijan henkilötietoja saattaa nimittäin esiintyä esimerkiksi sekä sähköpostiosoitteissa, sisäisissä viestintäkanavissa, kuten Slackissa tai Teamsissa, sekä

---

[246] Tietosuojakoulutuksen avulla esihenkilöt esimerkiksi todennäköisemmin tietävät, ettei työnhakijaa saa googlettaa tai työnhakijasta soittaa suosittelupuheluita ilman työnhakijan nimenomaista suostumusta. Lisäksi riski tietojen poistamattomuudesta voi laskea tietosuojakoulutusten avulla, sillä tällöin rekrytoivat työntekijät ovat tietoisia siitä, milloin työnhakijoiden henkilötiedot tulisi poistaa.

[247] Koulutuksen avulla rekrytoiva henkilöstö on tietoisempi siitä, mitä työnhakijalta saa esimerkiksi kysyä työhaastattelun aikana. Tämä sekä minimoi henkilötietoja että varmistaa sen, ettei työnhakijasta kerätä rekrytointiprosessin kannalta tarpeettomia henkilötietoja.

[248] Katso tarkemmin, Edilex, 2021. Tietosuojavaltuutetun toimiston ja Tieke Ry:n (Tietoyhteiskunnan kehittämiskeskus) toteuttamassa verkkokyselyssä vastaajina oli noin 350 yritystä.

[249] Syyt rekrytointijärjestelmän puuttumisesta voivat liittyä esimerkiksi järjestelmän kustannuksiin, tietosuojaosaamisen puuttumiseen tai yrityksen pieneen rekrytointivolyymiin.

tulostettuina papereina. Sen lisäksi, että työnhakijan henkilötiedot saadaan koottua yhden järjestelmän sisälle, ohjaa järjestelmä parhaimmillaan rekrytoivaa yritystä kohti tietosuojalainsäädännön vaatimuksia:

> *''Sen oon kyllä huomannut, kun oon ite ollu erilaisissa yrityksissä eri järjestelmien kanssa tekemisissä, että kun sulla on hyvä ja luotettava rekrytointijärjestelmä käytössä, niin kyllä se hyvin automaattisesti muokkaa sitä rekryprosessia niin että se on GDPR:n mukanen. Että se on kyllä äärimmäisen tärkeetä, että se rekrytointityökalu on kunnossa. Sillon kyllä ne riskitekijät sillä saralla saadaan hyvin hallintaan.''*
>
> *-Haastateltava 8*

Etenkin pienemmissä yrityksissä tietosuojaosaamista ei lähtökohtaisesti ole riittävästi[250]. Tähän tietosuojaoikeudelliseen ongelmaan rekrytointijärjestelmä voi tarjota apua: rekrytointijärjestelmissä on usein nimittäin valmiiksi luodut pohjat, joihin muokataan asiakasorganisaation toiveiden pohjalta rekrytoinnin eri työvaiheet. Parhaimmillaan järjestelmässä on myös vinkkejä siihen, kuinka toimia tietosuojavaatimusten mukaisesti. Rekrytointijärjestelmissä on esimerkiksi usein mahdollisuus asettaa automaattinen henkilötietojen poisto, jolloin järjestelmä poistaa työnhakijoiden henkilötiedot automaattisesti sille luotujen käskyjen pohjalta. Nämä ominaisuudet voivat muun muassa vähentää henkilötietojen poistamattomuuden tietosuojariskiä, sekä auttaa selkiyttämään rekrytoinnin prosessikuvausta ja työtehtävien vastuunjakoa.

Rekrytoivan yrityksen on hyvä huomioida, että rekrytointijärjestelmän hyötyjen saamiseksi, ei organisaation tarvitse valita markkinoiden kalleinta järjestelmää:

> *''Tietosuojariskejä voidaan hallita sillä, että laitetaan järjestelmät kuntoon. On myös olemassa tosi kevyitä rekrytointijärjestelmiä, niitten ei aina tarvi olla mitään super kalliita ja raskaita toimiakseen. Tällä varmistetaan se, et työhakemuksia ei lähetellä sähköpostilla. Ja sit on niissä rekryjärjestelmissä sekin hyvä puoli, et ne antaa sille hakijalla ammattimaisemman kuvan, et täällä sun tietoja ei käsitellä miten tahansa.''*
>
> *-Haastateltava 7*

Oheisen esimerkin mukaisesti rekrytointijärjestelmä viestii työnhakijalle, että rekrytoiva yritys huomioi tietosuojalainsäädännön vaatimuksia. Tämä voi lisätä rekrytoinnin osapuolten molemminpuolista luottamusta, kun työnhakija varmistuu siitä, että hänen

---

[250] Katso aiheesta lisää, Edilex, 2021.

henkilötietojansa kohdellaan organisaatiossa asianmukaisesti. Tällöin rekrytointiprosessista tulee myös läpinäkyvämpi, mikä jo itsessään lisää yleisten tietosuojaperiaatteiden toteutumista rekrytoinnin yhteydessä. Lisäksi rekrytointijärjestelmä voi vähentää henkilötietojen liiallisen jakamisen riskiä, sillä järjestelmään on usein mahdollista asettaa eri käyttöoikeuksia. Tällöin esimerkiksi HR:n edustajille voidaan asettaa laajemmat oikeudet, jolloin he pääsevät näkemään kaikki organisaatiossa avoinna olevat rekrytoinnit. Esihenkilöille voidaan puolestaan asettaa käyttöoikeus, joka antaa heille mahdollisuuden tarkastella vain oman tiimin rekrytointiprosesseja. Kokonaisuudessaan rekrytointijärjestelmä voi tehdä prosessista selkeämmän ja helposti hallittavamman, jolloin operatiivisten riskitekijöiden määrä voi laskea. Tällöin rekrytointijärjestelmä toimii myös ikään kuin inhimillisen työn tukena. Järjestelmä voi esimerkiksi vähentää inhimillisen muistin varassa olevien työtehtävien määrää, mikä puolestaan vähentää merkittävästi inhimillisistä tekijöistä johtuvia tietosuojariskejä.

5.9 Organisaation arvot ja yrityskulttuuri

Myös organisaation arvot[251] ja yrityskulttuuri[252] vaikuttavat keskeisesti rekrytointiprosessin tietosuojariskien hallinnan mahdollisuuksiin. Organisaation arvot nimittäin ohjaavat – tai niiden tulisi ohjata – esimerkiksi sitä, miten yritys käyttää resurssejaan sekä millaisesta työstä henkilöstöä palkitaan. Näillä tekijöillä on puolestaan vaikutusta siihen, millaisia tietosuojariskejä organisaatiossa ilmenee. Lisäksi organisaation arvot ohjaavat valintoja, joissa päätetään, ketkä yrityksessä etenevät esihenkilöasemaan. Mikäli esihenkilötehtäviin valitaan henkilöitä, joiden kiinnostus tietosuojalainsäädäntöä kohtaan on olematon, on selvää, että tietosuojariskejä esiintyy myös rekrytointien yhteydessä enemmän. Tällöin myös tietosuojakoulutusten pitäminen on lähtökohtaisesti turhaa.

---

[251] Organisaation arvot ovat asioita, joita pidetään tärkeinä ja tavoittelemisen arvoisina. Lisäksi ne määrittelevät, mitkä päämäärät ovat toisia tärkeämpiä. Arvojen on lisäksi nähty peilaavan yrityksen yleistä tahtotilaa: ne eivät ole pelkkiä sanoja, vaan niillä on toimintaa ohjaava vaikutus, ja ne tulevat käyttöön etenkin valintatilanteissa, joissa ei ole muuta selkeää ohjeistusta, ks. esim. Puohiniemi, 2003; Dolan, Garcia & Richley, 2006, s.26.

[252] Yrityskulttuuri on termi, jolla kuvataan organisaation tiedostettuja ja tiedostamattomia arvoja, rakenteita ja toimintatapoja, ja ne ohjaavat työntekijöiden ajattelua ja toimintaa. Lisäksi yrityskulttuuri erottaa yrityksen muista organisaatioista, ks. lisää Luukka, 2019, s.25.

Lisäksi yrityksen resurssien jako vaikuttaa esimerkiksi siihen, hyödynnetäänkö rekrytointien yhteydessä maksullista rekrytointijärjestelmää. Myös tietosuojaa edistävien toimintatapojen omaksuminen voi olla työntekijöiden näkökulmasta mielekkäämpää, mikäli yrityksen palkitsemisjärjestelmä tukee tällaista toimintaa. Arvojen olennaisuus osana tietosuojariskien hallintaa korostui myös haastatteluissa:

> *''Organisaation arvot voi toimintaa ohjatessaan pienentää niitä tietosuojariskejä. Et jos ne arvot hyvin vahvasti näkyy siellä organisaatiossa ja jokapäiväsessä toiminnassa.''*
>
> *-Haastateltava 3*

Lisäksi yrityksen arvot voivat vaikuttaa siihen, onko organisaatioon luotu erillinen HR-yksikkö. Rekrytointiprosessin tietosuojariskien näkökulmasta HR-yksikön olemassaololla voi puolestaan olla ratkaiseva vaikutus:

> *''Toisissa yrityksissä rekrytointai hoitaa ja valvoo semmonen aika asiaan vihkiytynyt HR, jolloin riskit saattaa olla pienemmät, kuin sellasissa yrityksissä, joissa ei oo erillistä HR-ammattilaista hoitamassa rekrytointia. Et kyllä jo se HR:n läsnäolo yleensä tekee prosessista ja käytännöistä selkeemmän.''*
>
> *-Haastateltava 3*

Organisaation yrityskulttuuri voi puolestaan vaikuttaa siihen, kuunnellaanko yrityksessä esiin nostettavia huolenaiheita tietosuojariskeihin liittyen:

> *''Organisaatiokulttuuri vaikuttaa niihin tietosuojariskeihin. Et kun esimerkiks HR kertoo, et mikä on lainmukasta ja hyväntavan mukasta, niin millanen kulttuuri siinä organisaatiossa on ottaa vastaan tällästä palautetta. Et kuunnellaanko sitä ja arvostetaanko sitä. Et jos huomataan, et yrityksessä tehään jotain väärin tietosuoja-asioissa, niin ollaanko halukkaita muuttamaan sitä toimintaa.''*
>
> *-Haastateltava 7*

Tietosuojariskien hallinnan kannalta yrityksen on tiedostettava, millaiset arvot ohjaavat sen toimintaa[253]. Siksi esimerkiksi esihenkilöiden valintakriteerien tulee perustua sille, että rooleihin valittavat henkilöt sitoutuvat noudattamaan voimassa olevia tietosuojasäädöksiä. Lisäksi yrityskulttuurin on tuettava toimintaa, jossa työntekijät voivat aidosti nostaa esille huomaamiaan tietosuojaoikeudellisia ongelmakohtia – ja näihin ongelmakohtiin on yrityksen johdon reagoitava.

---

[253] Kuten Hofstede on asian ilmaissut, tulee organisaation jäsenten noudattaa organisaation arvoja pysyäkseen organisaation jäseninä, ks. lisää Hofstede, 1998, s.483. Tämä tarkoittaa, että yrityksen johdon arvoista tulee väistämättä sen jäsenten toimintatapoja.

5.10 Riskienhallinnan räätälöinti organisaation tarpeita vastaavaksi

Koska organisaatiot ovat sekä ominaisuuksiensa että toimintaympäristöjensä suhteen erilaisia, vaihtelevat myös tietosuojariskien hallintaan tarvittavat keinot yritysten välillä. Lisäksi käytössä olevat resurssit ja niiden oikeaoppinen allokointi ovat avainasemassa sen suhteen, miten yritys onnistuu rekrytointiprosessin tietosuojariskien hallinnassa[254]. Koska tietosuojariskeihin kohdistettavat resurssit ovat liike-elämässä rajalliset, korostuu resurssien tehokas ja oikea-aikainen käyttö. Siksi analysoin seuraavaksi, kuinka organisaatiot voivat räätälöidä tietosuojariskien hallintakeinoja itselleen sopiviksi. Tässä apuna toimii ISO 31000 -standardi[255], jonka oppeja tutkielmassa hyödynnetään etenkin siihen, kuinka organisaatiot voivat *tunnistaa* rekrytointiprosessiensa keskeisiä tietosuojariskejä, *arvioida* niiden todennäköisyyttä, sekä *hallita* niiden ilmenemistiheyttä ja -laajuutta.

ISO 31000 -standardin oppien mukaisesti tietosuojariskien hallinnassa apuna voidaan käyttää niin kutsuttua PDCA-menetelmää[256], jonka mukaan riskienhallinta tulee jakaa neljään vaiheeseen. Nämä vaiheet ovat nimeltään suunnittelu, toimenpiteiden toteutus, arviointi, sekä toiminnan kehitys. Jotta rekrytoiva organisaatio voi varmistaa, että kaikki neljä vaihetta toteutuvat, on ne hyvä rytmittää esimerkiksi vuosikellon mukaisesti, jolloin rekrytointiprosessin tietosuojariskien hallinta lähtee vuoden alussa liikkeelle riskienhallintakeinojen suunnittelusta, ja päättyy vuoden loppupuolella koko prosessin kehittämiseen ennen seuraavaa vuotta. Tällöin joka kvartaalille osuu yksi riskienhallinnan neljästä vaiheesta. Vuosikellomainen ajattelu tietosuojariskien hallinnassa edesauttaa sekä riskienhallinnan jatkuvuutta että resurssien tehokasta käyttöä. Tämä sen vuoksi, että

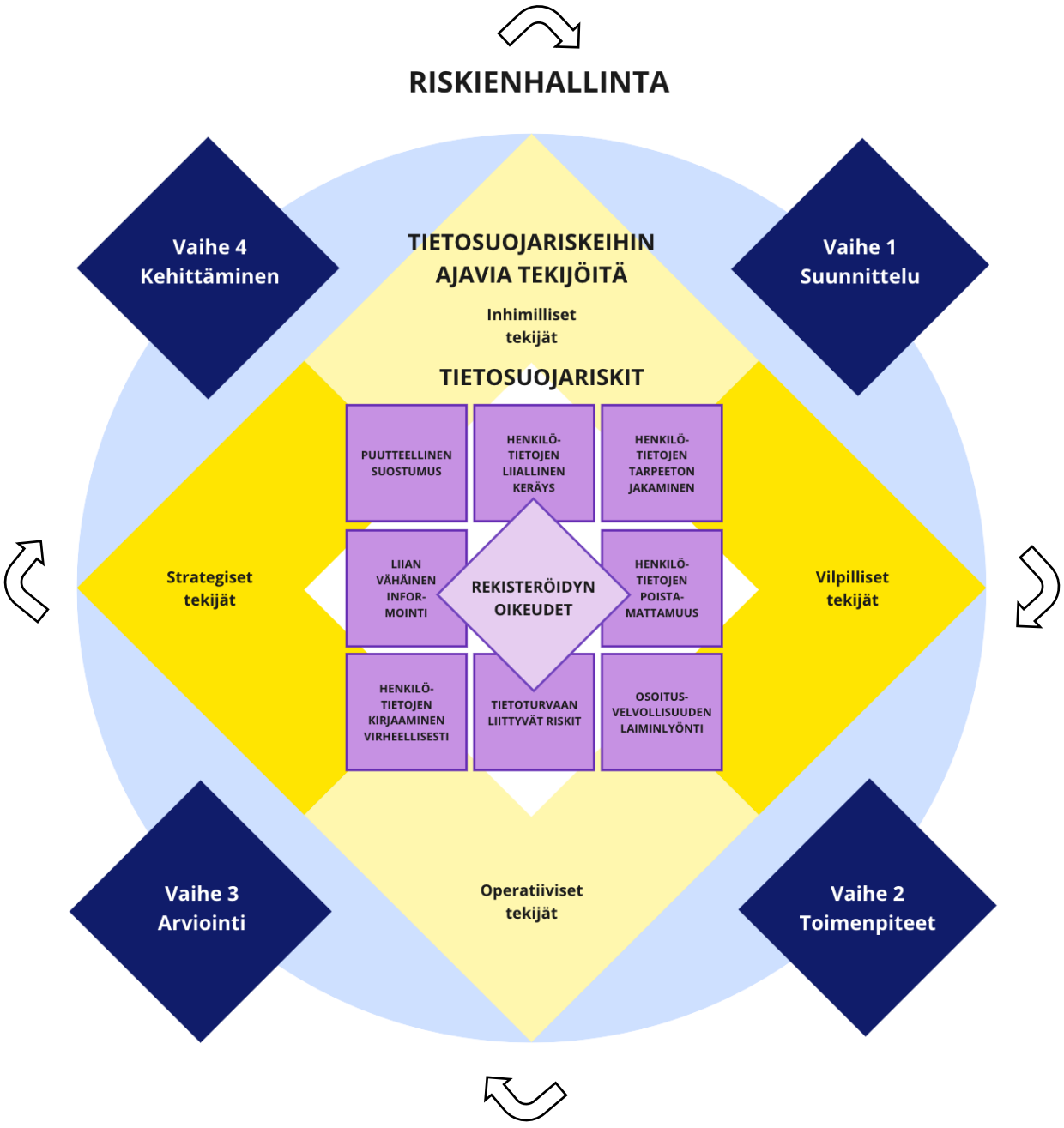
---

[254] Valtiovarainministeriö, 2017, s.14. Organisaation käytössä olevat resurssit vaikuttavat olennaisesti riskienhallinnan onnistumiseen.

[255] ISO 31000 -standardi on kansainvälisen standardointijärjestön (International Organization for Standardization) julkaisema ohje, joka auttaa organisaatioita riskienhallinnan kehittämiseen, Valtiovarainministeriö, 2017, s.12. Kaikki organisaatio voivat hyödyntää ISO 31000 -standardia erityyppisten riskien käsittelyyn: standardi ei siis ole suunnattu pelkästään tietosuojariskien hallintaan. ISO 31000 -standardi ei ole myöskään suunnattu pelkästään riskienhallinnan ammattilaisten käyttöön, vaan sitä voivat hyödyntää kaikki, jotka ovat tehtävissään tekemisissä riskienhallinnan ja siihen liittyvän päätöksenteon kanssa, ks. lisää Standardoinnin keskusjärjestö Suomessa (SFS).

[256] Iivari & Laaksonen, 2009; Valtiovarainministeriö, 2017, s.10. PDCA-menetelmä saa nimensä sanoista plan-do-check-act, eli vapaasti suomennettuna suunnittele-toteuta-arvioi-kehitä.

vuosikellon avulla riskienhallinnan jatkuvuus voidaan varmistaa myös seuraavina vuosina. Samanaikaisesti yrityksellä on myös mahdollisuus hoitaa tietosuojariskien hallintaa keskitetysti vuosikelloajattelun avulla: yrityksen *eri prosessien* tietosuojariskien hallinta on mahdollista yhtenäistää samaan vuosikelloon. Oheisessa kuviossa (kuvio 9) on havainnollistettu tietosuojariskien hallinta vuosikelloajattelun mukaisesti.



Kuvio 9. Tietosuojariskien hallinta vuosikelloajattelun mukaisesti.

Rekrytointiprosessin tietosuojariskien hallinta lähtee oheisen kuvion (kuvio 9) mukaisesti liikkeelle suunnittelusta. Suunnitteluvaiheessa keskeistä on *tunnistaa* organisaation rekrytointiprosessin tietosuojariskit, sekä *tehdä riskianalyysi*, jossa arvioidaan näiden yksittäisten tietosuojariskien todennäköisyyttä ja vaikutusta. Jotta rekrytoiva yritys voi tunnistaa rekrytointiprosessiensa keskeisimmät tietosuojariskit, tulee organisaation ensin kyetä muodostamaan kokonaiskuva nykyisistä rekrytointiprosesseistaan[257]. Olennaista on täten yksityiskohtaisen *prosessikuvauksen* luominen: rekrytoivan yrityksen tulee käsittää, mistä työvaiheista heidän rekrytointiprosessinsa koostuu, ketä prosessiin osallistetaan, mitä henkilötietoja hakijoista kerätään, kuinka usein prosessi toistuu, sekä millaiset hakijamäärät ovat yritykselle tyypillisiä. Myös organisaation koon ja toimialan vaikutuksia henkilötietoriskeihin on määrä analysoida. Lisäksi rekrytointiprosessin tietosuojariskejä voidaan hahmottaa arvioimalla yrityksen käytössä olevia järjestelmiä sekä niiden tietoturvallisuutta, organisaation arvoja, johtamistyylejä, sekä prosessien toimivuutta.

Tietosuojariskien tunnistamisessa organisaatiot voivat hyödyntää esimerkiksi tämän tutkielman tuloksia: tutkielmassa on esitelty kahdeksan rekrytointiprosessissa yleisesti esiintyvää tietosuojariskiä, ja edellä mainitussa kuviossa (kuvio 9) nämä on kuvattu lilan värisiin laatikoihin. Käymällä tämän listauksen läpi, organisaatio voi hahmottaa, muodostavatko jotkin tutkielmassa mainituista tietosuojariskeistä merkittäviä tietosuojariskejä heidän rekrytointiprosesseissaan. Tietosuojariskien tunnistamisessa myös riskin alkuperän hahmottaminen voi auttaa: tässä tutkielmassa tietosuojariskejä aiheuttavat tekijät on jaettu inhimillisiin, operatiivisiin, vilpillisiin ja strategisiin tekijöihin. Näiden riskejä aiheuttavien tekijöiden tunnistaminen omassa organisaatiossa voi auttaa rekrytoivia yrityksiä paikantamaan omien rekrytointiprosessiensa tietosuojariskejä[258]. Tämän jälkeen suunnitteluvaiheessa tulee keskittyä siihen, mitä tietosuojariskejä on tarpeen käsitellä ja mikä on näiden riskien välinen käsittelyjärjestys. [259] Organisaation on nimittäin

[257] Tietosuojariskejä arvioitaessa rekisterinpitäjän on hyvä hahmottaa omia henkilötietojen käsittelyyn liittyviä toimintatapojansa, sekä arvioida henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitus, Tietosuojavaltuutetun toimisto, Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi.
[258] Tietosuojariskejä aiheuttavista inhimillisistä, operatiivisista, vilpillisistä ja strategisista tekijöistä löytyy lisätietoa tutkielman sivuilta 63–67.
[259] Valtiovarainministeriö, 2017, ohje, s.19–26; ISO 31000 -standardi.

huomioitava, ettei tietosuojariskejä ole mahdollista välttää kokonaan[260], joten yrityksen on tehtävä valintoja siitä, mihin tietosuojariskeihin pureudutaan ensisijaisesti.

Vuosikellon mukaisesti tietosuojariskien hallinnan seuraava vaihe koostuu riskienhallintakeinojen valinnasta sekä valittujen toimenpiteiden läpiviennistä. Tutkielman tutkimustulokset voivat olla apuna myös tässä vaiheessa riskienhallintaprosessia: rekrytoiva yritys voi arvioida, tulisiko heidän hyödyntää tutkielmassa mainittuja rekrytointiprosessin tietosuojariskien hallintakeinoja[261]. Organisaation on myös hyvä tiedostaa, että riskienhallinnassa olennaista ei ole vain *valita* riskienhallintakeinoja vaan myös *vastuuttaa* jokainen valittu riskienhallintakeino jollekin yksikölle tai henkilölle. Sovittujen riskienhallintakeinojen toteutumista on siis valvottava aktiivisesti[262]. Jokaiselle rekrytointiprosessin tietosuojariskille tuleekin valita niin kutsuttu *riskin omistaja*[263], joka seuraa riskienhallintakeinojen vaikutuksia. Myös se on päätettävä, kuka on se organisaation taho, joka valvoo riskien omistajien toimintaa sekä riskienhallinnan aktiivista toteutumista organisaatiossa. Lisäksi on hyvä sopia yhdessä, miten riskienhallinnasta tulee organisaatiossa raportoida ja millaisella aikataululla.

Kun rekrytointiprosessin tietosuojariskeistä ja niiden hallintakeinoista on muodostettu kokonaiskuva, on kolmantena vaiheena riskienhallinnassa valittujen keinojen arviointi. Arvioinnin tavoitteena on tulla tietoiseksi valittujen riskienhallintakeinojen vaikuttavuudesta ja tehokkuudesta[264]. Tietosuojariskien hallintakeinojen arvioinnin apuna tulee käyttää niitä raportteja, joita riskienhallinnan edellisessä vaiheessa on yhteisesti sovittu käytettävän. Keskeistä on, että rekrytoiva yritys analysoi, *mitkä* riskienhallintakeinot ovat

---

[260] Riskienhallinnassa keskeistä on myös kyetä hyväksymään osa riskeistä, ks. lisää Ilmonen, Kallio, Koskinen & Rajamäki, 2016, s.132. Toki tietoduojariskien osalta riskien hyväksymisessä tulee olla hyvin tarkkana, sillä tietosuojariskien toteutuessa yritys ei ainoastaan heikennä omia mahdollisuuksiaan tehdä liikevoittoa vaan myös loukkaa rekisteröidyn lakiin perustuvia oikeuksia.

[261] Lue lisää tutkielmassa ehdotetuista rekrytointiprosessin tietosuojariskien hallintakeinoista tutkielman sivulta 68.

[262] Valtiovarainministeriö, 2017, ohje, s.26–27; ISO 31000 -standardi.

[263] Riskin omistajalla tarkoitetaan tutkielmassa henkilöä tai tahoa, jolla on valtuudet ja vastuu hallita riskiä. Riskin omistajan lisäksi usein on paikallaan nimetä riskitoimenpiteiden vastuuhenkilö, joka seuraa ja koordinoi tietyn riskin hallintaan liittyviä toimenpiteitä käytännössä, Valtiovarainministeriö, 2017, liite, s.4.

[264] Valtiovarainministeriö, 2017, ohje, s.28; ISO 31000 -standardi.

toimineet rekrytointiprosessin tietosuojariskien hallinnassa. Olennaista on myös saada selville, *miksi* osa riskienhallintakeinoista on yrityksessä toiminut. Tämä edesauttaa yritystä hahmottamaan, minkä tyyppiset riskienhallintakeinot sopivat heidän yritykselleen, sekä millaisia aikataulutuksia, raportointimuotoja ja vastuunjakotoimia heidän kannattaa tulevaisuudessa priorisoida.

Tietosuojariskien hallinnan neljäs ja viimeinen vaihe käsittää sisälleen riskienhallinnan kehittämisen[265]. Tässä vaiheessa riskienhallintaprosessia oleellisinta on pyrkiä parantamaan tulevan vuoden riskienhallinnan vuosikelloa: tarkoitus on ottaa opiksi mahdollisista virheistä, joita kuluvana vuotena on tehty ja toisaalta pyrkiä lisäämään sellaista riskienhallintaa, joka on *kyseisessä* rekrytoivassa yrityksessä koettu hyödylliseksi. Tässä kohtaa riskienhallintaprosessia rekrytoivan yrityksen on myös hyvä analysoida, kuinka tietosuojariskien hallinta tullaan tulevana vuotena rekrytointiprosessien osalta toteuttamaan: yrityksen tulisi erityisesti tarkastella, onko sen toimintaympäristöön ilmaantunut uudentyyppisiä tai -laajuisia tietosuojariskejä sekä ovatko vuoden alussa analysoidut tietosuojariskit todellisuudessa olleet kyseiselle yritykselle olennaisia tietosuojariskejä[266]. Tämä antaa rekrytoivalle yritykselle tulevan vuoden alkuvuodesta mahdollisuuden keskittyä niihin tietosuojariskeihin, jotka todella ovat yritykselle merkittäviä uhkia. Kokonaisuudessaan rekrytointiprosessin tietosuojariskien tunnistaminen ja hallinta vaatii jatkuvaa ja pitkäjänteistä työtä.

[265] Valtiovarainministeriö, 2017, ohje, s.10; ISO 31000 -standardi.
[266] Vuosikelloajattelun mukaisesti vuoden viimeisellä kvartaalilla on hyvä seurata riskiarviointien toteutumista sekä arvioida, ovatko asetetut riskit todellisuudessa olleet merkittäviä yrityksen kannalta, Valtiovarainministeriö, 2017, liite, s.21.

6 Lopuksi

6.1 Yhteenveto ja henkilötietojen käsittelyn paradoksi

Päätavoitteena tutkielmassa oli luoda tietosuoja-asetuksen vaatimusten mukaisia ja liike-elämän tarpeet täyttäviä toimintaehdotuksia rekrytointiprosessin tietosuojariskien hallintaan. Lisäksi tutkielmassa käsiteltiin henkilötietojen välttämättömyyttä osana rekrytointiprosessia ja toisaalta työnhakijan oikeuksia omiin henkilötietoihinsa. Myös se tuotiin esille, miksi tietosuojariskien hallinta on yritysten näkökulmasta olennaista, sekä mitä tietosuojariskejä rekrytointiprosessiin sisältyy. Näin tutkielmassa vastattiin kaikkiin asetettuihin tutkimuskysymyksiin. Tutkielman johdannon mukaisesti tutkielman päätutkimuskysymys oli muotoiltu seuraavasti:

Miten henkilötietojen suojan tietosuojariskejä voidaan hallita rekrytointiprosessissa?

Lisäksi tutkielman neljä alatutkimuskysymystä oli muotoiltu alla esitetyn mukaisesti:

1) *Miksi rekrytointiprosessissa on tarpeenmukaista kerätä henkilötietoja?*
2) *Miten oikeudellinen sääntely suojaa työnhakijan henkilötietoja rekrytointiprosessissa?*
3) *Miksi rekrytointiprosessin tietosuojariskien hallinta on organisaatioille olennaista?*
4) *Mitä tietosuojariskejä työnhakijan henkilötietoihin kohdistuu rekrytointiprosessissa?*

Metodologisina keinoina tutkielmassa hyödynnettiin sekä lainoppia että kvalitatiivisia haastatteluja. Rekrytointiprosessin keskeisimpiä tietosuojariskejä tutkielmassa löydettiin yhteensä kahdeksan. Tietosuojariskien hallintaan tutkielmassa esitettiin myös kahdeksan eri keinoa, minkä lisäksi riskienhallintakeinojen räätälöintiin annettiin ohjeita ISO 31000 -standardiin pohjautuen.

Tutkimustulosten ohella on hyvä huomioida, että henkilötietojen käsittelyyn kohdistuu paradoksi: ihmisten henkilötietoja pyritään lainsäädännön keinoin suojaamaan tehokkaammin, vaikka yhteiskunnan verkostomainen toimintatapa ja tiedon alati moninaistuvat käyttötarkoitukset miltei vaativat yhä yksityiskohtaisemman ja ajantasaisemman tiedon jakamista yksityishenkilöiltä. Tämä on saanut aikaan myös sen, että yksilöt ovat

valmiita jakamaan ja julkaisemaan itsestään yhä enemmän tietoa. Yksilöt saattavatkin samanaikaisesti vaatia yrityksiltä yhä huolellisempia ja tietoturvallisempia tapoja käsitellä henkilötietojansa, vaikka mahdollisesti itse käsittelisivät omia henkilötietojansa hyvinkin huolettomasti yksityiselämässään. Siksi tietosuojalainsäädännön uudistaminen tai rekrytoivien yritysten tietosuojariskien hallinnan kehittäminen eivät pysty täydellisesti poistamaan tietosuojariskien olemassaoloa – muutoksen olisi lähdettävä sekä yksityishenkilöistä itsestään että laajemmin verkostoituneen yhteiskunnan toimintatavoista.

6.2 Tutkimustulosten merkitys

Tutkimustulokset ovat uutuusarvoltaan merkittäviä, sillä aikaisempi tutkimus on keskittynyt lähinnä tulkitsemaan ja systematisoimaan vaikeaselkoista tietosuojalainsäädäntöä ja sen asettamia velvollisuuksia. Tämä tutkielma sen sijaan antaa tietosuoja-asetuksen mukaisia liiketoiminnallisia *toimintaehdotuksia* tietosuojariskien hallintaan. Tutkielma onkin pyrkinyt pelkän lainopillisen tulkinnan ja systematisoinnin sijaan myös *ohjeistamaan* liiketoimintaa – eli rekrytointiprosessin tietosuojariskien hallintaa – oikeudellisesta näkökulmasta. Tutkielman tuloksia on mahdollista hyödyntää käytännön rekrytointityön tukena: tutkielmassa esiin tuodut rekrytointiprosessin tietosuojariskit ovat aitoja työelämän riskejä ja ne ovat tietosuojalainsäädännön näkökulmasta merkittäviä – rikkovathan ne toteutuessaan lainsäädännön asettamia vaatimuksia. Todettakoon myös, että rekrytointiprosessin tietosuojariskien hallinta on olennaista – tai sen tulisi olla – jokaiselle organisaatiolle, joka rekrytointia toteuttaa.

Tutkimustulokset tietosuojariskeistä ovat ajankohtaisia myös sen vuoksi, että tiukentunut tietosuojalainsäädäntö ohjaa yrityksiä kohti tietosuojariskien hallintaa: uudistetulla tietosuoja-asetuksella on riskiperustainen lähtökohta ja rekisterinpitäjän velvollisuudet pakottavat rekrytoivia yrityksiä oppimaan organisaationsa tietosuojariskeistä sekä niiden oikea-aikaisesta hallinnasta. On myös hyvä huomioida, että nimenomaisesti *rekrytointiprosessin* tietosuojariskejä käsittelevät tutkimustulokset ovat ajankohtaisia sen vuoksi, että tietosuojariskien tunnistaminen ja hallinta on hyvä aloittaa rekrytointiprosessista, koska lähes jokainen yritys hyödyntää rekrytointia osana liiketoimintaansa. Lisäksi

rekrytointiprosessi on yksi eniten henkilötietoja sisältävistä prosesseista organisaatioiden sisällä. Täten rekrytoinnin aikaisista tietosuojariskeistä tietoiseksi tuleminen voi auttaa organisaatiota tunnistamaan ja hallitsemaan tietosuojariskejä myös muissa prosesseissaan.

Tutkielman tuloksia on hyvä kuitenkin myös kyseenalaistaa: tutkielmassa hyödynnetyt lainopilliset tulkinnat ja systematisoinnit ovat aina myös normatiivisia kannanottoja voimassa olevan oikeuden merkityssisällöstä, eikä lainoppi ole koskaan täysin objektiivista tai epäpoliittista[267]. Se, millaisiin tulkintoihin ja ratkaisuehdotuksiin tutkielmassa on päädytty, nojaa väistämättä jossain määrin sekä itse tutkijan että tutkimusympäristön ja yhteiskunnan ideologioihin ja nykytilaan.

6.3 De lege ferenda: tietosuojan tuleva oikeussäännöstö

Tietosuojaa koskeva oikeussäännöstö painottuu tällä hetkellä yksilöiden ja organisaatioiden oikeuksiin, velvoitteisiin ja sanktioihin. Tiedon käyttötarkoitusten jatkuva lisääntyminen, yhä osittain tuntematon tekoäly, henkilötiedon käsitteen alati laajeneva perusta, sekä globaalin maailman lisääntyvä digitalisuus aiheuttavat kuitenkin sen, että velvoitteet tietosuojan toteutumisesta tulisi ainakin osittain olla myös viranomaisilla. Tulevaisuuden oikeussäännöstössä viranomaisten vastuu tietosuojariskien hallinnasta saattaakin kasvaa. Kuten Keller osoittaa, on tietosuojalainsäädännön vaatimusten täydellinen noudattaminen yritysten toimesta mahdotonta:

> *''Millään yrityksellä ei tule ikinä olemaan riittäviä resursseja GDPR:n aukottomaan noudattamiseen. Tietosuojavastaavan parhaasta tahdosta huolimatta kaikki yrityksen työntekijät eivät osaa toteuttaa tietosuojaa päivittäisessä työssään, tai yritys ei ole pystynyt irrottamaan tarvittavaa investointia tietosuojaa edistävään teknologiaan.''*[268]

Tämän vuoksi on aiheellista nostaa esille, mitä viranomaiset voivat tehdä. Yhtenä ratkaisuehdotuksena voitaisiin esimerkiksi pitää sitä, että lainsäädännön keinoin pyrittäisiin

[267] Hirvonen, 2011, s.50–51. Lainopilliset kannanotot perustuvat aina määrättyihin ideologisitoumuksiin, ja ne usein heijastelevat yhteiskunnassa valtaa pitävien arvoja ja tarkoitusperiä.
[268] Keller, 2023, s. 227.

pelkän hallinnollisen seuraamusmaksun sijaan ohjaamaan yritysten toimintaa kohti tietosuojatumpia toimintatapoja kehotusten ja rajoitusten kautta. Valtio voisi lainsäädännön keinoin esimerkiksi kieltää tiettyjen palveluntarjoajien tai tiettyjä ohjelmistoja käyttävien palveluntarjoajien käytön, jolloin myös resurssien osalta rajoittuneemmat yritykset voisivat toiminnassaan huomioida herkemmin tietosuojattuja ja -turvallisia toimintatapoja ja palveluntarjoajia[269].

6.4 Jatkotutkimusehdotukset

Koska tietosuojaa koskeva tutkimus on hyvin pitkälti keskittynyt tulkitsemaan ja systematisoimaan tietosuojalainsäädännön sirpaleista ja vaikeaselkoista ydinsisältöä, kaivataan tämän tutkielman kaltaista tutkimusta tietosuojariskien tunnistamisesta ja riskienhallintakeinojen hahmottamisesta lisää. Jotta tietosuojariskien hallinta on organisaatioissa mahdollista toteuttaa tehokkaasti, tulee tutkimuksen myötä ensin löytää *oikeusnormiston mukaiset* keinot, joilla se on ylipäänsä mahdollista. Lisäksi tietosuojariskien hallintakeinojen tutkiminen edesauttaa oikeuspohjan luomista: kun tiedämme, kuinka tietosuojariskejä tulisi hallita, on oikeuden säätäjillä paremmat lähtökohdat säätää oikeusnormistoa kohti tietosuojatumpaa yhteiskuntaa.

Tietosuojariskien tunnistamisen ja riskien hallintakeinojen tutkimisen ohella tuleva tutkimus olisi syytä kohdistaa siihen, kuinka *vastuu* tietosuojalainsäädännön määräysten toteutumisesta siirtyy yhä enemmän yksityishenkilöille. Tässäkin tutkielmassa on tuotu esille, että nykypäivänä työnhaussa ei enää riitä henkilötietojen lähettäminen CV:n ja hakemuskirjeen muodossa potentiaalisille työnantajille. Etenkin asiantuntijatyössä esimerkiksi LinkedIn-profiilin luominen ja sinne omien henkilötietojen jakaminen muodostuu väistämättä yhä suuremmaksi edellytykseksi työn saamisesta. Tällaisten tietoyhteiskunnallisten ilmiöiden tutkiminen olisi ensiarvoisen tärkeää: vain sitä kautta voimme hahmottaa, kuinka esimerkiksi verkottunut yhteiskunta, tekoälyn kehitys,

[269] Joidenkin näkemysten mukaan tietosuojan tulisi kyetä vallankäytön ohjailun ja rajoittamisen lisäksi kieltämään tietosuojan vastaiset käytännöt, ks. lisää Keller, 2023, s.83–84.

digitaalisuuden moniulotteisuus ja henkilötietojen moninaistuneet käyttötavat vaikuttavat myös tietosuojariskien syntyyn ja tietosuojariskien muodostumisen alkuperään.

Lopuksi todettakoon, että rekrytointiprosessi – sekä muut henkilötietoja sisältävät prosessit – tulevat aina sisältämään henkilötietoihin kohdistuvia tietosuojariskejä. Täydellistä riskittömyyttä on mahdotonta saavuttaa. Täten tämän tutkielman tutkimustulosten mukaisesti tietosuojariskien hallinnassa olennaisinta on kartoitus kyseessä olevan organisaation rekrytointiprosessin tietosuojariskeistä, riskienhallintakeinojen kriittinen arviointi ja valinta sekä hallittu käyttöönotto. Loppujen lopuksi myös tietosuojariskien hallinta on laskelmoitua riskinottoa. Kuten Karl Popper on asian aikanaan todennut:

> *”Jokainen ratkaisu johonkin ongelmaan nostaa esille uusia ratkaisemattomia ongelmia, sitä enemmän, mitä syvällisempi alkuperäinen ongelma oli ja mitä rohkeampi sen ratkaisu. Mitä enemmän opimme todellisuudesta ja mitä syvällisempää oppimisemme on, sitä tietoisempaa, spesifisempää ja artikuloituneempaa on tietomme siitä, mitä emme tiedä, tietomme tietämättömyydestä.”*[270]

[270] Karl Popper, 1995, s.29.

Lähteet

Aalto-Setälä, M., & Viitaila, M. (2018). Tietosuoja pähkinänkuoressa: tietosuojaopas yrityksille. *Keskuskauppakamari. Helsinki*.

Aarnio, A. (1975). *Laki, teko ja tavoite: tutkimus tavoitteellisuudesta lain tulkinnassa ja sen soveltamisessa.* Lainopillisen ylioppilastiedekunnan kustannustoimi.

Aarnio, A. (1978). *Mitä lainoppi on?* Tammi.

Aarnio, A. (1989). *Ottakaamme oikeussäännöt vakavasti.* Oikeus 1989. s. 112–122.

Aarnio, A. (2006). *Tulkinnan taito: Ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta*. WSOY.

Aarnio, A. (2011). *Luentoja lainopillisen tutkimuksen teoriasta*. Helsingin yliopiston oikeustieteellinen tiedekunta.

Aarnio, A. (2014). *Oikeutta etsimässä: Erään matkan kuvaus*. Talentum.

Ahokas, N. (2012). *Yrityksen sisäinen valvonta*. Edita Publishing Oy.

Alapuranen, L., Lehtonen, L., Koskinen, S. & Wiberg, M. (2020). *Henkilötietojen käsittely työelämässä* (s. 7–167). (3. uudistettu painos). Edita.

Alasoini, T. (2015). Digitalisaatio muuttaa työtä – millaista työelämää uudistavaa innovaatiopolitiikkaa tarvitaan. *Työpoliittinen aikakauskirja*, 2(2015), 26–37.

Alftan, M., Blummé, N., Heikkala, J., Kontula, L., Miettinen, O., Pakarainen, E., Sinersalo, K., Sjölund, R., Sundvik, P., Tarvainen, J., Tikkanen, R., Turakainen, O., Urrila, A. & Vesa, J. (2008). *Corporate Governance sisäisen valvonnan ja riskienhallinnan näkökulmasta*. 2. painos. Edita Publishing Oy.

Alhonsuo, S., Nilsen, A., Nousiainen, S., Pellikka, T. & Sundberg, S. (2012). *Finanssitoiminnan käsikirja.* Bookwell Oy.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3*, 563060.

Andreasson, A., Koivisto, J., & Ylipartanen, A. (2016). *Tietosuojakäsikirja johdolle*. (3. painos). Tietosanoma.

Andreasson, A. & Ylipartanen, A. (2022). *Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus (GDPR).* (2. päivitetty laitos). Tietosanoma.

Berthon, P., Ewing, M. & Hah, L. (2005). Captivating company: Dimensions of attractive ness in employer branding. *International Journal of Advertising*, vol 24(2), s.151–172.

Brunila, A. (2014). Teknologian uudet vallankumoukset muuttavat maailmaa vauhdilla. *Tieteessä Tapahtuu*, 32(1). Noudettu 14. syyskuuta 2023 osoitteesta https://journal.fi/tt/article/view/40863

Burri, M. & Schär, R. (2016). The reform of the EU data protection framework: outlining key changes and assessing their fitness for a data-driven economy. *Journal of Information Policy*, *6*, 479–511.

COSO – Committee of Sponsoring Organizations of the Tradeway Commission. (2017). *Enterprise Risk Management. Integrating with Strategy and Performance*. Executive Summary.

Coverdill, J. E. & Finlay, W. (2017). *High Tech and High Touch: Headhunting, Technology, and Economic Transformation*. Cornell University Press.

Dolan, S. L., Garcia, S. & Richley, B. (2006). *Managing by Values*. Hampshire, Palgrave MacMillan.

Edilex. (2020). *TSV 18.05.2020. Työnhakijoiden henkilötietojen kerääminen tarpeettomasti.* Noudettu 21. syyskuuta 2023 osoitteesta https://www.edilex.fi/tsv/20200583

Edilex. (5. toukokuuta 2021). *Tietosuojavaltuutetun toimisto ja tietoyhteiskunnan kehittämiskeskus Tieke Ry: Tietosuoja-asetus tunnetaan, mutta käytännön soveltamisessa riittää vielä haasteita.* Noudettu 03. elokuuta 2023 osoitteesta https://www.edilex.fi/uutiset/69155

Edilex. (14. elokuuta 2023). *Yleisen tietosuoja-asetuksen toimivuudesta ja sen soveltamisesta liittyvistä kokemuksista voi lausua 6. syyskuuta 2023 saakka*. Noudettu 29. syyskuuta 2023 osoitteesta https://www.edilex.fi/uutiset/85953

Elinkeinoelämän keskusliitto. (2023). *EU:n palkka-avoimuusdirektiivi ja sen täytäntöön pano Suomessa.* Noudettu 5. tammikuuta 2024 osoitteesta https://ek.fi/wp-content/uploads/2023/12/Palkka-avoimuusdirektiivi-Leppanen-EK-marraskuu-2023.pdf

ETN ohjeet 4/2019. *Euroopan tietosuojaneuvoston antamat ohjeet 25 artiklan mukaisesta sisäänrakennetusta ja oletusarvoisesta tietosuojasta*. (Versio 2). Noudettu 8. marraskuuta 2023 osoitteesta https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_fi.pdf

ETN suuntaviivat 05/2020. *Asetuksen 2016/679 mukaista suostumusta koskevat suuntaviivat.* Versio 1.1. Noudettu 18. joulukuuta 2023 osoitteesta https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fi.pdf

Euroopan komissio. (2022a). *Tietosuoja EU:ssa*. Noudettu 15. syyskuuta 2023 osoitteesta https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_fi

Euroopan komissio. (2022b). *EU-lainsäädännön tyypit*. Noudettu 01. elokuuta 2023 osoitteesta https://ec.europa.eu/info/law/law-making-process/types-eu-law_fi

Evans, A. (2019). *Managing Cyber Risk*. Milton: Routledge.

Glon, C. (2014). Data Protection in the European Union: A Closer Look at the Current Patchwork of Data Protection Laws and Proposed Reform That Could Replace Them All. *International Journal of Legal Information*, 42(3), s.471–492.

Halpert, B. (2011). *Auditing Cloud Computing: A Security and Privacy Guide*. New Jersey: Hoboken.

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

HE 9/2018 vp. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi.

HE 75/2000 vp. Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiksi siihen liittyviksi laeiksi.

Helsilä, M. & Salojärvi, S. (2009). *Strategisen henkilöstöjohtamisen käytännöt*. Talentum Media.

Hirsjärvi, S., Remes, P. & Sajavaara, P. (2009). *Tutki ja kirjoita* (15. painos). Tammi.

Hirsjärvi, S. & Hurme, H. (2000). *Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö.* Yliopistopaino.

Hirvonen, A. (2000). *Oikeuden käynti: Antigonen laki ja oikea oikeus*. Loki-Kirjat.

Hirvonen, A. (2011). *Mitkä metodit? Opas oikeustieteen metodologiaan*. Yleisen oikeustieteen julkaisuja 17.

Huilaja, H. (2019). *Rekrytoinnin sosiaalinen järjestys–tutkimus työhön sopivuuden neuvottelukontekstista* [väitöskirja, Lapin yliopisto]. Lauda. Noudettu 05. syyskuuta 2023 osoitteesta https://urn.fi/URN:ISBN:978-952-337-148-4

Huhtamäki, S., Saarnilehto, A., Huhtamäki, A. & Tähti, A. (1992). *Hyvä tapa. Oikeusperiaatteet ja oikeuskäytäntö – tutkimusprojektin seminaarin 12.11.1992 alustukset.* Turun yliopisto.

Hofstede, G. H. (1998). Attitudes, values, and organizational culture: disentangling the concepts. *Organization studies,* 19(3), s.477–493.

Honkanen, H. (2005). *Henkilöarviointi työelämässä*. Tammi.

Honkaniemi, L. (2007). *Viisaat valinnat*. Gummerus.

Hoppe, T., & Laine, T. (2014). *Työnhakuopas: Mitä, miten, missä?* Talentum.

Hoppu, K. (2021). Hyvä kauppatapa elintarvikeketjussa. *Liikejuridiikka*, *2021*(2), 52–83.

Husa, J., Mutanen, A. & Pohjolainen, T. (2008). *Kirjoitetaan juridiikkaa: Ohjeita oikeustieteellisten kirjallisten töiden laatijoille* (2. painos). Talentum.

Hyttinen, S. Henkilöstön elinkaari organisaatiossa. Teoksessa Westman, A. L. & Kuusisto, T. (toim.). *Arvoja, sitoutumista ja oppimista*, (s.120–132).

Hyvärinen, H., Hulkko, P. & Ohvo, S. (2002). *Yksityisoikeuden Perusteet*. (painos 1–2). WSOY.

Iivari, M. & Laaksonen, M. (2009). *Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen.* Helsinki: Tietosanoma.

Ilmonen, I., Kallio, J., Koskinen, J. & Rajamäki, M. (2016). *Johda riskejä – Käytännön opas yrityksen riskienhallintaan.* 2. painos. Finva.

Jackson C. (2010). *Network Security Auditing.* Cisco Press, Indianapolis.

Jaskela, S., Guichon, J., Page, S. A. & Mitchell, I. (2018). Social workers' experience of moral distress. *Canadian Social Work Review*, *35*(1), s.91–107.

Jobst, A. (2007). Operational Risk – The Sting is Still in the Tail but the Poison Depends

on the Dose. *IMF Working Paper – Monetary Fund*, 237(7), s.4–72. https://doi.org/10.5089/9781451868036.001

Joki, M. (2021). *Henkilöstöasiantuntijan käsikirja* (7., uudistettu painos.). Kauppakamari.

Järvinen, P. (2022). *Digiajan tietosuoja. Turvaa henkilötietosi, torju identiteettivarkaudet, suojaudu urkinnalta.* Tammi.

Kaijala, M. (2016). *Rekrytointi: Tehtävään vai yhtiöön?* Alma.

Kaijala, M. & Tolvanen, R. (2020). *Henkilöstö - strateginen investointi?* (1. painos.). Kauppakamari.

Kaisto, J. (2005). *Lainoppi ja oikeusteoria*. Edita.

Kanninen, H. Euroopan yhteisön oikeuden normihierarkia ja kansallinen lainsoveltaja. Teoksesta: *Puhuri käy, muuttuva suomalainen ja eurooppalainen valti-osääntömme.* Toimittaneet: H. Kanninen, H. Koskinen, A. Rosas, M. Saksin ja K. Tuori. 2009. Edita Publishing Oy.

Kanninen, O. & Virkola, T. (2021). *Rekrytointisyrjintä ja sen vastaiset keinot.* Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja, 2021(27). http://urn.fi/URN:ISBN:978-952-383-326-5

Karhu, J., Tolonen, H. & Ämmälä. T. Heikomman suoja. Teoksessa Saarnilehto, A., Annola, V., Hemmo, M., Karhu, J., Kartio, L., Tammi-Salminen, E., Tolonen, J., Tuomisto, J. & Viljanen, M. 2012. *Varallisuusoikeus*. (2. painos.). Sanoma Pro Oy.

Kansallinen turvallisuusviranomainen – Katakri. (2020). *Tietoturvallisuuden auditointi työkalu viranomaisille.* Noudettu 15. joulukuuta 2023 osoitteesta https://um.fi/katakri-tietoturvallisuuden-auditointityokalu-viranomaisille

Kauhanen, J. (2012). *Henkilöstövoimavarojen johtaminen.* (10.–11. p.). Talentum.

Kreitzer, L., Brintnell, S. E. & Austin, W. (2020). Institutional barriers to healthy workplace environments: From the voices of social workers experiencing compassion fatigue. *The British Journal of Social Work*, *50*(7), s.1942–1960.

Kuopus, J. (1985). Tietosuoja – kehityspiirteitä Suomessa ja ulkomailla. *Hallinnon tutkimus*, 4(1), s.121–138.

Kupi, E., Keränen, J. & Lanne, M. (2009). *Riskienhallinta osana pk-yritysten strategista johtamista.* Teknologian tutkimuskeskus.

Kurkela, M. S. (2014). Yritystoiminnan riskeistä ja riskien hallintainstrumenteista. Edilex. www.edilex.fi/artikkelit/14498

KOM, (2010) 609. *Euroopan komission tiedonanto.* Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: kattava lähestymistapa henkilötietojen suojaan Euroopan unionissa. KOM (2010) 609 lopullinen.

KOM (2012) 11. *Euroopan komission ehdotus.* Euroopan parlamentin ja neuvoston asetus yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta. KOM (2012) 11 lopullinen.

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. (2022). *Tietosuoja* (2. painos.). Alma Talent.

Koskenniemi, M. (2022). Mistä oikeustieteessä on kysymys?. *Lakimies*, *120*(7–8), s.1016–1030.

Laakso, S. (1990). *Oikeudellisesta sääntelystä ja päätöksenteosta.* Valtion painatuskeskus, valtionhallinnon kehittämiskeskus.

Lambert, P. (2017). *Understanding the New European Data Protection Rules*. CRC Press.

Lecklin, O. (2006). *Laatu yrityksen menestystekijänä*. (5. uudistettu painos.). Hämeenlinna Karisto.

Liappis, H., Pentikäinen, M. & Vanhala, A. (2019). *Menesty yritysvastuulla: käsikirja kokonaisuuteen.* Edita Publishing Oy.

Louisot, J–P. & Ketcham, C. (2014). *ERM – Enterprise Risk Management: Issues and Cases*. John Wiley & Sons.

Luukka, P. (2019). *Yrityskulttuuri on kuningas*. Helsinki, Alma Talent.

Maijoor, S. (2000). The Internal Control Explosion. *Internal Journal of Auditing*, 4, s.101–109.

Miles, S. A. & Larcker, D. F. (2010). Do you have a plan for finding your next CEO?. *Corporate Board*, 31, s.11–15.

Mouzakiti, F. (2015). Transborder Data Flows 2.0: Mending the Holes of the Data Protection Directive. *European Data Protection Law Review (EDPL)*. 1(1), s.39–50.

Määttä, T. & Paso, M. (2022). *Johdatus oikeudellisen ratkaisun teoriaan*. Helsingin ylio-

pisto, oikeustieteellinen tiedekunta.

Määttä, T. (2015). Metodinen pluralismi oikeustieteessä–ympäristöoikeudellisen tutkimuksen suuntaukset ja menetelmät. Teoksessa Miettinen, T.(toim.), *Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta*, (s.135–222). Edilex.

Neuvonen, R. (2014). *Yksityisyyden suoja Suomessa*. Lakimiesliiton kustannus.

Neuvonen, R. (2019). *Viestintä- ja informaatio-oikeuden perusteet* (2. painos.). Kauppakamari.

Nieminen, K., Lähteenmäki, N. & Aaltonen, O. (2021). *Empiirinen oikeustutkimus*. Gaudeamus.

Nieminen, K. (2022). *Mikä on LinkedIn? Markkinoinnin trendit.* Noudettu 24. marraskuuta 2023 osoitteesta https://markkinoinnintrendit.fi/linkedin/

Nykänen, P. (2013). Oikeusjärjestys ja sen erityispiirteet. Teoksessa P. Nykänen (toim.) *Johdatus oikeusjärjestykseen,* (s.13–79). Tampereen yliopisto, Johtamiskorkeakoulu.

Nyyssölä, M. (2018). *Yksityisyyden suoja työsuhteessa*. Alma Talent.

Oikeusministeriö, Pohjalainen, A. & Ylikoski, L. (2020). EU: n yleisen tietosuoja-asetuksen soveltamiskokemuksia Suomessa: Lausuntotiivistelmä. http://urn.fi/URN:ISBN:978-952-259-799-1

Oikeusministeriö, Talus, A. (2016). *Tietosuoja-asetus – uutta ja vanhan vahvistamista.* https://oikeusministerio.fi/blogi-hakutulos/-/blogs/anu-talus-tietosuoja-asetus-uutta-ja-vanhan-vahvistamista

Ojanen, T. (2016). *EU-oikeuden perusteita*. (3.painos). Edita.

Oker-Blom, M. (2009). Oikeustaloustieteen eli taloudellisten argumenttien merkityksestä Raimo Siltalan oikeuslähdeopissa. Teoksessa E. Kolehmainen (toim.) *Oikeus ja kritiikki: 1, Raimo Siltalan Oikeustieteen tieteenteoria*. Helsingin yliopiston oikeustieteellinen tiedekunta.

Oliver, C. (2013). Including moral distress in the new language of social work ethics. *Canadian social work review/Revue Canadienne de service social*, s.203–216.

O'Meara, B., Petzall, S. & Stanley Petzall. (2013). *Handbook of Strategic Recruitment and*

Selection: A Systems Approach. Emerald Publishing Limited.

Paanetoja, J. (2017). *Työoikeus tututuksi – käsikirja*. Edita.

Parnila, K. (2017). *Työsuhde tutuksi: Esimiehen selviytymisopas* (2. painos). Helsingin Kamari Oy.

Pentikäinen, M. (2019, 26. syyskuuta). Yritysvastuu on vastuuta ihmisistä. *Defensor Legis*, (4), 568–577.

Pesonen, H. (2007). *Laatua – Asiantuntijaorganisaation laatuopas.* Juva : WS Bookwell.

Pfister, J. (2009). *Managing Organizational Culture for Effective Internal Control.* Physica-Verlag Berlin Heidelberg.

Phillips, J. M. & Gully S. M. (2017). Global Recruiting. Teoksessa H. W. Goldstein, J. Passmore, E. D. Pulakos, & C. Semedo (toim.) *Wiley Blackwell Handbook of the Psychology of Recruitment, Selection and Employee Retention*. (s.29–52). Wiley-Blackwell.

Phillips, J. M. & Gully, S. M. (2012). *Staffing Forecasting and Planning*. Society for Human Resource Management.

Popper, K.R. (1995). *Arvauksia ja kumoamisia. Tieteellisen tiedon kasvu*. Tammer-Paino Oy. Tampere.

Puohiniemi, M. (2003). *Löytöretki yrityksen arvomaailmaan*. Espoo, Limor Kustannus.

Purdy, G. (2010). ISO 31000:2009 – Setting a New Standard for Risk Management. *Risk Analysis*. 30(6), s.881–886.

Puusa, A., Juuti, P., & Aaltio, I. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Gaudeamus.

Pöyhönen, J. (1988). *Sopimusoikeuden järjestelmä ja sopimusten sovittelu*. Vammala.

Pöyhönen, J. (1999). Hyvä tapa, Oikeusperiaate. Teoksessa *Encyclopedia Iuridica Fennica. Suomalainen oikeustietosanakirja. Seitsemäs osa: Oikeiden yleistieteet*, 197–199, 791–795. Toim. Heikki E.S Mattila. Helsinki: Suomalainen lakimiesyhdistys.

Raman, P., Kayacık, H. G. & Somayaji, A. (2011, kesäkuu). Understanding data leak prevention. Teoksessan *6th Annual Symposium on Information Assurance (ASIA'11)*, 27. Noudettu 22. syyskuuta 2023 osoitteesta https://people.scs.carleton.ca/~soma/pubs/raman-asia2011.pdf

Ratsula, N. (2016a). *Compliance: Eettinen ja vastuullinen liiketoiminta*. Talentum Pro.

Ratsula, N. (2016b). *Yrityksen sisäinen valvonta.* Edita Publishing Oy.

Redondo, A. R. & Mariz, F. (2022). How can European regulation on ESG impact business globally?. *Journal of risk and Financial Management*, 15(7), 291.

Rinne, U. (2018). Anonymous job applications and hiring discrimination. *IZA World of Labor.* 2018(48) doi.org.10.15185/izawol.48.v2

Robles, M. (2018). 5 Data Privacy Rights Introduced by GDPR. *Risk management*, 65(5), 12–13.

Roper, C. (1999). *Risk Management for Security Professionals*. Burlington: Elsevier Science.

Rötkin, L. (2015). *Terveisiä pomolle.* Talentum Media.

Saarenpää, A. & Wiatrowski, A. (toim.). (2016). *Society trapped in the network: does it have a future?*. Network Society as a Paradigm for Legal and Societal Thinking, NETSO Research Project. University of Lapland.

Saarinen, M. (2013). *Työsuhdeasioiden käsikirja*. Edita.

Sajama, S. (2015). Mikä tekee tutkimuksesta tieteellisen? Teoksessa Miettinen, T. (toim.), *Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisen opinnäytteiden vaatimuksista, metodista ja arvostelusta*, (s.2–23). Edilex.

Secudo, G., Elia, G., Margherita, A. & Leitner, K.H. (2022). Strategic decision making in project management: a knowledge visualization framework. *Management Decision*, 60(4), s.1159–1181. https://doi.org/10.1108/MD-02-2021-0196

Siltala, R. (2003). *Oikeustieteen tieteenteoria.* Helsinki.

Suomen riskienhallintayhdistys. (2023). *Riskien luokittelu*. Noudettu 7. joulukuuta 2023 osoitteesta https://pk-rh.fi/riskien-luokittelu.html

Syrjänen, P. (2006). *Yksityisyyden suoja ja henkilöarviointi*. Tampere University Press.

Tala, J. (2000). Lainsäädäntö, ajankohtaisia kehityspiirteitä. Teoksessa *Oikeusolot 2000 – Katsaus oikeudellisten instituutioiden toimintaan ja oikeusongelmiin.* OPTL:n julkaisu 173.

Talvio, C. & Välimaa, M. (2004). *Yhteiskuntavastuu ja johtaminen*. Edita.

Tessian. (2020). *Psychology of Human Error - Understand the mistakes that compromise*

your company's cybersecurity. Noudettu 22. syyskuuta 2023 osoitteesta https://www.tessian.com/research/the-psychology-of-human-error/

Thun, J–H. & Hoenig, D. (2011). An Empirical Analysis of Supply Chain Risk Management in German Automotive Industry. *International Journal of Production Economics*. 131(1) s. 242–249.

Tiedeyhteiskunnan kehittämiskeskus. (2022). *GDPR2DSM – Tietosuojaosaamista pk-yrityksille.* Noudettu 21. elokuuta 2023 osoitteesta https://tieke.fi/hankkeet/gdpr2dsm/

Tietosuojavaltuutetun toimisto, (n.d.). *Automaattinen päätöksenteko ja profilointi*. Noudettu 7. marraskuuta 2023 osoitteesta https://tietosuoja.fi/automaattinen-paatoksenteko-profilointi

Tietosuojavaltuutetun toimisto, (n.d.). *Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteutumiseksi.* Noudettu 15. marraskuuta 2023 osoitteesta https://tietosuoja.fi/arvioi-riskit

Tietosuojavaltuutetun toimisto, (n.d.). *Luottamuksellisuus ja turvallisuus*. Noudettu 5. marraskuuta 2023 osoitteesta https://tietosuoja.fi/luottamuksellisuus-ja-turvallisuus

Tietosuojavaltuutetun toimisto, (n.d.) *Rekisteröidyn oikeudet*. Noudettu 5. marraskuuta 2023 osoitteesta https://tietosuoja.fi/rekisteroidyn-oikeudet

Tietosuojavaltuutetun toimisto, (n.d.). *Rekisteröidyn suostumus.* Noudettu 3. marraskuuta 2023 osoitteesta https://tietosuoja.fi/rekisteroidyn-suostumus

Tietosuojavaltuutetun toimisto, (n.d.). *Vaikutustenarviointi.* Noudettu 9. marraskuuta 2023 osoitteesta https://tietosuoja.fi/vaikutustenarviointi

Tietosuojavaltuutetun toimisto. (2020). *Työelämän tietosuojan käsikirja – Toimintaohjeita yksityisyyden ja henkilötietojen suojan toteuttamiseksi työpaikalla.* Noudettu 14. joulukuuta 2023 osoitteesta https://tietosuoja.fi/documents/6927448/8214540/Työelämän+tietosuojan+käsikirja+2020-+Tietosuojavaltuutetun+toimisto.pdf

Tietosuojavaltuutetun toimisto. (2022a). *Menestystä tietosuojasta – seminaarissa*

tuetaan pk-yritysten tietosuojaosaamista. Noudettu 01. elokuuta 2023 osoitteesta https://tietosuoja.fi/-/menestysta-tietosuojasta-seminaarissa-tuetaan-pk-yritysten-tietosuojaosaamista

Timonen, P. (1998). *Johdatus lainopin metodiin ja lainopilliseen kirjoittamiseen*. Helsinki.

Tolonen, H. (2003). *Oikeuslähdeoppi*. WSOY lakitieto.

Tutkimuseettinen neuvottelukunta (TENK). (2021, 16. marraskuuta). *Ihmistieteiden eettisen ennakkoarvioinnin ohje. Noudettu* 07. syyskuuta 2023 osoitteesta https://tenk.fi/fi/ohjeet-ja-aineistot/ihmistieteiden-eettisen-ennakkoarvioinnin-ohje#4_2

Tuomi, J. & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi* (Uudistettu laitos.). Kustannusosakeyhtiö Tammi.

Ulrich, C., O'donnell, P., Taylor, C., Farrar, A., Danis, M. & Grady, C. (2007). Ethical climate, ethics stress, and the job satisfaction of nurses and social workers in the United States. *Social science & medicine*, *65*(8), s.1708–1719.

Vaahtio, E. L. (2005). *Rekrytointi menestystekijänä*. Edita Prima Oy.

Vacca, J. (2009). *Computer and Information Security Handbook*. Burlington: Morgan Kaufmann.

Valtiovarainministeriö, Rousku, K. (2017). *Ohje riskienhallintaan.* Noudettu 16. maaliskuuta 2024 osoitteesta http://urn.fi/URN:ISBN:978-952-251-862-0

Valtionvarainministeriö. (2020). *Julkisen hallinnon digitaalinen turvallisuus – Julkisen hallinnon ICT.* Noudettu 20. elokuuta 2023 osoitteesta https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162169/VM_2020_23.pdf?sequence=2&isAllowed=y

Valtioneuvosto. (2021). *Tietoturvan ja tietosuojan parantaminen yhteiskunnan kriittisillä toimialoilla: Työryhmän loppuraportti.* Noudettu 15. syyskuuta 2023 osoitteesta *https://julkaisut.valtioneuvosto.fi/handle/10024/162783*

Varanto, J. (2011). *Henkilötietolaki käytännössä.* Talentum.

Viitala, R. (2014). *Henkilöstöjohtaminen: Strateginen kilpailutekijä*. (4. painos). Edita.

Viitala, R. (2021). *Henkilöstöjohtaminen: keskeiset käsitteet, teoriat, trendit*. Edita.

Viitala, R., & Järlström, M. (2014). *Henkilöstöjohtaminen uuden edessä: Henkilöstöbaro-*

metrin nostamat kehityshaasteet. Vaasan yliopisto.

Vilkka, H. (2021). *Tutki ja kehitä*. (5. painos). PS-kustannus.

Viscelli, T., Hermanson, D. & Beasley, M. (2017). The Integration of ERM and Strategy: Implications for Corporate Governance. *Accounting Horizons.* 32(2), s.69–82.

Voigt, P. & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR) – A Practical Guide. Springer* International Publishing.

Waddill, D. (2018). *Digital HR: A Guide to Technology-Enabled Human Resources*. Society For Human Resource Management.

WP (Working Party). 248 rev.01 (2017). *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679.* Noudettu 9. marraskuuta 2023 osoitteesta https://ec.europa.eu/newsroom/article29/items/611236

WP (Working Party). 260 rev.01 (2017). *Guidelines on Transparency under Regulation 2016/679*. Noudettu 13. joulukuuta 2023 osoitteesta https://ec.europa.eu/newsroom/article29/items/622227

Österberg, M. (2015). *Henkilöstöasiantuntijan käsikirja*. Kauppakamari.

Säädösluettelo

2000/C 364/01	Euroopan unionin perusoikeuskirja
SopS 19/1990	Euroopan ihmisoikeussopimus
EPNAs 2016/679	Euroopan unionin yleinen tietosuoja-asetus / TSA
731/1999	Suomen perustuslaki
1050/2018	Tietosuojalaki
759/2004	Laki yksityisyyden suojasta työelämässä / työelämän tietosuojalaki / YksTL
527/2007	Luottotietolaki
726/2014	Turvallisuusselvityslaki
1333/2021	Yhteistoimintalaki

Oikeustapausluettelo

Tietosuojavaltuutetun päätökset

Liitteet

Liite 1. Tutkimuksen kvalitatiivinen lähdeaineisto

Tutkielmassa hyödynnetään oikeusdogmatiikan tukena kvalitatiivista tutkimusotetta. Laadullisten haastatteluiden avulla tutkielmassa selvitetään liike-elämän nykytilaa: millaisia tietosuojariskejä organisaatiot kokevat rekrytointiprosessissa, sekä miten he näitä tietosuojariskejä pyrkivät hallitsemaan. Huomion arvoista on se, etteivät haastattelut avaa tutkielmassa lainsäädännön sisältöä – kuten tietosuojaoikeudellisia oikeuksia tai velvollisuuksia – vaan tuovat ilmi organisaatioiden kokemuksia ja tuntemuksia. Siksi laadullinen tutkimusote[271] toimii tässä talousoikeudellisessa tutkimuksessa tukimetodina.

Tutkimuksen kvalitatiivinen lähdeaineisto on kerätty haastattelemalla kymmentä HR-alan ammattilaista. Haastattelut olivat puolistrukturoituja teemahaastatteluja ja niiden keskimääräinen kesto oli 43 minuuttia. Kaikki haastattelut pidettiin Teams-sovelluksen välityksellä syksyllä 2023 ja jokainen haastattelu tehtiin suomen kielellä. Puolistrukturoitu teemahaastattelu[272] sopii tähän tutkimukseen, sillä se mahdollistaa kvalitatiivisen aineiston vertailun, jättäen kuitenkin tilaa haastateltavien tarpeellisille lisähuomautuksille. Haastateltavien tarpeeksi laaja osaaminen henkilöstöhallinnon työtehtävistä varmistettiin asettamalla valittaville henkilöille kriteerejä: haastateltavan tuli olla toiminut rekrytointiin liittyvissä työtehtävissä vähintään viisi vuotta. Lisäksi ainakin puolet työkokemuksesta piti sijoittua tietosuoja-asetuksen 2016/679 voimaantulon jälkeiseen aikaan.

Haastatteluiden laadun varmistamiseksi jokainen haastateltava sai haastattelukysymykset itselleen ennakkoon sähköpostin välityksellä, jolloin heillä oli mahdollisuus tutustua kysymyksiin ennen haastattelua. Lisäksi haastattelutilanteista pyrittiin saamaan

---

[271] Katso tarkemmin kvalitatiivisen tutkimusmetodin käsitteestä ja kyseisen metodin valintaperusteista tutkielman sivuilta 10–12.

[272] Puolistrukturoitu haastattelu tarkoittaa sitä, että kaikille haastateltaville esitetään samat tai lähes samat kysymykset samassa järjestyksessä. Toiset määritelmät antavat käsitteeseen vapautta ja toteavat, että myös puolistrukturoiduissa haastatteluissa kysymysten käsittelyjärjestystä voidaan vaihtaa haastateltavien välillä. Keskeistä on, että tässä haastattelumuodossa haastateltava saa vapautta esittää omia ajatuksia strukturoituja haastatteluja enemmän, ks. lisää Hirsjärvi ja Hurme, 2000, s.47.

mahdollisimman neutraaleja: haastateltavat saivat päättää itse, mikä kellonaika ja päivämäärä sopi heille parhaiten haastattelun toteuttamiseen. Lisäksi haastattelijana pyrin käyttämään haastatteluissa mahdollisimman neutraalia äänensävyä, eikä haastateltavaa johdateltu johdattelevilla jatkokysymyksillä. Lyhytsanaisia haastateltavia kehotettiin syventämään näkemyksiään ja toisaalta puheliaita haastateltavia ohjattiin tilanteen vaatiessa takaisin teeman äärelle. Tämän ohella jokainen haastattelu nauhoitettiin osallistujien luvalla ja vastaukset litteroitiin haastattelupäivän aikana kirjalliseen muotoon.

Tutkielman analysointimenetelmänä hyödynnän aineistolähtöistä sisältöanalyysiä. Sisältöanalyysi[273] mahdollistaa rekrytointiprosessin tietosuojariskien ja riskien hallinnassa käytettävien toimintatapojen tulkitsemisen ja systematisoinnin, sillä sen avulla haastatteluissa kerätty tieto on mahdollista tiivistää ja ryhmitellä helposti ymmärrettävään muotoon. On hyvä huomioida, että tutkielman kvalitatiivisen aineistolähtöisellä sisältöanalyysillä tarkastelen vain haastatteluissa esiin nousseita ilmiöitä. Tutkielmassa oikeuslähteisiin kohdistuva analysointi luokitellaan puolestaan lainopilliseksi tulkinnaksi ja systematisoinniksi.

[273] Vilkka, 2021, s. 163. Aineistolähtöinen sisältöanalyysi on tapa analysoida kerättyä dataa, ja se koostuu kolmesta eri vaiheesta: 1) aineiston pelkistämisestä, 2) aineiston ryhmittelystä sekä 3) käsitteiden luomisesta. Pelkistämisen avulla aineistoa tiivistetään ja siitä karsitaan turha tieto pois. Ryhmittelyn avulla tiivistetty tieto kootaan johdonmukaiseksi kokonaisuudeksi ja käsitteiden luomisen kautta tavoitellaan merkityskokonaisuuden luomista.

Liite 2. Haastattelurunko

1) TAUSTATIEDOT

- Millainen työtausta sinulla on HR-alalta?
- Kuinka kauan olet toiminut rekrytointitehtävissä?
- Millainen rooli ja vastuu sinulla on ollut rekrytointiin liittyvissä työtehtävissä?
- Minkä kokoisissa organisaatioissa ja millä toimialalla olet toiminut rekrytointitehtävissä?

2) REKRYTOINTIPROSESSI JA TYÖNHAKIJAN HENKILÖTIEDOT

- Mistä työvaiheista rekrytointiprosessi koostuu? (suorahaku vs. perinteinen rekrytointi)
- Keitä työntekijöitä rekrytointiprosessiin on hyvä osallistaa mukaan?
- Mitä henkilötietoja työnhakijasta on tarpeenmukaista kerätä rekrytointiprosessissa?
- Miksi työnhakijasta on tarpeenmukaista kerätä henkilötietoja rekrytointiprosessissa?
- Missä vaiheessa rekrytointiprosessia työnhakijasta kerätään henkilötietoja?
- Kenellä tulee olla pääsy työnhakijan henkilötietoihin ja miksi?
- Missä vaiheessa rekrytointiprosessia kerätyt henkilötiedot kokemuksesi mukaan poistetaan?

3) HENKILÖTIETOIHIN KOHDISTUVAT TIETOSUOJARISKIT

- Millaisia tietosuojariskejä työnhakijan henkilötietojen suojaan kohdistuu rekrytointiprosessissa?
- Missä rekrytointiprosessin työvaiheissa tietosuojariskit yleisimmin ilmenevät?
- Millä ulkoisilla tekijöillä tai organisaation ominaisuuksilla on vaikutusta rekrytointiprosessin tietosuojariskien todennäköisyyteen? (toimiala, yritysmuoto, organisaation koko, kilpailijoiden toiminta, organisaation arvot tms.)
- Millaisia vaikutuksia rekrytointiprosessin tietosuojariskien toteutumisella voi olla organisaatiolle?

4) TIETOSUOJARISKIEN HALLINTA

- Miten rekrytointiprosessin tietosuojariskejä voidaan hallita?
- Oletko hyödyntänyt rekrytointiprosessissa ISO 31000 -standardin mukaisia riskienhallintatyökaluja tietosuojan varmistamiseksi?
- Oletko hyödyntänyt rekrytointiprosessissa muita riskienhallintatyökaluja tietosuojan varmistamiseksi? Jos kyllä, mitä nämä olivat?
- Millä tavalla riskienhallintatyökalut edistävät tietosuojan toteutumista rekrytointiprosessissa?
- Nouseeko mieleesi muuta mainitsemisen arvoista rekrytointiprosessin tietosuojariskien hallinnasta?

Liite 3. Saatekirje

Vaasan yliopisto
UNIVERSITY OF VAASA

Talousoikeudellinen tutkimus tietosuojariskien hallinnasta rekrytointiprosessissa

Hyvä HR-alan ammattilainen,

Kiitos halustasi osallistua pro gradu -tutkielmani tekoon. Tästä saatekirjeestä löydät tietoa tutkimuksen tarkoituksesta, toteutustavasta sekä eettisistä linjauksista.

Mikä on tutkimuksen tarkoitus?
Pro gradu -tutkielmani tavoitteena on luoda lainsäädännön vaatimusten mukaisia ja liiketoiminnan tarpeet täyttäviä toimintaohjeistuksia siihen, miten työnhakijan henkilötietoihin kohdistuvia tietosuojariskejä voidaan hallita rekrytointiprosessissa. Tavoitteen saavuttamiseksi tutkielmassa nostetaan esille yleisimpiä rekrytointiprosessin tietosuojariskejä. Lisäksi tutkielmassa syvennytään siihen, miksi työnhakijan henkilötietojen kerääminen ja tietosuojariskien hallinta on perustelua.

Kuka toteuttaa tutkimuksen ja käyttää tutkimustuloksia?
Tutkimus toteutetaan osana Vaasan yliopiston talousoikeuden maisteriohjelmaa. Tulen hyödyntämään tutkimuksen aikana kerättyä materiaalia pro gradu- tutkielmani teossa, minkä jälkeen tutkielma arvioidaan yliopistolla sisäisten arviointiohjeiden mukaisesti. Valmis pro gradu -tutkielma julkaistaan Vaasan yliopiston avoimessa julkaisuarkistossa nimeltä Osuva. Täten tutkimustulokset tulevat olemaan julkisesti esillä.

Miten kerättyä aineistoa ja haastateltavien henkilötietoja käsitellään?
Haastateltavilta henkilöiltä kerättävää tutkimusaineistoa sekä haastateltavien henkilötietoja käsitellään Euroopan unionin yleisen tietosuoja-asetuksen 2016/679 vaatimusten mukaisesti. Tarkempi informaatio kerättävän aineiston ja henkilötietojen käsittelystä annetaan haastattelun alussa. Tutkimusaineiston ja henkilötietojen käsittely perustuu haastateltavien henkilöiden antamaan suostumukseen ja haastateltavana sinulla on myös oikeus vetäytyä tutkimuksesta. Kaikki haastateltavat ja heidän vastauksensa anonymisoidaan. Lisäksi tutkielmassa noudatetaan tutkimuseettisen neuvottelulautakunnan (TENK) asettamia tutkimusetiikan ohjeita sekä tutkimusetiikan eurooppalaisia käytäntöjä (The European Code of Conduct for Research Integrity).

Arvokkaasta tutkimusavustanne kiittäen,
Hanna Salo
puh. xxx
xxx@student.uwasa.fi