Minna Honkanen

Tietosuoja etätyössä

Laskentatoimen ja rahoituksen yksikkö
Talousoikeuden pro gradu -tutkielma
Talousoikeuden maisteriohjelma

Vaasa 2022

VAASAN YLIOPISTO
Laskentatoimen ja rahoituksen yksikkö
Tekijä: Minna Honkanen
Tutkielman nimi: Tietosuoja etätyössä
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Talousoikeus
Työn ohjaaja: Pekka Vainio
Valmistumisvuosi: 2022 **Sivumäärä:** 80

TIIVISTELMÄ:
Etätyö on työnteon muoto, jossa työtä suoritetaan osittain tai kokoaikaisesti työnantajan tilojen ulkopuolella. Etätyössä hyödynnetään tietoliikenneyhteyksiä, ja tavallisimmin työntekopaikkana on työntekijän koti. Työsuhteessa tehtävään etätyöhön sovelletaan samaa työlainsäädäntöä, kuin työnantajan tiloissa tehtävään työhön. Koronaviruspandemia muutti työnteon muotoja, ja ainakin osittainen etätyö on tullut monessa organisaatiossa jäädäkseen. Nopea siirtyminen etätyöhön pandemian alkaessa aiheutti sen, että tarkempi sopiminen etätyöstä jäi monessa organisaatiossa tekemättä.

Etätyön yleistymisen myötä henkilötietojen käsittelyä sisältäviä työtehtäviä tehdään yhä useammin työnantajan tilojen ulkopuolella. Tässä tutkimuksessa selvitetään, millaisia riskejä etätyö voi aiheuttaa tietosuojalle, mitä etätyössä tapahtuvasta henkilötietojen tietoturvaloukkauksesta aiheutuu rekisteröidylle, työnantajalle ja työntekijälle, sekä miten etätyön tietosuojariskejä voidaan ehkäistä. Tutkimusongelmaan pureudutaan lainopillisin eli oikeusdogmaattisin keinoin selvittämällä voimassa olevien oikeusnormien sisältöä tietosuojan ja etätyön kannalta. Merkittävin rooli on EU:n yleisellä tietosuoja-asetuksella, koska se muodostaa yhdessä tietosuojalain kanssa perustan tietosuojasääntelylle Suomessa.

Työnantajan vastuulla on varmistaa tarvittavat toimenpiteet tietojen suojaamiseksi etätyössä. Työnantajan on annettava etätyöntekijälle tiedot tietosuojaan liittyvästä lainsäädännöstä ja yrityssäännöistä. Työntekijä on velvollinen noudattamaan työnantajan ohjeita. Etätyössä työnantajan mahdollisuudet valvoa työtä ovat työntekijän yksityisyyden suojan ja kotirauhan vuoksi rajatummat, kuin työnantajan tiloissa tehtävässä työssä. Tutkimuksen myötä voidaan todeta etätyön olevan työnteon muoto, joka aiheuttaa henkilötietojen paljastumisen ulkopuolisille todennäköisemmin, kuin työnantajan tiloissa tehtävässä työssä. Työnantajan puutteelliset ohjeet tietosuojaa koskien, suojaamattomat tietoliikenneyhteydet ja työvälineet, työntekopaikka sekä henkilötietoja sisältävien asiakirjojen säilytys ja hävittäminen ovat tekijöitä, jotka voivat aiheuttaa henkilötietojen tietoturvaloukkauksen etätyössä. Erityistä huolellisuutta edellyttävät arkaluontoiset henkilötiedot.

Etätyössä henkilötietoja voidaan käsitellä turvallisesti, kun työnantaja on selvillä tietosuojasääntelyn asettamista edellytyksistä, ja huomioi etätyön osana henkilöstön tietosuojaohjeistusta. Etätyön huomioiminen tietosuojatyössä kannattaa, koska osaavalla henkilöstöllä varmistetaan lainmukaiset toiminta- ja asiakasprosessit sekä saavutetaan asiakkaiden ja sidosryhmien luottamus. Henkilötietojen tietoturvaloukkausten ehkäiseminen on kannattavaa myös siksi, että toteutuessaan ne voivat aiheuttaa aineellisia ja aineettomia vahinkoja maineen menettämisen ja taloudellisten tappioiden muodossa asiakkaalle, työnantajaorganisaatiolle ja työntekijälle.

AVAINSANAT: Tietosuoja, etätyö, henkilötiedot, tietoturva, tietovuodot

Sisällys

Kuviot

Taulukot

Lyhenteet

EIS	Euroopan neuvoston ihmisoikeussopimus
EU	Euroopan unioni
EY	Euroopan yhteisö
HE	Hallituksen esitys
KKO	Korkein oikeus
YK	Yhdistyneet kansakunnat

1 Johdanto

1.1 Tutkimusaiheen kuvaus ja tutkimuskysymykset

Työnteon paikkasidonnaisuus on muuttunut. Suomessa säännöllinen, kotona tehtävä etätyö on yleistynyt 2010-luvulla hiljalleen. Vuosina 2018 ja 2019 kotona työskentelevien osuus pysyi samalla tasolla ollen tällöin 14 prosenttia. Koronaviruspandemian myötä etätyöskentelyn määrä vuonna 2020 kaksinkertaistui, ja marraskuussa 2020 etätyötä ilmoitti tekevänsä 31 prosenttia työllisistä.[1] Parhaimmillaan noin puolet suomalaisista palkansaajista työskenteli etänä. Työntekijät toivovat etätyön jatkuvan myös pandemian jälkeen, sillä noin 90 prosenttia etätyötä tekevistä palkansaajista haluaisi jatkaa etätöitä vähintään neljäsosan työajastaan.[2]

Etätyö mahdollistaa työntekijälle muun muassa työaikaan ja työjärjestelyihin liittyvän vapauden ja joustavuuden, työn ja vapaa-ajan paremman yhdistämisen sekä säästöä työmatkakustannuksissa. Työmotivaatio ja työhyvinvointi lisääntyvät, kun työn ja vapaa-ajan yhdistäminen helpottuu. Toisaalta etätyö vähentää sosiaalisia kontakteja ja voi johtaa työyhteisöstä eristäytymiseen. Työ- ja vapaa-aika voivat sekoittua toisiinsa, ja työergonomia ei välttämättä ole samalla tasolla, kuin työpaikalla. Työnantajan kannalta etätyö voi lisätä teknisiä ongelmia ja tietoturvallisuusriskejä.[3]

Etätyön lisääntymisen myötä työntekijät, jotka käsittelevät työssään henkilötietojen suojaan kuuluvia tietoja, työskentelevät yhä useammin työnantajan tilojen sijaan esimerkiksi kotonaan. Tällöin työnantajan ohjeistus etätyön säännöistä ja erityisesti tietoturvallisuudesta etätyössä nousevat tärkeään asemaan. Työntekijällä itsellään on oikeus yksityisyyteen. Etätyössä korostuukin perustuslailla suojattua kotirauhaa koskevat

[1] Leskinen 2020.
[2] Sutela 2021.
[3] Helle 2004, s. 17–20, 25.

kysymykset, sillä etätyöntekijä työskentelee usein kotoansa käsin[4]. Työntekijän yksityisyyden suoja ja kotirauha rajoittavat työnantajan mahdollisuuksia selvittää työntekijän olosuhteita etätyössä. Tämän vuoksi työn valvominen vaikeutuu myös tietosuojaan liittyvien kysymysten osalta. Etätyössä tietosuojaan kohdistuu erilaisia riskejä lähityöhön verrattuna, ja henkilötietoja käsittelevän työntekijän oma toiminta ja ymmärrys tietosuojasääntelyyn liittyvistä seikoista nousevat merkittävään rooliin tietosuojan toteutumisessa.

Tämän tutkimuksen aiheena on tietosuoja etätyössä. Tutkimuksessa tarkastellaan lainsäädännön asettamia vaatimuksia henkilötietojen käsittelylle, ja heijastetaan näitä etätyöhön. Tutkimuksessa selvitetään, millaisia riskejä etätyö voi aiheuttaa tietosuojalle. Lisäksi selvitetään, mitä henkilötietoihin kohdistuvasta tietoturvaloukkauksesta voi seurata rekisteröidylle, rekisterinpitäjälle, henkilötietojen käsittelijälle ja työntekijälle, joka käsittelee työssään henkilötietoja rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa. Lopuksi tarkastellaan organisaation keinoja ehkäistä henkilötietoihin kohdistuvia tietoturvaloukkauksia. Tutkimuksessa vastataan seuraaviin kysymyksiin:

Mitä velvoitteita lainsäädäntö asettaa henkilötietojen käsittelylle etätyössä?
Millaisia riskejä tietosuojaan kohdistuu etätyössä?
Mitä etätyössä tapahtuneesta henkilötietojen tietoturvaloukkauksesta seuraa rekisteröidylle, rekisterinpitäjälle, henkilötietojen käsittelijälle ja työntekijälle?

1.2 Tutkimusmenetelmä ja lähdeaineisto

Tämän tutkimuksen tutkimusmenetelmänä on lainoppi eli oikeusdogmatiikka. Lainopin tehtävänä on tuottaa mahdollisimman varmaa tietoa oikeusjärjestyksen sisällöstä[5]. Lainopilla tutkitaan voimassa olevaa oikeutta selvittämällä oikeusnormien, eli

[4] Helle 2004, s. 199.
[5] Aarnio 2011, s. 12.

oikeussääntöjen ja oikeusperiaatteiden, sisältöä. Lainopin avulla selvitetään myös lain ja muiden oikeuslähteiden tarjoaman materiaalin merkitystä. Lisäksi lainoppi systematisoi voimassa olevaa oikeutta järjestämällä lainsäätäjän tuottamaa materiaalia oikeudenaloittain. Oikeusjärjestelmän yhtenäisyys ja johdonmukaisuus syntyy lainopin systematisoinnin kautta.[6]

Lainoppi sisältää praktisen ja teoreettisen ulottuvuuden. *Aarnio* käyttää näistä termejä käytännöllinen lainoppi ja teoreettinen lainoppi. Praktinen eli käytännöllinen lainoppi keskittyy perinteisesti oikeussääntöjen sisällön selvittämiseen eli tulkintaan, ja teoreettinen lainoppi puolestaan oikeussäännösten systematisointiin. Vaikka kummallakin lainopin ulottuvuudella on omat metodinsa, ovat ne vuorovaikutussuhteessa keskenään.[7] Teoreettisen lainopin avulla muodostetaan ja pidetään ajan tasalla eri alojen yleiset opit. Käytännöllisellä lainopilla testataan yleisten oppien pätevyys, jolloin selviää, mitä korjauksia yleisiin oppeihin täytyy tehdä. Teoreettisen lainopin ja käytännöllisen lainopin vuorovaikutussuhde lisää lainopin ymmärrystä oikeusjärjestyksestä, ja kasvattaa varmuutta oikeusjärjestyksen tulkintatavoista.[8] Tämän tutkimuksen menetelmä painottuu käytännölliseen lainoppiin, koska tutkimuksessa tulkitaan voimassa olevaa tietosuojalainsäädäntöä etätyön näkökulmasta.

Oikeuslähteet on perinteisesti jaettu vahvasti velvoittaviin, heikosti velvoittaviin ja sallittuihin oikeuslähteisiin. Vahvasti velvoittavia oikeuslähteitä ovat eduskunnan säätämät lait ja lain tasoiset säännökset. Vahvasti velvoittavat oikeuslähteet ovat ensisijaisia oikeuslähteitä, mutta jos ne eivät tarjoa yksiselitteistä ratkaisua oikeudelliseen ongelmaan, voidaan hyödyntää heikosti velvoittavia oikeuslähteitä. Heikosti velvoittavia oikeuslähteitä ovat hallituksen esitykset ja niitä koskevat mietinnöt ja lausunnot sekä oikeuskäytäntö. Vahvasti ja heikosti velvoittavien oikeuslähteiden lisäksi voidaan hyödyntää sallittuja oikeuslähteitä, joita ovat muun muassa oikeuskirjallisuudessa esitetyt argumentit,

[6] Hirvonen 2011, s. 21–25.
[7] Aarnio 1997, s. 36–37.
[8] Aarnio 2011, s. 104–105.

kansainväliset vertailukohdat ja reaaliset argumentit. Reaalisilla argumenteilla tarkoitetaan asia-argumentteja, esimerkiksi ratkaisuvaihtoehtojen seurauksilla argumentointia.[9]

Tässä tutkimuksessa hyödynnetään vahvasti velvoittavia, heikosti velvoittavia ja sallittuja oikeuslähteitä. Vahvasti velvoittavia oikeuslähteitä ovat aihealueeseen liittyvät lait, tärkeimpänä EU:n yleinen tietosuoja-asetus[10]. Heikosti velvoittavina oikeuslähteinä hyödynnetään muutamia oikeustapauksia, mukaan lukien tietosuojavaltuutetun päätöksiä. Lisäksi tutkimuksessa käytetään lähdemateriaalina oikeuskirjallisuutta ja liiketaloudellista kirjallisuutta.

1.3 Keskeiset käsitteet

Tämän tutkimuksen keskeisimmät käsitteet koostuvat etätyöhön ja tietosuojaan liittyvästä termistöstä. *Etätyöllä* tarkoitetaan sellaista työtä, jota tehdään varsinaisen työpaikan ulkopuolella. Etätyö voi olla jatkuvaa, satunnaista tai säännöllistä. Etätyön edellytyksenä joidenkin määritelmien mukaan on tietotekniikan käyttö työvälineenä. Työn on lisäksi oltava luonteensa puolesta sellaista, jota voisi tehdä myös työpaikalla.[11] Suomessa etätyön määritelmässä ei ole edellytetty tietotekniikan käyttöä[12]. Tyypillistä etätyölle ovat ajasta ja paikasta riippumattomat työjärjestelyt. Etätyössä siirretään tietoa ihmisten sijaan. Etätyön toimeksiantajana on työnantaja, joka voi olla yritys tai muu organisaatio.[13]

Tietoturvan ja tietoturvallisuuden tarkoituksena on varmistaa, että tiedot ovat käytettävissä, ne ovat oikeita ja niiden luvaton käyttö on estetty suojaamalla ne.

[9] Korpisaari 2016, s. 18–22.
[10] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27. päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).
[11] Vilkman 2016, luku 1.
[12] Helle 2004, s. 45.
[13] Salminen 1997, s. 11.

Tietoturvallisuuden katsotaan koostuvan usein tietojen saatavuudesta, eheydestä ja luottamuksellisuudesta.[14] Luottamuksellisuus tarkoittaa, että tieto on salassa pidettävää, ja ainoastaan sellaiset tahot, joilla on tiedonsaantioikeus ja käyttöoikeus tietoon, voivat saada sen käyttöönsä. Luottamuksellisuus voidaan toteuttaa esimerkiksi käyttöoikeuksien hallinnalla, jolloin käyttäjille annetaan työtehtävien hoitamisen perusteella tarpeelliset käyttöoikeudet järjestelmiin. Eheys tarkoittaa sitä, että tietoa ei muuteta hallitsemattomasti, vaan sitä voivat muuttaa sellaiset käyttäjät, joilla on tarvittava käyttöoikeus tiedon muuttamiseen. Saatavuus puolestaan merkitsee sitä, että tiedot ovat saatavilla niitä tarvitseville käyttäjille.[15] Tietoturva voidaan jakaa karkeasti tekniseen ja hallinnolliseen tietoturvaan. *Tietoturva ja tietosuoja* ovat kaksi erilaista kokonaisuutta.[16]

Tietosuoja (data protection) on vakiintunut ilmaisu kansainvälisesti, kun puhutaan henkilötietojen suojan oikeudellisesta sääntelystä. Tietosuoja turvaa luonnollisen henkilön eli *tiedon kohteen (data subject)* yksityisyyttä, oikeuksia ja etuja. Näin ollen tietosuoja ei suojaa ainoastaan tietoja. Tietosuoja-asetuksessa tai Suomen lain tasolla ei ole määritelty tietosuojaa käsitteenä. Ilmaisu on kuitenkin ollut Suomessa laajasti käytössä henkilörekisterilain[17] ja henkilötietolain[18] yhteydessä silloin, kun tarkoitetaan henkilötietojen käsittelyyn liittyviä oikeuksia ja velvollisuuksia koskevia säännöksiä. Laaja yksityisyyden suojaaminen on lähtökohtana tietosuojalainsäädännössä. Rekisteröidyn yksityisyyden suoja, oikeudet ja vapaudet ovat suojan kohteina tietosuoja-asetuksessa.[19] Tässä tutkimuksessa käsitteellä tietosuoja tarkoitetaan henkilötietojen suojaa.

Henkilötieto käsitteenä määritellään tietosuoja-asetuksen 4 artiklassa. Sen mukaan henkilötiedolla tarkoitetaan kaikkia luonnolliseen henkilöön liittyviä tietoja, joiden perusteella henkilö voidaan suoraan tai epäsuorasti tunnistaa. Nämä ovat niin sanottuja tunnistetietoja. Tunnistetietoja ovat esimerkiksi nimi, henkilötunnus, sijaintitieto tai

[14] Salminen 1997, s. 12.
[15] Rousku 2014, s. 47–50.
[16] Andreasson ja muut 2019, s. 133.
[17] Henkilörekisterilaki 471/1987, kumottu.
[18] Henkilötietolaki 523/1999, kumottu.
[19] Alapuranen 2020, s. 37–38.

verkkotunnistetieto. Myös henkilölle tunnusomaiset fyysiset, fysiologiset, geneettiset, psyykkiset, taloudelliset, kulttuuriset tai sosiaaliset tekijät ovat tunnistetietoja. Henkilötiedon käsite on laaja, sillä henkilötieto voi olla salainen tai julkinen. Tiedon ei tarvitse olla arkaluonteista tai intiimiä ollakseen henkilötieto, vaan ratkaisevaa on se, liittyykö tieto tunnistettavaan tai tunnistettavissa olevaan henkilöön.[20]

Henkilötietojen suoja kuuluu perusoikeuksien suojaan. Tietosuojalainsäädännöllä suojataan yksilöä, hänen yksityisyyttään ja tiedollista itsemääräämisoikeuttaan, jolloin on kyse henkilötietojen suojasta.[21] Henkilötietojen suoja sisältyy osittain yksityiselämän suojan piiriin, mutta kattaa laajemman alan, sillä henkilötietojen suojaan kuuluvat myös sellaiset henkilötiedot, jotka eivät sellaisinaan kuulu yksityiselämän suojaan. Esimerkiksi merkittävässä asemassa työskentelevän henkilön työpaikka tai työtehtävä kuuluu henkilötietojen suojan piiriin, mutta ei yksityisyyden suojaan.[22] Tässä tutkimuksessa henkilötietojen suojasta käytetään käsitettä tietosuoja.

Henkilötietojen tietoturvaloukkaus on tilanne, jossa jonkin tapahtuman seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, niitä luovutetaan luvattomasti tai niihin pääsee käsiksi sellainen taho, jolla ei ole käsittelyoikeutta kyseisiin tietoihin. Henkilötietojen tietoturvaloukkaus on kyseessä silloin, kun esimerkiksi henkilötietoja sisältävä USB-tikku häviää, ohjelmisto hakkeroidaan tai henkilötietoja sisältävä asiakirja postitetaan väärälle henkilölle.[23] Tässä tutkimuksessa käsitteellä *tietoturvaloukkaus* viitataan pääosin henkilötietojen tietoturvaloukkaukseen.

Henkilötietojen käsittelyllä tarkoitetaan kaikkia toimenpiteitä, jotka kohdistuvat henkilötietoihin aina niiden keräämisestä tuhoamiseen[24]. Tietosuoja-asetuksen 4 artiklassa henkilötietojen käsittely on määritelty seuraavasti:

---

[20] Korpisaari ja muut 2018, s. 53.
[21] Alapuranen 2020, s. 38.
[22] Korpisaari ja muut 2018, s. 5–6.
[23] Tietosuojavaltuutetun toimisto 2021a.
[24] Alapuranen 2020, s. 41.

> Tässä asetuksessa tarkoitetaan käsittelyllä toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten 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.

Rekisterinpitäjä on luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot yksin tai yhdessä toisten kanssa. *Henkilötietojen käsittelijä* tarkoittaa tahoa, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Yleensä kysymyksessä on toimeksianto- tai alihankintasuhde, jossa organisaatio rekisterinpitäjänä ulkoistaa henkilötietojen käsittelyn joltain osin henkilötietojen käsittelijälle. Esimerkkinä tällaisesta tilanteesta on ulkoistettu palkanmaksu. Rekisterinpitäjä on tällöin työnantaja, ja henkilötietojen käsittelijä palkanlaskennan ja palkanmaksun hoitava yritys. Työntekijä ei näin ollen ole henkilötietojen käsittelijä, vaan rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva henkilö.[25]

Henkilörekisteri tarkoittaa tietosuoja-asetuksen 4 artiklan mukaan mitä tahansa tietojoukkoa, joka on jäsennelty ja sisältää henkilötietoja. Tiedot ovat saatavissa rekisteristä tietyin perustein riippumatta siitä, onko tietojoukko keskitetty, hajautettu tai jaettu toiminnallisien tai maantieteellisten perusteiden mukaan. *Rekisteröity* tarkoittaa tietosuoja-asetuksen 4 artiklan mukaan luonnollista henkilöä, jota henkilötieto koskee.

1.4 Tutkielman rakenne

Tutkimus koostuu viidestä pääluvusta, joista ensimmäinen on johdanto. Johdannossa avataan tutkimusaihe ja tutkimuskysymykset, tutkimusmenetelmä ja käytettävä lähdeaineisto, tutkimuksen kannalta keskeisimmät käsitteet ja tutkimuksen rakenne.

[25] Alapuranen 2020, s. 42–44.

Johdannon jälkeen toisessa pääluvussa käsitellään tutkimusaiheeseen liittyvää oikeudellista sääntelyä omina kokonaisuuksiinaan, eli henkilötietojen suojan ja etätyön sääntelyä. Henkilötietojen suojaa koskevaa tietosuojalainsäädäntöä lähestytään taustoittamalla henkilötietojen suojan lainsäädännöllistä kehitystä menneisyydestä nykypäivän sääntelyyn. Tämän jälkeen käsitellään henkilötietojen suojaa perusoikeutena, sillä ihmis- ja perusoikeuksien merkityksen kasvu on vaikuttanut tietosuojalainsäädännön kehitykseen. Henkilötietosuojan perusoikeudellisen aseman tarkastelun jälkeen edetään tämän hetkiseen oikeudelliseen sääntelyyn, josta merkittävin rooli on EU:n yleisellä tietosuoja-asetuksella. Tietosuoja-asetusta tarkastellaan erityisesti sen tarkoituksen, henkilötietojen käsittelyn periaatteiden, rekisteröidyn oikeuksien ja rekisterinpitäjän velvollisuuksien osalta, sillä nämä ovat oleellisia asioita henkilötietojen lainmukaisessa käsittelyssä. Käsittelyn periaatteita, rekisteröidyn oikeuksia ja rekisterinpitäjän velvollisuuksia heijastetaan etätyöhön.

Toisen pääluvun alaluvuissa neljä ja viisi käsitellään etätyön asemaa lainsäädännössä ja etätyöhön liittyvää eurooppatasoista sopimusta. Etätyön oikeudellista asemaa koskevien alalukujen jälkeen siirrytään kolmanteen päälukuun, jossa käsitellään etätyön aiheuttamia tietosuojariskejä riskityyppi kerrallaan. Neljännessä pääluvussa tarkastellaan mitä seurauksia rekisteröidylle, rekisterinpitäjälle, henkilötietojen käsittelijälle ja rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa henkilötietoja käsittelevälle työntekijälle voi aiheutua, jos kolmannessa pääluvussa läpikäydyt etätyön riskit tietosuojalle toteutuvat ja henkilötietojen tietoturvaa loukataan. Viimeisenä neljännessä pääluvussa käsitellään organisaation keinoja ehkäistä tietojasuojariskejä ja keinoja varautua niihin. Viimeisenä tutkimuksessa on viides pääluku, jossa koostetaan yhteenvedoksi oleellisimmat asiat käsitellyistä aihepiireistä ja johtopäätöksistä.

2 Tietosuojan ja etätyön oikeudellinen sääntely

2.1 Tietosuojasääntelyn taustaa

Henkilötietojen suojaan liittyviin ongelmiin herättiin 1970-luvulla tietotekniikan kehityksen ja automaattisen tietojenkäsittelyn käyttöönoton seurauksena. Kiinnostus henkilötietojen suojaan oli sekä kansainvälistä että kansallista, ja uudet oikeudelliset ongelmat aiheuttivat tarpeen lainsäädännön kehittämiselle. Henkilörekisterilaki hyväksyttiin Suomessa vuonna 1987, ja se astui voimaan tammikuussa 1988. Lakia säädettäessä huomioitiin kansainväliset sopimukset ja suositukset. Henkilörekisterilaki oli yleislaki, jota sovellettiin silloin, kun muissa laeissa tai ennen sitä annetuissa asetuksissa ei toisin säädetty. Tämän niin sanotun toisen polven tietosuojalain periaatteet ovat edelleen nähtävissä henkilötietosuojalainsäädännössä. Näitä periaatteita ovat muun muassa rekisterinpidon itsesääntelyperiaatteen toteuttaminen ja hyvä rekisteritapa. Myös tarpeellisuusvaatimus koskien henkilörekistereitä ja niiden sisältämiä tietoja, arkaluonteisten tietojen rekisteröinnin rajoittaminen, virheellisten tietojen oikaisuvelvollisuus, tietojen luovutusrajoitukset, tietojen suojausvelvollisuus, vanhojen henkilörekisterien hävittämisvelvollisuus, rekisteröidyn oikeus tarkastaa häntä koskevat tiedot sekä oikeus kieltää tietojensa luovuttaminen suoramarkkinointia varten ovat edelleen nähtävissä lainsäädännössä.[26]

Henkilörekisterilakia seurasi henkilötietolaki. Tarve lainsäädännön uudistamiselle syntyi Euroopan yhteisön hyväksyttyä vuonna 1995 henkilötietodirektiivin[27], jota kutsuttiin myös tietosuojadirektiiviksi. Kansallinen perusoikeusjärjestelmä uusittiin samana vuonna. Yksilön perusoikeuksien ja -vapauksien korostuminen sekä henkilötietodirektiivi vaikuttivat henkilötietojen käsittelyyn. Henkilörekisterilaki ei vastannut enää täysin vaatimuksia. Henkilötietolaki tuli voimaan kesäkuussa 1999.[28] Sen myötä lisättiin

[26] Alapuranen 2020, s. 12.
[27] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja niiden tietojen vapaasta liikkuvuudesta.
[28] Alapuranen 2020, s. 13.

rekisteröityjen tiedonsaantioikeuksia, ja rekisterinpitäjän oli annettava rekisteröidylle oma-aloitteisesti ja aiempaa laajemmin tietoja häntä koskevien tietojen käyttötarkoituksista[29].

Henkilötietodirektiivin myötä EU:n jäsenvaltioiden välillä oli eroavaisuuksia henkilötietojen suojan sääntelyssä. Euroopan komissio julkaisi tammikuussa 2012 ehdotuksen uudeksi henkilötietojen suojaa koskevaksi sääntelyksi.[30] EU:n yleinen tietosuoja-asetus astui voimaan 24.5.2016. Kansallisella tasolla sitä alettiin soveltaa 25.5.2018. Henkilötietodirektiivin aiheuttamien eroavaisuuksien lisäksi haluttiin vahvistaa rekisteröityjen itsemääräämisoikeutta ja luoda EU:lle tietosuojakehys, joka olisi ajanmukainen, vahva, kattava ja yhtenäinen. Tietosuoja-asetus nähtiin keinona lujittaa digitaalisia sisämarkkinoita parantamalla luottamusta online-palveluihin. Lisäksi haluttiin tehostaa tietosuojasääntöjen täytäntöönpanon valvomista.[31] Tietosuoja-asetus muodostaa tällä hetkellä merkittävän osan henkilötietosuojan oikeudellisesta sääntelystä, sillä se velvoittaa kaikkia EU:n jäsenvaltioita, ja sitä sovelletaan kaikilta osin sellaisenaan[32].

2.2 Henkilötietojen suoja perusoikeutena

Henkilötietojen suoja liittyy tiiviisti ihmis- ja perusoikeuksiin. Ihmisoikeuksilla tarkoitetaan tiivistetysti kaikille ihmisille kaikkialla peruuttamattomasti ja luovuttamattomasti kuuluvia oikeuksia. Tarkemmin ottaen ihmisoikeudet ovat yleismaailmallisia, luovuttamattomia, jakamattomia ja perustavanlaatuisia. Tämä tarkoittaa sitä, että ne kuuluvat jokaiselle ihmiselle kaikkialla maailmassa, niitä ei voida ottaa pois esivallan päätöksellä tai edes ihmisen omalla suostumuksella, ne ovat keskenään yhtä tärkeitä ja niissä on pohjimmiltaan kysymys sekä vapaudesta jostakin että oikeudesta johonkin.[33] Kansainvälisillä sopimuksilla ja valvontamekanismeilla määritellään ja valvotaan ihmisoikeuksien

[29] HE 96/1998, s. 1.
[30] Alapuranen 2020, s. 13.
[31] Andreasson ja muut 2019, s. 27.
[32] Korpisaari ja muut 2018, s. 7.
[33] Ihmisoikeusliitto 2021.

toteutumista. Yhdistyneiden kansakuntien ihmisoikeuksien julistus sekä muut sen piirissä tehdyt sopimukset ihmisoikeuksista ovat keskeisimpiä sopimuksia. Euroopassa tärkein on Euroopan neuvoston ihmisoikeussopimus (jäljempänä EIS). Sopimusta valvoo Euroopan ihmisoikeustuomioistuin.[34] Henkilötietojen suojaan tiiviisti liittyvä ihmisoikeus on oikeus yksityisyyteen, eli yksityisyyden suoja.

Ihmisoikeudet asettavat minimitason lainsäädäntövaatimuksiin, kun taas perusoikeuksilla voidaan ylittää ihmisoikeuksilla turvattu minimitaso. Perusoikeuksilla tarkoitetaan oikeuksia, jotka on säädetty kansallisessa lainsäädännössä ja kuuluvat kaikille kyseisen valtion lainkäyttöpiirissä oleville ihmisille. Suomen lainsäädännössä perusoikeudet on turvattu perustuslaissa[35].[36] Kansalliset perusoikeudet muotoiltiin nykyiseen muotoonsa vuoden 1995 perusoikeusuudistuksen myötä. Uudistuksen taustalla oli perusoikeuksien vanhentuneisuus kansainvälisiin sopimuksiin nähden. Myös toisen maailmansodan jälkeinen eurooppalainen valtiosääntökehitys ja Euroopan yhdentymiskehitys lisäsivät tarvetta kansallisen perusoikeusjärjestelmän uudistamiselle.[37] Henkilötietojen suoja tuli uudistuksen myötä kansalliseksi perusoikeudeksi. Perustuslain 10.1 §:n mukaan ”jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla”.

Perustuslain lisäksi Suomi on EU:n jäsenvaltiona sitoutunut Euroopan unionin perusoikeuskirjaan[38], joka laadittiin vuonna 2000. Ennen perusoikeuskirjaa EU-oikeus keskittyi lähinnä taloutta koskeviin perusvapauksiin, eli ihmisten, tavaroiden, palveluiden ja pääomien vapaaseen liikkuvuuteen. Euroopan yhteisöjen tuomioistuimen ja EU-tuomioistuimen ratkaisukäytäntöön perusoikeudet kuuluivat jo ennen perusoikeuskirjaakin. Perusoikeudet saavuttivat kuitenkin vahvemman aseman EU-oikeudessa perusoikeuskirjan myötä, ja nykyisen asemansa ne saivat vuonna 2007 hyväksytyn ja 2009 voimaantulleen

[34] Neuvonen 2019, s. 56.
[35] Suomen perustuslaki 731/1999.
[36] Neuvonen 2019, s. 56.
[37] Andreasson ja muut 2016, s. 31.
[38] Euroopan Unionin perusoikeuskirja 2000/C/364/01.

Lissabonin sopimuksen myötä.[39] Lissabonin sopimuksessa perusoikeuskirjalla todettiin olevan sama oikeudellinen arvo kuin perussopimuksellakin. Näin alun perin poliittinen perusoikeuskirja muuttui oikeudellisesti sitovaksi. Henkilötietojen suoja sai oman artiklan perusoikeuskirjaan Lissabonin sopimuksen myötä, ja henkilötietojen suojasta tuli yksiselitteinen perusoikeus EU:ssa.[40] EU:n perusoikeuskirjan 8 artikla sääntelee henkilötietojen suojaa seuraavasti:

> 1. Jokaisella on oikeus henkilötietojensa suojaan.
> 2. Tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi.
> 3. Riippumaton viranomainen valvoo näiden sääntöjen noudattamista

Henkilötietojen suoja on osa yksityisyyden suojaa. Yksityisyyden suoja on turvattu perustuslain 10.1 §:n lisäksi EIS:ssa ja EU:n perusoikeuskirjassa. EIS:n 8.1 artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa liittyvää kunnioitusta. EU:n perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan. YK:n ihmisoikeusjulistuksessa yksityisyyden suoja turvataan artiklassa 12. Sen mukaan kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa puuttua mielivaltaisesti, eikä kenenkään kunniaa ja mainetta tule loukata.

Yksilön oikeus solmia ja ylläpitää suhteita vapaasti muihin ihmisiin ja ympäristöön, sekä itsestään ja omista toimistaan määrääminen kuuluvat yksityisyyden suojaan. Taustalla on ajatus yksilön oikeudesta elää elämäänsä ilman viranomaisten tai muiden ulkoisten tahojen mielivaltaista tai aiheetonta puuttumista siihen.[41] Yksityisyys on kokonaisuutena laaja, sillä se kattaa fyysisen tilan lisäksi tiedollisen ulottuvuuden. Kotirauha,

[39] Neuvonen 2019, s. 61–62.
[40] Alapuranen 2020, s. 14.
[41] Alapuranen 2020, s. 32.

henkilötietojen suoja ja viestintätietojen suoja ovat esimerkkejä yksityisyyden suojan osa-alueista.[42]

Itsemääräämisoikeuden voidaan katsoa liittyvän yksityisyyden suojaan, vaikka se ei sellaisenaan ole perusoikeutena perustuslaissa. Yksityisyyden suoja turvaa itsemääräämisoikeuden perustuslain muiden säännösten kanssa. Esimerkiksi perustuslain 7 § :ssä säädetään jokaisen oikeudesta elämään sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen.[43] Itsemääräämisoikeus koostuu oikeudesta tietää, oikeudesta tietoon sekä tiedollisesta itsemääräämisoikeudesta. Itsemääräämisoikeuden vapaa ja tehokas käyttö oikeusvaltiossa edellyttää oikeutta tietää, joten oikeus tietää on avaintekijänä itsemääräämisoikeuden toteutumisessa. Jotta yksilön oikeus tietää toteutuisi, on yksilöllä oltava myös oikeus tietoon. Oikeutta tietoon ilmentää muun muassa perustuslain 12.2 §, jonka mukaan viranomaisen asiakirjat tai muut tallenteet ovat julkisia, ellei niiden julkisuutta ole lailla erikseen rajoitettu välttämättömien syiden vuoksi. Jokaisella on oikeus saada tietoa julkisesta asiakirjasta tai tallenteesta. Tiedollinen itsemääräämisoikeus tarkoittaa sitä, että yksilöllä on halutessaan oikeus olla yhteiskunnassa yksin sekä fyysisesti että tiedollisesti. Oikeus luottamukselliseen viestintään ja oikeus henkilötietojen suojaan perusoikeuksina turvaavat tiedollista itsemääräämisoikeutta. Yksilöllä on lähtökohtaisesti oikeus määrätä itseään koskevasta informaatiosta, ja siihen puuttumisesta on säädettävä erikseen laissa.[44]

2.3 EU:n yleinen tietosuoja-asetus

Tärkein tietosuojasääntelyyn liittyvä säädös Suomessa on EU:n yleinen tietosuoja-asetus (General Data Protection Regulation, GDPR). Tietosuoja-asetus ja kansallinen

[42] Neuvonen 2019, s. 26.
[43] Neuvonen 2019, s. 118.
[44] Saarenpää 2016, s. 213–216.

tietosuojalaki[45] muodostavat perustan tietosuojan yleissääntelylle Suomessa[46]. Lisäksi henkilötietojen suojasta säädetään useissa erityislaeissa. Erikoislainsäädännössä säädetään muun muassa eri rekistereistä ja viranomaisten rekistereistä. Kokonaisuus on näin ollen hajanainen ja tekninen.[47] Henkilötietojen käsittelyä koskevia lakeja ja yksittäisiä lain säännöksiä ovat esimerkiksi laki yksityisyyden suojasta työelämässä[48] eli niin sanottu työelämän tietosuojalaki, laki henkilötietojen käsittelystä poliisitoimessa[49] ja laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä[50]. Sääntelyn hajanaisuus on aiheuttanut epäselvyyksiä yksityisyyden ja julkisuuden keskinäisestä suhteesta. Myös viranomaisten toimivaltuudet informaation käsittelyssä ovat jääneet epätietoisuuteen. Sääntelyn hajanaisuus haastaa tietosuojasääntelyn sisällön kokonaisuuden hallintaa ja sitä kautta oikeaa soveltamista. Tämä vaikeuttaa myös tehokkaaseen informaatiohallintoon siirtymistä.[51] Hajanaisuuden lisäksi tietosuoja-asetuksen ja kansallisen tietosuojalain tähän mennessä lyhyt voimassaoloaika vaikuttaa siihen, että tietosuojaan liittyvät tulkinnat ja käytännöt etsivät vielä paikkaansa. Tulkinnassa onkin oleellista tunnistaa sääntelyn tavoitteet ja henkilötietolain systematiikka, jotta muun lainsäädännön sääntelyä on mahdollista analysoida.[52]

EU:n yleinen tietosuoja-asetus jättää jäsenvaltioille kansallista liikkumavaraa. Liikkumavaraa on kuitenkin aiempaan henkilötietodirektiiviin verrattuna vähemmän, sillä tietosuoja-asetus on jäsenvaltioissa suoraan velvoittavaa lainsäädäntöä. Suomessa tietosuoja-asetusta täydennetään ja täsmennetään aiemmin mainitulla kansallisella tietosuojalailla. Laki tuli voimaan 1.1.2019, ja sitä sovelletaan rinnakkain EU:n yleisen tietosuoja-asetuksen kanssa. Tietosuojalaissa säädetään muun muassa kansallisesta

[45] Tietosuojalaki 1050/2018.
[46] Andreasson ja muut 2019, s. 28.
[47] Neuvonen 2019, s. 233.
[48] Laki yksityisyyden suojasta työelämässä 759/2004.
[49] Laki henkilötietojen käsittelystä poliisitoimessa 616/2019.
[50] Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 784/2021.
[51] Korpisaari ja muut 2018, s. 3.
[52] Neuvonen 2019, s. 233.

valvontaviranomaisesta sekä sovitetaan yhteen henkilötietojen suojaa ja muita oikeuksia, kuten sananvapautta ja julkisuusperiaatetta suhteessa henkilötietojen suojaan.[53]

2.3.1 Tietosuoja-asetuksen tarkoitus

EU:n yleisen tietosuoja-asetuksen tarkoitukset ovat moninaiset. Sillä halutaan tukea vapautta ja turvallisuutta sekä luonnollisten henkilöiden hyvinvointia. Lisäksi talousunionin kehittäminen, taloudellinen ja sosiaalinen edistys, talouksien lähentäminen ja lujittaminen sisämarkkinoilla sekä oikeuden alueen kehittäminen vaikuttavat tietosuoja-asetuksen taustalla. Erityisesti yksityisen ihmisen oikeus omiin tietoihinsa halutaan tasapainottaa sen kanssa, että yritykset ja muut toimijat voivat kuitenkin käyttää tietoja yhteiskunnallisesti hyödyllisellä tavalla. Tarkoituksena ei näin ollen ole estää liiketoimintaa, joka perustuu henkilötietojen käsittelyyn, vaan luoda sille lailliset puitteet. Sisämarkkinoiden kehitystä pyritään edistämään henkilötietojen suojalla, sillä tietosuoja-asetuksen 1 artiklan kohdassa 3 todetaan, että henkilötietojen vapaata liikkuvuutta unionin sisällä ei saa rajoittaa eikä kieltää henkilötietojen käsittelyyn liittyvistä syistä.[54]

Tietosuoja-asetuksella pyritään siihen, että sen avulla vahvistetaan entisestään yksityisyydensuojaa verkkoympäristössä ja edesautetaan Euroopan digitaalitalouden kasvua. Uudistuksen katsotaan tukevan talouskasvua, työllisyyttä ja innovaatioita, sekä vähentävän yritysten hallintokustannuksia. Lisäksi halutaan lujittaa kuluttajien verkkoympäristöön kohdistuvaa luottamusta. Tavoitteet tietosuoja-asetukselle ovat näin ollen laajemmat, kuin yksilön yksityiselämän ja tietosuojan turvaaminen.[55]

Henkilötietoja jaetaan ja kerätään nykyisin aikaisempaan verrattuna merkittävästi enemmän teknologian nopean kehityksen ja globalisaation vuoksi. Tämä on tuonut osaltaan uusia haasteita henkilötietojen suojeluun. Henkilötietoja voidaan käyttää

[53] Andreasson ja muut 2019, s. 36–38.
[54] Korpisaari ja muut 2018, s. 34–35.
[55] Korpisaari ja muut 2018, s. 35.

organisaatioiden toiminnassa ennennäkemättömän laajasti teknologian ansiosta. Myös ihmiset itse saattavat omia henkilötietojaan julkisuuteen maailmanlaajuisesti muun muassa sosiaalisen median välityksellä. Tietosuoja-asetus pyrkii vastaamaan näistä toimista aiheutuviin tarpeisiin EU:n alueella digitaalitalouden kehittymiseksi, koska jäsenvaltiot eivät voi ainoastaan kansallisella lainsäädännöllä saavuttaa EU:n tavoitteita luonnollisten henkilöiden yhdenmukaisessa suojelussa ja henkilötietojen vapaassa liikkuvuudessa EU:ssa.[56]

Tietosuoja-asetus perustuu *riskiperusteiseen lähestymistapaan*. Riskiperusteinen lähestymistapa tarkoittaa sitä, että tietosuoja-asetuksen velvoitteita ja asianmukaisia suojatoimia on tarkasteltava suhteessa henkilötietojen käsittelystä rekisteröidyn oikeuksille ja velvollisuuksille aiheutuvaan riskiin. Rekisteröidyn suoja korkean riskin toiminnassa halutaan varmistaa, mutta toisaalta tavoitteena on välttää vähäriskisten toimien ylisääntelyä. Tietojen laatua, luonnetta, käsittelytarkoitusta ja laajuutta arvioidaan, kun tarkastellaan aiheutuvaa riskiä. Mitä tunnistettavammassa muodossa tieto on ja mitä yksilöivämpään ja pitkäaikaisempaan käyttöön sitä käsitellään, sitä suuremmat ovat myös riskit ja näin ollen myös velvoitteet sekä edellytetyt suojakeinot.[57]

Riskiperusteisen lähestymistavan lisäksi tietosuoja-asetuksen lähtökohtana on, että tietosuoja on oletusarvoista ja sisäänrakennettua. Tietosuoja-asetuksen johdannon kohdassa 78 avataan oletusarvoisen ja sisäänrakennetun tietosuojan tarkoitusta. Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet osoittaakseen, että tietosuoja-asetusta on noudatettu. Sovellusten, palvelujen ja tuotteiden suunnittelemisessa ja kehittämisessä tulisi ottaa huomioon tietosuojavelvoitteet, jos sovellukset, palvelut tai tuotteet perustuvat henkilötietojen käsittelyyn tai käsittelevät henkilötietoja tehtävänsä täyttämiseksi.

[56] Korpisaari ja muut 2018, s. 37.
[57] Andreasson ja muut 2019, s. 28–29.

Tietosuoja-asetuksen tarkoituksena ei ole se, että oikeus henkilötietojen suojaan on absoluuttinen. Henkilötietojen suojan on sen sijaan oltava oikeassa suhteessa sen tehtävään yhteiskunnassa ja oikeassa suhteessa muihin perusoikeuksiin verrattuna. Asetuksessa pyritään kunnioittamaan kaikkia perusoikeuksia sekä ottamaan huomioon EU:n perusoikeuskirjan vapaudet ja periaatteet. Huomioitavia vapauksia ja periaatteita ovat jokaisen oikeus yksityis- ja perhe-elämään, kodin ja viestinnän kunnioittaminen, oikeus henkilötietojen suojaan, ajatuksen, omantunnon ja uskonnon vapaus, sananvapaus ja tiedonvälityksen vapaus, elinkeinovapaus, oikeus tehokkaisiin oikeussuojakeinoihin ja oikeudenmukaiseen oikeudenkäyntiin sekä oikeus kulttuuriseen, uskonnolliseen ja kielelliseen monimuotoisuuteen.[58]

2.3.2 Henkilötietojen käsittelyn periaatteet

Henkilötietojen käsittelyyn liittyy EU:n yleisessä tietosuoja-asetuksessa määritellyt periaatteet, joiden varaan koko tietosuoja-asetus rakentuu. Nämä tietosuojaperiaatteet ilmaisevat lainsäädännön perussisällön, mutta samalla niillä on itsessään suoraa normatiivista voimaa. Periaatteet ovat osin päällekkäisiä.[59] Käsittelyä koskevista periaatteista säädetään tietosuoja-asetuksen 5 artiklassa kohdissa 1 ja 2, joista kohta 1 sisältää kuusi alakohtaa (kohdat a-f). Henkilötietojen käsittelyä koskevat periaatteet ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus sekä osoitusvelvollisuus. Näitä periaatteita tulee noudattaa aina henkilötietoja käsiteltäessä, myös etätyössä. Etätyössä työnantajan mahdollisuudet valvoa työntekijän työtä ovat joiltain osin rajoitetumpia, kuin lähityössä. Työnantaja ei rekisterinpitäjänä kykene valvomaan täysin sitä, miten työntekijä käsittelee henkilötietoja. Tärkeää onkin, että työnantaja informoi työntekijää henkilötietojen käsittelylle asetetuista vaatimuksista, jotta työntekijä voi noudattaa henkilötietojen käsittelyn periaatteita huolellisesti etätyössä.

[58] Korpisaari ja muut 2018, s. 36.
[59] Alapuranen 2020, s. 50.

Tietosuoja-asetuksen 5 artiklan a alakohdan mukaan käsittelyn on oltava *lainmukaista, kohtuullista ja läpinäkyvää.* Rekisteröidyn edut on otettava huomioon henkilötietojen käsittelyssä, eikä tietoja saa väärinkäyttää. Käsittelylle on lainmukainen peruste ainoastaan, kun jokin tietosuoja-asetuksen 6 artiklassa säädetty käsittelyn edellytys täyttyy. Suhteellisuus ja tietynlainen tasapaino ovat edellytyksenä kohtuullisuusperiaatteen toteutumiselle. Läpinäkyvyyden periaate turvaa käsittelyn avoimuutta, kun yksilöllä on mahdollisuus valvoa itseään koskevien tietojen käsittelyä. Tässä auttaa rekisterinpitäjän velvollisuus informoida rekisteröityä henkilötietojen käsittelyssä.[60]

Etätyössä lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaate toteutuu silloin, kun henkilötietoja käsitellään tietosuoja-asetuksen ja muun tilanteeseen sovellettavan kansallisen lainsäädännön mukaisesti. Läpinäkyvää käsittely etänä on silloin, kun se on rekisteröidyn kannalta läpinäkyvää. Etätyö ei voi olla syynä esimerkiksi sille, että rekisteröidyllä ei olisi mahdollisuutta tietää, mitä tietoja hänestä kerätään ja mihin tarkoitukseen niitä käsitellään. Kohtuullisuus eli eräänlainen reiluus henkilötietojen käsittelyssä etätyössä toteutuu, kun rekisteröidyn edut huomioidaan ja tietoja ei väärinkäytetä[61].

Käyttötarkoitussidonnaisuudesta säädetään 5 artiklan alakohdassa b. Käyttötarkoitussidonnaisuus tarkoittaa sitä, että henkilötiedot kerätään tiettyä, nimettyä ja laillista käyttötarkoitusta varten. Henkilötietoja ei saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla. Kuitenkaan arkistointia, tieteellistä tai historiallista tutkimusta tai tilastollista tarkoitusta varten käyttöä ei katsota sopimattomaksi alkuperäisen tarkoituksen kanssa. Tästä säädetään erikseen tietosuoja-asetuksen 89 artiklan kohdassa 1. Käyttötarkoitussidonnaisuuden tehtävänä on suojata rekisteröityjen oikeuksia heitä koskevien henkilötietojen käsittelyn suhteen, sekä toisaalta mahdollistaa rekisterinpitäjälle henkilötietojen käsittely jatkossa tietyissä rajoissa. [62]

[60] Alapuranen 2020, s. 50–51, 53.
[61] Alapuranen 2020, s. 50.
[62] Korpisaari ja muut 2018, s. 92.

Käyttötarkoitussidonnaisuus on yhteydessä suunnitelmallisuuden periaatteeseen. Henkilötietoja on käsiteltävä vain ennalta määriteltyjen tarkoitusten mukaisesti, ja vastuussa määrittelystä on rekisterinpitäjä. Jos ulkopuolinen taho, eli henkilötietojen käsittelijä, käsittelee henkilötietoja rekisterinpitäjän lukuun, se ei saa käyttää käsiteltäviä tietoja muihin käyttötarkoituksiin, kuin mihin rekisterinpitäjä on ennalta määrittänyt tietoja käytettävän.[63]

Tietojen minimointi on tietosuoja-asetuksen 5 artiklan c alakohdassa säädetty periaate, joka edellyttää, että henkilötiedot ovat asianmukaisia, olennaisia ja rajoitettuja siihen nähden, mikä niiden käyttötarkoitus on. Tietojen minimointi on näin ollen yhteydessä tarpeellisuuden vaatimukseen. Henkilötietojen käsittelyssä on huomioitava tietojen käyttötarkoitus, sillä minimointiperiaatteen mukaan tietoja on käsiteltävä mahdollisimman vähän ja niitä tulee säilyttää mahdollisimman lyhyt aika.[64] Tietojen minimoinnin periaate toteutuu, kun henkilötiedot eivät ole liian laajoja käsittelyn tarkoitukseen nähden, ja ne poistetaan rekisteristä, kun niitä ei enää tarvita[65]. Tämä on huomioitava myös etätyössä. Vaikka valtaosa henkilötietoja sisältävistä rekistereistä on nykyisin sähköisessä muodossa, voi työntekijälle tulla eteen tilanne, että hän joutuu tulostamaan henkilötietoja sisältäviä asiakirjoja työtään varten. Henkilötietoja sisältävät asiakirjat tulee myös etätyössä hävittää turvallisesti heti, kun tietoja ei enää tarvita.

Täsmällisyyden periaatteesta säädetään tietosuoja-asetuksen 5 artiklan d alakohdassa. Sen mukaan henkilötietojen on oltava täsmällisiä ja tarpeen vaatiessa päivitettyjä. Kaikkien kohtuullisten toimenpiteiden avulla on varmistettava, että käsittelyn tarkoituksiin nähden epätarkat tai virheelliset tiedot poistetaan tai vaihtoehtoisesti oikaistaan viipymättä. Täsmällisyyden periaate edellyttää rekisterinpitäjää käymään säännöllisesti läpi henkilötietoja varmistaen tällä tavoin tietojen ajantasaisuuden[66]. Vaikka rekisterinpitäjän vastuulla onkin kohtuullisin toimenpitein varmistaa, että käsittelyn tarkoituksiin

[63] Alapuranen 2020, s. 57.
[64] Alapuranen 2020, s. 61.
[65] Korpisaari ja muut 2018, s. 93.
[66] Korpisaari ja muut 2018, s. 93.

nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan, on työntekijän hyvä tiedostaa tämä käsitellessään henkilötietoja. Jos etätyöntekijä huomaa, että käytössä on liian laajoja, epätarkkoja tai virheellisiä tietoja käsittelyn tarkoituksiin nähden, on tietojen minimoinnin ja täsmällisyyden periaatteiden noudattamiseksi tiedot korjattava oikeiksi tai poistettava ne. Jos työntekijä ei ole varma, ovatko tiedot virheellisiä tai liian laajoja ja vaativatko ne näin ollen poistamista, hän voi varmistaa asian työnantajaltaan.

Säilytyksen rajoittaminen edellyttää sitä, että henkilötietojen säilytysajan tulee olla mahdollisimman lyhyt. Jos peruste tietojen käsittelemiselle jatkuu, voi tietojen säilyttämisaika olla pitkäkin. Rekisterinpitäjällä voi olla jopa lakiin perustuva velvollisuus säilyttää tietoja tietyn ajan.[67] Säilytyksen rajoittamisesta säädetään tietosuoja-asetuksen 5 artiklan e alakohdassa. Sen mukaan henkilötietoja on säilytettävä niin, että rekisteröity on niistä tunnistettavissa ainoastaan niin kauan, kuin on tarpeen käsittelyn tarkoitusten toteuttamista varten. Poikkeuksena tähän on tietosuoja-asetuksen 89 artiklan 1 kohdassa luetellut edellytykset yleisen edun mukaisista arkistointitarkoituksista, tieteellisistä tai historiallisista tutkimustarkoituksista tai tilastollisista tarkoituksista. Tällöin henkilötietoja voidaan säilyttää pidempiä aikoja. Henkilötiedot on siis poistettava tai anonymisoitava, jos niitä ei enää tarvita eikä laki velvoita säilyttämään niitä[68]. Etätyöntekijän on varmistettava, ettei säilytä sellaisia tietoja itsellään, joiden säilyttämiseen työnantajallakaan rekisterinpitäjänä tai henkilötietojen käsittelijänä ei ole enää oikeutta.

Henkilötietojen *eheyden ja luottamuksellisuuden* periaatteet liittyvät tietoturvallisuuteen. Tietoturvallisuus on oikeudellisesta näkökulmasta katsottuna tietojen luottamuksellisuuden, eheyden ja käytettävyyden ylläpitämistä ja suojaamista. Ylläpitäminen ja suojaaminen ovat oikeudellinen velvollisuus, vaatimus ja kriteeri.[69] Eheys ja luottamuksellisuus turvataan tietosuoja-asetuksen 5 artiklan f alakohdassa niin, että

[67] Korpisaari ja muut 2018, s. 94.
[68] Korpisaari ja muut 2018, s. 94.
[69] Alapuranen 2020, s. 66.

henkilötietojen asianmukainen turvallisuus varmistetaan suojaamalla tiedot luvattomalta ja lainvastaiselta käsittelyltä, sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Tiedot tulee suojata käyttäen asianmukaisia teknisiä ja organisatorisia toimia. Henkilötietojen käsittelyssä on varmistettava, ettei asiattomilla ole pääsyä tietoihin. Tekniset ja organisatoriset toimenpiteet sisältävät esimerkiksi tietojen suojaamisen salasanoilla, järjestelmän aikalukituksen ja tietoihin pääsyn rajoittamisen ainoastaan niille, jotka todellisuudessa tarvitsevat tietoja.[70]

Etätyössä eheyden ja luottamuksellisuuden periaate korostuu. Työnantaja voi teknisillä ja organisatorisilla toimenpiteillä varmistaa henkilötietojen lainmukaisen käsittelyn. Etätyössä työtä tehdään usein sellaisissa olosuhteissa, ettei työnantaja voi täysin varmistua siitä, että asiattomien pääsy tietoihin on estetty etätyötilassa. Työnantajan on annettava ohjeet työntekijöille tietoturvallisuuden ja tietosuojan noudattamisesta etätyössä. Tällöin työntekijän vastuulle jää noudattaa työnantajan ohjeita ja varmistaa, että asiattomat eivät pääse käsiksi tietoihin. Asiaton tarkoittaa ketä tahansa ulkopuolista henkilöä tai tahoa, joka ei käsittele henkilötietoja rekisterinpitäjän lukuun tai rekisterinpitäjän alaisuudessa. Muun muassa etätyöntekijän perheenjäsenet ovat ulkopuolisia, eikä heillä näin ollen saa olla pääsyä henkilötietoihin.

Tietosuoja-asetuksen 5 artiklan kohta 2 määrää yhdestä rekisterinpitäjän velvollisuudesta, joka on samalla yksi käsittelyn periaatteista. *Osoitusvelvollisuus* kuuluu rekisterinpitäjälle. Rekisterinpitäjä vastaa siitä, että 5 artiklassa säädettyjä henkilötietojen käsittelyä koskevia periaatteita on noudatettu ja sen on pystyttävä myös osoittamaan se. Rekisterinpitäjälle on jätetty valta päättää, mitä teknisiä ja organisatorisia keinoja se käyttää osoitusvelvollisuuden toteuttamiseksi. Osoitusvelvollisuus edellyttää rekisterinpitäjältä tiettyjen toimenpiteiden tekemistä ja kirjaamista, eli dokumentointia. Toimenpiteisiin vaikuttaa esimerkiksi organisaation koko, henkilötietojen määrä ja se, millaisia henkilötietoja käsitellään.[71]

[70] Korpisaari ja muut 2018, s. 94–95.
[71] Tietosuojavaltuutetun toimisto 2021b.

2.3.3 Rekisteröidyn oikeudet

EU:n yleinen tietosuoja-asetus turvaa rekisteröidyn, eli tietojen käsittelyn kohteena olevan henkilön, oikeuksia. Oikeuksia on tietosuoja-asetuksessa lisätty verrattuna aiemaan sääntelyyn. Se, mistä rekisteröityä koskevat tiedot on kerätty ja millä perusteella henkilötietoja käsitellään, vaikuttavat rekisteröidyn oikeuksiin. Rekisteröidyn tietosuojaa on pyritty parantamaan esimerkiksi ohjaamalla rekisterinpitäjää tietojen vastuulliseen ja läpinäkyvään käsittelyyn.[72] Rekisteröidyn oikeuksia ja vapauksia turvaa tietosuoja-asetuksen riskiperusteinen lähestymistapa. Sääntelyn riskiperusteinen lähestymistapa tarkoittaa sitä, että tietosuoja-asetuksen velvoitteet ja suojatoimet suhteutetaan siihen riskiin, mikä rekisteröidyn oikeuksille ja vapauksille henkilötietojen käsittelystä aiheutuu.[73]

Rekisteröidyn oikeuksista säädetään tietosuoja-asetuksen kolmannessa luvussa artikloissa 12–22. Näistä 12 artikla on menettelysäännös, joka sääntelee tarkemmin rekisteröidyn tietosuojallisten oikeuksien käytännön toteuttamista. Artikloita 13–22 luetaan rinnakkain 12 artiklan kanssa.[74] Lisäksi rekisteröidyn oikeuksista säädetään artikloissa 77 ja 79, jotka liittyvät rekisteröidyn oikeussuojakeinoihin rekisterinpitäjiä, henkilötietojen käsittelijöitä ja valvontaviranomaisia vastaan. Rekisteröidyn oikeudet ja rekisterinpitäjän velvollisuudet ovat osittain päällekkäisiä, koska tietyt oikeudet aiheuttavat velvollisuuksia rekisterinpitäjälle.

Artikla 12 on siis menettelysäännös, joka sisältää informointivelvollisuuden. Sen mukaan rekisterinpitäjän on toimitettava rekisteröidylle kaikki käsittelyä koskevat tiedot tiiviisti esitetyssä, läpinäkyvässä, helposti ymmärrettävässä ja helposti saatavilla olevassa muodossa. Rekisterinpitäjän on myös arvioitava antamansa informaation kieltä ja johdonmukaisuutta. Informoinnin sisältöön ja ajankohtaa vaikuttaa se, mistä tiedot on saatu. Kun

[72] Korpisaari ja muut 2018, s. 171, 174.
[73] Andreasson ja muut 2019, s. 28–29.
[74] Andreasson ja muut 2019, s. 167.

tietoja kerätään rekisteröidyltä, on informoinnin tapahduttava tietojen keräämisen aikana. Jos tietoja saadaan muualta, informaatio annetaan kohtuullisessa ajassa, kuitenkin viimeistään kuukauden kuluttua tietojen saamisesta. Informointivelvollisuutta ei ole, jos tiedot on esimerkiksi saatu muualta kuin rekisteröidyltä, ja tietojen hankinnasta tai luovuttamisesta säädetään lainsäädännössä, jota rekisterinpitäjään sovelletaan.[75] Tällä hetkellä Suomessa on vakiintunut artiklan 12 noudattamiseksi käytäntö, jossa rekisteröidyn informointia toteutetaan organisaation internetsivujen kautta[76].

Rekisteröidyllä on *oikeus saada pääsy tietoihinsa*. Tästä säädetään tietosuoja-asetuksen artikloissa 12 ja 15. Artiklassa 12 säädetään tarkemmin menettelystä, jota rekisterinpitäjän on noudatettava, kun rekisteröity pyytää pääsyä tietoihinsa. Tämän vuoksi artikla 12 on niin sanottu menettelysäännös, kuten aiemmin ilmeni. Artiklassa 15 kuvataan ne tiedot, jotka rekisteröidylle on annettava tämän pyynnöstä. Rekisteröidyllä on oikeus tietää, käsitelläänkö hänen henkilötietojaan. Jos henkilötietoja käsitellään, on rekisteröidyllä oikeus tietää, mitä henkilötietoja hänestä on tallennettu, mistä tiedot on hankittu, mitä varten tiedot on hankittu, kauanko tietoja säilytetään, luovutetaanko tietoja johonkin, käsitelläänkö tietoja automaattisesti ja miten rekisteröity voi käyttää oikeuksiaan.[77] Artiklan 12 mukaan rekisterinpitäjällä on velvollisuus toimittaa pyydetyt tiedot maksutta ilman aiheetonta viivytystä, viimeistään kuukauden kuluttua pyynnön vastaanottamisesta. Määräaikaa voidaan tarvittaessa jatkaa kahdella kuukaudella, jos tietopyyntö on monimutkainen ja laaja. Tietopyynnöstä aiheutunut kohtuullinen maksu voidaan periä, jos jäljennöksiä tiedoista pyydetään useita. Jos tietopyyntöjä esitetään toistuvasti tai tietopyyntö on perusteeton ja kohtuuton, rekisterinpitäjä voi kieltäytyä toimittamasta tietoja tai periä toimittamisesta aiheutuneet kustannukset. Jos tietoja ei toimiteta, saa rekisteröity asiasta kirjallisen todistuksen, jossa kerrotaan rekisteröidyn oikeussuojakeinot, kuten valituksen tekeminen tietosuojavaltuutetulle.[78]

[75] Andreasson ja muut 2019, s. 165–167.
[76] Andreasson ja muut 2019, s. 166.
[77] Korpisaari ja muut 2018, s. 212.
[78] Andreasson ja muut 2019, s. 167.

Rekisteröidyllä on *oikeus tietojen oikaisemiseen*. Tietojen oikaisemisesta säädetään artikloissa 12, 16 ja 19.[79] Artiklan 16 mukaan rekisteröidyllä on oikeus vaatia, että häntä koskevat virheelliset tiedot oikaistaan ja puutteelliset tiedot täydennetään. Oikaiseminen voi olla virheellisten tietojen korjaamista, vanhentuneiden tietojen korjaamista tai poistamista sekä puutteellisten tietojen täydentämistä. Tiedot on oikaistava, täydennettävä tai poistettava ilman aiheetonta viivytystä, joten tietojen oikaisemisoikeuteen sovelletaan myös artiklaa 12.[80] Tietojen tallennushetken olosuhteet määrittävät sen, ovatko tiedot tarpeettomia tai virheellisiä[81]. Artiklassa 19 säädetään rekisterinpitäjän ilmoitusvelvollisuudesta koskien henkilötietojen oikaisua tai poistoa tai käsittelyn rajoittamista. Sen mukaan rekisterinpitäjän on ilmoitettava henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu. Ilmoitusta ei tarvitse tehdä, jos se aiheuttaa kohtuutonta vaivaa tai on mahdotonta. Rekisterinpitäjän on myös ilmoitettava vastaanottajista rekisteröidyille, jos rekisteröity sitä pyytää.

Joissain tilanteissa rekisteröidyllä on *oikeus tietojen poistamiseen* eli *oikeus tulla unohdetuksi.* Oikeutta tietojen poistamiseen koskevat artiklat 12, 17 ja 19. Varsinaisesti siitä säädetään artiklassa 17. Rekisteröidyllä on oikeus pyytää henkilötietojensa poistamista tietyin edellytyksin. Samoin rekisterinpitäjän on poistettava henkilötiedot, jos tietyt edellytykset poistamiselle täyttyvät. Henkilötiedot on poistettava, kun niille ei ole enää tarvetta. Tarvetta ei enää ole, kun niitä ei tarvita alkuperäiseen käsittelyn tarkoitukseen, eikä muutakaan lainmukaista käsittelyn perustetta ole olemassa. Jos lainmukaisuus tietojen käsittelemiselle on olemassa, tarpeettomat tiedot tulee poistaa ja lainmukaista perustetta varten olevat tiedot säilyttää.[82]

Rekisteröidyllä on oikeus rajoittaa häntä koskevien henkilötietojen käsittelyä. *Oikeus käsittelyn rajoittamiseen* tarkoittaa sitä, että rekisterinpitäjän on pidättäydyttävä

[79] Andreasson ja muut 2019, s. 168.
[80] Korpisaari ja muut 2018, s. 217, 220.
[81] Andreasson ja muut 2019, s. 168.
[82] Korpisaari ja muut 2018, s. 223–225.

henkilötietojen käsittelystä, kunnes rekisteröityä koskevat henkilötiedot on asianmukaisesti tarkistettu, korjattu tai täydennetty. Tästä säädetään 18 artiklassa, ja myös artiklat 12 ja 19 koskevat tätä oikeutta.[83] Rajoittamisen edellytyksenä on epäselvyys sen osalta, pitäisikö tiedot poistaa vai ei. Tällainen tilanne voi olla esimerkiksi silloin, kun rekisteröity kiistää tietojensa paikkansapitävyyden, tai kun käsittely on lainvastaista ja rekisteröity vastustaa tietojen poistamista, mutta vaatii niiden käytön rajoittamista. Myös se, kun tietoja ei enää tarvita alkuperäiseen tarkoitukseen, mutta rekisteröity tarvitsee niitä oikeusvaadetta varten, on perusteltava syy käsittelyn rajoittamiselle. Käsittelyä voidaan rajoittaa lisäksi silloin, kun rekisteröity on vastustanut tietojensa käsittelyä tietosuoja-asetuksen tiettyjen artiklojen mukaisesti, mutta päätöstä ei ole vielä tehty.[84]

Rekisteröidyllä on tietosuoja-asetuksen 20 artiklan mukaan oikeus siirtää itse toimittamansa itseään koskevat tiedot toiselle rekisterinpitäjälle. Tämä *oikeus siirtää tiedot järjestelmästä toiseen* tarjoaa rekisteröidylle mahdollisuuden hankkia ja käyttää uudelleen omia tietojaan eri palveluissa ja omiin tarkoituksiinsa. Käytännössä siirto-oikeuden taustalla on ajatus siitä, ettei ihmisten tarvitsisi jäädä käyttämään tiettyä palvelua tai sovellusta sen vuoksi, että omien palveluun syötettyjen tietojen siirtäminen toiseen palveluun olisi työlästä tai jopa mahdotonta tietojen suuren määrän vuoksi. Näin estetään riippuvuuden syntyminen yhteen palveluun. Tietojen siirtämisoikeudella mahdollistetaan tietojen siirto järjestelmästä toiseen, kun rekisteröity voi hankkia ja käyttää uudelleen omia tietojaan omiin tarkoituksiinsa. Tiedot voi vastaanottaa rekisterinpitäjältä ja tallentaa itselleen myöhempää käyttöä varten, tai siirtää henkilötiedot suoraan rekisterinpitäjältä toiselle. Tietojen siirtäminen on rekisteröidylle maksutonta. Kohtuullinen maksu voidaan periä, jos pyynnöt ovat ilmeisen perusteettomia ja kohtuuttomia.[85] Tiedot siirretään koneluettavassa muodossa, mikäli se on mahdollista[86].

[83] Andreasson ja muut 2019, s. 168.
[84] Korpisaari ja muut 2018, s. 236–237.
[85] Korpisaari ja muut 2018, s. 242–243.
[86] Andreasson ja muut 2019, s. 169.

Vastustamisoikeus tarkoittaa rekisteröidyn oikeutta vastustaa henkilötietojensa käsittelyä henkilökohtaiseen, erityiseen tilanteeseensa vetoamalla. Vastustamisoikeus kuuluu rekisteröidylle silloinkin, kun käsittely perustuu yleistä etua koskevaan asiaan tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseen. Vastustamisoikeudesta säädetään tietosuoja-asetuksen 21 artiklassa. Jotta rekisteröidyn henkilötietoja voidaan vastustuksesta huolimatta käsitellä, tulee käsittelyyn olla huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn oikeudet, vapaudet ja edut.[87] Rekisterinpitäjän on kerrottava rekisteröidylle tämän vastustamisoikeudesta viimeistään silloin, kun rekisteröityyn ollaan ensimmäisen kerran yhteydessä. Oikeus on esitettävä selkeästi ja erillään muusta informoinnista.[88] Vastustamisoikeus liittyy vain osaan käsittelyperusteista, ja huomattavan tärkeä ja perusteltu syy rekisteröidyn tietojen käsittelylle voi syrjäyttää vastustamisoikeuden. Rekisterinpitäjän tulee pystyä tällöin osoittamaan perusteltu syy tietojen käsittelylle.[89]

Rekisteröidyllä on *oikeus olla joutumatta automaattisen päätöksenteon kohteeksi*. Tähän oikeuteen sisältyy myös profiloinnin estäminen. Profilointi on määritetty tietosuoja-asetuksen 4 artiklassa. Profiloinnilla tarkoitetaan mitä tahansa henkilötietojen automaattista käsittelyä, jossa arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia. Arviointiin voi liittyä esimerkiksi luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, sijantiin ja liikkeisiin liittyviä asioita, joita analysoidaan ja ennakoidaan. Rekisteröidyn oikeudesta olla joutumatta automaattisen päätöksenteon ja profiloinnin kohteeksi säädetään tietosuoja-asetuksen 22 artiklassa. Käytännössä oikeus tarkoittaa sitä, että rekisteröity voi vaatia, että häntä koskevat päätökset laatii ihminen. Päätöksen tulee kuitenkin olla sellainen asiakirja, jolla on rekisteröidylle oikeudellisia vaikutuksia. Näin esimerkiksi automaatilla lähetettävä suoramarkkinointikirje voi rekisteröidyn vastustamisesta huolimatta olla automaattinen. Automaattisen päätöksenteon kieltämiseen on olemassa poikkeuksia, kuten välttämättömyys

[87] Andreasson ja muut 2019, s. 169.
[88] Korpisaari ja muut 2018, s. 253.
[89] Alapuranen 2020, s. 98–99.

rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemisessä tai lainsäädännön antama nimenomainen lupa.[90]

Rekisteröidyllä on *oikeus tehdä valitus valvontaviranomaiselle* ja *oikeus tehokkaisiin oikeussuojakeinoihin rekisterinpitäjää ja henkilötietojen käsittelijää vastaan*. Oikeudesta tehdä valitus valvontaviranomaiselle säädetään tietosuoja-asetuksen 77 artiklassa. Jos henkilö katsoo, että käsittelyssä rikotaan EU:n yleistä tietosuoja-asetusta, hänellä on oikeus tehdä valitus vakinaisen asuin- tai työpaikkansa sijainnin mukaiselle valvontaviranomaiselle. Hänellä on oikeus käyttää myös muita hallinnollisia muutoksenhaku- tai oikeussuojakeinoja. Tietosuoja-asetuksen 79 artiklan mukaan henkilö voi nostaa kanteen rekisterinpitäjää tai henkilötietojen käsittelijää vastaan, jos hän katsoo, ettei hänen henkilötietojensa käsittelyssä ole noudatettu EU:n yleistä tietosuoja-asetusta ja tämän vuoksi hänen oikeuksiaan on loukattu.[91]

Rekisteröidyn oikeudet on tunnistettava ja otettava huomioon kaikessa henkilötietojen käsittelyssä. Etätyö ja etätyössä käsiteltävät henkilötiedot eivät tuo tähän poikkeusta. Työntekijän on työolosuhteista riippumatta tunnistettava rekisteröidyn oikeudet ja ne tilanteet, joissa rekisteröity vetoaa oikeuksiinsa. Työnantajan on rekisterinpitäjän tai henkilötietojen käsittelijän asemassa informoitava työntekijää rekisteröidyn oikeuksista ja niiden noudattamisesta, jotta työntekijä voi tunnistaa tilanteet ja reagoida esimerkiksi rekisteröidyn tietopyyntöihin. Rekisteröidyn oikeuksien tunnistaminen on tärkeää siksi, että juuri rekisterinpitäjän alaisuudessa henkilötietoja käsittelevä työntekijä voi olla se ensisijainen taho, jolle rekisteröity osoittaa vaatimuksensa. Työntekijä voi edesauttaa rekisteröidyn oikeuksien ja rekisterinpitäjän velvollisuuksien toteutumista tiedostamalla rekisteröidyn oikeudet.

[90] Korpisaari ja muut 2018, s. 257–260.
[91] Andreasson ja muut 2019, s. 170.

2.3.4 Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet

Rekisteröidyn oikeuksia käsittelevät tietosuoja-asetuksen 3 luvun artiklat 12–22 avaavat joiltain osin myös rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksia. Oikeudet ja velvollisuudet ovat osittain päällekkäisiä, koska jotkin rekisteröidyn oikeudet voivat aiheuttaa rekisterinpitäjälle tai henkilötietojen käsittelijälle velvollisuuksia. Tietosuoja-asetuksen 3 luvun artiklat 13 ja 14, joissa säädetään rekisteröidylle toimitettavista tiedoista, sisältävät velvoitteita. Lisäksi neljännessä luvussa säädetään erikseen rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksista. Yleisiä velvollisuuksia sisältyy artikloihin 24–31, jotka liittyvät rekisterinpitäjän vastuuseen, sisäänrakennettuun ja oletusarvoiseen tietosuojaan, yhteisrekisterinpitäjiin, EU:n ulkopuolelle sijoittuneisiin rekisterinpitäjiin, tietojenkäsittelyyn rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa, selosteeseen käsittelytoimista sekä yhteistyöhön valvontaviranomaisten kanssa[92]. Myös artiklat 32–38 sisältävät rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksia.

Tietosuoja-asetuksen 3 luvun artiklassa 13 määrätään tiedoista, jotka rekisterinpitäjän on toimitettava rekisteröidylle silloin, kun henkilötietoja kerätään rekisteröidyltä itseltään. Artiklassa 14 säädetään rekisteröidylle toimitettavista tiedoista silloin, kun tietoja ei ole saatu rekisteröidyltä, vaan jostain muualta. Toimitettavat tiedot on lueteltu melko tyhjentävästi molemmissa artikloissa. Toimitettavat tiedot riippuvat siitä, millaisiin tarkoituksiin henkilötietoja kerätään. Toimitettavia tietoja ovat muun muassa tiedot rekisterinpitäjän identiteetistä ja yhteystiedoista, mahdollisen tietosuojavastaavan yhteystiedot tapauksen mukaan, henkilötietojen säilytysaika tai säilytysajan määrittämiskriteerit, jos tarkkaa aikaa ei voida antaa, sekä rekisteröidyn oikeus pyytää pääsyä itseään koskeviin henkilötietoihin. Artiklat 13 ja 14 perustuvat artiklaan 12, joka on menettelysäännös myös näille artikloille. Artiklat 13 ja 14 ilmentävät näin ollen rekisterinpitäjän informointivelvollisuutta.

[92] Korpisaari ja muut 2018, s. 267.

Rekisterinpitäjällä ja henkilötietojen käsittelijällä on yleisiä velvollisuuksia, joista säädetään tietosuoja-asetuksen 4 luvussa. Rekisterinpitäjän vastuuta käsittelee artikla 24. Sen mukaan rekisterinpitäjän on toteutettava tarvittavat *tekniset ja organisatoriset toimenpiteet*, joilla voidaan varmistaa ja osoittaa, että henkilötietojen käsittelyssä noudatetaan EU:n yleistä tietosuoja-asetusta. Teknisiä toimenpiteitä ovat esimerkiksi laitteisiin ja järjestelmiin pääsyn valvonta, luvattoman käytön esto, tapahtumien kirjaaminen järjestelmissä, käyttöoikeuksien määrittäminen järjestelmiin sekä järjestelmien suojaaminen tietoturvauhkilta. Organisatorisia toimenpiteitä ovat hallinnolliset toimenpiteet, kuten henkilöstön ohjeistus, toimintalinjaukset sekä organisaatiojärjestelyt.[93] Toimenpiteitä tulee tarkistaa ja päivittää tarvittaessa. Rekisterinpitäjän vastuu on yleissäännös, joka ulottuu rekisterinpitäjän lisäksi rekisterinpitäjän lukuun henkilötietoja käsittelevään henkilötietojen käsittelijään[94].

Yleissäännöksen lisäksi tietosuoja-asetuksen artikloissa 25–31 säädetään rekisterinpitäjän ja henkilötietojen käsittelijän vastuista. Artiklassa 25 säädetään *sisäänrakennetusta ja oletusarvoisesta tietosuojasta*. Se tarkoittaa sitä, että tietosuojan tulisi olla mukana tietojärjestelmien suunnittelussa alusta asti, ja tietosuoja tulisi huomioida henkilötietojen käsittelytoimissa koko tiedon elinkaaren ajan.[95] Jotta tietosuoja olisi sisäänrakennettua ja oletusarvoista, rekisterinpitäjän on toteutettava sellaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan henkilötietojen käsittelyn vastaavaan tietosuoja-asetuksen vaatimuksia. Teknisiä ja organisatorisia toimenpiteitä ovat esimerkiksi tietojen pseudonymisointi, jolla tarkoitetaan henkilötiedon muuttamista sellaiseen muotoon, ettei tietoa voi enää yhdistää tiettyyn henkilöön ilman lisätietoja[96]. Lisäksi rekisterinpitäjän vastuulla on teknisten ja organisatoristen toimenpiteiden avulla varmistaa, että oletusarvoisesti käsitellään ainoastaan tarkoituksen mukaisia, tarpeellisia henkilötietoja.

[93] Korpisaari ja muut 2018, s. 272–273.
[94] Korpisaari ja muut 2018, s. 268.
[95] Korpisaari ja muut 2018, s. 277.
[96] Tietosuojavaltuutetun toimisto 2021c.

Artikla 26 määrittelee yhteisrekisterinpitäjien vastuita. Yhteisrekisterinpitäjällä tarkoitetaan vähintään kahta rekisterinpitäjää, jotka määrittelevät yhdessä käsittelyn tarkoitukset ja keinot[97]. Yhteisrekisterinpitäjien tulee yhteisellä järjestelyllä läpinäkyvällä tavalla määrittää kunkin vastuualueet tietosuoja-asetuksen velvoitteiden noudattamiseksi. Järjestelyn yhteydessä voidaan nimetä rekisteröidylle yhteispiste, ja järjestelyn keskeisten osien on oltava rekisteröidyn saatavilla. Siitä on käytävä ilmi rekisterinpitäjien todelliset roolit ja suhteet rekisteröityihin nähden. Yhteisrekisteristä huolimatta rekisteröidyn oikeudet kuhunkin rekisterinpitäjään ja rekisterinpitäjää vastaan säilyvät.

EU:n yleinen tietosuoja-asetus sääntelee myös unionin ulkopuolisten rekisterinpitäjien ja henkilötietojen käsittelijöiden velvollisuuksia, kun käsitellään unionin alueella olevien rekisteröityjen henkilötietoja. Asetuksen 27 artiklan mukaan rekisterinpitäjän tai henkilötietojen käsittelijän on nimettävä edustaja unionin aluetta varten. Edustaja voi olla luonnollinen henkilö tai oikeushenkilö, ja sen on oltava sijoittuneena johonkin niistä jäsenvaltioista, jossa rekisteröidyt ovat. Rekisterinpitäjän ja käsittelijän vastuut eivät poistu edustajan myötä, vaan edustaja toimii yhteyshenkilönä valvontaviranomaisen ja rekisterinpitäjän välillä kirjallisella valtuutuksella. Edustaja voi joutua täytäntöönpanotoimien kohteeksi, jos rekisterinpitäjä tai henkilötietojen käsittelijä ei noudata tietosuoja-asetuksen säännöksiä. Edustajaa ei tarvitse nimetä, jos henkilötietojen käsittely on satunnaista eikä kohdistu laajasti 9 artiklan 1 kohdassa tarkoitettuihin erityisiin tietoryhmiin, kuten rotuun, etniseen alkuperään, poliittisiin mielipiteisiin tai rikostuomiota ja rikkomuksia koskeviin henkilötietoihin. Käsittelyyn ei myöskään tule liittyä henkilön oikeuksiin ja vapauksiin kohdistuvaa riskiä. Edustajan nimeäminen ei koske myöskään viranomaisia tai julkishallinnon elimiä.[98]

Henkilötietojen käsittelijän vastuusta säädetään tarkemmin tietosuoja-asetuksen 28 artiklassa. Sen mukaan käsittelijöinä saa käyttää vain sellaisia, jotka toteuttavat asianmukaiset tekniset ja organisatoriset toimet sitä varten, että käsittely on asetuksen mukaista

[97] Korpisaari ja muut 2018, s. 283.
[98] Korpisaari ja muut 2018, s. 286–289.

ja käsittelyssä varmistetaan rekisteröidyn oikeuksien suojelu. Rekisterinpitäjän vastuulla on käyttää vain sellaisia henkilötietojen käsittelijöitä, jotka pystyvät suoriutumaan henkilötietojen käsittelystä tietosuoja-asetuksen vaatimusten mukaisesti. Rekisterinpitäjä kontrolloi, kuka henkilötietoja käsittelee. Rekisterinpitäjä ja henkilötietojen käsittelijä tekevät keskenään kirjallisen sopimuksen, jossa sovitaan käsittelyn ehdoista.[99] Silloin, kun käsitellään henkilötietoja rekisterinpitäjän ja henkilötietojen käsittelyn alaisuudessa, niitä ei saa käsitellä muuten kuin rekisterinpitäjän ohjeet määräävät, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä niin vaadita. Tästä säädetään tietosuoja-asetuksen 29 artiklassa. Työntekijä käsittelee henkilötietoja rekisterinpitäjän tai henkilötietojen käsittelijän, eli työnantajan, alaisuudessa. Näin ollen työntekijä ei saa käsitellä henkilötietoja vastoin työnantajan antamia ohjeita.

Rekisterinpitäjän ja tarpeen mukaan rekisterinpitäjän edustajan on ylläpidettävä selostetta käsittelytoimista, jotka ovat sen vastuulla. Selosteessa käsiteltävät tiedot luetellaan tietosuoja-asetuksen 30 artiklassa. Rekisterinpitäjän selosteen sisältö on laajempi, kuin henkilötietojen käsittelijän. Rekisterinpitäjän on ilmoitettava selosteessa rekisterinpitäjän ja tietosuojavastaavan tiedot, käsittelyn tarkoitukset, kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä, ryhmät, joille henkilötietoja luovutetaan, tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle, tietojen säilytysajat sekä kuvaus teknisistä ja organisatorisista turvatoimista. Käsittelijän tulee puolestaan ilmoittaa käsittelijän ja tietosuojavastaavan tiedot, minkälaisia toimia käsittelijä tekee rekisterinpitäjän lukuun, tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle sekä kuvaus teknisistä ja organisatorisista turvatoimista. Selosteen tulee olla kirjallinen ja saatavilla sähköisessä muodossa.[100]

Rekisterinpitäjän ja henkilötietojen käsittelijän tai tarvittaessa näiden edustajan on tehtävä tietosuoja-asetuksen 31 artiklan mukaan yhteistyötä valvontaviranomaisen kanssa pyydettäessä, jotta valvontaviranomainen voi suorittaa sille kuuluvat tehtävät. Artiklat

[99] Korpisaari ja muut 2018, s. 290–296.
[100] Korpisaari ja muut 2018, s. 298–303.

33 ja 34 käsittelevät rekisterinpitäjän ja henkilötietojen käsittelijän ilmoitusvelvollisuutta tietoturvaloukkauksien yhteydessä. Artiklan 33 mukaan rekisterinpitäjän on ilmoitettava valvontaviranomaiselle tietoturvaloukkauksesta. Loukkauksesta on ilmoitettava ilman aiheetonta viivytystä, mahdollisuuksien mukaan 72 tunnin kuluessa valvontaviranomaiselle. Ilmoitusta ei tarvitse tehdä, jos tietoturvaloukkauksesta ei aiheudu todennäköisesti luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuvaa riskiä. Saman artiklan mukaan henkilötietojen käsittelijän on ilmoitettava tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä. Artiklassa 34 säädetään puolestaan tietoturvaloukkauksen ilmoittamisesta rekisteröidylle. Rekisterinpitäjän on ilmoitettava rekisteröidylle tietoturvaloukkauksesta ilman aiheetonta viivytystä, jos loukkaus todennäköisesti aiheuttaa korkean riskin luonnollisen henkilön oikeuksille ja vapauksille.

Tietosuoja-asetuksen artiklassa 32 säädetään käsittelyn turvallisuuteen liittyvistä toimenpiteistä. Siinä säädetään muun muassa niistä teknisistä ja organisatorisista toimenpiteistä, jotka rekisterinpitäjän tai henkilötietojen käsittelijän on toteutettava käsittelyn turvallisuuden takaamiseksi. Lisäksi artiklan 32 kohdassa 4 velvoitetaan rekisterinpitäjä tai henkilötietojen käsittelijä toteuttamaan sellaisen toimenpiteet, jotta niiden alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaadita.

Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksia ilmentävät myös tietosuoja-asetuksen artiklat 35, 36 ja 37. Artiklassa 35 säädetään siitä, milloin rekisterinpitäjän on tehtävä tietosuojaa koskeva vaikutustenarviointi ja mitä sen tulee vähintään sisältää. Artiklan 36 mukaan rekisterinpitäjän on ennen käsittelyä kuultava valvontaviranomaista, jos vaikutustenarvioinnin perusteella käsittely aiheuttaa korkean riskin. Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuutena on artiklan 37 mukaan tietosuojavastaavan nimittäminen tietyissä tilanteissa.

2.4 Etätyön asema lainsäädännössä

Etätyötä omana terminään ei tunneta työlainsäädännössä. Etätyötä koskee sama lainsäädäntö, joka koskee työn tekemistä yleensäkin. Lainsäädännöllisen perustan työn ja näin myös etätyön sääntelyyn muodostavat työsopimuslaki[101], työaikalaki[102] ja työturvallisuuslaki[103].[104] Työlainsäädännön muodostaman pohjan lisäksi työhön sovelletaan työ- ja virkaehtosopimuksia, jotka ovat ammattiliiton ja työnantajien tekemiä sopimuksia jonkin alan vähimmäistyöehdoista. Työ- ja virkaehtosopimusten tarkoituksena on turvata työntekijälle työlainsäädäntöä paremmat työehdot. Lisäksi on olemassa työsääntöjä ja työehtosopimuksiin perustuvia sopimuksia, jotka sovitaan yhteistoimintaneuvotteluissa. Työsäännöt ja työehtosopimuksiin perustuvat sopimukset eivät saa heikentää työntekijän lainsäädäntöön, työehtosopimukseen tai työsopimukseen perustuvia etuja. Lainsäädännön ja sopimusten lisäksi voi olla vielä työpaikalla noudatettu käytäntö. Se tarkoittaa sitä, että jos työpaikalla on noudatettu tiettyä käytäntöä vakiintuneesti pitkähkön aikaa, katsotaan siitä tulleen työsuhteen ehto. Työnantaja ei voi yksipuolisesti muuttaa tällaista työpaikalla noudatettua käytäntöä.[105]

Etätyöntekijän juridiseen asemaan vaikuttaa lähinnä se, tehdäänkö etätyötä työsuhteessa, julkisoikeudellisessa palvelussuhteessa vai yrittäjänä. Työsuhteessa tai virkasuhteessa olevien etätyötä säännellään työlainsäädännöllä ja etätyön puitesopimuksella[106]. Lisäksi etätyöstä voidaan määrätä alakohtaisissa sopimuksissa ja suosituksissa[107]. Joskus etätyöntekijän työehdoista sovitaan vielä erillisellä, henkilökohtaisella etätyösopimuksella[108].

[101] Työsopimuslaki 55/2001.
[102] Työaikalaki 872/2019.
[103] Työturvallisuuslaki 738/2002.
[104] Työsuojeluhallinto 2020.
[105] Erto 2022a.
[106] Etätyötä koskeva puitesopimus 2002.
[107] Helle 2004, s. 86.
[108] Helle 2004, s. 135.

Työntekijän asema lainsäädännöllisesti ei muutu etätyössä verrattuna lähityöhön, jos työntekijä on työ- tai virkasuhteessa. Etätyön voidaan katsoa näin ollen olevan tapa organisoida työtä, ei oma työsuhdemuotonsa.[109] Koska etätyössä on kyse tavasta tehdä normaalia työsuhteista työtä, ei tarvetta etätyöntekijän juridiselle määrittelylle ole olemassa. Etätyöhön liittyy kuitenkin muutamia poikkeuksia työlainsäädännön soveltamisen osalta.[110] Näitä poikkeuksia ovat muun muassa jotkin vahinko- ja vakuutustilanteet sekä työnantajan työnjohto-oikeuden toteuttaminen.

2.5 EY:n etätyötä koskeva puitesopimus

Etätyön eurooppalainen puitesopimus on ensimmäinen laaja ja kattava sopimus Euroopassa, jossa on sovittu etätyöhön siirtymisen periaatteista ja etätyön ehdoista. Ennen puitesopimusta Suomessa on ollut olemassa vain joitakin laintasoisia säännöksiä sekä alakohtaisia ja paikallisia sopimuksia sekä suosituksia etätyölle.[111]

Tarve etätyön puitesopimukselle syntyi EU:n yhteiskuntastrategian pohjalta Lissabonissa maaliskuussa 2000. EU:sta haluttiin kilpailukykyinen ja dynaaminen tietoyhteiskunta, jossa työllisyysaste nousisi 61 prosentista lähelle 70 prosenttia vuoteen 2010 mennessä. Työllisyysstrategian pohjalta Eurooppa-neuvosto kehotti työmarkkinaosapuolia neuvottelemaan sopimuksia työn nykyaikaistamisesta ja joustavista työjärjestelyistä. Tämä oli pitkälti syynä etätyön noususssa työmarkkinaosapuolten neuvottelun aiheeksi.[112]

EY:n etätyötä koskeva puitesopimus allekirjoitettiin 16.7.2002 ja sen osapuolina ovat Euroopan työmarkkinaosapuolet UNICE/UAPME, CEEP ja EAY[113]. Kyseessä on Eurooppa-tason työmarkkinakeskusjärjestöjen välinen sopimus etätyöstä, joten sen

[109] Helle 2004, s. 57–58.
[110] Helle 2004, s. 42.
[111] Helle 2004, s. 69.
[112] Helle 2004, s. 70.
[113] Kuntatyönantajat 2005.

voimaansaattamisesta vastasivat työmarkkinajärjestöt eri maissa[114]. Aikaa sopimuksen täytäntöönpanolle jäsenvaltioissa oli kolme vuotta sen allekirjoittamisesta, ja täytäntöönpano hoidettiin jäsenvaltion työmarkkinaosapuolten menettelyjen ja käytäntöjen mukaisesti. Suomessa puitesopimuksen kansallinen täytäntöönpano toteutettiin työmarkkinakeskusjärjestöjen allekirjoittamalla asiakirjalla ja sen mukaisilla toimenpiteillä.[115] Etätyön puitesopimus kattaa erittäin laajasti suomalaisen työmarkkinakentän, koska sopimuksessa ovat mukana palkansaajien ja työnantajien keskusjärjestöt. Puitesopimus takaa minimisuojan, sillä työehtosopimuksessa tai työpaikan käytäntöjen perusteella puitesopimusta paremmat ehdot etätyölle on säilytettävä.[116]

Etätyön puitesopimuksen tausta ja tarkoitukset kerrotaan sopimuksen 1 artiklassa. Puitesopimuksella on sekä yhteiskunnallisia tavoitteita että yksilön tasolle ulottuvia tarkoituksia. Sopimuksen mukaan etätyö nähdään keinona nykyaikaistaa työn organisointia sekä yrityksissä että julkisen palvelun organisaatioissa. Työntekijöille etätyö tarjoaa keinon vapaa-ajan ja työn yhteensovittamiseen sekä autonomian kasvattamiseen. Etätyö nähdään myös keinona kasvattaa tietoyhteiskunnan tarjoamia etuja Euroopan tasolla huomioimalla joustavuus ja turvallisuus samanaikaisesti. Työpaikkojen laatua nostetaan ja vajaakuntoisten mahdollisuudet työmarkkinoilla lisääntyvät, koska etätyö voi olla keino lisätä vajaakuntoisten työskentelymahdollisuuksia. Puitesopimuksen tavoitteena on, että etätyölle olisi Euroopan tasolla yleiset ja yhteiset puitteet. Tavoitteena puitesopimusta laatiessa oli, että sopimus saatettaisiin voimaan myös tulevissa EU:n jäsenmaissa.[117]

Etätyön puitesopimuksessa on yhteensä 12 artiklaa. Sopimuksen artikloissa säädetään etätyön määritelmästä ja sopimuksen soveltamisalasta, etätyön luonteesta, työsuhteen ehdoista, tietoturvasta ja yksityisyyden suojasta, työvälineistä, työsuojeluun liittyvistä

[114] Helle 2004, s. 69.
[115] Kuntatyönantajat 2005.
[116] Helle 2004, s. 70.
[117] Helle 2004, s. 84.

kysymyksistä, työjärjestelyistä, koulutuksesta ja kollektiivisista oikeuksista sekä sopimuksen täytäntöönpanosta ja seurannasta.

Koronapandemian myötä organisaatioissa siirryttiin laajasti nopealla aikataululla etätyöhön. Etätyön puitesopimuksen 3,5 ja 6 artiklat määrittävät etätyön vapaaehtoisen luonteen sekä tietoturvan ja työntekijän yksityisyyden suojan, jotka ovat oleellisia asioita tarkasteltaessa tietosuojaa etätyössä. Etätyön puitesopimuksen 3 artiklan mukaan etätyö perustuu vapaaehtoisuuteen. Etätyö on vapaaehtoista sekä työntekijälle että työnantajalle. Etätyötä voidaan edellyttää osana alkuperäistä toimenkuvaa, tai siihen voidaan siirtyä myöhemmin. Jos etätyöhön siirrytään myöhemmin, on siirtymisen oltava luonteeltaan vapaaehtoista. Työnantaja voi tarjota etätyötä, jos siitä ei ole sovittu alkuperäisessä toimenkuvassa. Työntekijä voi hyväksyä tai hylätä etätyötarjouksen. Jos työntekijä kieltäytyy etätyöstä, se ei sellaisenaan ole peruste työsuhteen päättämiselle tai kieltäytyneen työntekijän työsuhteen ehtojen muuttamiselle. Samoin työntekijä voi ilmoittaa olevansa halukas etätyöhön, jolloin työnantaja voi hyväksyä tai hylätä työntekijän ehdotuksen.

Etätyön puitesopimuksen 5 artiklan mukaan työnantaja on vastuussa tietoturvasta. Sen mukaan työnantajan on ryhdyttävä tarpeellisiin toimenpiteisiin, jotta etätyöntekijän ammatillisiin tarkoituksiin käyttämä ja käsittelemä tieto on asianmukaisesti suojattu. Lisäksi työnantajan on annettava etätyöntekijälle tiedot kaikesta asianmukaisesta lainsäädännöstä ja yrityssäännöistä, jotka koskevat tietosuojaa. Etätyöntekijän on noudatettava näitä annettuja sääntöjä. 5 artiklassa mainitaan, että työnantajan on tiedotettava erityisesti kaikista rajoituksista tietotekniikkalaitteisiin – ja välineisiin liittyen sekä sääntöjen laiminlyönnistä johtuvista seuraamuksista etätyöntekijälle. Työnantajan on kunnioitettava etätyöntekijän yksityisyyttä etätyön puitesopimuksen 6 artiklan mukaan. Jos mikä tahansa tarkkailujärjestelmä otetaan käyttöön, sen on oltava asetettuun tavoitteeseen nähden oikeassa suhteessa ja se on otettava käyttöön näyttöpäätedirektiivin 90/270 mukaisesti.

Etätyön tietosuojan kannalta etätyön vapaaehtoisuus on oleellista. Työntekijän ei tarvitse siirtyä etätyöhön, jos siitä ei ole sovittu alkuperäisessä toimenkuvassa. Kieltäytyminen etätyöstä työntekijän puolelta voi tulla kysymykseen esimerkiksi silloin, jos työntekijä käsittelee työssään henkilötietoja, ja tunnistaa, ettei henkilötietojen käsittely onnistu etätyössä ilman henkilötietojen käsittelyn lainmukaisuuden vaarantumista. Toisaalta työnantaja voi kieltäytyä työntekijän pyynnöstä tehdä etätyötä, jos työnantajalla ei ole mahdollisuutta varmistua tietosuojan toteutumisesta etätyössä. Työntekijän yksityisyyden suoja ja kotirauha rajoittavat työnantajan mahdollisuuksia selvittää etätyön olosuhteita. Työnantajan vastuulla on järjestää tietojen asianmukainen suojaus etätyössä, ja ohjeistaa työntekijää tietosuojaan liittyvästä lainsäädännöstä ja yrityssäännöistä. Etätyöntekijän vastuulle jää annettujen ohjeiden noudattaminen.

3 Tietosuojariskit etätyössä

3.1 Ohjeet henkilöstölle

Etätyö voi aiheuttaa tietoturvariskien kasvamista. Työnantajat ovat perinteisesti pitäneet tietoturvallisuuden vaarantumista jarruttavana tekijänä etätyöhön siirtymisessä. Tietojen turvaamisintressi on työnantajalla, koska työnantaja kantaa riskin silloin, jos tietoturva ei ole kunnossa. Vaikka työntekijä ei käsittelisi työssään henkilötietoja, on työntekijällä silti hallussaan sellaista tietoa esimerkiksi työnantajaorganisaatiostaan, johon ulkopuolisten ei toivota pääsevän käsiksi. Vastuu tietoturvasta on siis työnantajalla, mutta työntekijä voi omalta osaltaan varmistaa tietojen turvaamista.[118]

Kuten etätyön puitesopimusta käsittelevässä luvussa kävi ilmi, etätyön puitesopimuksen 5 artiklassa velvoitetaan työnantaja huolehtimaan tietojen suojaamisesta ja tiedottamaan etätyöntekijälle asiaankuuluvasta tietosuojalainsäädännöstä ja yrityssäännöistä. Etätyöntekijän velvollisuudeksi jää noudattaa työnantajan antamia ohjeita. Jos työntekijä laiminlyö annettuja ohjeita, voi siitä aiheutua hänelle seuraamuksia. Etätyön puitesopimuksen 5 artiklan mukaan työnantajan on tiedotettava etätyöntekijälle seuraamuksista, joita ohjeiden rikkomisesta aiheutuu. Seuraamuksen asiallisuus ja lainmukaisuus on aina riippuvainen tapauksen olosuhteista, ja sen on oltava työsopimuslain mukainen. Työnantajan laiminlyödessä velvollisuutensa ohjeistaa etätyöntekijää, kohdistuvat seuraamukset työnantajaan itseensä.[119]

Tietoturvallisuuden toteutuminen edellyttää lähtökohtaisesti sitä, että tietoturvallisuutta koskevat toimintaohjeet ovat olemassa ja työntekijöillä on niistä tieto. Etätyön osalta voidaan tarvita myös lisäohjeita ja lisätoimenpiteitä. Tietoturvallisuuden ja henkilötietojen suojan kannalta on oleellista, että etätyöntekijä noudattaa oikeanlaisia

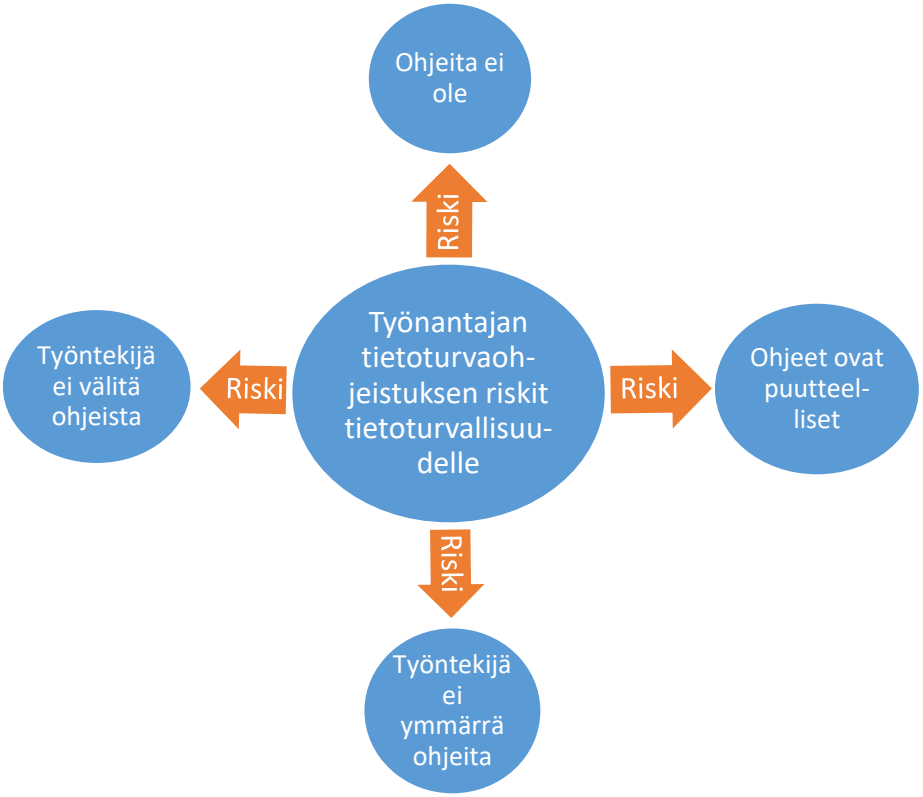
[118] Helle 2004, s. 191–192.
[119] Helle 2004, s. 194.

toimintatapoja. Luonnollisestikaan oikeat toimintatavat eivät toteudu, jos etätyöntekijä ei ole tietoinen niistä tai ohjeet ovat puutteellisia. Etätyöntekijä ei ole velvollinen selvittämään omaehtoisesti, ovatko turvallisuusjärjestelyt riittäviä tai ovatko annetut ohjeet toimintatavoista asianmukaisia.[120]

Henkilötietojen tietoturvallisuus voi olla uhattuna etätyössä silloin, jos työnantaja ei ole ohjeistanut riittävällä tavalla etätyöhön liittyvästä tietoturvallisuudesta. Ohjeet voivat olla puutteelliset tai virheelliset, ja aiheuttavat tällöin riskin tietoturvallisuudelle. Etätyöntekijä voi puutteellisten tai virheellisten tietoturvaohjeiden vuoksi rikkoa tietämättään tietosuojasääntelyä. Toisaalta ohjeet voivat olla myös vaikeasti ymmärrettäviä. Työntekijä ei välttämättä kykene soveltamaan vaikeasti ymmärrettäviä ohjeita käytännön työhönsä, jolloin tietoturvallisuus ja myös tietosuoja voivat vaarantua.

Etätyöntekijän oma toiminta voi vaarantaa tietosuojan. Riittävä, oikea ja ymmärrettävä ohjeistus ei toimi tarkoituksenmukaisesti, jos työntekijä on piittaamaton eikä välitä annetuista ohjeista. Tällöin työntekijän piittaamattomuus annettuja ohjeita kohtaan aiheuttaa riskin tietoturvallisuudelle. Etätyö ei tarkoita sitä, että työntekijän ei tarvitsisi noudattaa samoja ohjeita, kuin työnantajan tiloissa työskennellessä[121]. Seuraavassa kuviossa on esitetty nämä työnantajan tietoturvaohjeiden aiheuttamat riskitilanteet etätyössä tietosuojalle.

[120] Helle 2004, s. 195.
[121] Järvinen & Rousku 2017, s. 47.



Kuvio 1. Työnantajan tietoturvaohjeiden riskit tietoturvallisuudelle.

Koronapandemian myötä etätyö on yleistynyt Suomessa merkittävästi, ja monessa työpaikassa osittainen etätyö on tullut jäädäkseen. Laajamittainen siirtymä etätyöhön tapahtui nopeasti pandemian alkaessa, ja on mahdollista, että kaikki organisaatiot eivät ole laatineet ajantasaista etätyöhön liittyvää tietoturvaohjeistusta tietosuojaohjeistuksineen. Ohjeiden puuttuminen tai niiden vajavaisuus ovat riskejä tietosuojan toteutumiselle etätyössä. Etätyöntekijä ei välttämättä itsenäisesti tunnista tietosuojaan kohdistuvia uhkia, jotka johtuvat nimenomaan etätyöstä ja sen olosuhteista. Työntekijän vastuulla ei ole selvittää sitä, ovatko työnantajan antamat ohjeet tarkoituksenmukaiset ja ajantasaiset etätyötä ajatellen.

Vaikka työnantajan ohjeistus olisi asianmukainen, inhimillisiä virheitä voi tapahtua. Henkilöstö onkin tietyllä tapaa suurin tietoturvauhka, koska inhimilliset virheet ja erehdykset ovat mahdollisia aina, kun työtä tekee ihminen. Mitä kriittisemmästä toimenpiteestä on

kysymys, sen tärkeämpää on varmistua toimenpiteen oikeasta toteutuksesta. Joskus toinen henkilö voi havaita asioita, joita ei itse huomaisi. Toisen silmäparin onkin hyvä tarkistaa kriittisen toimenpiteen kohdalla, että kaikki on niin kuin on tarkoitettu.[122] Etätyössä työtä tehdään pääsääntöisesti yksin erillään muista, jolloin työyhteisön apu ei ole fyysisesti läsnä. Tällöin kynnys tarkistuttaa itseä askarruttavia asioita voi olla korkeampi, kuin se olisi työnantajan tiloissa tehtävässä työssä. Toimenpiteitä saatetaan suorittaa itsenäisemmin, jolloin tietoturvallisuuteen liittyvät virheet voivat lisääntyä.

3.2 Tietotekniikka ja tietoliikenneyhteydet

Digitalisoituminen on tällä hetkellä laaja-alaista. Digitalisaatiolla tarkoitetaan sitä, että ATK:n ja ICT:n tuomaan teknologiaan yhdistetään käyttäjän tai asiakkaan saama uudenlainen palvelukokonaisuus. Organisaatio voi rakentaa jonkin toimintonsa tehokkaammaksi ja automaattisemmaksi digitaalisuutta hyödyntämällä. Digitalisointi hyödyttää sekä organisaation liiketoimintaa, että parantaa asiakkaan käyttäjäkokemusta. Hyödyt voivat olla organisaatiolle ja asiakkaalle myös taloudellisia. Globalisaatio liittyy tiiviisti digitalisaatioon, koska palveluiden tuottaminen tai tietojen sijainti eivät noudata maantieteellisiä rajoja. Esimerkkinä digitalisaatiosta voidaan mainita automaattinen päätöksenteko, kun esimerkiksi päätöksen yksityislainalle voi saada lähes välittömästi. Kyseessä ei tällöin ole ihmisen tekemä päätös, vaan organisaation digitaalinen toimintaprosessi, jossa päätöksenteon hoitaa keinoäly.[123]

Digitalisaation lukuisten organisaatiota ja asiakkaita hyödyttävien ominaisuuksien lisäksi siihen liittyy myös kohonneita riskejä. Digitalisaation lisääntyessä tietoturvallisuuden ja tietosuojan merkitys kasvavat, koska mahdollisuus verkossa tapahtuviin rikoksiin lisääntyy. Henkilötiedot ovat tietoturvarikollisia kiinnostava tietojoukko, koska niitä voidaan käyttää hyödyksi erilaisissa rikoksissa. Tavaroiden ja palveluiden ostaminen ja myyminen

[122] Järvinen & Rousku 2017, s. 39–40.
[123] Järvinen & Rousku 2017, s. 12–13.

väärän henkilön nimissä ja identiteettivarkaus ovat esimerkkejä rikoksista, joissa hyödynnetään henkilötietoja. Toisaalta teknologia ja digitalisaatio ovat avanneet uudenlaisia tapoja tehdä asioita ja mahdollistaneet ajasta ja paikasta riippumattoman tietojenkäsittelyn.[124] Etätyö on esimerkki siitä, että teknologian ja digitalisaation ansiosta työtä voi tehdä ajasta ja paikasta riippumatta missä vain, jossa on siihen vaadittavat edellytykset.

Henkilötietojen käsittelyn turvallisuus liittyy tietoturvaan. Tietoturvallisuus on pääosin rakentunut kaiken muun päälle, koska internet-verkko rakennettiin alun perin mahdollisimman avointa viestintää varten. Tietoturvallisuutta ei ole otettu huomioon tietoliikenteen tai erilaisten päätelaitteiden suunnittelussa aiemmin, koska ei ole osattu edes kuvitella, mitä kaikkea laitteilla lopulta kyetään tekemään. Tietoturvan pitäisi nykypäivänä olla sisäänrakennettua, koska digitalisaatio ja toimintaympäristön muutos tulevat kiihtymään entisestään. Organisaation vastuulla on tunnistaa tietoturvaan liittyvät uhat, arvioida riskit ja antaa ohjeet työssä tarvittavien laitteiden ja palveluiden käyttämiseen.[125]

Etätyö edellyttää tarvittavaa tietoliikenneyhteyttä ja tietotekniikkaa etätyöntekopaikassa. Etätyöntekijällä itsellään tulee olla hyvä tietotekninen osaaminen, mutta toisaalta tekniset tuen tulee olla saatavilla ongelmatilanteissa. Myös työyhteisöltä, etenkin esimieheltä ja työtovereilta, vaaditaan tietoteknisiä taitoja etätyön onnistumiseksi, jotta kommunikointi etänä olevan työntekijän kanssa onnistuu sujuvasti. Työssä tarvittavan tiedon tulee olla saatavilla tietoverkossa, tiedonhallintajärjestelmien tulee toimia ja tietoturvallisuudesta on huolehdittava tarvittavien lisäjärjestelyiden voimin.[126] Tietotekniikkaan ja tietoliikenneyhteyksiin voi kohdistua hakkerointia, kyberhyökkäyksiä ja haittaohjelmien levittämistä. Nämä voivat johtaa tietoturvallisuuden ja tietosuojan vaarantumiseen. Tämän vuoksi tietoturvasta on tärkeää huolehtia erilaisten teknisten ratkaisujen avulla.

[124] Järvinen & Rousku 2017, s. 19–20.
[125] Järvinen & Rousku 2017, s. 23, 31.
[126] Helle 2004, s. 96.

Langaton lähiverkkoyhteys, eli WLAN (wireless local area network) voi olla riski tietoturvallisuudelle etätyössä. Avoimissa lähiverkkoyhteyksissä, joiden käyttöä ei ole rajoitettu ulkopuolisilta esimerkiksi verkon käyttöön edellytettävällä salasanalla, jää tietoturvallisuudesta huolehtiminen usein käyttäjän vastuulle. Pahantahtoisten tahojen on mahdollista kytkeytyä avoimeen WLAN-verkkoon ja lähettää sitä kautta haitallista liikennettä muille verkon käyttäjille tai laitteille. Organisaatiot hyödyntävät tämän vuoksi tietoturvallisuuden varmistamiseksi etäyhteyden suojaamismenetelmiä. Työt voi tehdä etänäkin turvallisesti, kunhan noudattaa työnantajan tietoturvamääräyksiä ja perushuolellisuutta palveluiden käytössä. Useissa organisaatioissa on tarkat ohjeet ja määräykset siitä, miten päätelaitteita ja tietoteknisiä palveluita tulee käyttää työnantajan tilojen ulkopuolella. Nämä ohjeet ja määräykset kuuluvat työnantajan työnjohtovallan piiriin, joten etätyöntekijän tulee hallita ohjeet ja määräykset hyvin, sekä soveltaa niitä omassa toiminnassaan.[127]

Tietojärjestelmään voi kohdistua uhkia, jotka paljastavat luottamuksellista tietoa, tiedon koskemattomuus menetetään tai tiedon saatavuus menetetään. Etätyössä kaiken tiedon on oltava saatavilla tietoverkkojen kautta. Sen vuoksi tietotekniikan ja tietoliikenneyhteyksien tietoturvallisuus on ehdoton edellytys etätyölle. Teknisten ratkaisujen avulla voidaan suojata tiedostot, hallita käyttöoikeuksia ja suojata tietoliikenneyhteyksiä.[128] Tietotekniikan ja tietojärjestelmien tulee olla ajan tasalla. Tietotekniikkaan ja tietojärjestelmiin liittyvät päivitykset saattavat tuntua käyttäjästä turhauttavilta, mutta niiden tarkoituksena on korjata ohjelmista löytyneitä virheitä ja parantaa sitä kautta myös tietoturvallisuutta.[129] Tietoturvallisuuden kannalta on tärkeää, että laitteiden ja järjestelmien päivitykset onnistuvat sujuvasti ja ajantasaisesti myös etänä työskenneltäessä. Pahimmillaan etätyön vuoksi väliin jäävät päivitykset voivat aiheuttaa tietojärjestelmiin aukkoja, joita tietoturvarikolliset voivat hyödyntää hakkeroimalla järjestelmät.

[127] Kyberturvallisuuskeskus 2014, s. 4, 11.
[128] Helle 2004, s. 195–196.
[129] Järvinen & Rousku 2017, s. 103.

Käyttäjätunnus ja salasana ovat tietoturvallisuuden keskeisimpiä tekijöitä. Niiden avulla varmistutaan siitä, että tietoihin pääsee käsiksi ainoastaan se henkilö, jolla on käyttöoikeus kyseisiin tietoihin. Palveluissa on alettu hyödyntämään vahvaa tai kaksivaiheista tunnistautumista, koska se tarjoaa yksinkertaiseen, yhdellä salasanalla tunnistautumiseen verrattuna paremman suojan. Kaksivaiheinen tunnistautuminen voidaan toteuttaa esimerkiksi niin, että käyttäjätunnuksen ja salasanan syöttämisen jälkeen pyydetään vielä erillinen vahvistuskoodi, joka lähetetään viestillä matkapuhelimeen tai sähköpostiin.[130] Etätyössä käyttäjätunnuksia ja salasanoja on säilytettävä sellaisessa paikassa, että ulkopuolisilla ei ole mahdollisuutta käyttää niitä hyväkseen. Palveluista uloskirjautuminen ja laitteen lukitseminen työpisteeltä poistuttaessa voi tuntua etätyössä yhdentekevältä, mutta tietoturvaan liittyvissä asioissa paras tapa on toimia ylikorostetun huolellisesti riskien minimoimiseksi. Rutiineiksi omaksutut tietoturvalliset toimintatavat pienentävät inhimillisten virheiden mahdollisuutta ja myös mahdollisuutta tietoturvaloukkauksiin. Etätyössä huolimattomasti säilytettävät käyttäjätunnukset ja salasanat sekä laitteiden lukitsemattomuus voivat aiheuttaa sen, että ulkopuolinen pääsee katsomaan järjestelmiä, joissa henkilötietoja on.

Etätyössä työhön käytettävää tietotekniikkaa säilytetään työpaikan sijasta kotona. Joissain tilanteissa tietokone voi jäädä autoon tai muuhun sellaiseen paikkaan, jossa se ei ole yhtä turvattuna, kuin se olisi työnantajan tiloissa. On mahdollista, että esimerkiksi tietokone varastetaan tai muita laitteita häviää. Etätyössä työntekijällä voi olla käytössään muun muassa asiakkaiden henkilötietoja sisältävä tietokone, matkapuhelin ja USB-tikku. Henkilötietoja sisältävän tiedonsiirron välineen häviäminen on tietoturvaloukkaus, ja etätyöntekijän on ilmoitettava hävinneestä laitteesta omaa organisaatioonsa. Organisaation IT-tuki saattaa pystyä paikantamaan laitteen etähallinnan avulla ja lukitsemaan sen. Jopa laitteen sisällön hävittäminen IT-tuen toimesta voi olla mahdollista. Ilmoitus laitteen häviämisestä tai varastamisesta on tehtävä välittömästi, koska nopea ilmoittaminen voi pienentää tietoturvaloukkauksen toteutumista.[131]

---

[130] Järvinen & Rousku 2017, s. 57.
[131] Järvinen & Rousku 2017, s. 59.

3.3 Työntekopaikka

Henkilötietojen suoja voi olla uhattuna työntekijän ja työntekopaikan sijainnin vuoksi. Etätyötä voidaan tehdä missä tahansa tilassa, jossa on tarvittavat työvälineet ja yhteydet etätyön tekemiselle. Useimmiten etätyöntekopaikkana on työntekijän koti, mutta esimerkiksi liikkuvassa etätyössä työntekopaikka vaihtelee. Etätyötä voidaan tehdä esimerkiksi junassa tai muissa julkisissa kulkuvälineissä, etätyötoimistossa tai hotellissa. Etätyöntekopaikasta sovitaan etätyösopimuksessa. Useimmiten sovitaan tietty työntekopaikka, mutta on myös mahdollista, että työntekijä valitsee itse työntekopaikkansa oman tilanteensa mukaan.[132]

Koronapandemian myötä Suomessa siirryttiin laajaan etätyöhön, mutta monella työpaikalla tarkempi sopiminen etätyön pelisäännöistä ja esimerkiksi etätyöntekopaikasta on voinut jäädä tekemättä. Etätyöntekopaikan valinnassa pitäisi ottaa huomioon työn luonne. Työssä, jossa käsitellään henkilötietoja, työntekopaikan tulisi olla sellainen yksityinen ja suljettu tila, että ulkopuolisilla ei ole mahdollisuutta nähdä tai kuulla henkilötietoihin liittyvää materiaalia. Tällainen paikka on esimerkiksi etätyöntekijän koti. Myös kotioloissa täytyy varmistua siitä, että perheenjäsenillä ei ole pääsyä työntekijän käsittelemiin henkilötietoihin. Työnantaja voi edellyttää ennen etätyöhön siirtymistä, että työntekijällä on kotonaan käytettävissä erillinen työhuone[133]. Työpisteen fyysiseen suojaukseen tulee kiinnittää huomiota etätyön tietoturvallisuutta tarkasteltaessa[134].

Vaikka etätyötä tehtäisiin sille varatussa erillisessä tilassa, kuten työhuoneessa, voivat perheenjäsenet joissain tilanteissa saada tietoonsa tietosuojan piiriin kuuluvia tietoja. Kotona sijaitseva työhuone on vain harvoin äänieristetty tila. Jos työ sisältää asiakaspalvelua puhelimitse, voivat perheenjäsenet kuulla henkilötietojen suojan piiriin kuuluvia tietoja. Yhden puhelun aikana saatetaan käydä läpi tunnistetietoja, jotka ovat

[132] Helle 2004, s. 126.
[133] Helle 2004, s. 127.
[134] Helle 2004, s. 196.

yhdistettävissä tiettyyn henkilöön. Myös organisaation sisäiset palaverit voivat sisältää keskustelua asiakkaista, jolloin henkilötiedot voivat olla yhdistettävissä henkilöön.

Perheenjäsenten lisäksi työntekijän tulee huomioida etätyöntekopaikassa muut ulkopuoliset henkilöt. Asunnon äänieristys voi olla puutteellinen, jolloin ääni kantautuu asunnon ulkopuolelle. Kun ääni kantautuu toiseen asuntoon tai esimerkiksi rappukäytävään, voi ulkopuolinen henkilö kuulla tietosuojan piiriin kuuluvia tietoja. Työntekijä saattaa puhua puhelimeen tai keskustella palaverissa asiakkaista, jolloin tiedot voivat pahimmillaan olla yhdistettävissä henkilöön. Vaikka varsinaisia henkilötietoja ei huonosta äänieristyksestä huolimatta ulkopuolisille asti kantautuisi, on vaarana organisaation sisäisten asioiden leviäminen ulkopuolisten tietoon. Tietojen leviäminen on kiusallista ja voi vaikuttaa organisaation luotettavuuteen asiakkaiden keskuudessa.

Työn tekeminen ulkotiloissa, kuten terassilla tai parvekkeella, on erittäin riskialtista tietosuojan näkökulmasta. Työntekijän pitäisi ulkotiloissa työskennellessään varmistua siitä, että ulkopuolisilla ei ole näkö- tai kuuloyhteyttä henkilötietoihin. Tämä voi useissa tilanteissa olla erittäin vaikeaa. Ulkopuoliset voivat saada tietoonsa tietosuojan piiriin kuuluvia tietoja esimerkiksi niin, että heillä on mahdollisuus nähdä etätyöntekijän käyttämän tietokoneen näyttö tai he kuulevat, kun etätyöntekijä keskustelee henkilötiedoista. Organisaation kannalta turvallisin vaihtoehto on, että henkilötietojen käsitteleminen ulkotiloissa, julkisissa kulkuvälineissä ja julkisissa tiloissa kielletään organisaation etätyötä ja tietoturvaa koskevissa ohjeissa.

3.4 Henkilötietoja sisältävät asiakirjat

Tietotekniset laitteet ja ohjelmistot, jotka sisältävät henkilötietoja, voidaan suojata käyttäjätunnuksilla ja salasanoilla. Etätyössä työntekijä saattaa hyödyntää sähköisten asiakirjojen lisäksi paperimuodossa olevia asiakirjoja, kuten tulosteita. Paperisten asiakirjojen lisäksi työntekijä voi tehdä muistiinpanoja käsin. Käsintehdyt muistiinpanot voivat sisältää tietosuojan piiriin kuuluvia tietoja. Koska henkilötietoja ovat kaikki sellaiset tiedot,

joiden perusteella henkilö voidaan suoraan tai epäsuorasti tunnistaa, on esimerkiksi käsin tehty muistiinpano asiakkaan nimestä, osoitteesta ja henkilötunnuksesta tietosuojan piiriin kuuluvaa tietoa. Etätyössä työntekijä ei välttämättä ajattele tulostetun asiakirjan tai käsintehdyn muistiinpanon olevan riski tietosuojalle, koska säilyttää sitä kotonaan. On kuitenkin mahdollista, että henkilötietoja sisältävät asiakirjat ja muistiinpanot päätyvät perheenjäsenen tai muun ulkopuolisen luettavaksi. Tällöin kyseessä on henkilötietojen tietoturvaloukkaus.

Asiakirjojen käyttö, säilytys ja hävittäminen voivat etätyössä erota suuresti siitä, miten työnantajan tiloissa toimitaan. Osittain työnantajan tiloissa ja osittain etänä tehtävä työ voi aiheuttaa sen, että asiakirjoja kuljetetaan työnantajan tilojen ja etätyöpaikan välillä. Tällöin asiakirjojen häviäminen tai jopa varastaminen on mahdollista. Häviämisen ja varastamisen lisäksi henkilötietoja sisältävien asiakirjojen hävittäminen voi etätyössä olla huolimatonta. Työnantajan tiloissa paperiset asiakirjat, jotka sisältävät henkilötietoja, voidaan hävittää tietoturvaroskisten avulla. Arkaluonteiset materiaalit laitetaan lukolliseen roskikseen, ja papereiden turvallisesta hävittämisestä vastaa jäteyhtiö. Toinen vaihtoehto on papereiden syöttäminen silppuriin, jolloin tiedot muuttuvat tunnistamattomaan muotoon.[135] Työntekijän kotona vastaavanlainen tietoturvallinen papereiden hävittäminen ei ole mahdollista. Jos työntekijä ei tuhoa asiakirjoja esimerkiksi polttamalla, voivat henkilötiedot päätyä vääriin käsiin roskiksesta.

Varmin tapa välttyä henkilötietoja sisältävien paperisten asiakirjojen päätymisestä ulkopuolisten käsiin on se, että etätyöntekijä ei tulosta tai käytä niitä lainkaan etätyössä. Työnantaja voi tietoteknisillä ratkaisuilla estää tulostamisen muilla laitteilla, kuin työnantajan tiloissa olevilla tulostimilla. Työnantajalla ei ole kuitenkaan mahdollisuutta vaikuttaa siihen, kirjaako työntekijä henkilötietoja paperille käsin. Tällöin korostuu työnantajan tietoturvaohjeistuksen tärkeys etätyöntekijälle. Etätyöntekijän tulee ensinnäkin ymmärtää, mitkä tiedot ovat henkilötietoja. Lisäksi työnantajan tulee ohjeistaa henkilötietoja sisältävien asiakirjojen säilyttämisestä ja tuhoamisesta etätyössä. Varmin tapa

[135] Järvinen & Rousku 2017, s. 53.

suojata henkilötiedot on, että asiakirjoja käsitellään etätyössä ainoastaan sähköisessä muodossa. Jos tämä ei jostain syystä ole mahdollista, tulee paperisia asiakirjoja ja muistiinpanoja säilyttää niin, että ulkopuolisella ei ole pääsyä niihin. Lukollinen kaappi, jonka avain on ainoastaan työntekijän saatavilla, on turvallinen vaihtoehto paperisten asiakirjojen säilyttämiselle.

3.5 Erityiset henkilötietoryhmät

Tietoturvallisuuden merkitys kasvaa erityisesti silloin, kun työskennellään arkaluontoisten tietojen parissa. Erityistä huolellisuutta etätyön tietosuojan kannalta edellyttävät erityiset henkilötietoryhmät. Aiemmin erityisiä henkilötietoryhmiä kutsuttiin arkaluonteisiksi tiedoiksi, mutta tietosuoja-asetuksen myötä nimitys muuttui[136]. Erityisistä henkilötietoryhmistä ja niiden käsittelystä säädetään tietosuoja-asetuksen 9 artiklassa. Sen mukaan erityisiin henkilötietoryhmiin luetaan sellaiset henkilötiedot, joista ilmenee rotu tai etninen alkuperä, poliittiset mielipiteet, uskonnollinen tai filosofinen vakaumus sekä ammattiliiton jäsenyys. Lisäksi erityisiin henkilötietoryhmiin kuuluvat geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten, terveyttä koskevat tiedot sekä luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevat tiedot.

Erityisten henkilötietoryhmien käsittely on tietosuoja-asetuksen 9 artiklan kohdan 1 mukaan lähtökohtaisesti kiellettyä. Erityisiin henkilötietoryhmiin kuuluvia henkilötietoja saa käsitellä, jos käsittelykieltoon on säädetty poikkeus tietosuoja-asetuksessa, unionin oikeudessa tai kansallisessa lainsäädännössä[137]. Erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyä ei voi myöskään kiertää siten, että käyttäisi sellaista henkilöä koskevaa kuvausta, joka ainoastaan välillisesti paljastaisi arkaluonteisia henkilötietoja[138]. Tietosuoja-asetus sallii erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyn silloin, jos

[136] Korpisaari ja muut 2018, s. 148.
[137] Tietosuojavaltuutetun toimisto 2022a.
[138] Korpisaari ja muut 2018, s. 151.

sekä yleinen että erityinen käsittelyperuste täyttyy. Yleisistä käsittelyperusteista säädetään tietosuoja-asetuksen artiklassa 6 ja erityisistä artiklassa 9. Erityisiä henkilötietoryhmiä voidaan käsitellä esimerkiksi silloin, kun käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi (6 artikla, kohta c) ja käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojelemiseksi, ja rekisteröity on fyysisesti tai juridisesti estynyt antamaan suostumustaan (9 artikla, kohta c).

Erityisten henkilötietoryhmien käsittelylle tulee olla laillinen peruste kaikessa käsittelyssä, myös etätyössä. Etätyöntekijän on hyvä tiedostaa tietojen arkaluontoisuus. Erityisiin henkilötietoryhmiin kuuluvien tietojen paljastuminen ulkopuoliselle voi aiheuttaa uhkan rekisteröidyn oikeuksille ja vapauksille. Etätyössä erityisistä henkilötietoryhmistä puhuttaessa, niitä ylös kirjatessa ja niiden säilyttämisessä tulee huomioida etätyön ympäristö. Muun muassa huonosti suojattu työtila tai tietojen huolimaton säilyttäminen voivat aiheuttaa sen, että erityisiin henkilötietoryhmiin kuuluvia tietoja päätyy ulkopuolisten tietoon.

Jos henkilötietojen käsittelyyn kohdistuu todennäköisesti korkea riski luonnollisten henkilöiden oikeuksille ja vapauksille, edellyttää tietosuoja-asetus vaikutustenarvioinnin eli DPIA:n (*data protection impact assessment*) tekemistä. Erityiset henkilötietoryhmät luokitellaan sellaisiksi korkean riskin tiedoiksi, joiden käsittely edellyttää vaikutustenarvioinnin tekemistä. Vaikutustenarvioinnilla tarkoitetaan prosessia, jossa rekisterinpitäjä arvioi suunniteltua henkilötietojen käsittelyä ja sen hyväksyttävyyttä tietosuojaperiaatteiden toteutumisen kannalta. Vaikutustenarvioinnissa arvioidaan käsittelyn aiheuttamat uhat rekisteröidyn oikeuksille ja vapauksille, riskien todennäköisyys ja vaikuttavuus. Jos käsittelyyn sisältyy todennäköisesti korkea riski rekisteröidyn oikeuksille ja vapauksille, valitaan tekniset ja organisatoriset keinot, joilla riski saadaan laskettua hyväksyttävälle tasolle.[139]

[139] Andreasson ja muut 2019, s. 67–68.

Henkilötietojen käsittely voidaan aloittaa vasta sitten, kun vaikutustenarvioinnissa todetut riskit on saatu hyväksyttävälle tasolle. Tämä tarkoittaa sitä, että vaikutustenarviointi on tehtävä ennen henkilötietojen käsittelyn aloittamista. Vaikutustenarvioinnista säädetään tietosuoja-asetuksen 35 artiklassa. Sen mukaan vaikutustenarviointiin on vähintään sisällytettävä järjestelmällinen kuvaus käsittelytoimista ja käsittelyn tarkoituksista sisältäen tarvittaessa rekisterinpitäjän oikeutetut edut, arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden, arvio rekisteröidyn oikeuksiin ja vapauksiin kohdistuvista riskeistä suunniteltujen käsittelytoimien osalta sekä ne toimenpiteet, joilla näihin riskeihin puututaan. Etätyö voi olla sellainen työnteon muoto, jonka käyttöönotto edellyttää vaikutustenarviointien päivitystä erityisten henkilötietoryhmien osalta etätyön mukaisiksi.

Syksyllä 2020 kävi ilmi erittäin laaja erityisiin henkilötietoryhmiin kuuluviin tietoihin kohdistunut tietomurto, kun Psykoterapiakeskus Vastaamoon kohdistunut tietomurto ilmoitettiin tietosuojavaltuutetun toimistolle. Vastaamon asiakkaiden nimet, osoitteet, henkilötunnukset ja potilaskertomukset olivat päätyneet tietomurron kohteeksi. Rikollinen julkaisi Tor-verkossa varastamiaan tietoja, ja ne sisälsivät arkaluontoisia tietoja asiakkaiden yksityiselämästä. Varastettujen tietojen avulla rikollinen yritti kiristää Vastaamolta lunnaita, jotta tietojen julkistaminen lopetetaan.[140] Vastaamon tapaus on esimerkki siitä, mitä pahimmillaan voi tapahtua erityisiin henkilötietoryhmiin kuuluvien tietojen, kuten potilaskertomusten, vuotamisesta ulkopuolisille. Tämän vuoksi etätyössä käsiteltävien erityisiin henkilötietoryhmiin kuuluvien tietojen kanssa tulee olla erittäin huolellinen.

[140] Rimpiläinen 2020.

4 Tietoturvaloukkauksen seuraukset

4.1 Seuraukset rekisteröidylle

Rekisteröidyn henkilötietoihin kohdistuvasta tietoturvaloukkauksesta ei automaattisesti aiheudu seurauksia suoraan rekisteröidylle itselleen. Mahdolliset seuraukset rekisteröidylle riippuvat siitä, mitä tietoja rekisteröidystä on joutunut ulkopuolisille, kenelle tiedot ovat päätyneet ja käytetäänkö tietoja jollain tapaa hyväksi. Jos seurauksia aiheutuu, voivat ne olla fyysisiä, aineellisia, aineettomia, taloudellisia tai sosiaalisia[141]. Seuraukset voivat näin ollen olla hyvin moniulotteisia ja aiheuttaa haittaa rekisteröidyn oikeuksille ja vapauksille monella tapaa.

Tietoturvaloukkaus voi aiheuttaa rekisteröidylle taloudellisia menetyksiä, maineen vahingoittumista, salassa pidettävien henkilötietojen paljastumista tai rikollisuuden, kuten identiteettivarkauden, kohteeksi joutumista. Taloudellista menetystä voi seurata esimerkiksi maksukorttitietojen päätymisestä rikollisten saataville. Rekisteröidyn maine voi vahingoittua, jos häntä koskevat arkaluonteiset tiedot leviävät tietoturvaloukkauksen seurauksena. Arkaluonteiset tiedot voivat johtaa myös rekisteröityyn kohdistuviin kiristys- tai kiusaamistilanteisiin. Pelkän sähköpostiosoitteen paljastuminen väärälle taholle voi aiheuttaa sähköpostiin tulvivia kalasteluyrityksiä ja ei-toivottua mainontaa. Rekisteröityyn kohdistuva identiteettivarkaus on mahdollinen silloin, jos rikollinen saa käsiinsä esimerkiksi rekisteröidyn henkilötunnuksen.[142]

Identiteettivarkauden myötä rekisteröidylle voi aiheutua taloudellisia tappioita, kun rikollinen tilaa hänen lukuunsa tuotteita nettikaupoista. Tietoturvaloukkauksella voi olla myös fyysisiä seurauksia rekisteröidylle. Esimerkiksi nimi- ja osoitetietojen paljastuminen voi pahimmassa tapauksessa johtaa rekisteröidyn taustan tai muiden syiden vuoksi

[141] Andreasson ja muut 2019, s. 171.
[142] Tietosuojavaltuutetun toimisto 2022b.

siihen, että rekisteröity joutuu väkivallan uhriksi. Rikoksen uhriksi joutuminen on äärimmäinen seuraus henkilötietoihin kohdistuvasta tietoturvaloukkauksesta.

Tietoturvaloukkauksen seuraukset rekisteröidylle eivät välttämättä ilmene välittömästi tietoturvaloukkauksen tapahduttua. Henkilötietojen hyödyntäminen haitallisiin tai jopa rikollisiin tarkoituksiin voi tapahtua vasta monen vuoden kuluttua tietoturvaloukkauksesta. Tämän vuoksi rekisteröidyn voi olla vaikea havaita hänen tietoihinsa kohdistunutta tietoturvaloukkausta. Henkilötietoja käsittelevän organisaation on kerrottava rekisteröidylle, jos aiheutunut tietoturvaloukkaus aiheuttaa todennäköisesti korkean riskin rekisteröidyn oikeuksille ja vapauksille.[143]

Etätyö voi erityispiirteidensä vuoksi myötävaikuttaa tietoturvaloukkauksen aiheutumiseen. Etätyössä käytettävän tietotekniikan sekä verkko- ja etäyhteyden puutteellinen suojaaminen voi aiheuttaa henkilötietojen vuotamisen verkkoon. Jos etätyössä käsitellään erityisiin henkilötietoryhmiin kuuluvia tietoja, voi niiden vuotaminen verkkoon aiheuttaa rikoksen uhriksi joutumisen lisäksi sosiaalisia seurauksia rekisteröidylle. Esimerkiksi tiedot rekisteröidyn yksityiselämästä ja terveydentilasta voivat vaikuttaa hänen maineeseensa ja sosiaalisiin suhteisiinsa. Etätyössä huolimattomasti säilytettävät tai hävitettävät henkilötietoja sisältävät asiakirjat voivat päätyä rikollisiin käsiin, jolloin rekisteröity voi joutua muun muassa identiteettivarkauden kohteeksi. Jos etätyötä tehdään sellaisessa paikassa, jossa ulkopuolisilla on pääsy henkilötietoihin, seuraukset rekisteröidylle voivat yhtä lailla aiheuttaa aineellisia ja aineettomia seurauksia. Kuten muissakin tietoturvaloukkauksissa, etätyössä tapahtuvien tietoturvaloukkausten seuraukset riippuvat siitä, mitä tietoja rekisteröidystä on päätynyt ulkopuolisille, kenelle tiedot ovat oikeudetta päätyneet ja päättääkö tiedot saanut henkilö hyödyntää tietoja.

Rekisteröidyllä on mahdollisuus reagoida hänen tietoihinsa kohdistuneeseen tietoturvaloukkaukseen, kun hän saa loukkauksesta tiedon. Tietosuoja-asetuksen VIII luvussa säädetään oikeussuojakeinoista, vastuusta ja seuraamuksista pääasiassa sellaisissa

[143] Tietosuojavaltuutetun toimisto 2022b.

tilanteissa, joissa joku katsoo itselleen tai toiselle tietosuoja-asetuksessa määrättyjen oikeuksien tulleen loukatuksi[144]. VIII lukuun sisältyvät artiklat 77–84. Tietosuoja-asetuksen artikla 77 turvaa rekisteröidyn oikeuden tehdä valitus valvontaviranomaiselle, jos hänen mielestään EU:n yleistä tietosuoja-asetusta on rikottu hänen henkilötietojensa käsittelyssä. Valitus tehdään sen jäsenvaltion valvontaviranomaiselle, jossa rekisteröity asuu, työskentelee tai jossa tietosuoja-asetusta on rikottu. Suomessa valvontaviranomaisena toimii tietosuojavaltuutettu. Artikla 78 säätelee rekisteröidyn oikeutta tehokkaisiin oikeussuojakeinoihin valvontaviranomaista vastaan. Tämä tarkoittaa sitä, että jokaisella rekisteröidyllä on oikeus nostaa kanne häntä oikeudellisesti sitovasta valvontaviranomaisen tekemästä päätöksestä. Kanne valvontaviranomaista vastaan nostetaan sen jäsenvaltion tuomioistuimessa, jossa valvontaviranomainen toimii. Suomessa rekisteröidyllä on näin ollen oikeus valittaa tietosuojavaltuutetun päätöksestä Helsingin hallinto-oikeuteen. Valvontaviranomaiselle tehtävän valituksen ja valvontaviranomaisen päätöksestä tehtävän valituksen lisäksi rekisteröidyllä on tietosuoja-asetuksen 79 artiklan mukaan oikeus nostaa kanne rekisterinpitäjää tai henkilötietojen käsittelijää vastaan. Kanne nostetaan siinä yleisessä alioikeudessa, jossa rekisterinpitäjällä tai henkilötietojen käsittelijällä on toimipaikka.[145]

Jos rekisteröity epäilee, että häntä koskevia henkilötietoja käsitellään väärin, rekisteröidyn on suositeltavaa ottaa yhteyttä ensimmäisenä rekisterinpitäjään. Tällöin rekisterinpitäjä voi tehdä tarvittavat toimenpiteet tilanteen korjaamiseksi, jos korjattavaa on. Rekisteröidyn itsensä lisäksi kuka tahansa ulkopuolinen, joka epäilee henkilötietojen käsittelyssä tapahtuvan virheitä, voi olla yhteydessä rekisterinpitäjään ja ilmoittaa tälle epäilyksensä näistä virheistä. Jos ilmoitus tulee ulkopuoliselta, on rekisterinpitäjän tapauksesta riippuen ilmoitettava asiasta rekisteröidylle. Lisäksi rekisterinpitäjä tekee tarvittaessa ilmoituksen tietosuojavaltuutetulle. Rekisteröidyn tai ulkopuolisen ilmoittajan

[144] Korpisaari ja muut 2018, s. 507.
[145] Korpisaari ja muut 2018, s. 508–516.

kannattaa harkita ilmoituksen tekemistä myös tietosuojavaltuutetulle, jotta voi varmistua asian etenemisestä ja puutteiden korjaamisesta henkilötietojen käsittelyssä.[146]

Tietosuojavaltuutetun toimisto ei ilmoita asian etenemisestä ja ratkaisusta ulkopuoliselle, mutta saattaa olla yhteydessä ilmoittajaan erityisestä syystä. Rekisteröity voi tehdä ilmoituksen tietosuojavaltuutetulle myös silloin, jos hän haluaa käyttää tietosuojaan liittyviä oikeuksiaan, mutta rekisterinpitäjä kieltäytyy. Tietosuojavaltuutettu voi määrätä rekisterinpitäjän toteuttamaan pyynnön, jos siihen on aihetta. Tietosuojavaltuutettu ei toimi kuitenkaan esitutkintaviranomaisena tai asiamiehenä, joten rikosasioissa rekisteröidyn on oltava yhteydessä poliisiin.[147]

Rekisteröidyllä on mahdollisuus hakea vahingonkorvausta hänen henkilötietoihinsa kohdistuneesta tietoturvaloukkauksesta. Vahingonkorvausta haetaan ensisijaisesti rekisterinpitäjältä. Jos rekisterinpitäjä ei suostu rekisteröidyn esittämiin vaatimuksiin, voi rekisteröity nostaa kanteen tuomioistuimessa tietosuoja-asetuksen perusteella.[148] Tietosuoja-asetuksen 82 artikla määrittää vastuun ja oikeuden korvauksen saamiseen. Sen mukaan henkilöllä on oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvaus aiheutuneesta vahingosta, jos hänelle aiheutuu asetuksen rikkomisesta aineellista tai aineetonta vahinkoa. Vahingonkorvausvelvollisuus voi olla merkittävä tekijä henkilötietoja käsitteleville tahoille silloin, kun ne harkitsevat, millaisia riskejä niiden kannattaa henkilötietoihin liittyen ottaa[149].

Oikeus vahingonkorvaukseen tietosuojasäännösten rikkomisen yhteydessä perustuu siihen, että säännösten rikkomisesta voi aiheutua henkilölle huomattaviakin vahinkoja. Tällöin vahingot on tarpeen saada korvattua. Vahingonkorvausta voi saada sekä aineellisesta että aineettomasta vahingosta. Aineellisia vahinkoja ovat puhtaat varallisuusvahingot. Rekisteröity voi menettää muun muassa ansiotuloja tai muita tuloja henkilötietojen

[146] Tietosuojavaltuutetun toimisto 2022c.
[147] Tietosuojavaltuutetun toimisto 2022c.
[148] Tietosuojavaltuutetun toimisto 2022d.
[149] Korpisaari ja muut 2018, s. 523.

lainvastaisen käsittelyn vuoksi esimerkiksi silloin, kun julkisuuteen vuotaa tietoa, joka johtaa luottamustoimen ja sen hoitamisesta maksettavien palkkioiden menettämiseen. Aineettomia vahinkoja voidaan korvata kärsimykseen perustuvalla korvauksella. Kärsimyksellä tarkoitetaan vahingonkorvausoikeudessa tunnetta, joka henkilölle aiheutuu häneen kohdistuvan oikeudettoman loukkauksen vuoksi. Kärsimyksen korvaaminen ei edellytä psyykkistä terveydentilan häiriötä. Henkilötietojen tietoturvaloukkausta koskeva vahingonkorvaus perustuu yleisen tietosuoja-asetuksen 82 artiklan lisäksi vahingonkorvauksiin liittyviin säännöksiin.[150] Jos tietoturvaloukkaukseen liittyy rikosasia, esimerkiksi yksityiselämään liittyvän tiedon levittäminen tai tietomurto, voi vahingonkorvausvaatimuksen esittää rikosoikeudenkäynnin yhteydessä[151].

4.2 Seuraukset rekisterinpitäjälle ja henkilötietojen käsittelijälle

Rekisterinpitäjä on se taho, joka määrittää miksi ja miten henkilötietoja käsitellään. Henkilötietojen käsittelijä on taho, joka käsittelee henkilötietoja rekisterinpitäjän puolesta.[152] Rekisterinpitäjä on vastuussa siitä, että se käyttää luotettavia henkilötietojen käsittelijöitä, jotka pystyvät suoriutumaan tehtävästä. Henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän tarkoituksia varten rekisterinpitäjän antamien ohjeiden mukaan. Jos henkilötietojen käsittelijä ryhtyy käsittelemään henkilötietoja omiin tarkoituksiinsa, tulee siitä rekisterinpitäjä.[153]

Rekisterinpitäjälle ja henkilötietojen käsittelijälle voi aiheutua rekisteröidyn tavoin aineellisia ja aineettomia vahinkoja henkilötietoihin kohdistuvista tietoturvaloukkauksista. Aineellisia vahinkoja ovat taloudelliset menetykset mahdollisten hallinnollisten sakkojen eli hallinnollisten seuraamusmaksujen, vahingonkorvausten ja oikeudenkäyntikulujen muodossa. Aineettomia vahinkoja ovat luottamuksen ja maineen rapistuminen

[150] Korpisaari ja muut 2018, s. 523, 526–527.
[151] Tietosuojavaltuutetun toimisto 2022d.
[152] Tietosuojavaltuutetun toimisto 2022e.
[153] Korpisaari ja muut 2018, s. 293.

asiakkaiden ja yhteistyökumppaneiden keskuudessa. Luottamuksen ja maineen menettäminen voivat johtaa välillisesti myös taloudellisiin tappioihin, kun asiakkaat siirtyvät käyttämään luotettavammaksi koetun kilpailijan tuotteita tai palveluita. Yhteistyökumppanit voivat asiakkaiden tavoin siirtyä käyttämään kilpailijaa tietoturvaa loukanneen organisaation sijaan.

Tietoturvaloukkaukset voivat johtaa valvontaviranomaisen asettamiin sanktioihin. Rekisterinpitäjä ja henkilötietojen käsittelijä voidaan määrätä muuttamaan toimintatapaansa henkilötietojen käsittelyn osalta, tai joissain tilanteissa asettaa jopa käsittelykieltoon. Nämä keinot perustuvat yleisen tietosuoja-asetuksen 58 artiklaan, jossa säädetään riippumattomien valvontaviranomaisten valtuuksista. Valvontaviranomaisella on tietosuoja-asetuksen 58 artiklan 2 kohdan mukaiset korjaavat toimivaltuudet. Valvontaviranomainen, joka Suomessa on tietosuojavaltuutettu, voi antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle varoituksen silloin, kun aiotut käsittelytoimet ovat todennäköisesti yleisen tietosuoja-asetuksen vastaisia. Huomautuksen rekisterinpitäjä tai henkilötietojen käsittelijä saa silloin, jos käsittelytoimet ovat olleet asetuksen vastaisia. Tietosuojavaltuutettu voi määrätä rekisterinpitäjän tai henkilötietojen käsittelijän noudattamaan rekisteröidyn pyyntöjä omien oikeuksiensa käyttämisen osalta. Myös rekisterinpitäjän tai henkilötietojen käsittelijän käsittelytoimet voidaan määrätä saattamaan asetuksen säännösten mukaisiksi, tarvittaessa tietyllä tavalla ja tietyn määräajan kuluessa. Tietosuojavaltuutetun antama määräys voi myös koskea sitä, että rekisterinpitäjän on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisteröidylle. Tietosuojavaltuutettu voi myös asettaa väliaikaisen tai pysyvän rajoituksen henkilötietojen käsittelylle, mukaan lukien käsittelykiellon. Tietosuojavaltuutettu voi määrätä tilanteesta riippuen hallinnollisen sakon.[154] Hallinnollisesta sakosta käytetään Suomessa pääosin nimikettä hallinnollinen seuraamusmaksu, koska se sopii Suomen oikeusjärjestelmään paremmin[155].

[154] Korpisaari ja muut 2018, s. 457.
[155] Korpisaari ja muut 2018, s. 535.

Etätyössä paperisten henkilötietoja sisältävien asiakirjojen häviäminen työnantajan tilojen ja etätyöpaikan välillä on tietoturvaloukkaus. Rekisterinpitäjän on ilmoitettava asiakirjojen häviämisestä rekisteröidyille, jos se todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille ja vapauksille. Jos rekisterinpitäjällä ei ole tiedossa, kenen tietoja hävinneet asiakirjat sisältävät, on tiedonanto tehtävä julkisesti tai muulla rekisteröidyn kannalta tehokkaalla tavalla. Tämä käy ilmi tietosuojavaltuutetun antamasta määräyksestä Kelalle. Kelan asiakkaiden toimistoon jättämiä asiakirjoja sisältämä postipaketti katosi matkalla skannauspisteeseen. Kelalla ei ollut mahdollisuutta selvittää, keiden tietoja paketti sisälsi. Tietosuojavaltuutettu määräsi Kelan rekisterinpitäjänä tiedottamaan rekisteröidylle tietoturvaloukkauksesta julkisella tiedonannolla tai muulla toimenpiteellä, jolla tiedottaminen on yhtä tehokasta.[156]

Tietosuoja-asetuksen 83 artiklassa säädetään hallinnollisten sakkojen määräämisen yleisistä edellytyksistä. Tietosuojalain 24 § täsmentää tietosuoja-asetusta hallinnollisten sakkojen osalta, ja siinä käytetään hallinnollisen sakon sijaan Suomen oikeusjärjestykseen paremmin sopivaa termiä hallinnollinen seuraamusmaksu. Tietosuoja-asetuksen 83 artiklan kohdan 1 mukaan hallinnollisten sakkojen määräämisen on oltava kussakin yksittäistapauksessa tehokasta, oikeasuhteista ja varoittavaa. Tietosuojalain 24.1 §:n mukaan hallinnollisen sakon määrää Suomessa seuraamuskollegio, ja seuraamuskollegion muodostavat puheenjohtajana toimiva tietosuojavaltuutettu yhdessä apulaistietosuojavaltuutettujen kanssa. Päätösvaltainen seuraamuskollegio on kolmijäsenisenä.

Hallinnollisen sakon määrästä säädetään tietosuoja-asetuksen 83 artiklan kohdassa 5. Hallinnollinen sakko voi olla enintään 20 miljoonaa euroa, tai neljä prosenttia yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Artiklan 83 kohdan 7 mukaan kukin jäsenvaltio voi asettaa sääntöjä siitä, voidaanko viranomaisille tai julkishallinnon elimille määrätä hallinnollisia sakkoja ja missä määrin niitä voidaan määrätä. Tietosuojalain 24.4 §:n mukaan Suomessa hallinnollista sakkoa ei voida määrätä julkishallinnon organisaatioille,

[156] Tietosuojavaltuutetun päätös 10.10.2019, diaarinumero 2691/171/19.

kuten valtion viranomaisille tai valtion liikelaitoksille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle tai evankelis-luterilaiselle kirkolle tai ortodoksiselle kirkolle taikka niiden seurakunnille tai muille elimille.

Tietosuojavaltuutetun toimisto antoi rekisterinpitäjille vuonna 2020 yhteensä 40 määräystä ilmoittaa tietoturvaloukkauksesta rekisteröidylle. Määräyksiä saattaa henkilötietojen käsittelytoimet tietosuoja-asetuksen mukaisiksi annettiin 33 kappaletta. Lisäksi tietosuojavaltuutetun toimisto antoi 36 huomautusta tietosuoja-asetuksen vastaisista käsittelytoimista. Seuraamuskollegio määräsi vuonna 2020 myös ensimmäiset hallinnolliset seuraamusmaksut. Seuraamusmaksuja määrättiin viidelle yritykselle, ja niiden suuruus vaihteli 7000 eurosta 100 000 euroon.[157] Suurin seuraamusmaksu tähän mennessä on määrätty Psykoterapiakeskus Vastaamolle joulukuussa 2021. Sen suuruus on 608 000 euroa.[158] Tähän mennessä määrätyistä seuraamusmaksuista voidaan todeta, että taloudelliset seuraukset henkilötietojen tietoturvaloukkauksesta voivat olla tietoturvaa loukanneelle organisaatiolle tuntuvat.

Maineen rapistumisen, tietosuojavaltuutetun antamien varoitusten, huomautusten ja määräysten sekä hallinnollisten seuraamusmaksujen ja vahingonkorvausten lisäksi rekisterinpitäjä ja henkilötietojen käsittelijä voivat joutua tietoturvaloukkauksesta rikosoikeudelliseen vastuuseen. Tietosuoja-asetuksen 84 artiklan 1 kohdassa velvoitetaan jäsenvaltiot vahvistamaan säännöt asetuksen rikkomisen seuraamuksista. Erityisesti seuraamukset on vahvistettava niiden rikkomisten osalta, joihin ei sovelleta hallinnollisia sakkoja. Seuraamusten on oltava hallinnollisten sakkojen tavoin tehokkaita, oikeasuhteisia ja varoittavia. Suomessa rangaistussäännökset määritetään tietosuojalaissa. Tietosuojalain 26.1 §:n mukaan rangaistus tietosuojarikoksesta säädetään rikoslain[159] 38 luvun 9 §:ssä.

[157] Tietosuojavaltuutetun toimisto 2021d, s. 10–11.
[158] Tietosuojavaltuutetun päätös 7.12.2021, diaarinumero 1150/161/2021.
[159] Rikoslaki 39/1889.

Rikoslain 38 luvun 9 §:n mukaan rekisterinpitäjä tai henkilötietojen käsittelijä tuomitaan tietosuojarikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Tietoturvaloukkauksen tapahduttua henkilötietojen käsittelijän on ilmoitettava siitä viipymättä rekisterinpitäjälle. Rekisterinpitäjä tekee tietoturvaloukkauksesta ilmoituksen tietosuojavaltuutetulle ja tarvittaessa myös rekisteröidylle. Henkilötietojen käsittelijä voi tehdä ilmoituksen itse suoraan tietosuojavaltuutetulle ja tarvittaessa rekisteröidylle, jos tästä on selvästi sovittu rekisterinpitäjän ja henkilötietojen käsittelijän välisessä sopimuksessa. Rekisterinpitäjällä on tästä huolimatta vastuu ilmoitusvelvollisuuden toteuttamisesta.[160]

4.3 Seuraukset työtekijälle

Työntekijä käsittelee henkilötietoja rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa. Tietojenkäsittelystä rekisterinpitäjän ja henkilötietojen käsittelijän alaisuudessa säädetään tietosuoja-asetuksen 29 artiklassa. Sen mukaan henkilö, jolla on pääsy henkilötietoihin, ja joka toimii henkilötietojen käsittelijän tai rekisterinpitäjän alaisuudessa, ei saa käsitellä henkilötietoja muuten, kuin rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä niin vaadita. Tämä tarkoittaa sitä, että työntekijän on noudatettava henkilötietojen käsittelyssä rekisterinpitäjän antamia ohjeita. Toisaalta työnantaja ei voi vaatia työntekijää toimimaan lain tai hyvän tavan vastaisesti[161].

Tietoturvaloukkauksesta voi aiheutua seurauksia rekisteröidyn, rekisterinpitäjän ja henkilötietojen käsittelijän lisäksi myös työntekijälle itselleen, jos hän ei toimi rekisterinpitäjän antamien ohjeiden tai lainsäädännön asettamien vaatimusten mukaan, ja aiheuttaa omalla toiminnallaan tietoturvaloukkauksen. Seuraukset työntekijälle riippuvat hänen

[160] Tietosuojavaltuutetun toimisto 2022f.
[161] Työsuojeluhallinto 2021.

osuudestaan tietoturvaloukkauksen aiheutumisessa, sekä tietoturvaloukkauksen aiheuttamista seurauksista.

Työnantajalla on työnjohtovalta eli direktio-oikeus. Työn valvominen, työn turvallisuudesta huolehtiminen, suoriutumisen mittaaminen sekä poikkeamiin reagoiminen ovat työnantajan työnjohtovaltaan perustuvia oikeuksia ja velvollisuuksia. Työntekijän velvollisuutena on tehdä työ työnantajan antamien ohjeiden ja määräysten mukaisesti.[162] Jos työntekijä rikkoo työnantajan antamia ohjeistuksia, voi hän saada siitä huomautuksen. Työntekijä voi saada varoituksen, jos virhe tai laiminlyönti on merkittävä. Työnantaja voi päättää työsuhteen, jos virheet ja laiminlyönnit ovat toistuvia. Yksikin rike voi johtaa työsuhteen päättämiseen, jos sen johdosta työnantajalta ei voida kohtuudella edellyttää työsuhteen jatkamista.[163]

Tietoturvaloukkaus etätyössä voi johtaa työntekijän osalta huomautukseen tai varoitukseen. Pahimmillaan työntekijän työsuhde voi päättyä. Nämä seuraukset edellyttävät toteutuakseen kuitenkin sitä, että työntekijä toimii työnantajan ohjeiden vastaisesti ja rikkoo sen vuoksi tietosuojaa aiheuttaen henkilötietojen tietoturvaloukkauksen. Jos työntekijä noudattaa työnantajan ohjeita ja tietoturvaloukkaus aiheutuu siitä huolimatta, on vastuu työnantajalla. Työntekijä ei ole velvollinen oma-aloitteisesti selvittämään työnantajan turvallisuusjärjestelyjen asianmukaisuutta[164].

Etätyö voi työskentelymuotona aiheuttaa tietoturvariskien kasvamista. Jos tietoturvariskit toteutuvat, ei työ välttämättä sovellu tehtäväksi etätyönä. Työnantaja voi määrätä työntekijän työskentelemään työnantajan tiloissa etätyön sijaan, jos työ on luonteeltaan sellaista, ettei sitä voi tehdä tietoturvallisesti etänä. Etätyön puitesopimuksen 3 artiklan 5 kappaleen mukaan etätyö on peruutettavissa työ- ja/tai työehtosopimuksen mukaisesti, jos etätyö ei kuulu alkuperäiseen toimenkuvaan. Peruuttaminen voi tapahtua

[162] Vilkman 2016, luku 8.
[163] Työsuojeluhallinto 2021.
[164] Helle 2004, s. 195.

työntekijän tai työnantajan pyynnöstä. Etätyö on näin ollen peruutettavissa, mutta peruutettavuuden toimintatavoista on sovittava. Ensisijaisesti peruutettavuudesta sovitaan työehtosopimuksessa, mutta jos tällaisia määräyksiä ei ole, sovitaan peruutettavuudesta työpaikan etätyön pelisäännöissä tai niiden puuttuessa etätyösopimuksessa.[165] Työantajan työnjohto-oikeuteen kuuluu pääsääntöisesti määrätä työn sisältö, suoritustapa, työaika ja työpaikka[166]. Näin ollen työnantaja voi päättää, sopiiko työ tehtäväksi etätyönä.

Etätyö voi olla työntekijälle mieluinen tapa tehdä työtä silloin, jos hän kokee sen parantavan viihtymistä työssä. Työntekijän näkökulmasta etätyö lisää vapaa-aikaa, tarjoaa työrauhaa, lisää työhyvinvointia ja vähentää työmatkaan kuluvaa aikaa sekä työmatkakustannuksia[167]. Jos työnantaja evää työntekijältä mahdollisuuden etätyöhön tietoturvariskin tai tietoturvaloukkauksen vuoksi, voi työntekijän kokemus työn mielekkyydestä heikentyä. Työntekijän onkin kannattavaa huolehtia omalta osaltaan tietoturvallisuudesta etätyössä, jotta säilyttää mahdollisuutensa etätyön tekemiseen.

Työntekijälle voi seurata tietoturvaloukkauksesta huomautuksen, varoituksen, työsuhteen päättämisen tai etätyömahdollisuuden menettämisen lisäksi taloudellista vahinkoa. Työntekijä voi olla vahingonkorvausvelvollinen työnantajaansa kohtaan, jos hän tahallaan tai huolimattomuudellaan rikkoo tai laiminlyö työsopimuksen ja työsopimuslain mukaisia velvollisuuksia ja aiheuttaa tällä tavoin työnantajalle vahinkoa. Tästä työntekijän vahingonkorvausvelvollisuudesta säädetään työsopimuslain 12 luvun 1.3 §:ssä. Vahinko korvataan vahingonkorvauslain[168] 4 luvun 1 §:n perusteiden mukaan. Työntekijä ei ole korvausvastuussa, jos viaksi jää lievä tuottamus.[169]

Työntekijä voi joutua tahallisesta henkilötietojen tietoturvaloukkauksesta rikosoikeudelliseen vastuuseen. Tietosuojalain 35 §:n mukaan se, joka henkilötietoja käsitellessään

[165] Helle 2004, s. 119–120.
[166] Työsuojeluhallinto 2021.
[167] Helle 2004, s. 17.
[168] Vahingonkorvauslaki 412/1974.
[169] Erto 2022b.

saa tietää jotakin toisen henkilön ominaisuuksista, henkilökohtaisista oloista, taloudellisesta asemasta tai toisen liikesalaisuudesta, ei saa luovuttaa tietoja oikeudettomasti sivulliselle tai käyttää niitä omaksi tai toisen hyödyksi tai vahingoksi. Jos työntekijä toimii näin, voidaan hänet tuomita rikoslain 38 luvun 1 §:n salassapitorikoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi. Hänet voidaan myös tuomita rikoslain 38 luvun 2 §:n salassapitorikkomuksesta sakkoon, jos teko on kokonaisuutena arvioiden vähäinen. Myös virkasuhteessa olevat työntekijät voidaan tuomita rikokseen tietosuojaa loukatessaan. Korkein oikeus katsoi poliklinikan vastaavan lääkärin syyllistyneen tuottamukselliseen virkavelvollisuuden rikkomiseen, kun hän oli katsonut puolisonsa sukulaisen arkaluontoisia potilastietoja, vaikka ei osallistunut tämän hoitamiseen. Sukulainen oli nimenomaan toivonut, ettei kyseinen lääkäri lukisi hänen tietojaan.[170] Tapaus korostaa yksityisyyden suojan merkitystä arkaluontoisten tietojen osalta. Erityisiin henkilötietoryhmiin kuuluvien tietojen käsittelyssä on oltava huolellinen, jottei seurauksia aiheudu. Tietoturvaloukkauksen havaitessaan työntekijän tulee olla välittömästi yhteydessä työnantajaansa. Jokaisen työntekijän velvollisuuksiin kuuluu ilmoittaa havaitsemistaan riskeistä ja uhkista, jotka liittyvät henkilötietojen käsittelyyn ja vaarantavat organisaation toiminnan tai rekisteröityjen oikeudet[171].

4.4 Varautuminen

Organisaation on edellä käsiteltyjen etätyön tietosuojalle aiheuttamien riskien ja henkilötietojen tietoturvaloukkausten seurausten näkökulmasta kannattavaa varautua näihin tietoturvatyön avulla. Huolellisella tietoturvatyöllä voidaan ehkäistä ja minimoida tietoturvaloukkausten haittoja. Tietosuojan tarkoituksena ei ole tietosuoja-asetuksen näkökulmasta vaikeuttaa henkilötietoja käsittelevien organisaatioiden liiketoimintaa, vaan vahvistaa yksityisyyden suojaa verkkoympäristössä ja edesauttaa samalla myös yritysten

[170] KKO 2014:86.
[171] Andreasson ja muut 2019, s. 173.

talouskasvua[172]. Parhaimmillaan organisaation tietosuojaosaaminen voi olla sen menestystekijä, jolla nautitaan asiakkaiden luottamusta[173].

Tietosuojaosaaminen menestystekijänä koostuu koko henkilöstön riittävästä tietosuojaosaamisesta ja tietoturvallisista tietojärjestelmistä. Yksi tapa järjestää ja toteuttaa tietosuojatyötä on sen organisointi järkevällä tavalla, tietosuojavastaavan tehokas hyödyntäminen sekä koko henkilöstön tietosuojaosaamisen varmistaminen. Organisointiin kuuluu henkilörekisterihallinnon suunnitteleminen ja järjestäminen, tietosuojavastaavan ja tietosuojaryhmän nimeäminen, tietosuojavastaavan työtehtävien määrittäminen kirjallisesti sekä riittävän työaika-, työväline-, ja koulutusresurssin tarjoaminen tietosuojavastaavalle. Tietosuojavastaavan hyödyntäminen on avainasemassa onnistuneessa tietosuojatyössä. Tietosuojavastaava voi toimia johdon tukena ja koko henkilöstön apuna. Henkilöstö osaa hyödyntää tietosuojavastaavan osaamista, kun henkilöstöä informoidaan tietosuojavastaavan tehtävistä ja toimenkuvasta. Tietosuojavastaavasta informoiminen myös organisaation kotisivuilla ja mahdollisella ilmoitustaululla on kannattavaa, sillä tällöin myös organisaation ulkopuolella ollaan tietoisia tietosuojatyön järjestämisestä organisaatiossa. Koko henkilöstön tietosuojaosaamisen voi varmistaa laatimalla asiakastietojen käsittelyohjeet ja jalkauttaa ne henkilöstölle kouluttamalla. Henkilöstön tietosuojaosaamisen testaaminen kertoo tietosuojaosaamisen tilanteen organisaatiossa. Lisäksi tärkeää on seurata, kehittää ja puuttua tarvittaessa tietosuojatyössä havaittuihin poikkeamiin.[174]

Tietosuojavastaavan nimittäminen on tietosuoja-asetuksen 37 artiklan mukaan pakollista tietyissä tilanteissa. Tilanteista, jolloin tietosuojavastaava on nimitettävä, säädetään tietosuoja-asetuksen 37 artiklan kohdan 1 alakohdissa a-c. Tietosuojavastaava on nimitettävä, jos tietojenkäsittelyä suorittaa jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään hoitava tuomioistuin (alakohta a). Tietosuojavastaava on

[172] Korpisaari ja muut 2018, s. 35.
[173] Andreasson ja muut 2019, s. 48.
[174] Andreasson ja muut 2019, s. 49–50.

nimitettävä myös silloin, jos rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat sellaisista käsittelytehtävistä, jotka luonteensa, laajuutensa ja/tai tarkoituksensa perusteella edellyttävät rekisteröityjen laajamittaista säännöllistä ja järjestelmällistä seurantaa (alakohta b). Lisäksi tietosuojavastaava on nimitettävä, jos rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat laajamittaisesta, erityisiin henkilötietoryhmiin tai rikostuomioihin tai rikkomuksiin liittyvistä henkilötietojen käsittelystä (alakohta c). Organisaatio voi milloin tahansa muulloinkin nimittää tietosuojavastaavan, ja monessa tilanteessa se on myös suositeltavaa[175]. Tietosuojatyön tukena ja osoitusvelvollisuuden noudattamisen apuna organisaatio voi hyödyntää sertifikaatteja. Tietosuojaa koskevat sertifikaattien avulla rekisteröity voi helposti arvioida organisaation tuotteiden ja palveluiden tietosuojan tasoa.[176]

Organisaatio voi varautua tietoturvaloukkauksiin huolellisen tietoturvatyön lisäksi tietoja kyberturvavakuutuksilla. Vakuuttamista kannattaa harkita, jos tietosuojaan ja tietoturvaan liittyvät riskit ovat sellaisia, että vakuuttaminen kannattaa. Vaikka vakuutukset eivät tarkoita sitä, että organisaatio voi laiminlyödä tietosuojaan liittyviä velvoitteitaan, voidaan niillä pienentää mahdollista syntyvää haittaa ja vahinkoa. Vakuutus voi korvata esimerkiksi verkkovarkauksista ja -kiristyksistä aiheutunutta taloudellista vahinkoa, vahingonkorvausvastuusta aiheutuneita kustannuksia, kriisinhallintakustannuksia, kuten tiedottamisesta ja vahingon torjumisesta aiheutuneita kustannuksia, sekä tietovuotoon liittyvän viranomaismenettelyn kustannuksia.[177]

Tietosuojavaltuutetun toimistoon vireille tulleiden asioiden määrä on moninkertaistunut tietosuoja-asetuksen voimaantulon jälkeen. Myös tietoturvaloukkauksista ilmoittaminen on lisääntynyt jokaisena vuotena. Tietoturvaloukkauksia tuli vireille 2220 kappaletta vuonna 2018, 3840 kappaletta vuonna 2019 ja 4276 kappaletta vuonna 2020. Vuoden 2020 tietoturvaloukkauksista 56 prosenttia oli tahattomia, ja yhdeksän prosenttia

[175] Korpisaari ja muut 2018, s. 347.
[176] Talus ja muut 2017, s. 13.
[177] Andreasson ja muut 2019, s. 154–155.

tahallisia. Järjestelmä- ja prosessivirheet aiheuttivat 29 prosenttia tietoturvaloukkauksista, ja Microsoft Office 365 -palveluihin liittyviä tietoturvaloukkauksia oli vuoden 2020 tietoturvaloukkauksista kuusi prosenttia. Suurin syy tietoturvaloukkauksien taustalla on se, että asioita suoritetaan yhtäaikaisesti ja kiireessä. Huolimattomuusvirheet lisääntyvät, kun henkilötietojen kanssa tehdään useita muita asioita samaan aikaan. Huolellisuuden lisäksi tietokantojen suojaus, järjestelmien testaus ja kunnollisesta ohjeistuksesta huolehtiminen ehkäisevät tietoturvaloukkauksia.[178]

Etätyö tuo mukanaan erityispiirteitä, jotka tulee huomioida tietosuojatyössä. Tietosuojaosaamisen kouluttamisella koko henkilöstölle vahvistetaan tietosuojatyön onnistumista ja tehostetaan asiakaspalvelua, kun henkilöstön ei tarvitse käsitellä henkilötietoja epävarmuudessa. Rekisterinpitäjän tai henkilötietojen käsittelijän ei tule olettaa, että sen alaisuudessa toimiva henkilöstö osaa soveltaa tietosuojaohjeistuksia kaikilta osin myös etätyöhön, etenkin jos organisaation tietosuojaohjeet ovat pintapuoliset eivätkä ota huomioon etätyötä. Etätyön tietosuojaosaamisen kouluttaminen henkilöstölle on tärkeää, koska etätyö on monessa organisaatiossa tullut jäädäkseen.

Tietosuojan nykytilan selvittämisen etätyön osalta voi aloittaa organisaation ohjeiden tarkastamisella ja päivittämisellä. Työnantajan tulee varmistaa tietojärjestelmien, tietoliikenneyhteyksien ja käytettävien laitteiden tietoturvallisuus etätyössä. Työntekijä voi kattavan tietoturvaohjeistuksen avulla tarkastaa ja tarvittaessa muokata omia etätyökäytäntöjään ja etätyöntekopaikkaansa. Paperisten asiakirjojen käyttämisestä etätyössä on ohjeistettava koko organisaation tasoisesti, jotta toimintatavat ovat mahdollisimman yhtenäiset. Myös erityiset henkilötietoryhmät on otettava huomioon etätyön suunnittelussa ja tietosuojan tarkastelussa. Seuraavassa taulukossa on esitetty etätyön tietosuojariskeihin perustuvat kysymykset, joita voidaan käyttää lähtökohtana etätyön tietosuojan tarkastelussa.

[178] Tietosuojavaltuutetun toimisto 2021d, s. 16–17, 31.

Ohjeet henkilöstölle	Onko tietosuojaa koskeva ohjeistus ajantasainen, riittävä ja käytännönläheinen? Onko ohjeistuksessa huomioitu etätyön aiheuttamat tietosuojariskit? Ymmärtääkö henkilöstö ohjeiden merkityksen ja niiden noudattamisen tärkeyden?
Tietojärjestelmät, tietoliikenneyhteydet ja käytettävät laitteet	Ovatko tietojärjestelmät, tietoliikenneyhteydet ja työssä käytettävät laitteet asianmukaisesti suojattu etätyössä? Onko varauduttu siihen, että laitteita voi kadota?
Työntekopaikka	Onko ulkopuolisilla näkö- tai kuuloyhteyttä etätyöpaikkaan? Onko ulkopuolisilla helppo pääsy henkilötietoihin etätyöpaikassa?
Asiakirjat	Käytetäänkö etätyössä paperisia asiakirjoja, kuten tulosteita tai muistiinpanoja, jotka sisältävät henkilötietoja? Missä asiakirjoja säilytetään? Miten asiakirjat hävitetään?
Erityiset henkilötietoryhmät	Käsitelläänkö etätyössä erityisiin henkilötietoryhmiin kuuluvia arkaluontoisia tietoja? Miten erityiset henkilötietoryhmät on otettu huomioon etänä tehtävässä henkilötietojen käsittelyssä?

Taulukko 1. Etätyön tietosuojan kysymyspatteristo.

5 Yhteenveto

Työnantajalla on vastuu etätyön tietoturvallisuudesta. Tietojärjestelmien suojaus ja työntekijän ohjeistaminen tietosuojaa koskevasta lainsäädännöstä ja yrityssäännöistä on työnantajan vastuulla. Työtehtävissä, joissa käsitellään henkilötietoja, on työnantajan rooli joko rekisterinpitäjä tai henkilötietojen käsittelijä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Työntekijä, joka käsittelee työssään henkilötietoja, on puolestaan rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva henkilö. Työnantaja on rekisterinpitäjän roolissa ollessaan vastuussa siitä, että henkilötietojen käsittelyssä noudatetaan asetuksen säännöksiä. Sen on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet henkilötietojen käsittelyn lainmukaisuuden varmistamiseksi sekä kyettävä osoittamaan, että asetusta on noudatettu. Jos työnantaja on henkilötietojen käsittelijä, on käsittelyn tapahduttava rekisterinpitäjän antamien ohjeiden mukaisesti. Työntekijä ei saa käsitellä henkilötietoja muuten, kuin rekisterinpitäjän antamien ohjeiden mukaisesti, ellei käsittely ole tällöin lain vastaista. Etätyössä tapahtuvassa henkilötietojen käsittelyssä tilanne ei muutu, vaan työntekijän vastuulla on silloinkin noudattaa työnantajan tietosuojaa koskevia ohjeita.

Henkilötietojen käsittelyssä on aina noudatettava tietosuoja-asetuksen mukaisia käsittelyn periaatteita. Nämä periaatteet ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys, käyttötarkoitussidonnaisuus, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen, eheys ja luottamuksellisuus sekä osoitusvelvollisuus. Etätyössä henkilötietojen käsittelyn on tapahduttava niin, että periaatteita noudatetaan. Etätyöllä ei ole omaa erillistä lainsäädännöllistä asemaansa, joten siihen sovelletaan samaa lainsäädäntöä, kuin muuhunkin työhön. Työnantajalla on työnjohtovalta ja oikeus valvoa työtä myös etänä. Työnantajalla ei ole mahdollisuutta toteuttaa työnjohtovaltaansa etätyössä täysimääräisesti, koska työntekijän yksityisyyden suoja ja kotirauha estävät työnantajaa tarkistamasta etätyön olosuhteita työntekijän kotona ilman tämän suostumusta. Johdon ja valvonnan muodot etätyössä muuttuvat, ja työn valvonnan painopiste on ohjauksen sijaan koulutuksessa. Etätyön lähtökohtana onkin tämän vuoksi työnantajan ja työntekijän välinen

luottamus. Työnantajan on kyettävä luottamaan siihen, että työntekijä hoitaa työnsä asianmukaisesti, vaikka hän ei ole läsnä työpöytänsä ääressä työnantajan tiloissa.[179] Nykyisin työtä voidaan valvoa läsnäolon lisäksi monella muullakin tavalla. Työnantajan työnjohto-oikeuden ja tietosuojan toteuttamisen kannalta ei lopulta ole kovin suurta merkitystä sillä, tehdäänkö työtä etänä vai työnantajan tiloissa sellaisissa työtehtävissä, jotka eivät ole sijainnista riippuvaisia. Työ tapahtuu molemmissa tilanteissa joka tapauksessa pääosin tietoverkkojen välityksellä tietojärjestelmissä, jolloin työnantaja voi valvoa työtä niiden välityksellä.

Etätyön olosuhteet voivat aiheuttaa kohonneita riskejä tietosuojalle. Tietoturvallisen työskentelyn edellytyksenä on henkilöstön riittävä ohjeistaminen ja kouluttaminen tietoturvallisuuteen ja tietosuojaan liittyvissä asioissa. Jos henkilöstölle laaditut ohjeet ovat puutteellisia, virheellisiä, vaikeaselkoisia tai hankalasti saavutettavia, kasvaa mahdollisuus henkilötietojen tietoturvaloukkauksen syntymiselle. Myös henkilöstön suhtautuminen annettuihin ohjeisiin vaikuttaa. Välinpitämättömyys ja huolimattomuus henkilötietojen käsittelyssä voi johtaa henkilötietojen tietoturvaloukkaukseen. Ohjeiden lisäksi heikosti suojatut tai täysin suojaamattomat tietoliikenneyhteydet, tietojärjestelmien heikko suojaustaso ja työssä käytettävien tietoteknisten laitteiden puutteellinen tietoturva kasvattavat mahdollisuutta tietoturvaloukkauksiin. Etätyössä käytettäviä laitteita myös säilytetään muualla, kuin työnantajan tiloissa. On mahdollista, että henkilötietoja sisältävä laite häviää tai se varastetaan.

Sillä, missä etätyötä tehdään, on merkitystä tietosuojan kannalta. Julkisessa tilassa tehtävä etätyö tai etätyöntekopaikan heikko äänieristys voivat johtaa siihen, että ulkopuolisille paljastuu työssä käsiteltäviä henkilötietoja. Henkilötiedot voivat paljastua ulkopuolisille myös paperisista asiakirjoista, joita säilytetään turvattomassa paikassa tai jotka hävitetään huolimattomasti. Erityistä riskialttiutta sisältyy etänä tehtävään työhön, jossa käsitellään erityisiin henkilötietoryhmiin kuuluvia arkaluontoisia tietoja. Niiden paljastuminen ulkopuolisille voi aiheuttaa uhkan rekisteröidyn oikeuksille ja vapauksille.

[179] Helle 2004, s. 128–129.

Henkilöstön ohjeistaminen etätyön tietosuojan käytännöistä on tärkeää etenkin erityisiä henkilötietoja käsiteltäessä.

Etätyön tietosuojariskien huomioimisella voidaan pienentää tietoturvaloukkausten todennäköisyyttä ja niiden seurauksia. Henkilötietojen tietoturvaloukkauksesta aiheutuvat seuraukset voivat olla erittäin ikäviä sekä rekisteröidylle, rekisterinpitäjälle, henkilötietojen käsittelijälle, että henkilötietoja käsittelevälle työntekijälle. Seuraukset riippuvat tietoturvaloukkauksen laadusta ja siitä, mihin tietoihin se kohdistuu. Seuraukset voivat olla aineellisia tai aineettomia. Vaikutukset voivat näkyä maineen menettämisenä tai taloudellisina tappioina. Rekisteröidylle aiheutuvista seurauksista ikävimpiä ovat sosiaaliset seuraukset, kuten maineen menettäminen ja rikoksen uhriksi joutuminen esimerkiksi identiteettivarkauden myötä. Rekisterinpitäjä ja henkilötietojen käsittelijä voivat menettää maineensa luotettavana organisaationa asiakkaiden keskuudessa. Taloudellisia tappioita voi syntyä seuraamusmaksujen ja vahingonkorvausten vuoksi. Työntekijä voi saada huomautuksen tai varoituksen ja pahimmillaan työsuhde voi päättyä. Myös työntekijä voi joutua tilanteeseen, jossa joutuu suorittamaan vahingonkorvauksia työnantajaorganisaatiolleen. Äärimmäisissä tapauksissa rekisterinpitäjä, henkilötietojen käsittelijä ja työntekijä voivat joutua rikosoikeudelliseen vastuuseen.

Paras tapa välttyä ikäviltä tietoturvaloukkausten seurauksilta on varautua niihin ennaltaehkäisevästi. Lähtökohtana etätyön aiheuttamien tietoturvaloukkausten ehkäisemisessä on organisaation toteuttama huolellinen tietosuojatyö. Tietosuojatyön organisointi ja selkeät vastuut helpottavat kokonaisuuden hallintaa. Tietosuojan kouluttaminen koko henkilöstölle parantaa osaamista koko organisaatiossa ja pienentää mahdollisuutta henkilöstön aiheuttamille tietoturvaloukkauksille. Etätyön erityispiirteet tulee huomioida sellaisten organisaatioiden tietosuojatyössä, joissa käsitellään henkilötietoja etänä. Etätyön pelisäännöistä on hyvä sopia joko etätyösopimuksella tai organisaation etätyötä koskevilla ohjeilla. Vaikka vakuutukset eivät toimi ennaltaehkäisevästi, voidaan niitä käyttää turvaamaan tietoturvaloukkauksen seurausten vaikutuksia.

Etätyön aiheuttamia henkilötietojen tietoturvaloukkauksia ei ole toistaiseksi tullut tiedoksi julkisuuteen. Näin ollen oikeuskäytäntöä etätyön tietosuojasta ei ole vielä muodostunut. Tietosuoja-asetus on ollut voimassa neljä vuotta, joten kotimainen oikeuskäytäntö on muutoinkin vielä kehittymässä. On mahdollista, että etätyö ei aiheuta suuria ongelmia tietosuojalle. Etätyömahdollisuutta ei kannata poissulkea tietoturvaloukkausten pelossa, koska henkilötietoja voidaan käsitellä etätyössä turvallisesti kohtuullisilla toimenpiteillä. Vakavien henkilötietojen tietoturvaloukkausten mahdollisuus on olemassa olosuhteista riippumatta aina, kun käsitellään henkilötietoja. Etätyössä tietyt riskitekijät korostuvat, kuten ulkopuolisten mahdollisuus päästä käsiksi henkilötietoihin. Etätyön riskejä silmällä pitäen olisi hyvä luoda pelisäännöt etätyölle, jos erillistä etätyösopimusta ei ole laadittu.

Lähteet

Aarnio, A. (1997). Oikeussäännösten systematisointi ja tulkinta. Teoksessa J. Häyhä (toim.), *Minun metodini* (s. 35–56). Werner Söderström Lakitieto Oy.

Aarnio, A. (2011). *Luentoja lainopillisen tutkimuksen teoriasta.* Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja.

Andreasson, A., Koivisto, J. & Ylipartanen, A. (2016). *Tietosuojakäsikirja johdolle* (2. uudistettu painos). Tietosanoma.

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

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

Erto. (2022a). *Työsuhteen ehdot.* Noudettu 2022-01-22 osoitteesta https://www.erto.fi/tyosuhdeopas/tyosuhde/tyosuhteen-ehdot

Erto. (2022b). *Vahingonkorvausvelvollisuus.* Noudettu 2022-04-24 osoitteesta https://www.erto.fi/tyosuhdeopas/tyosuhde/vahingonkorvausvelvollisuus

Etätyötä koskeva puitesopimus. (2002, 16. heinäkuuta). Noudettu 2021-05-19 osoitteesta https://akava.fi/wp-content/uploads/2020/02/Etatyon_puitesopimus.pdf

HE 96/1998. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi.

Helle, M. (2004). *Etätyö.* Edilex Libri.

Hirvonen, A. (2011). *Mitkä metodit? Opas oikeustieteen metodologiaan*. Yleisen oikeustieteen julkaisuja 17. Noudettu 2021-05-10 osoitteesta https://issuu.com/arihirvonen/docs/mitk___metodit_paino

Ihmisoikeusliitto. (2021). *Mitä ovat ihmisoikeudet?* Noudettu 2021-07-09 osoitteesta https://ihmisoikeusliitto.fi/ihmisoikeudet/

Järvinen, P. & Rousku, K. (2017). *Työpaikan tietoturvaopas. Tunnista uhat, hallitse riskit.* Alma Talent Oy.

Korpisaari, P., Pitkänen, O. & Warma-Lehtinen, E. (2018). *Uusi tietosuojalainsäädäntö.* Alma Talent Oy.

Korpisaari, P. (2016). *Johdatus viestintäoikeuteen.* Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja.

Kuntatyönantajat. (2005, 23. toukokuuta). *Sopimus etätyötä koskevan puitesopimuksen täytäntöönpanosta.* Noudettu 2021-05-19 osoitteesta https://www.kt.fi/henkilostojohtaminen/suositukset/etatyo-puitesopimuksen-taytantoonpano

Kyberturvallisuuskeskus. (2014). *Langattomasti, mutta turvallisesti. Langattomien lähiverkkojen tietoturvallisuudesta.* Noudettu 2021-11-27 osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

Leskinen, T. (2020, 22. joulukuuta). *Säännöllisesti kotona työskenteleminen on kaksinkertaistunut.* Tilastokeskus. Noudettu 2021-05-26 osoitteesta https://www.tilastokeskus.fi/tietotrendit/blogit/2020/saannollisesti-kotona-tyoskenteleminen-on-kaksinkertaistunut/

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

Rimpiläinen, T. (2020, 22. lokakuuta). *Psyoterapiakeskus Vastaamon kiristäjä julkaisi yöllä lisää erittäin arkaluontoisia potilaskertomuksia.* Yle. Noudettu 2022-04-17 osoitteesta https://yle.fi/uutiset/3-11606925

Rousku, K. (2014). *Kyberturvaopas. Tietoturvaa kotona ja työpaikalla*. Talentum.

Saarenpää, A. (2016). Oikeusinformatiikka. Teoksessa Niemi, M-L. (toim.), *Oikeus tänään/Osa I* (s. 67–273). (4. uudistettu painos). Lapin yliopiston oikeustieteellisiä julkaisuja.

Salminen, H. (toim.). (1997). *Tietoturvallisuus etätyössä.* Suomen Atk-kustannus.

Sutela, H. (2021, 18. lokakuuta). *Uusi normaali kutsuu – vanhaan ei ole paluuta, jos työntekijöiltä kysytään.* Tilastokeskus. Noudettu 2022-03-20 osoitteesta https://www.stat.fi/tietotrendit/blogit/2021/uusi-normaali-kutsuu-vanhaan-ei-ole-paluuta-jos-tyontekijoilta-kysytaan/

Talus, A., Autio, E., Hänninen, A., Pihamaa, H-T. & Kantonen, S. (2017, 27. tammikuuta). *Miten valmistautua EU:n tietosuoja-asetukseen?* Oikeusministeriö ja Tietosuojavaltuutetun toimisto. http://urn.fi/URN:ISBN:978-952-259-558-4

Tietosuojavaltuutetun toimisto. (2021a). *Pseudonymisoidut ja anonymisoidut tiedot.* Noudettu 2021-07-20 osoitteesta https://tietosuoja.fi/pseudonymisointi-anonymisointi

Tietosuojavaltuutetun toimisto. (2021b). *Osoita noudattavasi tietosuojasäännöksiä.* Noudettu 2021-09-01 osoitteesta https://tietosuoja.fi/osoitusvelvollisuus

Tietosuojavaltuutetun toimisto. (2021c). *Tietoturvaloukkaukset.* Noudettu 2021-07-23 osoitteesta https://tietosuoja.fi/tietoturvaloukkaukset

Tietosuojavaltuutetun toimisto. (2021d). *Tietosuojavaltuutetun toimiston toimintakertomus 2020*. Noudettu 2022-04-16 osoitteesta https://tietosuoja.fi/documents/6927448/92481282/Tietosuojavaltuutetun+toimisto+toimintakertomus+2020.pdf/f699746b-55fa-c464-f520-67933cb05578/Tietosuojavaltuutetun+toimisto+toimintakertomus+2020.pdf?t=1632724948372

Tietosuojavaltuutetun toimisto. (2022a). *Erityisten henkilötietoryhmien käsittely.* Noudettu 2022-04-09 osoitteesta https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely

Tietosuojavaltuutetun toimisto. (2022b). *Jos joudut tietoturvaloukkauksen kohteeksi.* Noudettu 2022-01-08 osoitteesta https://tietosuoja.fi/jos-joudut-tietoturvaloukkauksen-kohteeksi

Tietosuojavaltuutetun toimisto. (2022c). *Ilmoitus tietosuojavaltuutetulle.* Noudettu 2022-02-27 osoitteesta https://tietosuoja.fi/ilmoitus-tietosuojavaltuutetulle

Tietosuojavaltuutetun toimisto. (2022d). *Vahingonkorvausten vaatiminen tietosuoja-asetuksen rikkomisesta.* Noudettu 2022-04-23 osoitteesta https://tietosuoja.fi/vahingonkorvausten-vaatiminen

Tietosuojavaltuutetun toimisto. (2022e). *Henkilötietojen käsittely.* Noudettu 2022-04-23 osoitteesta https://tietosuoja.fi/henkilotietojen-kasittely

Tietosuojavaltuutetun toimisto. (2022f). *Henkilötietojen käsittelijän velvollisuudet.* Noudettu 2022-04-23 osoitteesta https://tietosuoja.fi/henkilotietojen-kasittelijan-velvollisuudet

Työsuojeluhallinto. (2020, 15. syyskuuta). *Etätyö*. Työsuojelu.fi. Noudettu 2021-05-10 osoitteesta https://www.tyosuojelu.fi/tyoolot/tyoymparisto/etatyo

Työsuojeluhallinto. (2021, 19. huhtikuuta). *Oikeudet ja velvollisuudet työssä.* Noudettu 2022-04-23 osoitteesta https://www.tyosuojelu.fi/tyosuhde/oikeudet-ja-velvollisuudet-tyossa

Vilkman, U. (2016). *Etäjohtaminen: Tulosta joustavalla työllä.* Talentum Pro. https://verkkokirjahylly-almatalent-fi.proxy.uwasa.fi/teos/DAEBIXCTEB#/kohta:ET((c4)JOHTAMINEN((20)Tulosta((20)joustavalla((20)ty((f6)ll((e4)((20)/piste:b0

Oikeustapausluettelo