LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

EU:n tietosuoja-asetuksen tuomat muutokset yrityksen henkilötietojen käsittelyyn

Vienonen, Olli

2018 Laurea

Laurea-ammattikorkeakoulu

EU:n tietosuoja-asetuksen tuomat muutokset yrityksen henkilötietojen käsittelyyn

Olli Vienonen
Liiketalous
Opinnäytetyö
Toukokuu, 2018

Laurea-ammattikorkeakoulu **Tiivistelmä**
Liiketalous
Tradenomi (AMK)

Olli Vienonen

EU:n yleisen tietosuoja-asetuksen tuomat muutokset yrityksen henkilötietojen käsittelyyn

Vuosi 2018 Sivumäärä 51

Opinnäytetyön aiheena ovat Euroopan unionin yleisen tietosuoja-asetuksen (2016/679) myötä tulevat muutokset Suomen kansalliseen lainsäädäntöön sekä vaikutukset yrityksien toimintaan. Vuonna 2016 voimaan tullut tietosuoja-asetus yhtenäistää unionin tietosuojalainsäädäntöä ja lisää rekisterinpitäjien velvollisuuksia mahdollistaen rekisteröidyille paremmat oikeudet omien henkilötietojensa hallintaan. Tietosuoja-asetus tulee olla EU:n jäsenvaltioissa kansalliseen lainsäädäntöön sovellettuna 25.5.2018 mennessä.

Opinnäytetyössä keskitytään tietosuoja-asetuksen sisältöön ja vertaillaan sitä tietosuojauudistusta edeltäneeseen EU:n lainsäädäntöön eli pääosin tietosuojadirektiiviin (95/46/EC) ja Suomen kansalliseen lainsäädäntöön kuten henkilötietolakiin (523/1999). Lainopillisessa opinnäytetyössä tavoitteena on selvittää yrityksen henkilötietojen käsittelyyn tulevia muutoksia tietosuoja-asetuksen myötä. Pääasiallisina lähteinä opinnäytetyössä ovat EU:n viralliset asiakirjat muun muassa tietosuoja-asetukseen liittyvästä lainvalmistelusta ja EU:n lainsäädäntö sekä Suomen kansallinen lainsäädäntö sekä tietosuoja-asetuksen rinnalle tulevan tietosuojalain valmisteluaineisto. Lisäksi lähteinä käytettiin henkilötietojen käsittelyä ja tietosuojaa käsittelevää kirjallisuutta tukemaan lainsäädännön tulkintaa.

EU:n yleisen tietosuoja-asetuksen myötä kaikkien jäsenvaltioiden tietosuojakäytännöt yhtenäistyvät palvelemaan EU:n kansalaisia ja yrityksiä, edistämällä digitaalisten sisämarkkinoiden kehitystä. Rekisterinpitäjänä toimivien yritysten toiminnan läpinäkyvyys lisääntyy ja yrityksiltä velvoitetaan avoimuutta rekisteröityjä kohtaan koskien henkilötietojen käsittelyä, joka näkyy esimerkiksi rekisterinpitäjän informointivelvollisuudessa.

Asiasanat: Tietosuoja-asetus, perusoikeudet, rekisterinpitäjä, rekisteröity

Laurea University of Applied Sciences **Abstract**
Degree Programme in Business Administration
Bachelor's Thesis

Olli Vienonen

Changes brought by the European Union's General Data Protection regulation to the processing of personal data in companies

Year 2018 Pages 51

The subject of the thesis is the upcoming changes to the Finnish national legislation and the impact on the activities of companies due to the EU's General Data Protection Regulation (2016/679). General Data Protection Regulation, which entered into force in 2016, harmonizes the overall legal data protection framework in the EU and adds responsibilities of data controllers, enabling the data subjects to have better rights to manage their personal data. The regulation should be implemented in the EU Member States by 25 May 2018.

The thesis focuses on the content of the General Data Protection Regulation and compares it with the previous legislation in EU, mainly Data Protection Directive (95/46/EC) and Finnish national legislations such as the Personal Data Act (523/1999). In this legal thesis, the main target is to find out about the changes to company's personal data processing with the regulation. The main sources of the thesis were the official documents of the EU, including current legislation and legislative drafting concerning the regulation, as well as Finnish national legislation and the preparatory material for the Finnish data protection law that will be used alongside the regulation. In addition, the literature on personal data processing and data protection was used as a source to support the interpretation of legislation.

With the EU's General Data Protection Regulation, the data protection practises across all the Member States will be harmonized to serve EU citizens and businesses by promoting the development of the digital single market. The transparency of the companies controlling activities is increased and the companies are obliged to be open towards data subjects about the processing of personal data, which is displayed in the information obligation of the controller.

Keywords: General Data Protection regulation, fundamental rights, data controller, data subject

Lakiluettelo

Euroopan parlamentin ja neuvoston asetus (2016/679)

Euroopan parlamentin ja neuvoston direktiivi (2016/680)

Euroopan parlamentin ja neuvoston direktiivi (95/46/EY)

Henkilörekisterilaki (471/1987)

Henkilötietolaki (523/1999)

Laki yksityisyyden suojasta työelämässä (759/2004)

Perustuslaki (731/1999)

Työsopimuslaki (55/2001)

Sisällys

1 Johdanto

Opinnäytetyössä käsitellään Euroopan unionin yleisen tietosuoja-asetuksen (2016/679) tuomia muutoksia Suomen kansalliseen lainsäädäntöön ja aikaisempaan EU:n henkilötietodirektiiviin (95/46/EY). Näiden muutosten kautta tarkastellaan asetuksen vaikutuksia yrityksissä tapahtuvaan henkilötietojen käsittelyyn. EU:n yleinen tietosuoja asetus (2016/679) astui voimaan 24.5.2016 Euroopan unionin virallisessa lehdessä ilmestymisen jälkeen, jota seurasi kahden vuoden siirtymäaika. Asetuksen 99 artiklan mukaan, sitä sovelletaan sellaisenaan kaikkien EU:n jäsenvaltioiden lainsäädännössä 25.5.2018 lähtien. Asetuksen resitaalissa 10 kerrotaan, että jäsenvaltioilla on jonkin verran kansallista liikkumavaraa asetuksen sääntöjen täsmentämiseen.

Asetus vahvistaa koko EU:n yhteisiä sääntöjä, joita sovelletaan kaikkiin EU:n alueella palveluja tarjoaviin yrityksiin. Säännöillä vältetään tilanne, jossa erilaiset kansalliset tietosuojasäännöt hankaloittaisivat rajatylittävää tietojenvaihtoa. Asetus lisää myös jäsenvaltioiden välistä yhteistyötä, jolla varmistetaan yhteisien tietosuojasääntöjen soveltaminen yhdenmukaisesti EU:n alueella. Tämä mahdollistaa reilut kilpailumahdollisuudet ja pienillä sekä keskisuurilla yrityksillä on paremmat mahdollisuudet hyödyntää esimerkiksi digitaalisia sisämarkkinoita tehokkaasti.[1] Edellä mainitun taustoittamisen perusteella voidaan ymmärtää, miksi EU:n alueella yhtenäistetään tietosuojalainsäädäntöä. Lähtökohtaisesti asetuksen resitaalissa 2 kerrotaan sen palvelevan kansalaisia ja sisämarkkinoita sekä takaavan tietojen turvallisen ja vapaan liikkuvuuden.[2]

2 Opinnäytetyön tavoitteet ja oikeudelliset tutkimusmetodit

Opinnäytetyön tarkoituksena on selventää EU:n yleisen tietosuoja-asetuksen tuomia muutoksia ja vaatimuksia yrityksen henkilötietojen käsittelyyn sekä sivuta yleisen tason vaikutuksia. Tavoitteena on määritellä tietosuojalainsäädäntöön liittyviä käsitteitä ja syventyä henkilötietojen käsittelyyn sekä käsittelyperusteisiin.

Tutkimusmateriaalina opinnäytetyössä käytettiin kansainvälistä ja kansallista tietosuojalainsäädäntöä esimerkiksi Euroopan parlamentin ja neuvoston asetusta (2016/679) sekä Henkilötietolakia (523/1999). Tämän lisäksi hyödynnetiin käsitteiden määrittelyssä ja lainsäädännön sisällön täydentämisessä tietosuojaa käsittelevää kirjallisuutta.

---

[1] Eurooppa-neuvosto 2015. EU:n tietosuojauudistus: neuvosto ja parlamentti yhteisymmärrykseen.
[2] Euroopan parlamentin ja neuvoston asetus 2016/679 resitaali 2.

Opinnäytetyöni on lainopillinen eli oikeusdogmaattinen. Oikeusdogmatiikassa pyritään selvittämään voimassa olevia säädöksiä ja normeja, johon opinnäytetyökin keskittyy.[3] Oikeusdogmatiikan ominaisuuksiin kuuluu systematisoida, analysoida ja esittää oikeuslähteisiin tai oikeudellisiin oppeihin pohjautuvaa perusteltua kritiikkiä.[4]

Lainopissa on pohjimmiltaan kyse kahden tekstin muodostamasta kokonaisuudesta, jossa lainopillisen kommentaaritekstin avulla tulkitaan, selitetään ja yhtenäistetään kohdetekstinä eli tulkinnan kohteena olevaa lakitekstiä ja muuta oikeuslähdeaineistoa.[5] Metodisesti lainoppi on humanistinen tulkintatiede, jonka metodiopissa yhdistyvät tutkijan oivaltamisen logiikka sekä tiedeyhteisösidonnainen perustelemisen logiikka. Metodiopin pääpainona on perustelemisen logiikka eli oikeudellisen tulkinnan sijoittaminen tulkintakontekstiin, jonka tutkimuksellinen suunta määräytyy institutionaalisen oikeuslähdeopin ja vallitsevien oikeudellisten argumentaatiomallien mukaan.[6] Oikeudellisen metodiopin säännöt ovat muutettavissa, jos voimassa olevan oikeuden tai yhteiskunnallisten olosuhteiden muutos sitä vaatii. Euroopan yhteisöjen tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen ratkaisuista ilmenevien oikeusohjeiden soveltaminen edellyttää tuomarilta ja lainopin tutkijalta innovatiivista oikeudellista lukutaitoa.[7]

3 EU-oikeuden suhde kansalliseen oikeuteen

Euroopan unionin (EU) antamat asetukset velvoittavat jäsenvaltioita suoraan sellaisenaan. Asetuksien voimaantulo tapahtuu välittömästi, kun ne on julkaistu EU:n virallisessa lehdessä. Asetuksien tarkoituksena on jäsenvaltioiden lainsäädännön yhdenmukaisuuden varmistaminen. Direktiivien osalta lainsäädäntöjen yhtenäisyys saavutetaan niiden tulosten osalta. Direktiivit puolestaan ovat muokattavissa sopivaksi kansalliseen lainsäädäntöön tietyissä rajoissa, kuitenkin niiden tarkoittamaa tulosta muuttamatta.[8] EU:lla on mahdollisuus antaa myös oikeudellisesti sitomattomia normeja, joita ovat esimerkiksi suositukset ja lausunnot.[9]

Tietosuoja-asetus (2016/679) on aikaisempaan tietosuojadirektiiviin (95/46/EY) verrattuna suoraan velvoittava. Tietosuojadirektiivin (95/46/EY) resitaalin 9 mukaan jäsenvaltioilla on käytettävissään toimenpidemarginaali. Laillisen tietojenkäsittelyn yleiset edellytykset tulee täyttää marginaalin rajoissa. Tämä johti siihen, että Euroopassa oli useita erilaisia henkilötietojen käsittelyä koskevia lainsäädäntöjä. Tietosuoja-asetuksen resitaalin 10 mukaan asetuk-

---

[3] Aarnio 2011, 13.
[4] Jyränki & Husa 2012. 73.
[5] Siltala 2003, 494.
[6] Siltala 2003,496.
[7] Siltala 2003, 498.
[8] Penttinen & Talus 2017, 18-19.
[9] Penttinen & Talus 2017, 23.

sen myötä tästä päästään eroon, yhtenäinen soveltaminen varmistetaan kaikkialla unionissa ja sen lainsäädäntö yhtenäistyy.

EU-oikeus on osana kaikkien sen jäsenvaltioiden oikeusjärjestelmää. EU-oikeus on etusijainen suhteessa kansalliseen lainsäädäntöön, suoraan sovellettava ja omaa täten välittömän oikeusvaikutuksen.[10] EU-oikeuden yleinen periaate lojaliteettiperiaate velvoittaa jäsenvaltiot toteuttamaan EU-oikeuden täytäntöön panemiseksi aiheelliset yleis- ja erityisoimenpiteet. Toimenpiteillä voidaan poistaa EU-oikeuden rikkomisesta aiheutuva lainvastainen seuraus.[11] Kansainvälisen oikeuden tasolla kansainvälisen ja valtionsisäisen oikeuden suhdetta määrittää pacta sunt servanda-periaate, joka viittaa siihen, että sopimukset on pidettävä. Valtiolla on tällöin velvollisuus täyttää kansainvälisoikeudelliset velvoitteensa. Velvollisuuden negatiivisen ulottuvuuden myötä kansallinen lainsäätäjä ei voi esimerkiksi säätää vastoin kansainvälisoikeudellista velvoitteita olevaa lakia. Positiivinen ulottuvuus velvoittaa valtiota sovittamaan yhteen valtionsisäisen oikeusjärjestyksen kansainvälisoikeudellisten velvoitteidensa kanssa ja sen myötä ryhtyä toimenpiteisiin täyttääkseen kyseiset velvoitteet.[12]

Dualismin ja monismin käsitteillä kuvataan kansainvälisen oikeuden ja valtionsisäisen oikeuden välistä suhdetta. Dualismin mukaan kansainvälinen oikeus ja valtionsisäinen oikeusjärjestys ovat toisistaan erillisiä normijärjestelmiä. Kansainvälisen oikeuden säädös on tällöin osa kansallista oikeutta, kun se on saatettu voimaan. Monismissa kansainvälinen oikeus ja valtionsisäinen oikeus ymmärretään osaksi samaa normikokonaisuutta. Valtion ollessa kansainvälisoikeudellisesti sitoutunut, tulee kansainvälinen velvoite voimaan kansalliseen oikeuteen. Sitoutuminen kuitenkin usein edellyttää valtion parlamentin hyväksymistä tai muuta kansallista päätöksentekoa.[13]

EU-oikeus määrää kansainvälisen oikeuden asemasta kansallisessa oikeudessa, jota pidetään sen yhtenä ominaispiirteenä. Tämä määräämiskyky ilmenee esimerkiksi jäsenvaltiota suoraan velvoittavissa asetuksissa. Kansalliset tuomioistuimet usein perustavat ratkaisunsa antaa etusija EU-oikeudelle ristiriitaiseen kansalliseen oikeuteen nähden niihin valtionsisäisen oikeuden ratkaisuihin tilanteissa, joissa EU-oikeuden etusija tai valtioinsisäinen voimassaolo ja sovellettavuus on tunnustettu.[14] EU-oikeuden ja kansallisen oikeuden suhde ei ole aina samanlainen. Suhdetta tulkitessa tulee ottaa huomioon ratkaistavana oleva oikeudellinen ongelma. Perim-

[10] Penttinen & Talus 2017, 55.
[11] Penttinen & Talus 2017, 65-66.
[12] Ojanen 2010, 53.
[13] Ojanen 2010, 54.
[14] Ojanen 2010, 54-56.

mäisenä kysymyksenä suhdetta tarkastellessa on se, kenellä on lopulta toimivalta päättää EU:n oikeuden pätevyydestä ja yleisestä unionin toimivallasta.[15]

4 Yksityisyyden suoja perusoikeutena

Lissabonin sopimus (2007/C 306/01) toi muutoksia Euroopan unionin perusoikeuskirjaan (2012/C 326/02) verrattuna perustuslakisopimukseen (2004/C 310/1). Perusoikeuskirja oli aiemmin sellaisenaan osana perustuslakisopimusta, mutta Lissabonin sopimuksen myötä sen oikeudellistaminen toteutettiin viittaamalla uudelleen hyväksyttyyn perusoikeuskirjaan. Uudella perusoikeuskirjalla saavutettiin sama arvo perussopimuksiin nähden, mutta se ei ollut enää osana tekstiä sopimuksissa Euroopan unionista tai unionin toiminnasta.[16]

Perusoikeuden ja ihmisoikeuden käsitteitä määritellään muodollisin ja aineellisin perustein. Muodollisen määritelmän perusoikeudet ovat perustuslaissa turvattuja oikeuksia. Tällaisia perustuslaissa turvattuja oikeuksia koskee erityinen pysyvyys ja oikeudellinen luonne, johtuen perustuslain tasoisuudesta ja korotetusta lainvoimasta. Käytännössä perustuslain korotettu lainvoima vaikeuttaa sen säätämistä, muuttamista tai kumoamista. Tavallisien lakien kohdalla muutosten hyväksyminen voidaan tehdä äänten enemmistöllä. Aineellisen määrittelyn perusteella sekä perusoikeudet ja ihmisoikeudet ovat erityisasemassa olevia oikeuksia.[17]

Lissabonin sopimukseen (2007/C 306/01) lisättiin artikla 16b, jolla korvattin aiempi artikla 286. Artiklan mukaan jokaisella on oikeus henkilötietojensa suojaan. Lisäksi Euroopan parlamentti ja neuvosto antoivat luonnollisten henkilöiden suojaa koskevat säännöt, jotka koskevat unionin toimielimiä ja laitoksia sekä jäsenvaltioita, kun he suorittavat henkilötietojen käsittelyä. Samassa yhteydessä annettiin säännöt henkilötietojen vapaasta liikkuvuudesta.[18] Osaltaan EU:n tietosuojadirektiivi (95/46/EY) sitovana säännöksenä, velvoitti jäsenvaltioita muuttamaan lainsäädäntöään EU:n tietosuojalainsäädännön perustason mukaiseksi. Direktiivi perustui tietojen käsittelyyn yleiskäsitteenä, joka sisälsi henkilötietojen keräämisen, tallentamisen, luovuttamiseen ja muun käytön.[19] Eurooppalaisen tietosuojalainsäädännön edistykselle keskeisenä askeleena voidaan pitää myös taloudellisen kehityksen ja yhteistyön järjestön (OECD) antamaa tietosuojasuositusta vuodelta 1980. Suosituksessa käsitellään henkilötietojen

---

[15] Ojanen 2010, 57-58.
[16] Lissabonin sopimus: Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta (2007/C 306/01) artikla 6
[17] Ojanen 2010, 115.
[18] Lissabonin sopimus: Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta (2007/C 306/01) artikla 16
[19] Syrjänen 2007, 90.

keräämistä ja laatua, rekisteröidyn tarkastusoikeutta, tietoturvaa ja kansainvälisten tiedonsiirtojen yleisperiaatteita.[20]

Yksityisyys perusoikeutena on ennen kaikkea yksilön itsemäärämisoikeutta. Yksityisyyden suoja on mahdollisesti suurimmillaan tilanteissa, joissa yksilön henkilötietoja saadaan käsitellä vain perustuen rekisteröitävän suostumukseen. Suostumuksen tulisi olla vapaaehtoinen ja sen epääminen ei saisi aiheuttaa yksilölle negatiivisia jälkiseurauksia. EU:n perusoikeuskirja ja tietosuojadirektiivi nimenomaan korostivat itsemääräämisoikeutta ja suostumusta ensisijaisena oikeutuksena henkilötietojen käsittelylle. Henkilökohtainen suostumus ei kuitenkaan välttämättä ole mahdollista esimerkiksi yleistyneessä massamuotoisessa henkilötietojen käsittelyssä. Luottamuksellisuus henkilötietojen käsittelyssä turvaa tiedot, joihin kajoaminen merkitsee henkilön yksityisyyden loukkaamista. Tällaisten tietojen luovuttaminen tulisi tapahtua ainoastaan yksilön suostumuksen tai lainsäädännön perusteella. Luottamuksellisuuteen liittyy myös salassapito eli silloinkin, kun luottamuksellisten tietojen vaihto ja luovutus on mahdollistettu tulee tiedot pitää ulkopuolisten ulottumattomissa.[21]

Yksityiselämän suoja käsittää neljä oikeushyvettä: yksityiselämä, kunnia, kotirauha ja henkilötiedot, jotka kaikki yhdessä muodostavat suojatun alan. Mikään edellämainituista käsitteistä ei yksinään kata kokonaisuudessaan yksityiselämän suojaa. Yksityiselämään kuuluu ulottuvuutena yksilön oikeus vapaasti solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön sekä oikeus määrätä itsestään. Kunniaan liittyy ulottuvuuksia, joita ei voida helposti lukea osaksi yksityiselämää. Tällainen kunnian ulottuvuus on esimerkiksi yhteiskunnallinen arvonanto tai maine, joka voidaan pikemminkin lukea yhteisölliseksi asiaksi yksityisen sijaan. Henkilötietojen suojaan liittyy henkilörekistereihin liittyviä lain asettamia velvoitteita rekisterinpitäjälle. Rekisteröidyllä on näiden myötä myös oikeuksia esimerkiksi tietojensa tarkastamiseen.[22]

4.1 Yksityisyyden suoja perustuslaissa

Suomessa yksityisyyden suojaa ohjattiin henkilörekisterilailla (471/1987). Sillä luotiin puitteet lailliseen henkilötietojen käsittelyyn. Huomion kohteena henkilörekisterilain 1 § mukaan on henkilötietojen kerääminen, tallettaminen, käyttäminen ja luovuttaminen sekä valtion turvallisuuden varmistaminen ja hyvän rekisteritavan noudattaminen. Uusi henkilötietolaki (523/1999) astui voimaan EU:n tietosuojadirektiivin (95/46/EY) antaman kehyksen mukaisena. Henkilötietolain tarkoituksena on 1 § mukaan toteuttaa yksityiselämän suojaa ja muita sitä

[20] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of the Personal Data 23.08.1980.
[21] Syrjänen 2007, 92-93.
[22] Jyränki & Husa 2012, 418-419.

turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä kehittää hyvää tietojenkäsittelytapaa ja sen noudattamista.

Suomen perustuslaillisia perusoikeuksia koskevat oikeudet uudistuivat vuonna 1995. Perustuslain 10 § vastaa sisällöltään vuoden 1995 perusoikeusuudistuksen yhteydessä uudistettun hallitusmuodon 8 §:ää.[23] Vuonna 2000 voimaan tulleessa perustuslaissa kuin myös muussakin lainsäädännössä oli havaittavissa perusoikeuksien aseman korostuminen. Perusoikeuksien velvoittavuus koskee etenkin lainsäätäjää, sillä valtion on huolehdittava lainsäädäntötoimissaan siitä, että perustuslailliset oikeudet toteutuvat eri elämänalueilla. Perusoikeudet tulee ottaa huomioon myös käytännön hallinnossa ja tuomioistuintoiminnassa.[24] Perusoikeusuudistuksen valmistelussa käytettiin huomattavasti hyväksi kansainvälisiä ihmisoikeussopimuksia ja uudistusta perusteltiin kansainvälisten valvontaorgaanien ihmisoikeusvalitusten johdosta tehdyillä ratkaisuilla.[25]

Erityisesti perusoikeuksilla on merkitystä julkisen vallan ja yksilön välisessä suhteessa, jota kutsutaan vertikaalivaikutukseksi. Tämän lisäksi perusoikeuksilla katsotaan olevan horisontaalivaikutus, eli ne vaikuttavat myös yksilöiden välisiin suhteisiin. Esimerkiksi työntekijän ja työnantajan välisessä suhteessa horisontaalivaikutus voi tulla esiin. Sen merkityksen selkeä osoittaminen on kuitenkin haastavaa ja se voi periaatteessa olla välitöntä, jolloin tuomioistuimessa yksilö voi vedota suoraan perustuslaillisiin oikeuksiinsa ilman alemmanasteisen lainsäädännön välitystä. Välillisellä horisontaalivaikutuksella tarkoitetaan sitä, että perusoikeuksiin ei voida vedota suoraan, mutta tavallista lakia sovellettaessa tulee ottaa huomioon niiden olemassaolo. Tämä johtaa siihen, että välillinen horisontaalivaikutus vaikuttaa muun muassa tavallisen lain tulkintaan ja kyseisen ajattelutavan mukaan tavallinen laki saa sisältöä perusoikeuksista.[26]

Perustuslain (731/1999) 10 § koskee yksityiselämän suojaa, joka turvaa jokaiselle yksityiselämän, kunnian ja kotirauhan. Henkilötietojen suoja ja luottamuksellisen viestin salaisuus kuuluvat tämän perusoikeuden alaan. Hallintotoiminnassa ja julkisissa palveluissa yksityiselämän suoja edellyttää esimerkiksi yksityiselämää koskevien tietojen salassapitoa. Yleisesti henkilötietojen käsittelyssä on noudatettava sitä koskevia velvoitteita ja rajoituksia. Luottamuksellisen viestin salaisuudella estetään henkilökohtaisen viestinnän erilaisten muotojen hallinnollinen valvonta.

---

[23] Viljanen 2011, 389.
[24] Nyyssölä 2014, 19.
[25] Jyränki & Husa 2012, 87.
[26] Nyyssölä 2014, 19-20.

4.2 Tietosuoja, tietosuoja-asetus ja tietosuojalaki

Tietosuojan käsite tuli yleiseen keskusteluun toisen maailmansodan aikana ja sen jälkeen. Viimeistään tietosuojaa lainsäädännössä koskevat kysymykset ja ongelmat tulivat esille 1960 – luvun lopulla. Ensimmäisenä varsinaisena tietosuojalakina voidaan pitää Saksan liittotasavallassa vuonna 1970 säädettyä lakia ja ensimmäinen valtakunnallinen tietosuojalaki oli Ruotsin datalagen vuonna 1973.[27]

Tietosuojaa ja yksityisyyden suojaa ei voida rinnastaa käsitetasolla, koska tietosuojaan kuuluu yksityisyyden lisäksi muitakin elementtejä.[28] Henkilötietojen suoja eli tietosuoja tarkoittaa henkilötietojen käsittelyn laillisia edellytyksiä ja toimintaa, kunnioittaen yksilön perusoikeuksia ja yksityisyyttä. Tietosuoja ei ole ainoastaan henkilötietojen salassapitoa vaan myös julkisten ja salassa pidettävien henkilötietojen käsittelyn lainmukaisia toiminnallisia edellytyksiä ja mahdollisuuksia. Tietosuoja ei ole ainoa perusoikeus, joka vaikuttaa yksilön yksityisyyden suojaan. Yksityisyyden suoja muodostuu perusoikeuksista kuten yksilön itsemääräämisoikeus ja oikeuksista yksityiselämään, kunniaan, yhdenvertaiseen kohteluun, henkilökohtaiseen koskemattomuuteen, ihmisarvoiseen kohteluun, turvallisuuteen ja vaikutusvaltaan itseään koskevissa asioissa.[29]

Tiedollinen itsemääräämisoikeus on osa yksilön itsemääräämisoikeutta, mutta informaatiooikeudellisena periaatteena se on lähtökohtana henkilötietojen suojalle eli tietosuojalle. Laintasolla tietosuoja määrittää rekisterinpitäjälle vaatimuksia tietoturvallisuuden varmistamisesta.[30]

Euroopan unionin tietosuojalainsäädännön uudistaminen käynnistettiin vuonna 2012. Aikaisempi tietosuojalainsäädäntö ei ollut enää riittävä vastaamaan kehittyneen globaalin tietoympäristön vaatimuksiin. Uudistuksen avulla pyritään turvaamaan henkilötietojen suoja perusoikeutena, digitaalitalouden kehitys ja tehostetaan rikollisuuden sekä terrorismin torjuntaa. Uudistamisen tuloksena syntyivät tietosuojadirektiivi (2016/680) ja yleinen tietosuoja-asetus (2016/679). Molemmat astuivat voimaan 24.5.2016 ja kansallinen täytäntöönpaneminen tehdään direktiivin osalta 6.5.2018 ja tietosuoja-asetuksen 25.5.2018 mennessä.[31]

Uudistuksen merkittävimpinä etuina yrityksille voidaan unionin yhtenäisen lainsäädännön lisäksi pitää niin sanottua yhden luukun järjestelmää ja samoja sääntöjä kaikille sijaintimaasta

---

[27] Syrjänen 2007, 87.
[28] Syrjänen 2007, 87.
[29] Voutilainen 2012, 51.
[30] Voutilainen 2012, 37.
[31] Eduskunta. Tietoa eduskunnasta. EU:n tietosuojauudistus. 2018.

riippumatta. Yhden luukun järjestelmällä tarkoitetaan sitä, että yrityksen tarvitsee ottaa yhteyttä vain yhteen tietosuojaviranomaiseen unionin yhtenäisen säännöstön mahdollistamana. Tämä helpottaa liiketoiminnan harjoittamista EU:n alueella. Tietosuoja-asetus sitoo myös EU:n ulkopuolelle sijoittuneita yrityksiä jos ne tarjoavat tuotteita tai palveluja unionin markkinoilla. Unionin ulkopuolisten yritysten tulee tästä lähtien noudattaa ainakin tietosuojan osalta tiukempia normeja, joka luo unionissa toimiville yrityksille tasavertaisemmat kilpailumahdollisuudet.[32]

Tärkeinä muutoksina tietosuoja-asetuksessa tietosuojadirektiiviin nähden ovat lisääntynyt alueellinen sovellettavuus myös EU:n ulkopuolella, seuraamusjärjestelmä ja vahvistavat muutokset suostumukseen. Näiden lisäksi rekisteröidyn oikeuksiin tuli rekisterinpitäjän ilmoitusvelvollisuus tietomurroista, jotka aiheuttavat riskin yksilön oikeuksille ja vapauksille. Lisäksi rekisteröidyn pääsyä tietoihin on laajennettu ja oikeus tulla unohdetuksi on lisätty erillisenä artiklana asetukseen. Rekisteröidyllä on asetuksen myötä myös oikeus siirtää tietojaan toiselle rekisterinpitäjälle tietyissä tapauksissa. ”Privacy by Design” eli niin sanottu sisäänrakennetun tietosuojan konsepti tulee asetuksen myötä lainmäärittelemäksi velvoitteeksi, joka johtaa rekisterinpitäjien liiketoiminnassa siihen, että uusia toimintoja suunnitellessa tulee ajatella myös asiaa tietosuojan kannalta. Asetus velvoittaa myös tietyissä tapauksissa yrityksiä nimittämään tietosuojavastaavan.[33]

Tietosuoja-asetuksen tarkoituksena on korvata tietosuojadirektiivi (95/46/EC). Se suunniteltiin yhtenäistämään tietosuojalainsäädäntöä unionissa, turvaamaan EU:n kansalaisten tietoturvaa ja muuttamaan yritysten lähestymistapaa suhteessa tietosuojaan.[34] Vuoden 2012 uudistamisjulistuksen jälkeen vuonna 2014 Euroopan parlamentti vahvisti oman versionsa asetuksesta. Kesällä 2015 Euroopan unionin neuvosto hyväksyi oman versionsa ensimmäisessä lukemistilaisuudessa, jonka jälkeen asetus siirtyi lainsäädäntötyön viimeiseen vaiheeseen.[35]

Lainsäädännön viimeisen vaiheen tapaamisissa käytiin läpi esimerkiksi tietosuojaperiaatteita, rekisteröityjen oikeuksia, rekisterinpitäjän ja käsittelijän rooleja ja tämän lisäksi monia muita kysymyksiä. Viimeinen vaihe kesti vuoden 2015 kesäkuusta joulukuuhun, jolloin parlamentti ja neuvosto sopivat lakitekstin olevan viimeisessä muodossaan, kun se allekirjoitetaan tammikuussa 2016. Lopulta molemmat hyväksyivät asetuksen huhtikuun 2016 aikana ja toukokuussa asetus julkaistiin Euroopan unionin virallisessa lehdessä. Julkaisusta 20 päivän kuluttua asetus astui voimaan koko unionissa ja kahden vuoden siirtymäaika soveltamismääräaikaan alkoi.[36]

---

[32] Tietosuoja. Kysymyksiä ja vastauksia tietosuojauudistuksesta. 2016.
[33] EU GDPR. Key Changes. 2018.
[34] EU GDPR. Site Overview. 2018.
[35] EU GDPR. GDPR Timeline of Events. 2018.
[36] EU GDPR. GDPR Timeline of Events. 2018.

Oikeusministeriö asetti helmikuussa 2016 TATTI-työryhmän selvittämään yleisen tietosuoja-asetuksen edellyttämät toimenpiteet kansalliseen liikkumavaraan ja valmistelemaan muutoksia henkilötietojenkäsittelystä annettuun yleiseen kansalliseen lainsäädäntöön sekä koordinoimaan asiaan liittyvän erityislainsäädännön lainvalmistelutyötä. Työryhmä ehdotti säädettäväksi uuden tietosuojaa koskevan yleislain, tietosuojalain. Laki tulisi täsmentämään yleistä tietosuoja-asetusta.[37]

Helmikuussa 2018 valtioneuvoston lainsäädännön arviointineuvosto arvosteli hallituksen tekemää luonnosta tietosuojalaista puutteelliseksi. Arviointineuvosto kiinnitti huomiota varsinkin esiluonnoksen vaikealukuisuuteen ja siihen, että sen perusteella ei kyetä muodostamaan käsitystä lain taloudellisista ja yhteiskunnallisista vaikutuksista. Neuvoston mukaan luonnoksessa olisi pitänyt käsitellä huolellisemmin kilpailullisia vaikutuksia siitä, että seuraamusuhka on erilainen viranomaisille verrattuna yksityisiin toimijoihin. Myös kotitalouksille kohdistuvat seuraamukset jäivät epäselviksi. Neuvosto piti hyvänä sitä, että lakia valmisteltiin työryhmässä ja sitä varten oli tehty perusteellisesti oikeusperustaa sekä –käytäntöjä ja nykylain tilaa koskevaa selvitystyötä. Arviointineuvosto painotti, että esitystä tulisi korjata ennen sen antamista eduskunnalle käsiteltäväksi.[38]

Hallituksen esitys (9/2018 vp) maaliskuussa 2018 käsitteli henkilötietojen käsittelyyn sovellettavaa yleislakia eli tietosuojalakia. Tietosuojalaki on esityksen mukaan yleistä tietosuoja-asetusta täydentävä ja täsmentävä, jolloin se ei muodosta itsenäistä ja kattavaa sääntelykokonaisuutta, vaan sitä sovelletaan rinnakkain asetuksen kanssa. Ehdotetussa tietosuojalaissa säädetään henkilötietojen käsittelyn oikeusperusteesta ja erityisiin henkilötietoryhmiin luokiteltavien tietojen käsittelystä eräissä tapauksissa, tietoyhteiskunnan palvelujen lapselle tarjoamisen ikärajasta, valvontaviranomaisesta, oikeusturvasta sekä tietojenkäsittelyn erityistilanteista.[39]

5 Tietosuojaperiaatteet

Henkilötietojen suojalle pohjan luovat rekisterinpitäjän vastuut henkilötietojen käsittelyssä. Tällaiset velvollisuudet on säädetty henkilötietolaissa, mutta tämän lisäksi niitä on voitu säätää myös erityislainsäädännössä, kuitenkin viitaten henkilötietolain yleissääntelyyn. Velvollisuudet on kohdistettu rekisterinpitäjään, mutta kaikkien rekisterinpitäjän toimintaan ja henkilötietojen käsittelyyn osallistuvien tulee ottaa ne huomioon, koska velvollisuuksien toteu-

[37] EU:n yleisen tietosuoja-asetuksen täyttäntöönpanotyöryhmän (TATTI) mietintö 2017, 5-6.
[38] Valtioneuvoston kanslia. Lainsäädännön arviointineuvosto VNK/133/32/2018 2018.
[39] Eduskunta. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi 9/2018 vp.

tuminen tapahtuu vasta varsinaisesti käsittelytoiminnassa. Rekisterinpitäjällä on kuitenkin velvollisuus pitää huolta rekisteröidyn oikeuksista kaikissa käsittelyn vaiheissa.[40]

Tietosuoja-asetuksessa määritellään henkilötietojen käsittelyä koskevat periaatteet, jotka on otettava huomioon henkilötietoja käsiteltäessä. Ne rajoittavat sallittua henkilötietojen käsittelyä esimerkiksi rajoittamalla sitä, mitä tietoja on sallittua käsitellä ja millä tavoin. Tietosuojaperiaatteilla on käytännön tasolla tärkeä merkitys, koska usein arvioitaessa henkilötietojen käsittelyyn liittyvän toteutuksen lainmukaisuutta joudutaan miettimään uudestaan periaatetasolla mikä on sallittua. Tietosuoja-asetuksen periaatteet vastaavat pääosin jo aiemmin voimassa olleita henkilötietojen käsittelyn periaatteita, mutta joitain periaatteita ja käsitteitä on täsmennetty.[41]

5.1 Henkilötietolain periaatteet

Henkilötietolain 5 § esiintyvä henkilötietojen käsittelyä koskeva periaate on huolellisuusvelvoite. Se velvoittaa käsittelemään henkilötietoja lainmukaisesti, huolellisesti ja hyvää tietojenkäsittelytapaa noudattaen. Rekisterinpitäjän tulee ottaa myös huomioon yksityiselämän suojan loukkaamattomuus.

Huolellisuusvelvoitteeseen kuuluu myös henkilötietojen käsittelijöiden huolellinen tietojen käsittely ja tapa käsitellä tietoja siten, ettei käsittely ole lainvastaista tai tiedot päädy sivullisten käsiin. Huolellisuusvelvoite korostuu etenkin arkaluonteisten henkilötietojen käsittelyssä. Huolellinen tietojenkäsittely parantaa luottamusta henkilötietojen käsittelyyn ja se mahdollistaa myös asianmukaisen käsittelyn. Huolellisuus on merkittävä osa henkilötietojen käsittelyä etenkin luovutustilanteessa. Tietoja luovuttavan tahon on huolehdittava, että tietojen saajalla on oikeus käsitellä henkilötietoja ja tietoja luovutetaan vain siinä määrin kuin tiedonsaajan rekisterinpidon tarkoitukselle nähdään olevan tarpeen.[42]

Henkilötietolain periaatteisiin luetaan myös 6 § henkilötietojen käsittelyn suunnittelu. Tietojen kerääminen tulee perustella tarkoituksenmukaisella syyllä huomioon ottaen rekisterinpitäjän toiminta. Perusteluvaatimus tarkoittaa sitä, että rekisterinpitäjältä tulee löytyä rekisterinpitoa varten asianmukaiset perusteet sekä käsittelylle että toiminnalle ylipäätään. Henkilötietojen käsittelyn käyttötarkoitukset tulee määritellä ennen käsittelyn aloittamista, jolloin käsittelyn asianmukaisuus saadaan varmistettua etukäteen.[43]

---

[40] Voutilainen 2012, 301.
[41] Hanninen, Laine, Rantala, Rusi & Varhela 2017, 47.
[42] Voutilainen 2012, 301-302.
[43] Voutilainen 2012, 303.

Henkilötietolain 7 § olevan käyttötarkoitussidonnaisuus-periaatteen mukaan henkilötietojen käsittely ei saa olla ristiriidassa ennalta määrättyihin käsittelytarkoituksiin nähden. Henkilötietoja ei tule käyttää tai muuten käsitellä ennalta määrättyyn käyttötarkoitukseen yhteensopimattomalla tavalla.[44]

5.2 EU:n yleisen tietosuoja-asetuksen periaatteet ja muutokset

Yleisesti tietosuoja-asetuksen periaatteiden mukaan henkilötietoja tulee käsitellä lainmukaisesti, kohtuullisesti ja läpinäkyvästi. Läpinäkyvyys tulee tietosuoja-asetukseen uutena periaatteena. Käyttötarkoitussidonnaisuus asetuksen mukaan tarkoittaa sitä, että henkilötietojen keräämisen tulee perustua tiettyyn ennalta määrättyyn tarkoitukseen. Tietoja ei saa täten käsitellä tarkoituksesta poikkeavalla tavalla.[45] Tietosuojalaissa käytetty henkilötietojen käsittelyn suunnittelu sisältyy asetuksen käyttötarkoitussidonnaisuus periaatteeseen.[46]

Henkilötietolain mukainen huolellisuusvelvoite on osa tietosuoja-asetuksen lainmukaisuus, kohtuullisuus ja läpinäkyvyys periaatteita. Näiden asetuksen periaatteiden mukaan henkilötietoja on käsiteltävä lainmukaisesti ja asianmukaisesti, jotka olivat osana myös henkilötietolain huolellisuusvelvoitetta.[47] Käsittelyn tarkoituksen määrittely nojaa pääasiassa henkilötietojen suojaa varten muodostettuun oikeudelliseen kehykseen. Tarkoitusten määrittely rajoittaa perusteluita, joilla rekisterinpitäjät saavat käyttää keräämiään henkilötietoja. Kohtuullinen käsittely vaatii rekisterinpitäjältä käsittelyperusteiden rajaamista ja niiden kuvaamista hieman tarkemmin tietyissä tapauksissa. Läpinäkyvyys on tärkeää varsinkin, jos henkilötietoja kerätään useampaan kuin yhteen tarkoitukseen, jolloin myös tarkoituksien kuvaaminen rekisteröidyille tulee olla selkeää.[48] Jotta käsittelyn lainmukaisuus voidaan todeta, tulee ensin tunnistaa erityiset tarkoitukset jolla tietojen kerääminen on perusteltu.[49] Käsittelyn lainmukaisuus perustellaan tietosuoja-asetuksen (2016/679) 6 artiklassa mainituin edellytyksin.

Tietojen minimointi-periaatteen mukaan henkilötietojen tulee olla asianmukaisia ja tarpeellisia käsittelyn tarkoitukseen nähden. Sellaisia tietoja ei saa käsitellä, joka ei palvele tarkoitusta ja tietojen määrää sekä laatua tulee rajoittaa tarkoituksen mukaan.[50]
Täsmällisyydellä tarkoitetaan sitä, että kerättyjen tietojen tulee olla virheettömiä, ajantasaisia ja täsmällisiä. Rekisterinpitäjän tulee toteuttaa viipymättä kaikki kohtuulliset toimenpiteet varmistaakseen tarkoitukseen nähden virheellisten tietojen poistamisen tai oikaisun.

---

[44] Voutilainen 2012, 303.
[45] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 5.
[46] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 5 ja Henkilötietolaki 523/1999.
[47] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 5.
[48] 00569/13/EN WP 203 2013, 15-17
[49] 00569/13/EN WP 203 2013, 15
[50] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 5.

Henkilötietolaissa tietojen oikeellisuudesta huolehtiminen oli yksi rekisterinpitäjän velvollisuuksista, mutta poistamista tai oikaisemista viipymättä ei velvoitettu. Tietojen oikaisun vahvistaminen parantaa rekisteröidyn oikeuksia.[51]

Säilytyksen rajoittaminen on asetuksen myötä uusi periaate, jonka mukaan henkilötietoja tulee säilyttää muodossa, josta rekisteröity voidaan tunnistaa ainoastaan tietojenkäsittelyn tarkoitukselle tarpeellisen ajan. Säilyttäminen voi jatkua pidempään, jos henkilötietojen käsittely perustuu yleisen edun mukaisiin arkistointitarkoituksiin, tieteelliseen tai historiallisiin tutkimustarkoituksiin tai tilastollisiin tarkoituksiin.[52] Rekisterinpitäjän tulee määritellä henkilötietoa keräävien prosessien elinkaari yksilön oikeuksia ja vapauksia käsittelevän tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdan vaatimusten mukaan. Rekisterinpitäjän tulee myös varmistaa tietojen ajantasaisuus koko elinkaaren ajan epätarkkuuksien välttämiseksi.[53]

Eheys ja luottamuksellisuus periaatteen mukaan henkilötietoja tulee käsitellä tavalla, jolla turvataan henkilötietojen turvallisuus, johon sisältyy suojaaminen tietojen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asiaankuuluvia teknisiä tai organisatorisia suojatoimia. Rekisterinpitäjän tulee pystyä osoittamaan noudattavansa kaikkia näitä periaatteita uuden osoitusvelvollisuuden myötä.[54] Edellä mainittu periaate ei ole uusi, koska se sisältyi tietojen suojaamista käsittelevään 32 § henkilötietolaissa.

Tietosuoja-asetuksen artiklan 25 mukaan rekisterinpitäjän tulee huolehtia, että lähtökohtaisesti käsitellään vain tarkoitukseen nähden tarpeellisia henkilötietoja. Rekisterinpitäjän toteuttamat tarpeelliset toimenpiteet velvoittavat tietojen määrää, laajuutta, saatavuutta ja säilytysaikaa. Toimenpiteillä varmistetaan, että henkilötiedot eivät päädy ulkopuolisille tahoille ilman rekisteröidyn suostumusta. Käsittelyn suunnittelun ja toteuttamisen yhteydessä rekisterinpitäjän tulee tehdä periaatteiden totetuttamiseksi vaadittavat toimenpiteet. Tällä varmistetaan, että periaatteet sidotaan osaksi henkilötietojen käsittelyä ja käsittely vastaa asetuksen vaatimuksia sekä suojaa rekisteröidyn oikeuksia. Toimenpiteiden suorittaminen vaatii kustannusten, uuden tekniikan, käsittelyn luonteen, laajuuden, tarkoituksen ja asiayhteyden huomioimista. Rekisterinpitäjän arvioitavaksi tulee myös henkilötietojen käsittelyn riskin suuruus ja sen vaatimat toimenpiteet, kuten pseudonymisointi ja muut suojatoimet.[55]

---

[51] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 5 ja Henkilötietolaki 523/1999..
[52] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 5.
[53] 17/EN/WP251 2018, 12.
[54] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 5.
[55] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 25.

Tietosuoja-asetuksen myötä valvontaviranomaisella on valtuus määrätä tästä eteenpäin hallinnollisia sakkoja ja myös muita sanktioita. Päätettäessä sakon määräämisestä ja määrästä, tulee ottaa huomioon muun muassa rikottu velvollisuus, rikkomisen tahallisuus, rikkomisen vaikutuksen alla olevien rekisteröityjen määrä, toimenpiteet rikkomisen korjaamiseksi sekä vaikutusten lieventämiseksi ja ilmoittamistapa valvontaviranomaiselle.[56]

Perustavanlaatuisten velvoitteiden rikkomisista aiheutuva hallinnollinen sakko on suuruudeltaan 20 miljoonaa euroa tai 4 % yrityksen edeltävän tilikauden maailmanlaajuisesta liikevaihdosta, riippuen kumpi on rahamääräisesti suurempi. Perustavanlaatuisiin velvoitteisiin kuuluvat käsittelyn perusperiaatteet, rekisteröidyn oikeudet, tietojen siirto EU:n ulkopuolelle ja valvontaviranomaisen määräyksen noudattamatta jättäminen. Muiden velvoitteiden rikkomisesta annettava hallinnollinen sakko on 10 miljoonaa euroa tai 2 % yrityksen edeltävän tilikauden vuotuisesta maailmanlaajuisesta liikevaihdosta. Tähän sakkoon liittyvät säännökset ovat rekisterinpitäjän ja henkilötietojen käsittelijän, sertifiointielimen ja valvontaelimen velvollisuudet.[57]

Rekisteröidylle tietosuoja-asetuksen rikkomisesta aiheutuneesta aineellisesta tai aineettomasta vahingosta, rekisterinpitäjällä tai henkilötietojen käsittelijällä on vahingonkorvausvastuu. Vahingon aiheuttaneesta tapahtumasta vastuussa oleva yritys on korvauksen maksuvelvollinen ja henkilötietojen käsittelijä yritys siinä tapauksessa, jos se ei ole noudattanut tietosuoja-asetuksen määrittämiä käsittelijöille osoitettuja velvoitteita tai se on toiminut rekisterinpitäjän ohjeistuksen vastaisesti. Useamman yrityksen ollessa vastuussa aiheutuneesta vahingosta, kukin vastaa koko vahingosta suhteessa vahingosta kärsineeseen rekisteröityyn, jolloin rekisteröity voi vaatia koko korvausta yhdeltä vastuussa olevalta yritykseltä. Tällaisessa tapauksessa korvauksen maksava yritys on oikeutettu perimään osuutta korvauksesta muilta vastuullisilta yrityksiltä, joka määräytyy yrityksen vastuun mukaan aiheutuneessa vahingossa.[58]

Tietosuojalainsäädännön seuraamusjärjestelmä painottuu jatkossa hallinnollisiin sakkoihin, mutta rikosoikeudellinen vastuu tulee kyseeseen tilanteissa, joissa henkilötietojen käsittelyn lainvastainen suorittaminen ei ole hallinnollisten sakkojen piirissä.[59] Aiemman lainsäädännön henkilörekisteririkos korvataan tietosuojarikosta koskevalla säännöksellä. Tietosuojarikos tarkoittaa tilannetta, jossa henkilö muutoin kuin rekisterinpitäjän tai henkilötietojen käsittelijän ominaisuudessa tahallaan tai törkeästä huolimattomuudesta saa käsiinsä henkilötietoja käyttötarkoitusta vastaamattomalla tavalla, luovuttaa tietoja tai siirtää tietoja vastoin asetuksen tai muuta henkilötietojen käsittelyä koskevaa lakia. Henkilö loukkaa tällaisissa tilanteissa re-

[56] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 83.
[57] Hanninen ym. 2017, 129-130.
[58] Hanninen ym. 2017, 130-131
[59] EU:n yleisen tietosuoja-asetuksen täytäntöönpanoryhmän (TATTI) mietintö 2017, 64.

kisteröidyn yksityisyyden suojaa tai aiheuttaa muuta vahinkoa sekä olennaista haittaa. Tietosuojarikokseen voi syyllistyä esimerkiksi työntekijä, joka tutkii rekisteröidyn tietoja vaikka tehtäviensä perusteella hänellä ei ole niiden käsittelyyn oikeutta.[60]

Tietosuojarikos voi olla kyseessä myös kun toimitaan vastoin tietosuoja-asetuksen tai muun henkilötietojen käsittelyä koskevan lain säätämää käsittelyn turvallisuutta. Rangaistavana menettelynä voidaan pitää tilannetta, jossa rekisterinpitäjän palveluksessa oleva henkilö heittää pois henkilörekisteriin liittyviä asiakirjoja huolehtimatta tietoturvallisesta hävittämisestä. Rangaistussäännökseen ei ole kuitenkaan ehdotettu oikeushenkilön rangaistusvastuuta eli yritys ei voi syyllistyä tietosuojarikokseen.[61]

5.3 Käsitteiden määrittely

Tietosuoja-asetuksessa on paljon erilaisia käsitteitä, joiden ymmärtäminen on tarpeen yritykselle toimintansa ja dokumentaationsa saattamiseksi asetuksen edellyttämälle tasolle. Henkilötietolaki sisältää osin samoja ja ainakin samankaltaisia käsitteitä, mutta osa käsitteistä on vielä Suomen lainsäädännölle tuntemattomia.[62]

Henkilötieto on henkilötietolain 3 § kohdan 1 mukaan kaikkea luonnollista henkilöä koskevaa tietoa, josta saadaan selville jotain henkilön ominaisuuksista tai elinolosuhteista ja ne voidaan yhdistää suoraa henkilöön tai henkilön perheeseen. Tietosuoja-asetuksen mukaan henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan henkilöön liittyvää tietoa. Tiivistettynä määritelmässä on kyseessä henkilötiedot, joiden perusteella saadaan tietoon kenestä on kyse. Tietosuoja-asetus tulee sovellettavaksi aina, kun kyseessä on tunnistettavan tai tunnistettavissa olevan henkilön tietojen käsittely.[63]

Rekisteröidyllä tarkoitetaan luonnollista henkilöä eli ihmistä, jonka henkilötietoja käsitellään. Tietosuoja-asetuksen perusteella yritykset eivät ole rekisteröityjä, mutta yrityksen yhteys- tai muut henkilöt ovat rekisteröityjä ja heidän tietojensa käsittely kuuluu asetuksen mukaisen henkilötietojen käsittelyn piiriin.[64]

Henkilötietolain 3 § kohdassa 3 rekisteri määritellään tietojoukoksi, joka sisältää käyttötarkoituksensa mukaisia henkilötietoja. Rekisteriä käsitellään osittain tai täysin automaattisen tietojenkäsittelyn avulla ja järjestettynä kortistoksi, luetteloksi tai muulla tietyn henkilön tietojen helpon löytämisen mahdollistavalla tavalla. Kohdassa 4 kerrotaan rekisterinpitäjän

[60] Hanninen ym. 2017, 131.
[61] Hanninen ym. 2017, 132.
[62] Hanninen ym. 2017, 19.
[63] Hanninen ym. 2017, 19-20.
[64] Hanninen ym. 2017, 20.

tarkoittavan henkilöä, instituutiota tai yhteisöä, joka käyttää rekisteriä ja määrää rekisterin käytöstä. Tietosuoja-asetuksessa edustaja on henkilö, joka toimii rekisterinpitäjän lukuun ja edustaa rekisterinpitäjää.[65]

Aikaisempi tietosuojalainsäädäntö perustui rekisterin käsitteeseen, kun tietosuoja-asetus keskittyy tietojen käyttötarkoitukseen. Asetuksessa rekisterillä tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, joista tietoja saadaan tietyin perustein riippumatta siitä, onko tietojoukko keskitetty, hajautettu tai muuten jaettu. Rekisterissä on kyse samaan käyttötarkoitukseen kerätyistä ja käytettävistä tiedoista. Rekisterinpitäjä on henkilötietojen keräämisestä ja käyttötarkoituksesta vastaava taho. Rekisterinpitäjä voi määritellä käsittelyn tarkoitukset ja keinot joko yksin tai muun tahon kanssa.[66] Sivullisella tarkoitetaan henkilötietolain 3 § kohdassa 6, jotain muuta henkilöä tai yhteisöä, joka ei ole rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä tai joka ei käsittele kahden viimeksi mainitun lukuun henkilötietoja. Tietosuoja-asetuksessa kolmas osapuoli on taho, jolla on oikeus käsitellä henkilötietoja rekisterinpitäjän, käsittelijän tai rekisteröidyn lisäksi.[67]

Henkilötietojen käsittely on toiminto, joka kohdistuu henkilötietoja sisältävään rekisteriin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Käsittelynä pidetään tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista, tietojen yhdistämistä, rajoittamista, poistamista tai tuhoamista. Laaja määritelmä tarkoittaa käytännössä sitä, että lähes kaikki henkilötietojen käyttäminen tavalla tai toisella luetaan käsittelyksi.[68] Henkilötietojen käsittelijällä tarkoitetaan tietosuoja-asetuksessa ja tietosuojadirektiivissä luonnollista henkilöä, oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Vastaanottaja on joku edellämainituista tahoista, jolle luovutetaan henkilötietoja. Viranomaisia, jotka saavat henkilötietoja tutkimukseen perustuen unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti eivät ole vastaanottajia. Kyseisten viranomaisten tulee noudattaa tästä huolimatta sovellettavia tietosuojasääntöjä käsittelyn tarkoitusten mukaisesti.[69] Henkilötietojen käsittelijä on käytännössä alihankkija tai yhteistyökumppani, joka käsittelee henkilötietoja rekisterinpitäjän puolesta. Käsittelyn keräämisestä ja käyttämisestä vastuussa on edelleen rekisterinpitäjä. Käsittelijän tulee noudattaa rekisterinpitäjän antamaa dokumentoitua ohjeistusta henkilötietojen käsittelyssä.[70] Vastaanottajalle tietojen luovuttamisessa on kyse siitä, että rekisterinpitäjä toimittaa ulkopuoliselle rekiste-

[65] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[66] Hanninen ym. 2017, 22.
[67] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[68] Hanninen ym. 2017, 20-21.
[69] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4 & Euroopan parlamentin ja neuvoston direktiivi 95/46/EY artikla 2.
[70] Hanninen ym. 2017, 22.

röityjen tietoja, joka ei ole henkilötietojen käsittelijä. Vastaanottajasta tulee tällöin luovutettavien tietojen rekisterinpitäjä.[71]

Yritys on asetuksen mukaan taloudellista toimintaa harjoittava henkilö tai oikeushenkilö, mukaan lukien taloudellista toimintaa harjoittavat kumppanuudet ja yhdistykset. Konserni tarkoittaa määräysvaltaa käyttävää yritystä ja sen alaisuudessa toimivia yrityksiä. Yritystä koskevat sitovat säännöt ovat henkilötietojen suojeluperiaatteita, joita rekisterinpitäjä noudattaa siirtäessään henkilötietoja kolmanteen maahan konsernin sisällä.[72]

Käsittelyn rajoittamisella pyritään siihen, että henkilötiedot merkitään tavalla, jolla niiden käsittelyn rajoittaminen on mahdollista myöhemmin.[73] Profiloinnilla tarkoitetaan henkilötietojen automaattista käsittelyä, jossa henkilötietoja hyödyntämällä arvioidaan ja ennakoidaan piirteitä, jotka liittyvät henkilön ominaisuuksiin, työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin kiinnostuksen kohteisiin, käyttäytymiseen, sijaintiin tai liikkeisiin.[74] Yritystoiminnassa profilointia käytetään yleisesti esimerkiksi markkinoinnin ja myynnin apuvälineenä.[75]

Pseudonymisointi on henkilötietojen käsittelyä, jossa tietoa ei voida yhdistää rekisteröityyn ilman lisätietoja. Lisätiedot tulee säilyttää erillään ja niihin käytetään teknisiä toimenpiteitä, joilla voidaan estää henkilötietojen yhdistäminen henkilöön.[76] Anonymisoinnilla tarkoitetaan henkilötiedon tunnistettavuuden poistamista tavalla, jolla tietojen yhdistäminen rekisteröityyn ei ole enää mahdollista. Anonyymit tiedot eivät sisälly tietosuojalainsäädäntöön tai tietosuoja-asetukseen.[77]

Henkilötietojen turvaloukkauksella tarkoitetaan toimintaa, jonka seurauksena käsitellyt tiedot vahingossa tai lainvastaisesti tuhoutuvat, häviävät, muuttuvat, luvattomasti luovutetaan tai ulkopuolinen pääsee tietoihin käsiksi.[78] Rekisterinpitäjien ja henkilötietojen käsittelijöiden tulee kartoittaa tietoturvaan liittyvät riskit ja pyrittävä niiden ehkäisyyn kohtuullisin keinoin.[79]

---

[71] Hanninen ym. 2017, 23.
[72] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[73] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[74] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[75] Hanninen ym. 2017, 21.
[76] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[77] Hanninen ym. 2017, 21.
[78] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[79] Hanninen ym. 2017, 23.

Geneettiset henkilötiedot koskevat henkilön perittyjä tai hankittuja geneettisiä ominaisuuksia, joista saadaan selville yksilöllistä tietoa henkilön fysiologiasta tai terveydentilasta ja jotka saadaan henkilöstä otetusta biologisesta näytteestä analysoimalla.[80] Biometrisillä tiedoilla tarkoitetaan kaikkia henkilön fyysisiin ja fysiologiisiin ominaisuuksiin liittyviä teknisellä käsittelyllä saatuja henkilötietoja. Biometrisiä tietoja ovat esimerkiksi sormenjälki sekä kasvokuva ja niiden perusteella henkilö voidaan tunnistaa tai henkilön tunnistaminen varmistaa.[81] Terveystiedot ovat henkilön fyysiseen tai psyykkiseen terveyteen liittyviä henkilötietoja joihin kuuluu myös tiedot terveyspalvelujen tarjoamisesta, jotka ilmaisevat henkilön terveydentilan.[82]

Valvontaviranomainen on jäsenvaltion nimittämä riippumaton viranomainen. Osallistuva valvontaviranomainen toimii valtiossa jossa rekisterinpitäjän toimipaikka on. Kyseiselle viranomaiselle on tehty valitus tai käsittely vaikuttaa merkittävästi valvontaviranomaisen jäsenvaltiossa asuviin rekisteröityihin.[83] Päätoimipaikkana pidetään rekisterinpitäjän keskushallinnon sijaintia unionissa paitsi sellaisissa tilanteissa, joissa päätökset käsittelyn tarkoituksista ja keinoista tehdään jossain muussa toimipaikassa. Päätoimipaikka on tällöin se paikka missä päätökset käsittelystä ja päätoiminen käsittely tehdään, joka pätee myös rekisterinpitäjiin joiden keskushallinto ei ole unionissa.[84] Rajatylittävällä käsittelyllä tarkoitetaan henkilötietojen käsittelyä, jota suoritetaan useassa eri valtiossa. Myös sellainen käsittely jota suoritetaan rekisterinpitäjän tai käsittelijän ainoassa toimipaikassa, joka vaikuttaa merkittävästi useamman jäsenvaltion rekisteröityihin on rajatylittävää käsittelyä.[85]

Rekisteröidyn suostumus on määritelty aiempaa tarkemmin tietosuoja-asetuksessa. Sen mukaan suostumus on vapaaehtoinen, yksilöity ja tietoinen tahdonilmaisu. Suostumuksella rekisteröity hyväksyy henkilötietojensa käsittelyn ilmaisemalla suostumuksensa. Tahdonilmaisun tulee olla yksiselitteinen, joka vahvistaa rekisteröidyn oikeuksia. Yksiselitteisen tahdonilmaisun avulla väärinkäsitysten syntyminen tahdonilmaisun antamisessa ei ole niin helppoa. Asetukseen on lisätty, että suostumuksen on oltava annettu lausuma tai selkeä toimenpide suostumuksen antamisesta.[86]

---

[80] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[81] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[82] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[83] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[84] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[85] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.
[86] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 4.

6 Rekisteröidyn oikeudet

Rekisteröidyllä on oikeus selvittää, mitä tietoja hänestä on kerätty ja talletettu sekä mahdollisuus saattaa asia viranomaisten tutkittavaksi tarvittaessa. Rekisteröidyn halutessa käyttää laissa säädettyjä oikeuksia tai kun hänellä on kysyttävää henkilötietojensa käsittelystä, tulee hänen ensisijaisesti ottaa yhteyttä asianomaiseen rekisterinpitäjään.[87]

Jos asiaa ei saada selvitettyä rekisterinpitäjän kanssa, rekisteröity voi ottaa yhteyttä tietosuojavaltuutetun toimistoon. Epäiltäessä henkilötietojen käsittelyyn liittyvää rikosta voidaan olla yhteydessä myös poliisiviranomaisiin asian selvittämiseksi.[88]

6.1 Ilmoitettavat tiedot

Henkilötietolain 24 § vaaditaan, että henkilötietoja kerättäessä rekisteröidyltä, rekisterinpitäjän tulee toimittaa rekisteröidylle tiedot rekisterinpitäjän ja edustajan henkilöllisyydestä, käsittelyn tarkoituksista, mahdolliset vastaanottajat, pyyntöihin ja kysymyksiin vastaamisvelvollisuus ja seuraukset vastaamatta jättämisestä. Tämän lisäksi tulee ilmoittaa rekisteröidyn oikeuksista saada hänestä kerätyt henkilötiedot ja oikaista ne.

Henkilötietojen käsittelyn kuvaaminen voi tapahtua tietosuojaselosteella. Selosteessa kuvatun käsittelyn tulee oikeasti vastata tietosuoja-asetuksen asettamia edellytyksiä, eikä ainoastaan aiemman rekisteriselosteen muokkaaminen riitä. Tietosuojaseloste on helppoa toteuttaa linkkinä verkkopalvelun yhteydessä.[89]

Rekisterinpitäjän kerätessä tietoja joltain muulta kuin rekisteröidyltä itseltään voidaan informointivelvollisuudesta poiketa, jos tietojen antaminen rekisteröidylle on mahdotonta tai kohtuuttoman hankalaa. Tilanteissa joissa tiedot on kerätty jostain muualta kuin rekisteröidyltä, pitää viranomaisen huomioida päätöksiä tehdessään tietojen ajantasaisuus. Tietojen oikeellisuus tulee tällöin varmistaa hallintolain 32 § mukaisella selvityspyynnöllä ennen päätöksentekoa, jos päätös aiheuttaa rekisteröidylle merkittäviä oikeudellisia vaikutuksia. Menettelyyn liittyy myös hallintolain 34 § säännös, jonka mukaan asianosaisella on oikeus tulla kuulluksi ennen asian ratkaisua.[90] Jos henkilötietoja kerätään muualta kuin rekisteröidyltä, tulee rekisterinpitäjän toimittaa myös kerätyt henkilötietoryhmät. Tiedot tulee toimittaa

[87] Tietosuoja. Rekisteröidyn oikeudet. 2014.
[88] Tietosuoja. Rekisteröidyn oikeudet. 2014.
[89] Hanninen ym. 2017, 75.
[90] Voutilainen 2012, 308-309.

henkilötietojen ensimmäisen luovutuksen yhteydessä ja jos luovutusta ei tehdä niin ilmotus tapahtuu rekisteröitäessä.[91]

Tietosuoja-asetuksen mukaan rekisterinpitäjän tulee toimittaa rekisteröidyltä tietoja kerättäessä rekisterinpitäjän ja mahdollisen edustajan yhteystiedot, tietosuojavastaavan yhteystiedot, käsittelyn tarkoitukset ja oikeusperusteet. Tämän lisäksi tulee kertoa rekisterinpitäjän eduista, jos käsittelyn lainmukaisuus perustuu rekisterinpitäjän tai kolmannen osapuolen etujen toteutumiseen. Rekisterinpitäjän on ilmoitettava rekisteröidylle tieto vastaanottajaryhmistä ja tietojen siirtämisestä kolmansiin maihin eli EU tai ETA –alueen ulkopuolelle. Jos tietoja aiotaan siirtää kolmanteen maahan, tulee rekisterinpitäjän vahvistaa kyseisen maan tietosuojan hyväksytty taso tai hyväksymätön taso.[92]

6.2 Tiedonsaantioikeus

Henkilötietolain 26 § mukaan rekisteröidyllä on tarkastusoikeus, jonka mukaan rekisteröidyllä on oikeus saada vapaasti ja kohtuullisin väliajoin veloituksetta tieto käsitelläänkö hänestä tietoja vai ei sekä vähintään tieto käsittelyn tarkoituksista, tietoryhmistä ja tietojen vastaanottajista. Käsitellyt tiedot tulee toimittaa rekisteröidylle ymmärrettävässä muodossa. Rekisteröidylle tulee toimittaa kaikkia tiedot alkuperästä lähtien ja informoida häntä automaattisen käsittelyn logiikasta. Rekisteröidyllä on oikeus saada virheelliset ja puutteelliset tiedot oikaistuksi, poistetuksi tai suojatuksi, etenkin tilanteissa joissa ne eivät ole lainmukaisia. Henkilötietoja vastaanottaville tahoille tulee ilmoittaa tietojen oikaisusta ja poistosta.

Henkilötietolain 29 § mukainen oikaisuoikeus kuuluu myös tietosuoja-asetukseen. Rekisterinpitäjän tulee korjata, poistaa tai täydentää viipymättä rekisteröidyn vaatimuksesta virheelliset tiedot. Rekisteröity voi myös itse toimittaa täydennettäviä tietoja, jotta aiemmin puutteelliset tiedot voidaan korjata.[93]

Tietosuoja-asetuksessa rekisteröidyn oikeuksiin kuuluu saada tieto, että käsitelläänkö häneen liittyviä henkilötietoja. Rekisteröidyllä on oikeus päästä omiin henkilötietoihin sekä tieto käsittelyn tarkoituksista, kerätyistä henkilöryhmistä, vastaanottajaryhmistä, säilytysajasta tai sen määrittämiskriteereistä, automaattisesta päätöksenteosta, tietojen alkuperästä, jos tietoja ei ole kerätty rekisteröidyltä, oikeuksista pyytää tietojen oikaisua tai poistamista ja valittaa valvontaviranomaiselle. Jos henkilötietoja siirretään kolmanteen maahan, tulee rekisteröityä informoida käytetyistä suojatoimista. Tiedot tulee toimittaa yleisesti käytetyssä sähköisessä muodossa, paitsi rekisteröidyn pyytäessä vaihtoehtoista toimitustapaa. Rekisteröidyn

---

[91] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY artikla 11.
[92] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 13.
[93] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 16.

halutessa useampia kopioita tiedoista voidaan periä kohtuullinen hallinnollisiin kustannuksiin perustuva maksu.[94]

6.3 Vastustamisoikeus

Tietosuojadirektiivissä rekisteröidyllä on oikeus milloin tahansa vastustaa henkilötietojensa käsittelyä tilanteeseensa liittyvien tärkeiden ja perusteltujen syiden vuoksi. Kansallinen lainsäädäntö saattaa kuitenkin ylittää tällaiset perustelut, mutta jos perustelut ovat muissa tapauksissa päteviä tulee rekisterinpitäjän lopettaa henkilötietojen käsittely kyseisen henkilön osalta. Rekisteröidyllä on oikeus myös vastustaa korvauksetta henkilötietojensa käsittelyä suoramarkkinointitarkoituksissa.[95]

Automaattiseen päätöksentekoon perustuvassa henkilötietojen käsittelyssä rekisteröidyllä on oikeus vastustaa tällaista käsittelyä, jos siitä aiheutuu oikeudellisia vaikutuksia, vaikutus kohdistuu merkittävästi rekisteröityyn, käsittely on yksin omaan automaattiseen tietojenkäsittelyyn perustuvaa tai se on tarkoitettu rekisteröidyn henkilökohtaisten ominaisuuksien arviointiin.[96]

Tietosuoja-asetuksessa rekisteröidyllä on aina oikeus vastustaa henkilötietojensa käsittelyä henkilökohtaiseen erityiseen tilanteeseen vedoten. Jos rekisterinpitäjä ei kykene osoittamaan perusteltua syytä tietojen käsittelemiselle, tulee käsittely lopettaa. Rekisterinpitäjän perusteltu syy voi olla sellainen, joka syrjäyttää rekisteröidyn oikeudet tai se on tarpeellinen käynnistettävälle oikeuskäsittelylle. Rekisteröity voi ilman erityisempää syytä vastustaa suoramarkkinointia, jonka jälkeen sitä varten kerättyjä tietoja ei saa enää käsitellä.[97] Asetuksessa rekisteröity voi vastustaa automaattiseen käsittelyyn joutumista, esimerkiksi profiloinnin avulla tapahtuvien päätösten kohteeksi. Poikkeuksena sellaiset päätökset, jotka ovat välttämättömiä rekisteröidyn ja rekisterinpitäjän sopimuksen täytäntöönpanossa, päätös on lainsäädännön hyväksymä tai päätös on perusteltu rekisteröidyn nimenomaisella suostumuksella.[98]

6.4 Tietosuoja-asetuksen uudet oikeudet

Tietosuoja-asetuksen myötä rekisteröity saa oikeudet tietojen siirtämiseen ja käsittelyn rajoittamiseen. Henkilötietolain 29 § tiedon korjaamisoikeuden mukaisella tavalla rekisteröidyl-

---

[94] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 15.
[95] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY artikla 14.
[96] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY artikla 15.
[97] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 21.
[98] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 22.

lä on asetuksenkin voimaantullessa artiklassa 17 oikeus saada poistetuksi rekisterinpitäjän hänestä keräämät henkilötiedot ilman aiheetonta viivytystä ja rekisterinpitäjällä on velvollisuus poistaa henkilötiedot ilman aiheetonta viivytystä. Tämän edellytyksenä on, että kerättyjä henkilötietoja ei enää tarvita tarkoitukseen johon ne kerättiin tai sille ei ole enää perusteltua syytä, rekisteröity peruuttaa suostumuksensa käsittelylle, joka on perustunut suostumukseen, tietojen poistaminen perustuu rekisterinpitäjän lakisääteisen velvoitteen noudattamiseen tai tiedot on kerätty tietoyhteiskunnan palveluiden tarjoamisen yhteydessä. Henkilötietojen julkistamisen jälkeen ja rekisterinpitäjän tietojen poistamisvelvollisuuden vuoksi, tulee rekisterinpitäjän käytettävissä olevan teknologian ja toteuttamiskustannusten puitteissa toteutettava kohtuulliset toimenpiteet ilmoittaakseen henkilötietoja käsitteleville rekisterinpitäjille rekisteröidyn tietojen poistamispyynnöstä.[99] Tätä niinsanottua oikeutta tulla unohdetuksi ei sovelleta esimerkiksi, jos käsittely on tarpeen oikeusvaateen laatimisessa, esittämisessä tai puolustamisessa.[100]

Oikeus käsittelyn rajoittamiseen pätee seuraavissa tilanteissa, kun rekisteröity kiistää henkilötietojen paikkaansapitävyyden, joka johtaa käsittelyn rajoittamiseen rekisterinpitäjän selvitystyön ajaksi. Henkilötietojen käsittely on lainvastaista ja rekisteröity ei halua tietojaan poistettavan vaan vaatii niiden käytön rajoittamista. Rajoittaminen on mahdollista myös, jos rekisterinpitäjällä ei ole tarvetta enää kyseisille henkilötiedoille aiemmin määritellyn käsittelyn tarkoituksen mukaan, mutta rekisteröity itse tarvitsee niitä oikeusvaateen laatimiseen, esittämiseen tai puolustamiseen. Rekisteröity voi vastustaa myös käsittelyä odottaessaan todennusta rekisterinpitäjän oikeutetuista eduista henkilötietojen käsittelylle suhteessa rekisteröidyn perusteisiin. Käsittelyn ollessa rajoitettua saa kyseisiä henkilötietoja käsitellä säilyttämistä lukuun ottamatta, pelkästään rekisteröidyn suostumuksella, oikeustoimien toteuttamiseen, toisen luonnollisen henkilön tai oikeushenkilön oikeuksien suojaamiseen tai valtiovallan tärkeään yleiseen etuun vedoten. Rekisterinpitäjän tulee ilmoittaa rekisteröidylle käsittelyn rajoituksen poistamisesta.[101]

Rekisteröidyllä on oikeus saada hänestä kerätyt henkilötiedot rekisterinpitäjältä jäsennellyssä ja yleisesti käytetyssä koneellisessa muodossa. Kyseisten tietojen siirtäminen toiselle rekisterinpitäjälle on mahdollista, jos käsittely on perustunut suostumukseen tai automaattiseen käsittelyyn. Siirtäminen rekisterinpitäjältä toiselle tulee kuitenkin olla teknisesti mahdollista ja siirto-oikeuden käyttäminen ei saa rajoittaa artiklan 17 mukaista tietojen poistamisoikeut-

[99] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 17.
[100] Hanninen ym. 2017, 62.
[101] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 18.

ta. Järjestelmästä toiseen siirtämistä ei sovelleta yleistä etua koskevan tehtävän tai julkisen vallan käyttämiseen liittyvässä käsittelyssä.[102]

7 Rekisterinpitäjän velvollisuudet

Englanninkielinen termi rekisterinpitäjälle on ”data controller”, joka kuvaa hyvin rekisterinpitäjän asemaa henkilötietojen käsittelyä hallitsevana ja siitä päättävänä tahona. Käsittelytilanteissa roolit määräytyvät sen mukaan, mikä taho määrittelee käsittelyn tarkoitukset ja keinot. Otetaan esimerkkinä työnantajayritykselle palkanlaskenta palvelua tarjoava yritys, joka tällaisissa tapauksissa käsittelee henkilökunnan tietoja tämän palvelun tarjoamiseksi. Tällöin palvelua tarjoava yritys tekee käsittelyä rekisterinpitäjän lukuun. Toisenlainen skenaario voi olla, että työnantaja yritys tarjoaa työsuhde-etuna jotain palvelua työntekijöilleen toiselta yritykseltä, jolloin tietoja ei todennäköisesti käsitellä rekisterinpitäjän ohjeistuksien mukaan. Työnantaja yrityksen työntekijöiden henkilötietojen käsittelyn tarkoituksiin voi kuulua työsuhteen oikeuksien ja velvollisuuksien täyttäminen, kun taas työsuhde-etua tarjoavalla yrityksellä esimerkiksi asiakashallinta ja suoramarkkinointi. Jälkimmäisessä tilanteessa voidaan tulkita palveluntarjoaja yrityksen olevan rekisterinpitäjä käsitellessään henkilötietoja eri tarkoituksin verrattuna työnantajayritykseen. Tällöin tarkoitetaan tietojen luovutusta rekisterinpitäjältä toiselle.[103]

Henkilötietojen luovuttamisessa on kyse siitä, että rekisterinpitäjä siirtää rekisteröityjen tietoja kolmannelle osapuolelle käsiteltäväksi tai siten, että vastaanottavasta osapuolesta tulee rekisterinpitäjä. Tietojen siirtyessä konsernin sisällä kyseessä on yleensä tietojen siirtäminen käsiteltäviksi eli ulkoistamistilanne, luovuttaminen rekisterinpitäjältä toiselle tai yhteinen rekisteri. Toimenpide määritellään konserniyhtiöiden roolin mukaan tietojen käsittelyssä. Siirto on kyseessä, kun vastaanottava yhtiö käsittelee tietoja siirtävien yhtiöiden tarkoitusten mukaisesti. Luovutuksessa vastaanottaja päättää itse tehtävistä käsittelytoimista ja yhteisrekisterissä kaikki konserniin kuuluvat yhtiöt yhdessä. Luovutustilanteissa kaikki henkilötietojen käsittelyssä rekisterinpitäjäksi määritellyt yritykset vastaavat tietosuoja-asetuksen noudattamisesta. Henkilötietojen luovuttamisen edellytyksenä on, että luovuttajalla ja vastaanottajalla on laillinen peruste henkilötietojen käsittelyyn.[104]

Tietosuoja-asetuksen 4. luvussa käsitellään rekisterinpitäjän velvollisuuksia. Tietosuojadirektiivissä (95/46/EY) rekisterinpitäjän velvollisuuksia käsiteltiin jaksoissa 8 ja 9. Osoitusvelvollisuuden mukaan rekisterinpitäjän tulee osoittaa noudattavansa tietosuoja-asetusta. Rekisterinpitäjä voi osoittaa noudattavansa tietosuoja-asetuksen säännöksiä toteuttamalla tarvitta-

[102] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 20.
[103] Hanninen ym. 2017, 24-25
[104] Hanninen ym. 2017, 93-95.

vat toimenpiteet ottaen huomioon käsittelyn luonteen, laajuuden, tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat riskit. Asianmukaiset toimenpiteet tulee toteuttaa myös, jotta käsittely koskisi ainoastaan sen tarkoituksen kannalta oleellisia henkilötietoja. Tämä velvollisuus koskee henkilötiedon määrää, laajuutta, säilytysaikaa ja saatavilla oloa.[105]

Rekisterinpitäjän tai tarvittaessa rekisterinpitäjän edustajan on ylläpidettävä selostetta vastuullaan olevista käsittelytoimista. Selosteen tulee sisältää rekisterinpitäjän, tietosuojavastaavan, edustajan ja mahdollisen yhteisrekisterinpitäjän yhteystiedot, käsittelyn tarkoitukset, kuvaus henkilötietoryhmistä, vastaanottajat, tiedot siirtämisestä kolmansiin maihin, säilytysmääräajat ja kuvaus organisatorisista sekä teknisistä turvatoimista. Selosteen ylläpito velvollisuus ei koske yritystä tai järjestöä, joka työllistää alle 250 työntekijää, paitsi jos käsittely aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille, ei ole satunnaista tai käsittely kohdistuu erityisiin tietoryhmiin sekä rikostuomioita tai rikkomuksia koskeviin henkilötietoihin.[106]

Turvallisuustason varmistamiseksi rekisterinpitäjän tulee toteuttaa toimenpiteinä tietojen pseudonymisointi ja salaus, taata palveluiden ja käsittelyjärjestelmien luottamuksellisuus, ylläpitää kykyä palauttaa tiedot nopeasti saataville ja varmistaa tietoihin pääsy fyysisen tai teknisen vian sattuessa. Rekisterinpitäjän pitää myös kehittää menettely, jolla säännöllisesti testataan, tutkitaan ja arvioidaan teknisten ja organisatoristen toimenpiteiden tehokkuus varmistaakseen tietojenkäsittelyn turvallisuus.[107]

Tietosuoja-asetuksen myötä rekisterinpitäjän tulee ilmoittaa tietoturvaloukkauksista valvontaviranomaiselle mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta. Ilmoitus voidaan jättää toimittamatta, jos loukkaus ei todennäköisesti synnytä rekisteröityjen oikeuksiin kohdistuvia riskejä. Ilmoituksen viivästyessä määräajasta, tulee rekisterinpitäjän ilmoittaa valvontaviranomaiselle perusteltu syy. Käsittelevän tahon tulee toimittaa selvitys loukkauksista rekisterinpitäjälle. Selvityksen sisältöön kuuluu kuvaus loukkauksesta, rekisteröidyt ryhmät ja lukumäärä, tehdyt toimenpiteet, joita rekisterinpitäjä on ehdottanut tai toteuttanut loukkauksen johdosta ja toimenpiteet joilla haittavaikutuksia on pyritty vähentämään. Rekisterinpitäjän tulee dokumentoida kohtaamansa tietoturvaloukkaukset ja dokumentoinnin tulee sisältää toimenpiteet, jotka loukkauksen johdosta tehtiin ja minkälaisia vaikutuksia loukkaus aiheutti. Dokumentoinnilla viranomainen voi tarkistaa, että tietosuoja-asetusta on noudatettu.[108]

---

[105] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 24 & 25.
[106] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 30.
[107] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 32.
[108] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 33.

Rekisteröidyille tulee ilmoittaa tietoturvaloukkauksesta viipymättä, kun se aiheuttaa riskin heidän oikeuksilleen ja vapauksilleen. Rekisteröidyille ilmoitetaan samat tiedot kuin valvontaviranomaiselle. Loukkauksista ei tarvitse ilmoittaa rekisteröidyille, jos rekisterinpitäjän toimenpiteet ovat estäneet rekisteröityjen tunnistamisen tiedoista. Ilmoitusvelvollisuutta ei ole myöskään, jos riski on todennäköisesti kertaluontoinen tai ilmoittaminen aiheuttaa kohtuutonta vaivaa. Valvontaviranomainen päättää viime kädessä ilmoittamisesta rekisteröidyille, jos ilmoitusta ei vielä tehty.[109]

Henkilötietojen käsittelyyn liittyvä korkea riski velvoittaa rekisterinpitäjän tekemään arvioinnin käsittelytoimien vaikutuksista. Mahdollinen tietosuojavastaava ohjaa rekisterinpitäjää vaikutustenarvioinnin tekemisessä. Vaikutustenarvioinnin tekeminen on aiheellista varsinkin, kun päätöksiä tehdään automaattisen käsittelyn perusteella ja päätöksellä on oikeusvaikutuksia tai muita merkittäviä vaikutuksia rekisteröitäviin. Laajamittainen käsittely, erityisiin henkilötietoryhmiin kohdistuva käsittely ja rikkomuksiin liittyvät tiedot tarvitsevat usein vaikutustenarviointia. Yleistä yleisölle avointa aluetta järjestelmällisesti valvovan on myös tehtävä vaikutusten arviointi.[110]

Yrityksen kuitenkin käsitellessä arkaluonteisia henkilötietoja tulee tietojen käsittelyyn kiinnittä erityistä huomiota. Tällaisissa tilanteissa tietojenkäsittelyyn liittyy tavallista korkeampi riski, mutta korkea riski voi liittyä myös henkilötietojen suuren määrän käsittelyssä vaikka tiedot eivät olisikaan varsinaisesti arkaluonteisia. Rekisterinpitäjän toiminnan tulee olla todella huolellista ja toimenpiteiden määrä todennäköisesti suurempi, jos käsittelyyn liittyy suuri määrä henkilötietoja tai ne ovat erittäin arkaluonteisia.[111] Arkaluonteisten henkilötietojen käsittely on kielletty yleisesti henkilötietolain 11 § ja tietosuoja-asetuksessa 9 artiklan 1 kohdan mukaan, mutta poikkeukset on lueteltu 12 § ja 9 artiklan 2 kohdassa. Arkaluonteisiin tietoihin eli erityisiin henkilötietoryhmiin kuuluvat tiedot joista ilmenee etninen alkuperä, poliittiset mielipiteet, vakaumus, ammattiliiton jäsenyys, geneettisiä tai biometrisiä tietoja, terveystiedot tai seksuaalinen suuntautuminen.[112]

8 Henkilötietojen käsittelijän velvollisuudet

Henkilötietojen käsittelijälle tulee lisää vastuita tietosuoja-asetuksen myötä, kun aiemmin velvoitteet koostuivat lähinnä tietoturvaan liittyvistä edellytyksistä ja sopimusvelvoitteista. Henkilötietojen käsittelijän tulee huomioida tarkasti roolinsa rajat. Käsittelijä tulkitaan rekisterinpitäjäksi, jos se alkaa määritellä itsenäisesti tietojen käsittelyn tarkoituksia. Tällöin kä-

[109] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 34.
[110] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 35.
[111] Hanninen ym. 2017, 26-27.
[112] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 9.

sittelijä yritystä alkavat sitoa kaikki rekisterinpitäjille asetetut velvoitteet. Tämän lisäksi yritys on syyllistynyt tietojenkäsittelysopimuksen rikkomiseen, koska tietosuoja-asetuksen mukaan sopimuksessa tulee sopia käsittelijän suorittavan käsittelytoimia ainoastaa rekisterinpitäjän määrittelemin tarkoituksin ja keinoin.[113]

Rekisterinpitäjän ja henkilötietojen käsittelijän yhteistyön pohjana tulee toimia unionin oikeuden tai jäsenvaltion lainsäädännön mukainen sopimus tai oikeudellinen asiakirja. Sopimus sitoo käsittelijää suhteessa rekisterinpitäjään ja siinä vahvistetaan käsittelyn kohde, kesto, luonne ja tarkotus, henkilötietojen tyyppi ja rekisteröidyt ryhmät, rekisterinpitäjän velvollisuudet ja oikeudet.[114] Tietosuoja-asetus edellyttää tällaisen tietojenkäsittelysopimuksen laatimista, kun käsittelijä käsittelee henkilötietoja rekisterinpitäjän puolesta tai lukuun. Kirjallinen sopimus tietojenkäsittelystä voidaan toteuttaa yksittäisellä sopimuksella tai jo aiemmin tehdyn sopimuksen liitteenä.[115] Tällaisella sopimuksella säädetään siitä, että käsittelijä käsittelee henkilötietoja rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti, mikä koskee myös henkilötietojen siirtoa kolmansiin maihin tai kansainväliselle järjestölle, paitsi jos käsittelijään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä vaaditaan toisin. Kyseisessä tapauksessa käsittelijä ilmoittaa rekisterinpitäjälle oikeudellisesta vaatimuksesta ennen käsittelytoimien aloittamista, paitsi jos tiedottaminen on kielletty kyseisessä laissa yleiseen etuun vedoten.[116]

Sopimuksella varmistetaan, että henkilötietojen käsittelyyn oikeutetut henkilöt sitoutuvat noudattamaan salassapitovelvollisuutta tai heitä koskee lakisääteinen salassapitovelvollisuus. Henkilötietojen käsittelijän tulee myös toteuttaa artiklan 32 mukaiset toimenpiteet tietojen turvaamiseksi ja täyttää ilmoitusvelvollisuus rekisterinpitäjälle tietoturvaloukkauksesta. Huomioon ottaen käsittelytoimien luonteen tulee käsittelijän auttaa rekisterinpitäjää asianmukaisin toimenpitein täyttämään rekisterinpitäjää velvoittavat rekisteröidyn oikeuksiin liittyvät pyynnöt. Henkilötietojen käsittelijän tulee poistaa tiedot ja olemassa olevat jäljennökset ellei säilytystä lain mukaan vaadita tai palauttaa käsittely palvelun tarjoamisen päätyttyä kaikki henkilötiedot rekisterinpitäjälle. Käsittelijän tulee antaa rekisterinpitäjälle tarpeelliset tiedot velvollisuuksien noudattamisen osoittamiseksi ja sallii rekisterinpitäjän tai sen valtuuttaman tahon suorittamaan tarkastuksia asiaan liittyen sekä osallistuu tarkastuksiin.[117]

Henkilötietojen käsittelijä ei saa käyttää alihankkijaa henkilötietojen käsittelyssä ilman rekisterinpitäjän erityistä tai kirjallista lupaa. Alihankkijoita sitovat yhtälailla tietosuoja-

---

[113] Hanninen ym. 2017, 27.
[114] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 28.
[115] Hanninen ym. 2017, 82.
[116] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 28.
[117] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 28.

asetuksen mukaiset henkilötietojen käsittelijän velvollisuudet. Henkilötietojen käsittelijä vastaa alihankkijoiden toimista, jolloin sille on hyödyllistä siirtää omia vastuitaan vastaavat ehdot alihankkijoille alihankintasopimuksissa.[118]

Rekisterinpitäjän lisäksi henkilötietojen käsittelijän tulee toimia pyynnöstä yhteistyössä valvontaviranomaisen kanssa viranomaisen tehtävän suorittamiseksi. Tämän lisäksi käsittelijän tulee laatia seloste rekisterinpitäjän lukuun suoritettavista käsittelytoimista.[119] Selosteessa tulee kertoa henkilötietojen käsittelijän, tietosuojavastaavan ja rekisterinpitäjien yhteystiedot, käsittelytoimet, tietojen siirtäminen EU- ja ETA-alueen ulkopuolelle, suojatoimet siirtojen tapahtuessa ja yleinen kuvaus teknisistä ja organisatorisista turvatoimista. Sekä rekisterinpitäjän että käsittelijän selosteiden on oltava kirjallisessa ja sähköisessä muodossa. Ne on toimitettava pyydettäessä valvontaviranomaiselle. Henkilötietojen käsittelijän selosteen tekemättä jättämiseen liittyvät samat ehdot kuin rekisterinpitäjän käsittelyselosteeseen, joka kuvattuna rekisterinpitäjän velvollisuuksia käsittelevässä luvussa.[120]

9 Tietosuojavastaava

Tietosuoja-asetuksen 37 artiklan mukaan rekisterinpitäjän ja henkilötietojen käsittelijän tulee nimittää tietosuojavastaava aina kun tietojenkäsittelyä suorittaa jokin muu elin kuin lainkäyttötehtäviään suorittava tuomioistuin, rekisterinpitäjän tai käsittelijän ydintehtävät muodostuvat käsittelytoimista tai laajamittaisesta erityisten henkilötietoryhmien käsittelystä. Konsernin sisällä voidaan nimittää yksi tietosuojavastaava edellyttäen, että hänet voidaan helposti tavoittaa jokaisesta toimipaikasta. Tietosuojavastaavan nimittämisessä tulee ottaa huomioon valittavan henkilön ammattipätevyys, asiantuntemus tietosuojalainsäädännöstä ja kokemuksen tuoma valmius suoriutua tehtävästä. Tietosuojavastaava voidaan nimittää yrityksen sisältä tai ulkoinen tietosuojavastaava voi hoitaa tehtävää palvelusopimuksen perusteella.[121] Yrityksessä voidaan nimittää tietosuojavastaava, vaikka se ei olisi heidän toiminnassaan välttämätöntä tietosuoja-asetuksen mukaan. Vaikka tietosuojavastaava nimitettäisiin vapaaehtoisesti, koskee nimittämistä samat vaatimukset kuin pakon edessä tehdyssä nimityksessä.[122]

Rekisterinpitäjän ja henkilötietojen käsittelijän tulee varmistaa, että tietosuojavastaava osallistetaan asianmukaisesti ja ajoissa kaikkien henkilötietojen suojaa koskevien asioiden käsittelyyn. Tietosuojavastaavaa tulee myös tukea artiklan 39 mukaisten tehtävien suorittamisessa mahdollistamalla tietosuojavastaavalle tarpeelliset resurssit tehtävien täyttämiseen, asian-

[118] Hanninen ym. 2017, 27-28.
[119] Hanninen ym. 2017, 28.
[120] Hanninen ym. 2017, 127.
[121] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 37.
[122] Hanninen ym. 2017, 121.

tuntemuksen ylläpitoon sekä pääsyn henkilötietoihin ja käsittelytoimiin. Tietosuojavastaava toimii siinä määrin itsenäisesti, että hänen ei tule ottaa vastaan ohjeita tehtäviensä hoitamisen yhteydessä ja rekisterinpitäjän sekä käsittelijän tulee varmistaa tämä. Tietosuojavastaavaa ei saa erottaa tai rangaista tehtäviensä hoitamisen johdosta. Tietosuojavastaavan raportoi tehtäviinsä liittyvistä asioista suoraa työnantajansa ylimpään johtoon. Rekisteröidyillä on oikeus ottaa tietosuojavastaavaan kaikissa heidän henkilötietojensa käsittelyyn liittyvissä asioissa ja tietosuojavastaavaa sitoo salassapitovelvollisuus unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti. Tietosuojavastaava voi myös suorittaa muita tehtäviä, jotka eivät kuitenkaan saa aiheuttaa eturistiriitoja tietosuojavastaavan tehtävien suorittamiseen liittyen.[123] Nimitystä suunnitellessa kannattaa laatia selkeät säännöt, mitkä tehtävät yrityksessä tai sen ulkopuolella saattavat olla eturistiriidassa tietosuojavastaavan tehtävän kanssa. Tietosuojavastaava ei ole vastuussa yrityksen tietosuoja-asetuksen velvollisuuksien noudattamisesta, vaan vastuu kuuluu aina rekisterinpitäjälle ja käsittelijälle. Yrityksen johdon tulee varmistaa ja osoittaa, että yritys noudattaa tietosuoja-asetusta.[124]

Tietosuojavastaavan tehtäviin kuuluu antaa rekisterinpitäjälle tai käsittelijälle sekä henkilötietoja käsitteleville työntekijöille ohjeistusta asetuksen ja lainsäädännön mukaisista velvollisuuksista. Tietosuojavastaan tulee valvoa yrityksen asetuksen noudattamista, kouluttaa henkilöstöä ja tehdä yrityksen sisällä tarkastuksia tietosuojaan liittyen. Tämän lisäksi hän valvoo tietosuojan vaikutustenarvioinnin toteutusta ja neuvoo sen tekemisessä. Tietosuojavastaava toimii myös yhteistyö- ja yhteyshenkilönä valvontaviranomaiseen. Tehtävien suorittaminen vaatii käsittelytoimiin liittyvien riskien sekä käsittelyn luonteen, laajuden asiayhteyden ja tarkoitusten huomioimista.[125]

10 Käsittelyperusteet

Henkilötietojen käsittely on tietosuoja-asetuksen mukaan lainmukaista jos vähintään yksi asetuksessa mainituista lainmukaisen henkilötietojen käsittelyn perusteista täyttyy. Pienien ja keskisuurien yrityksien toiminnassa yleisiä käsittelyperusteita ovat suostumus, sopimus ja oikeutettu etu. Henkilötietojen käsittelyyn voi soveltua samanaikaisesti useampi lainmukaisen käsittelyn edellytys.[126] Tietosuoja-asetuksen käsittelyperusteita vastaavat käsittelyn yleiset edellytykset löytyvät pääosin myös henkilötietolain 8 §:stä.

[123] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 38.
[124] Hanninen ym. 2017, 123.
[125] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 39.
[126] Hanninen ym. 2017, 29.

Henkilötietolain 11 § mukaan arkaluonteisia tietoja ei pääsääntöisesti saa käsitellä ja poikkeuksista on säädetty 12 §. Tietosuoja-asetuksen mukaisten poikkeussäännösten lisäksi henkilötietolaissa perusteina olivat muun muassa käsittely historiallista tai tieteellistä tutkmusta varten, vakaumukseen liittyvät tiedot rekisteröidyn suostumuksella ja ammattiliittoon kuulumisen selvittäminen rekisterinpitäjän oikeuksiin vedoten. Tietosuoja-asetuksessa on säädetään erityisistä perusteista, jotka täyttämällä yrityksellä on mahdollisuus käsitellä arkaluonteisia tietoja. Erityiset perusteet ovat nimenomainen rekisteröidyn antama suostumus, työlainsäädännöllinen hyväksyntä sekä oikeusvaateen laatiminen, esittäminen tai puolustaminen. Tällaisten tietojen käsittelyn välttäminen on yritykselle suositeltavaa, jos se ei ole toiminnan kannalta välttämätöntä.[127] Arkaluonteisten tietojen käsittelyn asiayhteys voi aiheuttaa huomattavia riskejä yksilön perusoikeuksille ja vapauksille, jonka vuoksi tietojen suojelemisen tulee olla tarkkaa.[128]

10.1 Suostumus

Suostumuksen pitää olla vapaaehtoinen yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn. Rekisteröity antaa suostumuksen henkilötietojen käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten.[129] Suostumukseen liittyvät säännökset tietosuoja-asetuksessa eivät eroa juurikaan nykyisen sääntelyn mukaisesta suostumuksesta. Ennen tietosuoja-asetuksen soveltamista kerättyjä suostumuksia ei tarvitse uusia, jos annettu suostumus vastaa asetuksen kuvausta suostumuksen luonteesta. Rekisterinpitäjän tulee pystyä osoittamaan suostumuksen noudattavan tietosuoja-asetusta ja, että rekisteröity on antanut suostumuksen henkilötietojen käsittelyyn.[130]

Rekisteröidyn antaessa suostumuksensa kirjallisessa muitakin asioita koskevassa ilmoituksessa, tulee pyyntö suostumukselle esittää selvästi erillään muista asioista. Pyynnön tulee olla helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä kielellä. Jos suostumuspyyntö ei noudata tietosuoja-asetusta se ei ole yksilöä sitova.[131] Suostumuksen peruuttamiseen on oikeus milloin tahansa ja sen tulee olla yhtä helppoa kuin sen antaminen. Peruuttamisella ei ole vaikutuksia suostumuksen perusteella suoritetun käsittelyn lainmukaisuuteen ja rekisteröidylle tulee ilmoittaa tästä ennen suostumuksen antamista.[132]

Suostumuksen vapaaehtoisuutta arvioitaessa tulee ottaa huomioon palvelujen tarjoamisen tai sopimuksen täytäntöönpanon ehdoksi asetetun suostumuksen tarve henkilötietojen käsitte-

---

[127] Hanninen ym. 2017, 41.
[128] Euroopan parlamentin ja neuvoston asetus 2016/679 resitaali 51.
[129] Hanninen ym. 2017, 30.
[130] Hanninen ym. 2017, 35-36.
[131] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 7.
[132] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 7.

lyyn. Täytäntöönpanon kannalta tarpeettomia tietoja ei tule käsitellä.[133] Tietoinen tahdonilmaisu vaatii sen, että rekisteröity tietää vähintään henkilötietoja käsittelevän tahon ja mihin tarkoitukseen tietoja käsitellään sekä kuinka pitkälle menevä käsittely on kyseessä.[134]

Tietoyhteiskunnan palveluihin liittyvään lapsen suostumukseen sovellettavat ehdot eritellään tietosuoja-asetuksen 8. artiklassa. Nimenomaista suostumusta sovellettaessa katsotaan, että kun kyseessä on tietoyhteiskunnan palvelujen tarjoaminen välittömästi lapselle niin käsittely on lainmukaista lapsen ollessa vähintään 16 –vuotias. Alle 16 –vuotiaan lapsen on saatava vanhempainvastuunkantajaltaan suostumus tai valtuutus. Rekisterinpitäjän tulee toteuttaa kohtuulliset toimenpiteet varmistaakseen lapsen vanhempainvasatuunkantajan antama suostumus tai valtuutus, ottaen huomioon käytettävissä oleva teknologia. Jäsenvaltiot voivat lainsäädännössään säätää asetuksen ikärajaa alemmas, mutta minimi ikäraja on 13 vuotta.[135]

10.2 Sopimus

Henkilötietojen käsittely voi olla lainmukaista sopimuksen täytäntöönpanemiseksi, jossa rekisteröity on osapuolena tai sopimuksen tekemistä edeltävien toimenpiteiden totetuttamiseksi rekisteröidyn pyynnöstä.[136] Sopimuksen täytäntöönpanoon liittyvä henkilötietojen käsittely voi sisältää esimerkiksi rekisteröidyn osoitteen käsittelyn, jotta tilatut tuotteet voidaan toimittaa rekisteröidylle. Henkilötietojen käsittely sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä soveltuu tilanteeseen, jossa henkilö pyytää yritystä lähettämään tarjouksen palvelustaan tai tuotteesta. Tietojen käsittely on asianmukaisesti perusteltua esimerkiksi pyyntöä koskevien tietojen säilyttämiseksi tietyn ajan.[137]

WP29-tietosuojatyöryhmän mukaan henkilötietojen käsittely sopimuksen täytäntöön panemiseksi soveltuu myös työsuhteeseen. Työnantaja on rekisterinpitäjä, joka käsittelee rekisteröidyn henkilötietoja työsopimuksen täytäntöön panemiseksi. Tällä perusteella mahdollistetaan palkka- ja tilitietojen käsittely palkkojen maksamiseksi.[138] Työntekijöiden henkilötietojen käsittely teknisen valvonnan toteuttamiseksi ei liity työsopimukseen, mutta se kuuluu työnantajan muihin oikeuksiin ja velvoitteisiin, joten se ei perustu sopimukseen.[139]

---

[133] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 7.
[134] Hanninen ym. 2017, 36.
[135] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 8.
[136] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 6.
[137] Hanninen ym. 2017, 30.
[138] Hanninen ym. 2017, 30.
[139] 17/EN/WP 249 2017, 12-21.

10.3 Lakisääteinen velvoite

Henkilötietojen käsittely saattaa olla tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Esimerkiksi osakeyhtiöissä on osakeyhtiölain mukaan pidettävä osakasluetteloa, jolloin osakkaiden henkilötietojen käsittely on tarpeen lain asettaman velvoitteen perusteella. Lakisääteinen velvoite pätee myös työantajien velvollisuuteen ilmoittaa palkkatiedot sosiaaliturva- tai veroviranomaisille.[140]

10.4 Elintärkeä etu

Lainmukainen käsittely on mahdollista, jos käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi. Elintärkeän edun käsittelyperuste voi soveltua esimerkiksi lentoyhtiön tai matkayhtiön käsitellessä matkustajatietoja vaaratilanteiden tai epidemian hoitamiseksi.[141] Lähtökohtaisesti henkilötietoja tulee voida käsitellä ainoastaan toisen luonnollisen henkilön elintärkeän edun perusteella, jos käsittelyllä ei ole muuta ilmeistä käsittelyn oikeusperustetta.[142]

10.5 Yleinen etu

Yleinen etu tai julkisen vallan käyttö pätee tilanteissa, joissa henkilötietojen käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi.[143] TATTI –työryhmän mietinnössä todetaan, että yleisen edun oikeusperustetta tulee säätää varmistaen, ettei julkisen sektorin käsittelyn oikeusperusteen osalta jää kohtia ilman huomiota. Kyseisen oikeusperusteen nojalla mahdollistettaisin henkilötietojen käsittely viranomaisten suunnittelu- ja selvitystehtävissä ja tieteellisessä tutkimustarkoituksessa. Yleistä etua voidaan käyttää julkisen sektorin suorittaman käsittelyn oikeusperusteena.[144] Tietosuoja-asetuksen mukaiset rekisteröidyn oikeudet pätevät myös yleisen edun ja julkisen vallan käyttöön liittyvään käsittelyyn.[145]

10.6 Oikeutettu etu

Oikeutetun edun perusteella käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseen. Oikeutettu etu on olemassa esimerkiksi tilanteessa, jossa rekisteröidyn ja rekisterinpitäjän välillä on merkityksellinen ja asianmukainen suhde.[146]

---

[140] Hanninen ym. 2017, 31.
[141] Hanninen ym. 2017, 31.
[142] Euroopan parlamentin ja neuvoston asetus 2016/679 resitaali 46
[143] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 6.
[144] EU:n yleisen tietosuoja-asetuksen täytäntöönpanoryhmän (TATTI) mietintö 2017, 50.
[145] Hanninen ym. 2017, 31.
[146] Hanninen ym. 2017, 32.

Asiakassuhde ja työsuhde ovat hyviä esimerkkejä tilanteista, joissa yritykselle mahdollistetaan henkilötietojen käsittely oikeutetun edun perusteella. Asiakassuhde voi olla joko vastikkeellista tai vastikkeetonta tuotteen tai palvelun tarjoamista. Asiakaan tietoja käsitellään yleensä yrityksessä tuotteiden toimittamiseksi, asiakasviestinnässä tai palvelujen kohdentamisessa.[147] Laki yksityisyyden suojasta työelämässä (2004/759) säätää työntekijöiden henkilötietojen käsittelystä. Edellä mainitun lain 3 § mukaan työnantaja saa käsitellä vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja, jotka liittyvät työsuhteen osapuolten oikeuksien, velvollisuuksien, työsuhde etuuksien tai työtehtävien erityisluonteeseen. Tarpeellisuusvaatimuksesta ei voida siis poiketa työntekijän suostumuksellakaan.

Konsernin tai muiden taloudellisten yhteenliittymien asiakkaiden tai työntekijöiden henkilötietojen käsittely yhteenliittymän sisällä on erillinen käsittelyperuste henkilötietolain 8 § kohdassa 6. Tietosuoja-asetuksen mukaan konserniin kuuluvalla yrityksellä saattaa olla oikeutettu etu siirtää konsernin sisällä henkilötietoja hallinnollisista syistä. Muutos henkilötietolakiin on siinä, että yrityksen tulee harkita milloin henkilötietojen suojaa vaativat rekisteröidyn oikeudet syrjäyttävät sisäisistä hallinnollisista syistä johtuvat oikeutetut edut. Konsernille osoitettu oikeutettu etu ei vaikuta yleisperiaatteisiin, joita sovelletaan tietojen siirtämiseen EU:n ulkopuolelle.[148]

Yrityksen oikeutetusta edusta huolimatta henkilötietojen käsittelyä ei sallita, jos henkilötietojen suojaa edellyttävät rekisteröidyn edut syrjäyttävät oikeutetut edut. Rekisterinpitäjä on vastuussa oikeutetun edun ja rekisteröidyn oikeuksien vertailemisesta.[149] WP29 – tietosuojatyöryhmä on todennut, että oikeutettua etua ei tule käyttää käsittelyperusteena sellaiseen tietojenkäsittelyyn, johon ei voida soveltaa mitään muista käsittelyperusteista. Oikeutettuun etuun nojaaminen ei ole mahdollista jos tietoja kerätään sen perusteella useista eri lähteistä ja eri käyttötarkoituksiin.[150] Rekisteröidyn oikeudet voivat syrjäyttää yrityksen oikeutetun edun, kun henkilötietoja käsitellään olosuhteissa, joissa rekisteröity ei voi kohtuudella odottaa jatkokäsittelyä.[151]

Yrityksen ollessa epävarma oikeutetusta edustaan henkilötietojen käsittelyssä, kannattaa sen kuvata perustelut käsittelyperusteen tulkinnalle. Perustelu edistää myös osoitusvelvollisuuden täyttämistä, vaikka viime kädessä kiistatilanteessa valvontaviranomainen tai tuomioistuin ar-

[147] Hanninen ym. 2017, 33-34.
[148] Hanninen ym. 2017, 34.
[149] Hanninen ym. 2017, 33.
[150] 844/14/EN/WP 217 2014, 26.
[151] Hanninen ym. 2017, 33.

vioi käsittelyn lainmukaisuuden. Oikeutettu etu ei poista rekisteröidyn oikeutta vastustaa henkilötietojen käsittelyä.[152]

Tietosuoja-asetuksessa mainitaan erikseen, että henkilötietojen käsittely suoramarkkinointi tarkoituksiin voidaan laskea oikeutetun edun piiriin.[153] Suoramarkkinointi on jatkossakin mahdollista potentiaalisille asiakkaille, kunhan vastaanottajille kerrotaan mahdollisuudesta kieltäytyä suoramarkkinoinnista. Tämä liittyy käsittelyn vastustamisoikeuteen myös profiloinnin osalta, kun se liittyy suoramarkkinointiin. Tietosuoja-asetuksessa ei tule sähköisen suoramarkkinoinnin sääntelyyn muutoksia, mutta siihen sovelletaan tietosuoja-asetuksen säännöksiä.[154]

11 Vaikutustenarvioinnin tekeminen

Tietosuojaa koskeva vaikutustenarviointi (data protection impact assessment) on prosessi, jossa tarkastellaan suunniteltuja toimenpiteitä, suojatoimia ja mekanismeja tietosuojan toteuttamiseksi. Toimenpiteiden tarkoituksena on lieventää henkilötietojen käsittelyssä luonnollisten henkilöiden oikeuksiin kohdistuvia riskejä. Vaikutustenarvioinnilla kuvataan henkilötietojen käsittelyä ja arvioidaan käsittelyn tarpeellisuutta suhteessa riskeihin sekä varmistetaan käsittelyn tietosuoja-asetuksen mukaisuus. Vaikutustenarviointi tukee myös osoittamisvelvollisuuden käytännön noudattamista.[155]

Tietosuoja-asetuksen 35 artiklan mukaan valvontaviranomaisen tulee laatia ja julkaista luettelo käsittelytoimista, jotka vaativat vaikutustenarviointia tai päinvastoin eivät vaadi. Nämä luettelot tulee toimittaa 68 artiklan mukaiselle perustettavalle tietosuojaneuvostolle. Rekisterinpitäjien ja käsittelijöiden henkilötietojen käsittelyn käytännesääntöjen noudattamista arvioidaan erityisesti vaikutustenarvioinnin yhteydessä. Rekisterinpitäjän tulee tarvittaessa tarkastella uudestaa tehtyä arviointia, jos käsittelytoimien riski muuttuu.[156] Unionin oikeuden tai lainsäädännön ollessa henkilötietojen käsittelyn perusteena, ei ole tarpeellista tehdä vaikutustenarviointia. Kyseisen käsittelyn oikeusperusteen hyväksymisen yhteydessä on tehty yleinen vaikutustenarviointi, mutta jäsenvaltio voi katsoessaan tarpeelliseksi toteuttaa arvioinnin ennen käsittelytoimien aloittamista.[157]

Rekisterinpitäjän tulee ennen käsittelyn aloittamista ennakkoon kuulla valvontaviranomaista, jos vaikutustenarvioinnissa on todettu käsittelyn aiheuttavan korkean riskin ja rekisterinpitäjä

---

[152] Hanninen ym. 2017, 33.
[153] Euroopan parlamentin ja neuvoston asetus 2016/679 resitaali 47.
[154] Hanninen ym. 2017, 34-35.
[155] Hanninen ym. 2017, 115.
[156] Euroopan parlamentin ja neuvoston asetus 2016/679, artikla 35.
[157] Euroopan parlamentin ja neuvoston asetus 2016/679, artikla 35.

ei ole pystynyt puuttumaan riskeihin. Valvontaviranomaisen katsoessa käsittelyn rikkovan tietosuoja-asetusta ja rekisterinpitäjän laiminlyödessä riskin vähentämiseksi tehtäviä toimenpiteitä, tulee viranomaisen kahdeksan viikon kuluessa kuulemispyynnöstä antaa kirjalliset ohjeet rekisterinpitäjälle tai tapauksesta riippuen henkilötietojen käsittelijälle. Määräaikaa voidaan pidentää kuuteen viikkoon, jos suunniteltu käsittely on monimutkaisempaa. Määräajan jatkamisesta tulee ilmoittaa asianosaisille kuukauden kuluessa kuulemispyynnön vastaanottamisesta.[158]

Vaikutustenarviointi on tarpeellista etenkin automaattisen käsittelyn yhteydessä, jossa ihmisten henkilökohtaisia ominaisuuksia arvioidaan ja se johtaa ihmisiä koskeviin oikeusvaikutuksiin tai muihin merkittäviin vaikutuksiin. Edellä mainitut edellytykset täyttyvät luottopäätöksiä tehtäessä verkossa, henkilön taloudellisen profiloinnin perusteella tai yrityksen kerätessä laajamittaisesti sosiaalisen median profiileista henkilötietoja henkilörekistereihinsä. Myös esineiden internetin (Internet of Things) sovellukset aiheuttavat mahdollisesti korkean riskin henkilöiden oikeuksille ja sovelluksia tarjoavien yrityksien tulee tällöin tehdä vaikutustenarviointi.[159] Vaikutustenarviointia vaaditaan myös käsiteltäessä arkaluonteisia henkilötietoja laajamittaisesti. Arkaluonteisina henkilötietoina voidaan tietosuoja-asetuksen määritelmää laajemmin pitää sähköisen kommunikaation sisältöä, sijaintitietoja ja taloudellisia tietoja.[160]

Suomessa ei ole ollut käytössä ennakkotarkastusmenettelyä vaikutustenarvioinnin tekemisestä, mutta voidaan tulkita, että sitä ei tarvitse tehdä ainakaan, jos käsittelyyn on saatu tietosuojalautakunnan lupa tai henkilötietojen käsittely on henkilötietolakia noudattaessa vaatinut ilmoituksen tietosuojavaltuutetulle. Tämä vaatii sen, että ilmoitus on tehty asianmukaisesti, eivätkä riskit ja käytetty teknologia ole muuttuneet. Jos aikaisemmin ilmoituksen tekemistä tietosuojavaltuutetulle ei ole velvoitettu ja henkilötietojen käsittelyyn arvioidaan tietosuoja-asetuksen tarkoittama korkea riski, tulee käynnissä olevista käsittelytoimista tehdä vaikutustenarviointi. Vaikutustenarviointi tulee tehdä joka tapauksessa, jos henkilötietojen käsittelytoimiin tulee muutoksia esimerkiksi tietojenkäsittelyteknologiaan tai käsittelyn tarkoitus muuttuu ja käsittelyyn arvioidaan korkea riski.[161]

Vaikutustenarvioinnin tekemättä jättäminen saattaa johtaa valvontaviranomaisen määräämään huomattavaan sakkoon. Jos vaikutustenarvioinnin tekemisestä ollaan epävarmoja, on suositeltavaa tehdä se joka tapauksessa tai ainakin dokumentoida syyt, joiden perusteella

---

[158] Euroopan parlamentin ja neuvoston asetus 2016/679, artikla 36.
[159] Hanninen ym. 2017, 115-116.
[160] 17/EN/WP 248 2017, 7-9.
[161] Hanninen ym. 2017, 116-117.

vaikutustenarviointi jätettiin tekemättä. Epäselvissä tapauksissa vaikutustenarvioinnin tekeminen auttaa rekisterinpitäjää noudattamaan tietosuojalainsäädäntöä.[162]

Vaikutustenarviointi tulisi tehdä ennen henkilötietojen käsittelyn aloittamista, vaikka osa käsittelytoimista olisi vielä tuntemattomia. Sitä voidaan pitää jatkuvana prosessina, joka päivittyy käsittelytoimiin tulevien muutosten yhteydessä ja sillä varmistetaan tietosuojan sekä yksityisyyden huomiointi. Vaikutustenarviointi edistää myös sellaisten ratkaisujen luomista, jotka edistävät asetuksen säädösten noudattamista. Voi olla tarpeellista käydä uudelleen läpi arvioinnin vaiheita, kun kehitystoimenpiteitä tehdään ja tekniset sekä organisatoriset toiminnot saattavat vaikuttaa käsittelyn aiheuttamiin riskeihin.[163]

Rekisterinpitäjä on päävastuussa vaikutustenarvioinnin tekemisestä, mutta yrityksen tietosuojavastaava tukee rekisterinpitäjää vaikutustenarvioinnissa. Tietosuojavastaavan tulee myös arvioida vaikutustenarvioinnin suorittamista ja toimintaa. Käsittelyn tapahtuessa täysin henkilötietojen käsittelijän toimesta, tulee käsittelijän avustaa rekisterinpitäjää vaikutustenarvioinnin tekemisessä ja antaa tarpeellinen informaation se tekemiseen.[164]

12 Tyypillistä henkilötietojen käsittelyä yrityksessä

Yrityksessä voidaan käsitellä erilaisten ryhmien henkilötietoja kuten asiakkaiden, henkilöstön ja yhteistyökumppanien tietoja. Lainmukaisen henkilötietojen käsittelyn lähtökohtana on, että työnantaja on perillä siitä, mitä henkilötietoja työpaikalla käsitellään ja lain mukaan saadaan käsitellä. Työnantajan tulee tietää nämä asiat, jotta voidaan todeta huolellisuusvelvoitteen täyttyneen.[165]

Työnantajan tulee työnhakijoiden ja työntekijöiden henkilötietoja kerätessään varmistaa tietojen tarpeellisuus ja ajantasaisuus. Työsuhteen kannalta tarpeettomien tietojen kerääminen on laissa kiellettyä. Työntekijän tiedot voidaan hankkia muiltakin tahoilta hänen suostumuksellaan tai pyynnöstä, mutta pääsääntönä on saada ne suoraa työntekijältä itseltään. Arkaluonteisten tietojen keräämiselle annetaan laissa mahdollisuus tietyissä tapauksissa ja usein niiden kerääminen on työsuhteessa tarpeellista. Arkaluonteisiin tietoihin luetaan muun muassa terveydentilaa ja ammattiliiton jäsenyyttä koskevat tiedot.[166]

Yleisesti ottaen työnantajan oikeus käsitellä työntekijän henkilötietoja perustuu osapuolten väliseen palvelussuhteeseen eli myös virkasuhteeseen. Työntekijöiden henkilötietoja käsitel-

[162] Hanninen ym. 2017, 117.
[163] 17/EN/WP 248 2017, 13.
[164] 17/EN/WP 248 2017, 13.
[165] Nyyssölä 2014, 41.
[166] Nyyssölä 2014, 48.

lään usein myös työpaikan ulkopuolella esimerkiksi palkkakirjanpidon ulkoistamistilanteissa, joka perustuu työnantajan toimeksiantosopimukseen. Ulkoisella käsittelijällä ei ole itsenäistä oikeutta käsitellä tietoja, vaan oikeus perustuu aina työnantajan oikeuteen ja toimeksiantosopimukseen.[167] Vaikka yritys ulkoistaisi palkkakirjanpidon, niin työnantajayrityksenä kuin rekisterinpitäjänä, se on edelleen vastuussa henkilötietojen käsittelystä. Rekisterinpitäjä yrityksen tulee varmistaa henkilötietoja käsittelevän kolmannen osapuolen täyttävän tietosuoja-asetuksen asettamat vaatimukset, joka toteutetaan yleensä toimeksiantosopimuksen yhteydessä.

Työntekijän arkaluonteisten henkilötietojen käsittelyä määritellään laissa yksityisyyden suojasta työelämässä (759/2004). Lain 2 luku käsittelee työntekijän henkilötietojen käsittelyn yleisiä edellytyksiä. Edellä mainitun lain 5 § erityissäännös mahdollistaa työnantajalle työntekijän terveydentilatietojen käsittelyn, tilanteissa joissa määritellyt tiedot saadaan työntekijältä itseltään tai hänen kirjallisen suostumuksensa turvin muualta. Edellämainitut ovat terveydentilatietojen käsittelyn muodollisia edellytyksiä. Tämän lisäksi tietojen käsittelylle tulee säädöksen mukaan olla erityinen aineelliseksi edellytykseksi luokiteltava syy, kuten sairausajan palkka tai vastaavan etuuden suorittaminen, poissaolon perustellun syyn selvittäminen tai työntekijän nimenomainen halu selvittää työkykynsä terveydentilatietojen perusteella.

Työntekijän luottotietojen saamiseen työnantajalla on oikeus ainoastaan poikkeustapauksissa. Luottotietojen hankkimisen edellytyksenä on, että henkilö palkataan erityistä luottamusta vaativaan tehtävään. Henkilöluottotietojen kerääminen vaatii tämän lisäksi yhden seuraavista edellytyksistä täyttyväksi: päätäntävalta merkittävistä taloudellisista sitoumuksista, luottojen myöntäminen ja valvonta, liike- ja ammattisalaisuudet, laajat tietojärjestelmien käyttöoikeudet, merkittävän raha- tai omaisuusmassan käsittely, omaisuuden vartiointi tai valvomaton työskentely yksityiskodissa. Työnantaja voi pyytää työntekijältä rikosrekisteriotetta työn liittyessä alaikäisten kasvatukseen, opetukseen tai hoitoon. Lisäedellytyksenä työsuhteen tulee kestää vuoden aikana vähintään kolme kuukautta. Rikosrekisteriote tulee työnantajalle vain nähtäväksi, eikä sitä saa tallettaa tai kopioida omaan käyttöön.[168]

Työsopimuslaki (2001/55) määrittelee työtodistusta koskevassa 6 luvun 7 §, että työsuhteen päättyessä työntekijällä on oikeus saada pyytäessään työnantajalta kirjallinen todistus työsuhteen kestosta ja työtehtävien laadusta. Työntekijän pyynnöstä todistuksessa tulee lisäksi mainita työsuhteen päättymisen syy sekä arviointi työntekijän suoriutumisesta työtehtävissään. Työnantajalla on velvollisuus toimittaa työtodistus työntekijälle, jos sitä pyydetään 10

[167] Nyyssölä 2014, 50.
[168] Mattinen, Orlando & Parnila 2017, 302-303.

vuoden kuluessa työsuhteen päättymisestä. Arvioinnilla varustetun työtodistuksen saamiseksi tulee pyyntö toimittaa 5 vuoden kuluessa työsuhteen päättymisestä. Työtodistus työsuhteen kestolla ja työtehtävillä tulee toimittaa myös 10 vuoden jälkeen, jos siitä ei aiheudu työnantajalle kohtuutonta haittaa. Samoin edellytyksin työnantajalla on velvollisuus antaa uusi todistus kadonneen tai turmeltuneen työstodistuksen tilalle.

Asiakkaiden kohdalla henkilötietojen kerääminen mahdollistaa yritykselle kuluttajien ostoskäyttäytymisen analysoinnin, tuotteiden kohdennetun markkinoinnin ja kaupallistamisen. Tietoja keräämällä yritys voi säästää markkinointikustannuksissaan ja kohdentaa markkinointia oikeille kohderyhmille ja parantaa tarjoamiaan palveluita asiakaspreferenssien avulla. Yrityksien teknisten mahdollisuuksien ja tietosuojasääntelyn kehittyminen johtaa tasapainotteluun edistyksellisen datan hyödyntämisen ja lainsäädännön määrittämien reunaehtojen välillä. Dataa saa ja kannattaa hyödyntää kuin ennen tietosuoja-asetusta, mutta yrityksen tulee ottaa huomioon lainmukaisen käsittelyn vaatimukset.[169]

13 Lainvalmistelu tietosuoja-asetuksessa

Nyky-yhteiskunnassa haasteina tietosuojalle pidetään teknologian nopeaa kehittymistä ja globalisaation myötä henkilötietojen keräämisen, käyttävien tahojen, käytön ja siirtojen jatkuvasti kasvavaa määrää. Sosiaalisen median mahdollistamat uudet tavat jakaa tietoa ja jatkuvasti kasvavien tietomäärien varastointi on tullut osaksi elämää suurelle osalle Euroopan internetin käyttäjistä. Asiakkaiden tietojen kerääminen, ryhmittely ja analysointi on usein tärkeä osa yritysten taloudellisen toiminnan ylläpitämistä.[170]

Komissio antoi vuonna 2012 ehdotuksen uudesta tietosuoja-asetuksesta ja tietosuojadirektiivistä. Ehdotuksessa huomioitiin aiemmassa tietosuojalainsäädännön kehysehdotuksessa esiin tulleita ongelmia ja kehityskohteita.[171] Ehdotusta tietosuoja-asetukseksi tarkastellessa tulee ottaa huomioon, että se ei täysin vastaa lopullisessa muodossa olevaa tietosuoja-asetusta (2016/679). Rakenne on muuttunut lainvalmisteluprosessin aikana ja luetellut artiklat ehdotuksesta tässä kappaleessa eivät välttämättä vastaa tietosuoja-asetuksen vastaavia. Esimerkiksi ehdotuksessa valvontaviranomaisten tehtäviä käsittelee 52 artikla ja tietosuoja-asetuksessa se on muuttunut 57 artiklaksi.[172]

Tietosuojadirektiivissä (95/46/EC) yksilöiden mahdollisuudet toteuttaa oikeuksiaan tietosuojan saralla eivät ole olleet täysin yhtenäiset jäsenvaltioiden välillä. Sama pätee myös kansal-

---

[169] Honkinen, Innanen, Lindgren, Pello, Rantanen, Siltala & Tuomala 2016, 138.
[170] COM(2012) 9 final, 2.
[171] COM(2012) 11 final, 1.
[172] Euroopan parlamentin ja neuvoston asetus 2016/679 artikla 57 & COM(2012) 11 final, 77.

listen valvontaviranomaisten mahdollisuksiin taata johdonmukaisuutta ja tehokkuutta säännösten soveltamisessa.[173] Tietosuoja-asetusta silmälläpitäen komissio ilmoitti kehityskohteiksi etenkin yksilöiden mahdollisuudet hallita henkilötietojensa käsittelyä, lainsäädännön suomien oikeuksien käyttämiseen, yleisen tietoturvan vahvistamisen ja henkilötietoja käsittelevien tahojen vastuullisuuden parantamisen. Yksilön henkilötietojen hallinnassa haluttiin kehitystä suostumuksen määrittelyyn, oikeuteen tulla unohdetuksi, rekisteröidyn pääsyyn omiin tietoihin ja niiden siirtämiseen sekä rekisterinpitäjän informaatiovelvollisuuteen. Suostumuksen osalta haluttiin muutta sen määritelmää siten, että sen on oltava vapaaehtoinen ja se on annettava joko nimenomaisella tahdonilmaisulla tai selkeällä myöntävällä toimella asiaa koskettavan yksilön toimesta. Oikeus tulla unohdetuksi tulee toteutua aina jos suostumus poistuu tai jos henkilötietojen säilyttämiselle ei ole muita lain asettamia perusteita. Yksilön pääsy tietoihin ja niiden siirto toiseen järjestelmään tulee taata. Rekisterinpitäjän informointivelvollisuus parantaa rekisteröityjen ymmärrystä siitä, miten heidän henkilötietojaan käsitellään, etenkin lapsia koskevassa käsittelytoiminnassa.[174]

Rekisteröidyn oikeuksien käyttämisen kehittämisessä keskityttiin kansallisten tietosuojaviranomaisten itsenäisyyteen ja vallankäyttöön sekä hallinnollisten- ja oikeussuojakeinojen parantamiseen. Tietosuojaviranomaisilla tulee olla tarvittavat resurssit hoitaa tehokkaasti valituksia, tutkintatoimenpiteitä ja mahdollisuudet sitoviin päätöksiin sekä määräysvalta antaa tehokkaita ja varoittavia sanktioita. Hallinnollisten- ja oikeussuojakeinojen käyttöä tulee vahvistaa tietosuoja lainsäädännön vaatimuksia rikottaessa. Tämä tulee ilmetä etenkin siinä, että pätevät tahot voivat toimia oikeudessa yksilön puolesta. Tietoturvan vahvistamisella pyritään rohkaisemaan yksityisyyttä vahvistavien teknologiaratkaisuiden, toiminnassa yksityisyyttä tukevien yleisasetusten ja yksityisyyden sertifiointijärjestelmien käyttöä. Tämän lisäksi rekisterinpitäjillä on velvollisuus ilmoittaa tietovuodoista asianosaisille ilman aiheetonta viivytystä ja tietosuojaviranomaisille 72 tunnin sisällä.[175]

Ehdotuksessa tietosuoja-asetukseksi oikeuksia käsiteltiin kolmannessa kappaleessa jaoteltuna viiteen osioon. Ensimmäinen osio käsitteli läpinäkyvyyttä. Artiklaan 11 ehdotettiin rekisterinpitäjän tietojen tarjoamisvelvollisuutta helposti saataville ja ymmärrettävään muotoon. Artiklan 12 sisällöksi ehdotettiin rekisterinpitäjän velvollisuutta mahdollistaa rekisteröidyille heidän oikeuksiensa käyttö ja niihin liittyviin pyyntöihin sovellettava asetuksen määrittelemä vastausaika. Artikla 13 käsittelee oikeuksia suhteessa tietojen vastaanottajiin eli myös yhteisrekisterinpitäjiin ja henkilötietojen käsittelijöihin.

---

[173] COM(2012) 9 final, 4.
[174] COM(2012) 9 final, 6-7.
[175] COM(2012) 9 final, 6.

Toisessa osiossa käsiteltiin tietojen tarjoamista ja rekisteröidyn pääsyä tietoihin. Artikla 14 määrittelee tarkemmin rekisterinpitäjän velvollisuuksia liittyen henkilötietojen käsittelyä koskevien tietojen tarjoamiseen rekisteröidylle, kuten säilytysajat ja valitusmahdollisuus tietojensiirtoon kansainvälisesti. Valitusvelvollisuutta käsittelyyn voidaan kuitenkin rajoittaa jos rekisterinpitäjällä on lainmukainen velvoite toteuttaa käsittelyä. Artikla 14 rakentuu tietosuojadirektiivin (95/46/EC) artiklojen 10 ja 11 pohjalle. Artikla 15, joka on muodostettu aiemman tietosuojadirektiivin artiklan 12 a kohdan perusteella, tarjoaa rekisteröidylle oikeuden päästä hänestä kerättyihin henkilötietoihin ja tuo muutoksia, kuten rekisterinpitäjän velvollisuus ilmoittaa tietojen säilytysajat ja oikeudet tietojen oikaisuun, poistamiseen ja valituksen tekemiseen.[176]

Kolmas osio täsmentää oikaisuoikeutta ja tietojen poistamista. Artikla 16 määrittää oikeuden tietojen oikaisuun, joka pohjautuu aiemman tietosuojadirektiivin artiklan 12 b kohtaan. Artikla 17 mahdollistaa rekisteröidylle oikeuden tulla unohdetuksi ja poistaa hänestä kerättyjä tietoja. Rekisterinpitäjällä on tämän myötä myös velvollisuus ilmoittaa muille henkilötietojen käsittelyyn osallistuville tahoille tietojen poistamisesta, oikaisusta tai rajoittamisesta. Artiklaan 18 tulee uusi rekisteröidyn oikeus tietojen siirtämiseen järjestelmästä toiseen. Tämä on mahdollista käsittelyn tapahtuessa sähköisessä järjestelmässä, jolloin rekisterinpitäjän tulee toimittaa tiedot yleisesti käytetyssä sähköisessä muodossa.[177]

Osiossa neljä käsitellään vastustusoikeutta ja profilointia. Artikla 19 mahdollistaa rekisteröidylle oikeuden vastustaa henkilötietojen käsittelyä. Se perustuu tietosuojadirektiivin artiklaan 14. Muutoksina tulee rekisterinpitäjän velvollisuus todistaa vastustusoikeuden toteutuminen ja itse vastustamisen vaikutus suoramarkkinointiin. Artikla 20 käsittää rekisteröidyn oikeuden olla joutumatta automaattisen käsittelyn kohteeksi. Se rakentuu tietosuojadirektiivin 15 artiklan 1 kohdan pohjalle muutoksin ja lisättyjen turvatoimien myötä.[178]

Osuudessa 5 käsitellään rajoituksia. Artikla 21 tarkentaa Euroopan unionin ja sen jäsenvaltioiden valtaa ylläpitää ja esitellä rajoituksia 5 artiklassa esiin tuleviin henkilötietojen käsittelyn periaatteisiin ja 11-20 artikloissa sekä artiklassa 32 oleviin rekisteöidyn oikeuksiin. Tämä pohjautuu tietosuojadirektiivin artiklaan 13.[179]

Henkilötietoja käsittelevien tahojen vastuullisuutta pyritään vahvistamaan tietyissä tapauksissa tietosuojavastaavan nimittämisvelvollisuudella, uudella sisäänrakennetun tietosuojan periaatteella ja uudella velvollisuudella tehdä tietosuojan vaikutustenarviointi riskialttiin henkilö-

[176] COM(2012) 11 final, 8-9.
[177] COM(2012) 11 final, 9.
[178] COM(2012) 11 final, 9.
[179] COM(2012) 11 final, 9.

tietojen käsittelyn yhteydessä. Tietosuojavastaavan nimittämisvelvollisuus koskee yli 250 henkilöä työllistäviä yrityksiä sekä yrityksiä joissa käsitellään suuria määriä tai arkaluontoisia henkilötietoja. Sisäänrakennettu tietosuoja viittaa siihen, että tietosuoja otetaan huomioon kaikessa liiketoiminta koskevassa suunnittelussa.[180]

Ehdotuksen kappaleessa 4 käsitellään rekisterinpitäjän ja käsittelijöiden vastuuta. Osuudessa yksi käsitellään artikloja 22-29. Artiklassa 22 otetaan kantaa rekisterinpitäjän osoitusvelvollisuuteen asetuksen noudattamisessa yrityksen sisäisten ohjeistusten ja toimintojen kautta. Artikla 23 käsittelee sisäänrakennettua tietosuojaa kaikessa toiminnassa. Artiklassa 24 tarkennetaan yhteisrekisterinpitäjien velvollisuuksia suhteessa rekisteröityyn. Artikla 25 asettaa vaatimuksia tietyissä tapauksissa Euroopan ulkopuolella toimiviin rekisterinpitäjille, kun asetusta voidaan soveltaa heidän toteuttamaanssa henkilötietojen käsittelyyn. Artiklassa 26 käydään läpi käsittelijän asemaa ja velvollisuuksia, perustuen tietosuojadirektiivin 17 artiklan 2 kohtaan. Muutoksia tulee esimerkiksi siihen, että milloin henkilötietoja käsittelevä taho määritellään yhteisrekisterinpitäjäksi. Artiklassa 27 määritellään rekisterinpitäjän ja henkilötietojen käsittelijän suhdetta, pohjautuen tietosuojadirektiivin artiklaan 16. Artikla 28 tuo rekisterinpitäjille ja käsittelijöille velvollisuuden ylläpitää dokumentaatiota käsittelytoimistaan, sen sijaan että niistä tehtäisiin yleinen ilmoitus valvontaviranomaisille, kuten tietosuojadirektiivin 18 artiklan 1 kohdassa ja 19 artiklassa on aiemmin määritelty. 29 artikla tarkentaa yhteistoimintaa valvontaviranomaisten ja rekisterinpitäjän sekä käsittelijöiden välillä.[181]

Neljännen kappaleen osiossa 2 käsitellään tietoturvaa. Artikla 30 velvoittaa rekisterinpitäjän ja käsittelijän tekemään tarvittavat toimet turvatakseen henkilötietojen käsittelyn, kohdentaen velvollisuuden noudattamisen rekisterinpitäjän varmistettavaksi tietosuojadirektiivin 17 artiklan 1 kohtaa täten muuttaen. Artikla 31 ja 32 velvoittaa ilmoittamaan tietosuojaloukkauksista, perustuen sähköisen viestinnän tietosuojadirektiivin (2002/58/EC) 4 artiklan 3 kohtaan.

Neljännen kappaleen osio 3 käsittelee vaikutustenarvioinnin tekemistä ja tähän liittyvään käsittelyyn vaadittavaa ennakkolupaa. Artikla 33 tuo rekisterinpitäjille ja käsittelijöille velvoitteen tehdä vaikutustenarviointi riskialttiille käsittelytoimille. Artikla 34 käsittelee tapauksia, jossa vaaditaan ennakkolupaa valvontaviranomaisilta henkilötietojen käsittelylle, perustuen tietosuojadirektiivin artiklaan 20.

Osiossa 4 määritellään vaatimus nimittää tietosuojavastaava. Artiklaan 35 tulee uusi velvoite tietosuojavastaavan nimittämiselle julkisella sektorilla ja yksityisellä sektorilla, jos kyseessä

---

[180] COM(2012) 9 final, 6-7.
[181] COM(2012) 11 final, 10.

on suuri yritys, jonka ydintoimintaan kuuluvaan henkilötietojen käsittelyyn liittyy säännöllistä ja systemaattista valvontaa. Tämä perustuu tietosuojadirektiivin 18 artiklan 2 kohtaan, jossa mahdollistettiin jäsenvaltioille soveltaa tätä velvoitetta yleisen ilmoitusvelvollisuuden sijaan. Artikloissa 36 ja 37 määritellään tietosuojavastaavan roolia ja ydintehtäviä.[182]

Osuudessa 5 käsitellään käytännesääntöjä ja sertifiointia. Artikla 38 käsittelee käytännesääntöjä, jotka rakentuvat tietosuojadirektiivin 27 artiklan 1 kohdassa olleelle periaatteelle, jossa tarkennetaan sääntöjä, menettelyitä ja valtuuksia komissiolle päättää käytännesääntöjen pätevyydestä. Artikla 39 tuo mahdollisuuden asettaa saataville sertifiointijärjestelmiä ja muita vastaavia merkintöjä toimijoille tietosuojaan liittyen.[183]

Tietosuojadirektiivin ongelmana pidetään sitä, että kaikissa jäsenvaltioissa oli erilainen tietosuojalainsäädäntö ja vaatimukset. Oikeudellinen ympäristö unionin sisällä oli pirstaloitunut ja se aiheutti oikeudellista epävarmuutta sekä eroja tietosuojan tasossa eri jäsenmaiden kansalaisten välillä.[184] Ongelmien tiedostamisen johdosta uudistuksessa haluttiin tehdä Euroopan unionista yhtenäismarkkina ainakin tietosuojan osalta ja sillä tavoin helpottaa yritysten liiketoiminnan levittäytymistä unionin sisällä. Kaikissa unionin jäsenvaltioissa otetaan käyttöön suoraan sovellettava tietosuoja-asetus. Asetuksen avulla yksinkertaistetaan sääntelyä vähentämällä byrokratiaa ja poistamalla muodollisuuksia, kuten yleiset ilmoitusvaatimukset. Tällä säästetään hallinnollisten rasitteiden osalta 130 miljoonaa euroa vuodessa. Erityisesti otetaan huomioon mikro-, pien- ja keskisuurten yritysten tarpeet, ottaen huomioon niiden merkityksen Euroopan talousympäristön kilpailukyvyn kannalta.[185]

Tietosuojaviranomaisten itsenäisyyttä ja toiminta valtuuksia kansallisen tietosuojan saralla haluttiin parantaa, jotta ne kykenevät tekemään tutkintaa, sitovia päätöksiä ja määrätä tehokkaita sekä varoittavia seuraamuksia. Samalla jäsenvaltioilta edellytetään mahdollistamaan tietosuojaviranomaisille tarpeelliset resurssit tehtäviensä suorittamiseen. Tietosuojalle EU:ssa perustetaan yhden luukun järjestelmä eli rekisterinpitäjien tarvitsee olla yhteydessä ainoastaan yhteen tietosuojaviranomaiseen unionin sisällä eli siinä jäsenvaltiossa, jossa yrityksen päätoimipaikka sijaitsee. Tietosuojaviranomaisille luodaan ympäristö, jossa ne voivat toimia yhteistyössä nopeasti ja tehokkaasti, mukaan lukien tietosuojaviranomaisten velvollisuus suorittaa tutkimuksia ja tarkastuksia toisen jäsenvaltion viranomaisen pyynnöstä ja tunnustaa yhteisymmärryksessä toistensa päätökset. Tietosuojaviranomaisille mahdollistetaan johdonmukaisuusmekanismi unionin tasolla, jotta voidaan varmistaa Euroopassa laajalla alalla vaikuttavien tietosuojaviranomaispäätösten kohtaaminen muiden asianosaisten tietosuojaviran-

[182] COM(2012) 11 final, 11.
[183] COM(2012) 11 final, 11.
[184] COM(2012) 9 final, 7.
[185] COM(2012) 9 final, 8.

omaisten kannan kanssa ja niiden lainmukaisuus EU-oikeudessa. Artiklan 29 tietosuojatyöryhmä nostetaan itsenäiseksi Euroopan tietosuoja lautakunnaksi parantaen sen panosta tietosuojalainsäädännön yhtenäisessä soveltamisessa ja luomalla vahvan perustan tietosuojaviranomaisten yhteistyölle.[186]

Tietosuoja-asetus ehdotuksessa viranomaisten itsenäisyyttä käsiteltiin kappaleessa 6 artiklojen 46-54 osalta. Osuudessa 1 artiklan 46 mukaan jäsenvaltioiden tulee nimittää valvontaviranomaiset, perustuen tietosuojadirektiivin 28 artiklan 1 kohtaan ja kasvattaa valvontaviranomaisten yhteistyötä unionin sisällä sekä komission kanssa. Artiklat 47 ja 48 tarkentavat valvontaviranomaisten itsenäisyyttä mahdollistaen oikeuskäytännön soveltamisen Euroopan unionin tuomioistuimessa. Artiklassa 49 määritellään säännöt valvontaviranomaisen nimittämiseen liittyen. Artiklassa 50 määrätään salassapitovelvollisuudesta valvontaviranomaisessa työskenteleville, joka perustuu tietosuojadirektiivin 28 artiklan 7 kohtaan.[187]

Osuudessa 2 määritellään valvontaviranomaisten velvollisuuksia ja valtuuksia. Artiklalla 51 määritellään valvontaviranomaista ja sen vastuuta yrityksistä, jotka toimivat hänen edustamassaan jäsenvaltiossa. Jäsenvaltioissa tulee varmistaa yhdenmukainen tietosuoja-asetuksen soveltaminen. Oikeusistuimet ovat vapautettuja valvontaviranomaisen valvonnasta, mutta eivät tietosuojaa koskevan lainsäädännön noudattamisesta. Artikla 52 säätää tietosuojaviranomaisten tehtävistä, kuten tutkinnan toteuttaminen ja valitusten käsittely sekä tietoisuuden lisääminen riskeistä, säännöistä, suojatoimista ja oikeuksista liittyen tietosuojaan. Artikla 53 tarjoaa valvontaviranomaisille uusia valtuuksia, kuten valta antaa hallinnollisia rangaistuksia sakkojen muodossa. Artikla 54 velvoittaa valvontaviranomaiset laatimaan vuosikertomuksia, jotka perustuvat tietosuojadirektiivin 28 artiklan 5 kohtaan.[188]

Tärkeäksi asiaksi muodostui myös se, että yksilön oikeuksien tulee päteä tietosuojan osalta myös tietojen siirtyessä esimerkiksi palveluntarjoajille EU:n ulkopuolelle. Tietosuoja-asetuksen vaatimusten tulee päteä siis siitä huolimatta missä unionin kansalaisen henkilötietoja käsitellään.[189] Uudistuksen tarkoituksena on rakentaa moderni, vahva, johdonmukainen ja kattava runko tietosuojalle Euroopan unionissa. Yksilöiden tietosuojan perusoikeuksia vahvistetaan, mutta muita oikeuksia kuten sananvapautta, lapsen oikeutta, oikeutta harjoittaa liiketoimintaa, oikeutta reiluun oikeudenkäyntiin ja salassapitovelvollisuutta jäsenvaltioiden kansallisessa lainsäädännössä kunnioitetaan edelleen. Uudistuksessa pyritään vahvistamaan

---

[186] COM(2012) 9 final, 8-9.
[187] COM(2012) 11 final, 12.
[188] COM(2012) 11 final, 12-13.
[189] COM(2012) 9 final, 10.

yksilöiden tietosuojaan liittyviä oikeuksia ja luottamusta digitaaliseen ympäristöön. Yrityksille ja julkiselle sektorille hyötynä on oikeudellisen ympäristön yksinkertaistaminen.[190]

14 Johtopäätökset

Suomessa henkilötietolaki on sisältänyt osan tietosuoja-asetuksessa määritellyistä rekisterinpitäjän velvollisuuksista, kuten huolellisuusvelvollisuuden sekä käyttötarkoitussidonnaisuuden henkilötietojen käsittelyssä ja ilmoitusvelvollisuuden valvontaviranomaiselle automaattista henkilötietojen käsittelyä silmällä pitäen. Uutena rekisterinpitäjän velvollisuutena tietosuoja-asetuksessa henkilötietolakiin verrattuna on tietoturvarikkomusten ilmoitusvelvollisuus valvontaviranomaisille ja rikkomuksen vaikutuksen alaisille rekisteröidyille.

Tietosuoja-asetuksen myötä rangaistusjärjestelmään tulee uusia sanktioita, kuten sakkorangaistus koskien rekisterinpitäjiä ja henkilötietojen käsittelijöitä. Sakkorangaistukseen päädytään jos edellämainitut eivät noudata tietosuoja-asetuksen määräyksiä tai esimerkiksi laiminlyövät ilmoitusvelvollisuutta ja sille asetettuja määräaikoja. Uuden osoitusvelvollisuuden myötä rekisterinpitäjän tulee pystyä todistamaan noudattavansa tietosuoja-asetusta ja huomioivansa henkilötietojen suojan kaikessa toiminnassaan.

Rekisteröityjen oikeuksia on myös käsitelty jo henkilötietolaissa, joista enemmän opinnäytetyön kappaleessa 6. Oikeuksiin tuli tarkennuksia tietosuoja-asetuksen myötä ja uusina oikeuksina voidaan pitää rekisterinpitäjän henkilötietojen käsittelyn läpinäkyvyyttä, oikeutta käsittelyn rajoittamiseen ja oikeutta siirtää tietojaan toisen rekisterinpitäjän järjestelmiin, jos se on teknisesti toteutettavissa.

Tietosuoja-asetuksen vaikutus ulottuu sekä julkisen että yksityisen sektorin toimijoihin. Vaikutukset kuitenkin saattavat erota riippuen yrityksestä ja käsittelytoiminnan luonteesta. Kaikkien henkilötietoja käsittelevien tahojen tule ottaa jatkossa huomioon toiminnassaan uudet rekisteröityjen oikeudet ja noudattaa rekisterinpitäjille sekä käsittelijöille määriteltyjä velvollisuuksia. Tietosuojavastaavan nimittämistä käsitellään opinnäytetyön kappaleessa 9, jossa käydään tarkemmin läpi perusteita nimittämiselle. Pääosin nimitysvelvollisuus koskee julkista sektoria tai vaihtoehtoisesti sellaista toimijaa, jonka ydintoimintoihin kuuluu laajamittaista henkilötietojen käsittelyä. Jokaisessa yrityksessä tulee jonkun vastata tietosuojan toteutumisesta, vaikka varsinaista tietosuojavastaavaa ei nimitettäisikään.

---

[190] COM(2012) 9 final, 12.

Lähteet

Aarnio, A. 2011. Luentoja lainopillisen tutkimuksen teoriasta. Helsinki: Unigrafia Oy Yliopistopaino.

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

Honkinen, T. & Innanen, A. & Lindgren, J. & Pello, J. & Rantanen, J. & Siltala, K. & Tuomala, S. 2016. Startup-juridiikan käsikirja. Liettua: BALTOprint.

Jyränki, A. & Husa, J. 2012. Valtiosääntöoikeus. Hämeenlinna: Kariston kirjapaino Oy.

Lehtonen, L. 2012. Henkilötietojen käsittely työelämässä. Työnantajan oikeus arkaluonteisten henkilötietojen käsittelyyn. 257-263. Teoksessa: Koskinen, S. & Alapuranen, L. & Heino, A-M. & Lehtonen, L. 2012. Henkilötietojen käsittely työelämässä. Porvoo: Bookwell Oy.

Mattinen, K. & Orlando, C. & Parnila, K. 2017. Palkanlaskenta käytännönläheisesti. Viro: Meedia Zone OÜ.

Mäenpää, O. 2013. Hallinto-oikeus. Helsinki: Sanoma Pro Oy.

Nyyssölä, M. 2012. Yksityisyyden suoja työsuhteessa. Viro: Print Best.

Ojanen, T. 2010. EU-oikeuden perusteita. Helsinki: Edita Prima Oy.

Raitio, J. 2013. Eurooppaoikeus ja sisämarkkinat. Liettua: Talentum Media Oy.

Siltala, R. 2003. Oikeustieteen tieteenteoria. Vammala: Vammalan Kirjapaino Oy.

Syrjänen, P. 2007. Luotettava henkilöarviointi ja yksityisyyden suoja. Jyväskylä: Gummerus Kirjapaino Oy.

Viljanen, P. 2011. Perusoikeudet. Yksityiselämän suoja. 389-412 Teoksessa: Hallberg, P. & Karapuu, T. & Ojanen, T. & Martin, S. & Tuori, K. & Viljanen, V-P. 2011. Perusoikeudet. Helsinki: WSOYPro Oy.

Voutilainen, T. 2012. Oikeus tietoon: informaatio-oikeuden perusteet. Helsinki: Edita Publishing Oy.

Virallislähteet

Article 29 – Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ”likely to result in a high risk” for the purposes of Regulation 2016/679. 17/EN/WP 248.

Article 29 – Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. 844/14/EN/WP 217.

Article 29 – Data Protection Working Party. Opinion 2/2017 on data processing at work. 17/EN/WP 249.

Article 29 – Data Protection Working Party. Opinion 03/2013 on purpose limitation. 00569/13/EN/WP 203.

Article 29 – Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. 17/EN/WP 251.

Communication from the commission to the European Parliament,the Council, the European economic and social committee and the committee of the regions. Safeguarding Privacy in a Connected World: A European Data Protection Framework for the 21st Century. COM(2012) 9 final.

EU:n yleisen tietosuoja-asetuksen täyttäntöönpanotyöryhmän (TATTI) mietintö. Oikeusministeriö, Helsinki 2017.

Euroopan unionin perusoikeuskirja (2012/C 326/02).

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

Lainsäädännön arviointineuvoston lausunto luonnoksesta hallituksen esitykseksi eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi yleiseksi lainsäädännöksi. VNK/133/32/2018.

Lissabonin sopimus: Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta (2007/C 306/01)

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012) 11 final.

Recommendation of the Council concerning Guidelines governing the Protection of Privaacy and Transborder Flows of the Personal Data 23.08.1980.

Sopimus Euroopan perustuslaista (2004/C 310/1).

Muut lähteet

http://tietosuoja.fi/fi/index/rekisteroidylle/rekisteroidynoikeudet.html
Viitattu 14.2. 2018.

http://valtioneuvosto.fi/artikkeli/-/asset_publisher/10616/arviointineuvosto-tietosuojalaista-hallituksen-esitysluonnoksessa-merkittavia-puutteita Viitattu 14.2.2018.

http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/kysymyksiajavastauksia.html Viitattu 14.2.2018.

https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/EUn-tietosuojauudistus.aspx Viitattu 14.2.2018.

https://www.eugdpr.org/ Viitattu 14.2.2018.

https://www.eugdpr.org/gdpr-timeline.html
Viitattu 14.2.2018.

https://www.eugdpr.org/key-changes.html
Viitattu 23.3.2018.

http://www.consilium.europa.eu/fi/press/press-releases/2015/12/18/data-protection/ Viitattu 15.3.2018.