LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

EU tietosuoja-asetuksen vaikutus mikroyrityk-seen

Kuronen, Nikolas

2018 Laurea

Laurea-ammattikorkeakoulu

EU tietosuoja-asetuksen vaikutus mikroyritykseen

Nikolas Kuronen
Liiketalous
Opinnäytetyö
Kuukausi, 2018

Laurea-ammattikorkeakoulu **Tiivistelmä**
Liiketalouden koulutusohjelma
Tradenomi (AMK)

Tekijä Nikolas Kuronen

EU tietosuoja-asetuksen vaikutus mikroyritykseen

Vuosi 2018 Sivumäärä 36

Opinnäytetyön tavoitteena on selvittää oikeuskirjallisuuden, lainsäädäntötekstien, ja oikeuskäytäntöjen avulla EU:n yleisen tietosuoja-asetuksen vaikutuksia suomalaiseen mikroyritykseen ja miten kyseisen yrityksen tulee varautua tietosuoja-asetuksen tuomiin määräyksiin ja käytänteisiin. Opinnäytetyön tietoperusta koostuu oikeuskirjallisuudesta, Euroopan unionin ja Suomen lainsäädännöstä ja lainsäädännön valmisteluaineistoista. Opinnäytetyö sisältää teoreettisen osuuden, jossa tarkastellaan EU:n yleisen tietosuoja-asetuksen vaikutuksia Suomen lainsäädäntöön ja mikroyrityksiin, sekä suunnitelman, miten työn kohteena oleva mikroyritys voi varautua tietosuoja-asetukseen.

Euroopan unionin yleisen tietosuoja-asetuksen asettamat määräykset ovat osaltaan vastaavia mitä suomen lainsäädännössä määritetään henkilötietojen käsittelystä. Uutena asiana tulee ottaa huomioon uudet rekisteröityjä henkilöitä koskevat oikeudet ja uudet määräykset rekisterinpitäjän toiminnassa. Tietosuoja-asetus vaikuttaa eri tavoin yrityksen toimintaan, riippuen miten yritys käsittelee tietoja ja millainen yritys on kyseessä. Opinnäytetyön kohteena olevan mikroyrityksen tulee varmistaa, että yrityksen tietojenkäsittely vastaa vaadittuja määräyksiä ja mahdolliset muutokset tulee tehdä siirtymäajan päättymiseen mennessä.

Asiasanat: Tietosuoja, EU, mikroyritys, henkilötieto

Laurea University of Applied Sciences
Degree Programme in Business Management
Bachelor's Thesis

Abstract

Name Nikolas Kuronen

Effects of the EU general data protection regulation on a microenterprise

Year 2018 Pages 36

The objective of the thesis is to research the effects of the EU general data protection regulation on Finnish microenterprises and how those enterprises should prepare for the new regulations concerning data processing. The knowledge base of the thesis consists of legal literature, legal regulations, law of the European union and preparatory legal materials.

In conclusion, most of the upcoming regulations in the EU general data protection regulation are already covered in the Finnish law regarding data processing. The EU data general data protection regulation adds new rights to the registered persons and new regulations for the data processing parties, both of which are important to take note of. The general data protection regulation also affects companies that process data and those companies must change their processes according to the regulations in the new EU regulation.

Keywords: data processing, EU legislation, personal data

Lakiluettelo

Henkilötietolaki (523/1999)

Kirjanpitolaki (1997/1336)

Suomen perustuslaki (731/1999)

Tietosuojadirektiivi (EU) 2016/680

Yleinen tietosuoja-asetus (EU) 2016/679

Sisällys

1 Johdanto

Suomen henkilötietolaki (523/1999) määrittää suomen kansalaisille yksityiselämän suojan ja muita sellaisia oikeuksia, joiden tavoitteena on ylläpitää perusoikeuksia henkilötietojen käsittelyn yhteydessä ja edistää hyvää tietojenkäsittelytapaa henkilötietojen käsittelyn yhteydessä. Henkilötietojen käsittelystä säädetään myös Euroopan unionin perusoikeuskirjan 8. artiklassa ja tätä sääntelyä varten Euroopan unionissa säädettiin vuonna 1995, joka takaa unionin kansalaisille tehokkaan tietosuojan.[1]

Euroopan unioni hyväksyi 27.4.2016 uuden tietosuoja-asetuksen (EU 2016/679), jonka tavoitteena on yhtenäistää tietosuojaan ja tietojenkäsittelyn kansallisia määräyksiä. Asetus sisältää aiempaa tarkempia määräyksiä henkilötietojen käsittelystä ja rekisteröityjen henkilöiden oikeuksista. Uusi tietosuoja-asetus määrittää myös uusia vastuita ja velvollisuuksia rekisterinpitäjille ja henkilötietojen käsittelijöille. Asetus on jo hyväksytty, mutta sen voimaantulemiseen on annettu Euroopan unionin toimesta siirtymäaika, jonka päätyttyä unionin jäsenvaltioiden tulee saattaa oma henkilötietojen käsittelyyn liittyvä lainsäädäntönsä tietosuoja-asetuksen määräysten tasoiseksi.[2]

Euroopan unionin tietosuoja-asetuksen tavoitteena on myös uudistaa nykyistä sääntelyä tietosuojaa kohtaan, koska tietosuojadirektiivi otettiin käyttöön aikana, jolloin teknologia ei ollut yhtä kehittynyttä kuin nykypäivänä se on. Tietosuoja-asetuksen tavoitteena on kattaa erilaiset henkilötietoja keräävät verkossa olevat palvelut. Näitä ovat muun muassa: sosiaalisen median verkkosivut, erilaiset sijaintiin perustuvat palvelut ja pilvipalvelut. Nykyteknologiaa varten tarvitaan säännöstö joka vastaa Euroopan unionin peruskirjan 8. artiklaa ja että se pysyy voimassa myös nykyaikana.[3]

Suomen nykyinen henkilötietolaki ennen tietosuoja-asetuksen voimaantuloa sisältää jo osan asetuksen määräyksistä. Suomen on omalta osaltaan helpompi muuttaa lainsäädäntöään yhtenäisemmäksi Euroopan unionin tietosuoja-asetuksen mukaiseksi, koska Suomen henkilötietolaki määrittää jo rekisteröidyn henkilön oikeuksia ja rekisterinpitäjän velvollisuuksia henkilötietojen käsittelyä kohtaan. Samanlainen, jo valmiiksi maan laissa oleva sääntely ei kuitenkaan päde kaikkien Euroopan unionin jäsenvaltioiden kohdalla ja tästä syystä unionissa halutaan yhtenäistää henkilötietojen käsittelyyn liittyviä määräyksiä. Osa tässä työssä käsiteltä-

---

[1] EU-tietosuojadirektiivi 95/46/EY
[2] Tietosuoja asetus (EU) 2016/679
[3] Tietosuoja asetus (EU) 2016/679

vistä rekisteröidyn oikeuksista, kuten tiedonsaantioikeus, oikeus tietojen oikaisemiseen ja informointioikeus ovat jo määritelty Suomen nykyisessä henkilötietolaissa. Myös osa rekisterinpitäjää ja henkilötietojen käsittelijää koskevista määräyksistä on jo olemassa henkilötietolaissa. Henkilötietolaki määrittää rekisterinpitäjälle huolellisuusvelvoitteen henkilötietojen käsittelyn yhteydessä, tietojen käsittelyn käyttötarkoitussidonnaisuuden ja turhien tietojen poistamisen velvollisuuden. Uutena tietosuoja-asetuksen myötä rekisterinpitäjälle tulee esimerkiksi velvollisuus ilmoittaa valvontaviranomaiselle tietoturvarikkomusten sattuessa ja erilaiset sanktiot, joita käytetään tietosuoja-asetuksen määräysten laiminlyönnin yhteydessä.

2 Opinnäytetyön tarkoitus ja tavoitteet

Opinnäytetyössä tarkastellaan Euroopan unionin uutta tietosuoja asetusta, joka astuu voimaan 25.5.2018 alkaen kaikissa Euroopan unionin jäsenmaissa. Opinnäytetyössä selvitetään, miten EU:n uusi tietosuoja-asetus vaikuttaa Suomen nykyiseen lainsäädäntöön ja tarkemmalla tasolla, miten asetus vaikuttaa mikroyrityksen toimintaan. Opinnäytetyön kohteena on hyvinkääläinen mikroyritys ja työn tavoitteena on auttaa yritystä varautumaan tietosuoja-asetuksen asettamiin vaatimuksiin.[4]

EU:n tietosuoja-asetusta käsitellään oikeuskirjallisuuden ja oikeudellisten käytäntöjen avulla. Oikeuskirjallisuus ja oikeuskäytännöt vastaavat kysymyksiin: mikä EU:n tietosuoja-asetus on, mitä se sisältää, miten se vaikuttaa Suomen jo olemassa olevaan lainsäädäntöön ja millainen vaikutus asetuksella on pk-tason yrityksiin suomessa.

Opinnäytetyössä selvitetään paikalliselle mikroyritykselle, miten EU:n tietosuoja-asetus vaikuttaa yrityksen toimintaan ja millä tavalla yrityksen tulee varautua tietosuoja-asetukseen, jotta yrityksen toiminta vastaa tietosuoja-asetuksessa määrättyjä toimenpiteitä. Opinnäytetyössä kerrotaan myös asetuksen taustaa, eli milloin tietosuoja-asetus päätettiin, miksi tämä asetus saatetaan voimaan Euroopan unionissa ja miten asetuksen käsittelyprosessi eteni.

3 Oikeustieteellinen tutkimusmenetelmä

[4] Tietosuoja asetus (EU) 2016/679

Oikeustieteessä ei ole niin sanottua objektiivista totuutta, minkä johdosta tekstin lukijan vakuuttaminen perustuu kirjoittajan valitsemaan kirjoittamistapaan. Oikeustiede on siis väitteiden punnitsemista ja perustelujen esittämistä. Oikeustieteellinen kirjoittaminen on omalla tavallaan luovaa ongelmanratkaisua, jossa tekstillä ei heti ole selkeää lopputulosta. Oikeudellisen kirjoittamisprosessin voi jakaa neljään eri päävaiheeseen. Nämä ovat ideointivaihe, jossa valitaan tutkimusaihe. Ideoinnin jälkeen on kehittelyvaihe, jossa ideaa selvennetään seuraavaa vaihetta varten, joka on tekstintuottamisen vaihe. Viimeisenä vaiheena voidaan pitää tekstin viimeistelyä, jossa teksti käydään läpi ja tarkistetaan virheiden varalta.[5] Opinnäytetyön kohdalla tutkimustyyppinä on tapaustutkimus, jossa käsitellään mikroyritystä ja niitä vaikutteita, jotka siihen kohdistuvat uuden Euroopan unionin tietosuoja-asetuksen voimaantulon myötä. Tapaustutkimuksessa on tyypillistä, että tutkimuskohteena on jokin yksittäinen tai pieni joukko ja miten jokin asia vaikuttaa tutkimuksen kohteeseen. Tutkimuksen tarkoituksena on kartoittava tutkimus mikroyritykselle, jonka tavoitteena on selvittää tietosuoja-asetuksen vaikutuksia kyseessä olevan yrityksen toimintaan ja miten tämän yrityksen tulee varautua asetuksen määräyksiin.[6]

Suuri osa oikeustieteellisestä tutkimuksesta on lainoppia. Lainoppi eli oikeusdogmatiikka perustuu jo olemassa olevien oikeuslähteiden varaan. Lainoppi on voimassa olevien oikeuslähteiden tilannekohtaista tulkintaa. Lainopin keskeinen tehtävä on voimassa olevan oikeuden jäsentäminen, jonka avulla pyritään luomaan ja kehittämään oikeustieteellisten käsitteiden järjestelmää. Myös oikeushistorialliset tutkimukset auttavat kehittämään lainoppia, sillä oikeushistoriassa voidaan verrata vanhaa ja uutta lainsäädäntöä keskenään.[7]

Oikeuslähteitä puolestaan ovat sellaiset lähteet, joissa on tietoa oikeudellisesta sisällöstä. Lait ja muut säädökset ovat oikeusdogmatiikan tutkimuksen kannalta erittäin tärkeä lähde. Säädöksiä ei yleensä tulkita pelkästään vaan niiden tulkinnan apuna käytetään usein muuta säädökseen liittyvää oikeustieteellistä aineistoa, kuten säädöksen taustaa, erilaisia oikeustapauksia ja oikeuskirjallisuutta.[8]

4 Käsitemäärittelyt

[5] Husa, Mutanen & Pohjalainen 2010, 13-14.
[6] Hirsjärvi 2014, 132-138.
[7] Husa, Mutanen & Pohjalainen 2010, 20-21.
[8] Husa, Mutanen & Pohjalainen 2010, 32-33.

Seuraavassa kappaleessa määritellään opinnäytetyössä käytettäviä käsitteitä ja mitä ne tarkoittavat. Opinnäytetyössä käytetyt käsitteet liittyvät pääasiassa Euroopan Union lainsäädäntöön sekä Suomen lainsäädäntöön ja kyseessä olevien lainsäädännön lainoppeihin ja tulkintaan.

4.1 Yksityiselämän suoja

Yksityiselämän suojalla tarkoitetaan Suomen perustuslain (731/1999) kymmenennessä pykälässä turvattua suojaa yksittäisen henkilön kohdalla. Perustuslain 10 § määrittää säännökset kotirauhan, kunnian ja yksityiselämän suojasta. Tämän lakipykälän 1 momentissa on myös maininta henkilötietojen suojaamisen säätelystä, joka tapahtuu henkilötietolain kautta.[9]

Perustuslain 10 § mukaan turvatut oikeudet sisältyivät jo osakseen vuonna 1919 tehtyyn alkuperäiseen perusoikeusluetteloon. Vuoden 1919 perusoikeusluettelo sisälsi määräykset kunnian turvaamiseen ja kotirauhan varmistamiseen. Vuonna 1995 tehty perustuslain uudistus yhdisti yksityiselämän suojan määräävän lain osaksi perustuslakia ja tässä yhteydessä myös yksityisyyden suojaa määrittävässä laissa otettiin huomioon kirje-, lennätin- ja puhelinsalaisuutta turvaava laajennus.[10]

4.2 Tietosuoja ja tietoturva

Tietosuojalla tarkoitetaan ihmisten yksityiselämän suojaa ja sitä turvaavia oikeuksia ja määräyksiä, kun käsitellään henkilötietoja. Tietosuojan tavoitteena on turvata tietojen kohteena olevan henkilön yksityisyys, oikeudet ja oikeusturva.[11] Tietoturvalla puolestaan tarkoitetaan niitä toimenpiteitä, jotka rekisterinpitäjän tulee huomioida henkilötietoja käsiteltäessä. Tietoturvaan liittyvillä toimilla varmistetaan tietojen käsittelyn luottamuksellisuus ja rekisteröidyn henkilön oikeuksien turvaaminen. Tietoturvan avulla toteutetaan tietojenkäsittelyn julkisuusperiaate siten, että sellaiset asiakirjat jotka eivät ole julkisia tai ovat salaisia asiakirjoja ovat käytössä vain silloin, kun niihin oikeutettu käyttötarkoitus. Tietoturvan avulla myös varmistetaan julkisten asiakirjojen pysyminen julkisina ja se, että niihin oikeutetuilla henkilöillä on pääsy kyseisiin asiakirjoihin.[12]

---

[9] Hallberg 2005, 1. luku 45.
[10] HE 309/1993
[11] Voutilainen 2012, 37.
[12] Voutilainen 2012, 37.

4.3 Mikroyrityksen määritelmä

Tilastokeskus määrittelee mikroyritykset sellaisiksi yrityksiksi, joiden palveluksessa on alle 10 työntekijää ja joiden vuosiliikevaihto on alle 2 miljoonaa euroa tai jotka täyttävät määritelmän riippumattomuudesta. Riippumattomia ovat ne yritykset, joiden omistuksesta ei ole 25 prosenttia tai enemmän yhden tai useamman yrityksen omistuksessa.[13] Uudistettu kirjapitolaki (1336/1997) hallituksen esityksen mukaisesti määrittelee mikroyritykseksi sellaisen yrityksen, joka täyttää päättyneellä ja sitä edeltävällä tilikaudella jonkin lain määrittelemistä ehdoista. Kirjanpitolain ehtoina ovat taseen loppusumman oltava enintään 350.000 euroa tai liikevaihdon oltava enintään 700.000 euroa tai, että yrityksen palveluksessa on tilikauden aikana ollut keskimäärin enintään 10 henkilöä.[14]

5 Euroopan Unionin oikeus

Euroopan Unionin oikeutta pidetään yleisesti ylikansallisena oikeusjärjestelmänä. Euroopan Unionin oikeuden mukana jäsenvaltioille ja EU:n toimielimille on luotu velvollisuuksia ja oikeuksia. EU-oikeus jaetaan kahteen pääasialliseen oikeuteen, jotka ovat primäärinen ja sekundäärinen oikeus.[15]

Primäärinen EU-oikeus asettaa omanlaisensa perustuslain EU:n toiminnalle ja päätöksenteolle. Primäärinen oikeus toimii tulkinnan ja pätevyyden perusteena sekundääriselle EU-oikeudelle. Sekundäärinen EU-oikeus syntyy EU:n toimielimien ja päätöstentekijöiden tekemistä ratkaisuista.[16]

5.1 Primäärinen EU-oikeus

Primääriseen EU-oikeuteen kuuluvat Euroopan Unionin perussopimukset kaikkien liitteiden ja pöytäkirjojen kanssa ja niihin tehdyt lisäykset tai muutokset. Esimerkiksi Euroopan Unionin

---

[13] Tilastokeskus 2016
[14] HE 208/2016
[15] Ojanen 2016, 38-39.
[16] Ojanen 2016, 39.

perustamissopimukset ovat tällöin primäärisen oikeuden alaisia sopimuksia. Primääriseen EU-oikeuteen kuuluvat myös jäsenvaltioiden liittymissopimukset, kuten esimerkiksi vuoden 1994 sopimus, jossa Itävalta, Suomi ja Ruotsi liittyivät osaksi Euroopan Unionia vuoden 1995 alusta alkaen.[17]

Euroopan Unionin primäärioikeus on muodostunut EU-oikeuden yleisten oikeusperiaatteiden mukaisesti. EU:n yleiset oikeusperiaatteet ovat luonnoltaan kirjoittamattomia ja perustavanlaatuisia. Jäsenvaltioiden yhteiset oikeusperiaatteet, perusoikeudet ja ihmisoikeudet ovat muodostaneet ovat olleet EU:n oikeusperiaatteiden kehittämisen taustalla ja ovat toimineet oikeusperiaatteiden vertailuaineistona. Yleiset oikeusperiaatteet ovat toimineet EU-oikeuden ratkaisujen taustalla sekä EU-oikeuden tulkinnan ja pätevyyden perustana. Kirjoitettu EU-oikeus sisälsi aiemmin paljon taloudellisia arvoja ja tavoitteita, joiden vastakohdaksi luotiin yleisten oikeusperiaatteiden kautta muunlaisia arvoja sekä periaatteita. Yleiset oikeusperiaatteet luokitellaan Euroopan Unionin primäärioikeuden alaisuuteen, jonka myötä yleiset oikeusperiaatteet tukevat sekundäärisen EU-oikeuden tulkintaa ja sen pätevyyttä.[18]

5.2 Sekundäärinen EU-oikeus

Sekundääristä EU-oikeutta nimitetään myös johdetuksi EU-oikeudeksi, sillä se muodostuu Euroopan Unionin toimielinten ja päätöksenteon menettelyissä. Lissabonin sopimuksen mukaisesti sekundäärinen oikeus voidaan jakaa lainsäädäntöön ja muihin oikeudellisiin menettelyihin. Lissabonin sopimuksella tarkoitetaan vuonna 2009 joulukuussa tullutta Euroopan Unionia koskevaa sopimusta, jossa Euroopan yhteisön ja Euroopan Unionin erittely poistettiin ja ne yhdistyivät yhdeksi Euroopan Unioniksi. Tämä sopimus myös poisti erittelyt Euroopan yhteisön lakien ja Euroopan Unionin lakien välillä.[19]

Euroopan Unionin lainsäätämisjärjestyksessä olevat asetukset, direktiivit ja päätökset kuuluvat sekundäärisen oikeuden alaisuuteen. Lainsäätämisjärjestyksen mukaan lainmukaisia päätöksiä voi antaa vain Eurooppa-neuvosto ja Euroopan parlamentti yhdessä.[20]

---

[17] Ojanen 2016, 39-40.
[18] Ojanen 2016, 39-40.
[19] Ojanen 2016, 40.
[20] Ojanen 2016, 40-41.

5.3 EU-säädösten toiminta

EU-säädökset jaetaan kolmeen eri pääkategoriaan niiden tehtävien ja tavoitteiden mukaisesti. Ensimmäinen niistä on kansallista oikeutta yhtenäistävä EU-sääntely. Tätä sääntelyä sovelletaan yleisimmin sellaisilla aloilla, joiden toiminta kuuluu yksinomaan Euroopan Unionille ja jossa EU pyrkii yhtenäistämään politiikkaansa. Yhtenäistävässä EU-sääntelyssä on yleisesti käytössä asetus. Yhtenäistävä EU-sääntely koskee usein suoraan jäsenvaltioita, eikä jäsenvaltioilla ole usein mahdollisuuksia vaikuttaa sääntelyyn.[21]

Toinen pääkategoria on kansallista oikeutta yhdenmukaistava EU-sääntely. Yhdenmukaistavalla sääntelyllä EU:n jäsenvaltiot velvoitetaan muuttamaan lainsäädäntöään EU:n sääntelyn mukaisesti, mutta yhdenmukaistava sääntely ei tule suoraan voimaan sellaisena kuin se on kansallisen lainsäädännön tilalle, mutta jäsenvaltioiden tulee muuttaa omaa lainsäädäntöään vastaamaan EU:n määräyksiä. Sääntelyssä EU käyttää direktiivejä.[22]

Yhdenmukaistava säätely sisältää eri asteita, jotka vaikuttavat lainsäädännön muuttamiseen jäsenvaltiossa. Täydellisellä harmonisoinnilla tarkoitetaan yhdenmukaistamisen tasoa tai laajuutta sitä koskevassa asiassa. Nämä ovat maksimidirektiivejä. Vähimmäisharmonisoinnilla tarkoitetaan vähimmäisdirektiivejä, jotka eivät estä jäsenvaltion omia kansallisia käsittelyjä direktiivien vaikutuksiin. Vähimmäisdirektiivejä on käytetty esimerkiksi Euroopan Unionin ympäristönsuojeluun liittyvillä aloilla.[23]

Osittaisella harmonisoinnilla tarkoitetaan Unionia koskevien yksittäisten asioiden säätelyä. Esimerkiksi Euroopan Unionin sisäistä televisiotoimintaa ja kuluttajansuojaa on säädelty osittaisen harmonisoinnin avulla.[24]

Kolmas pääkategoria on kansallista oikeutta yhteensovittava EU-sääntely. Sääntelyn tavoitteena on EU-jäsenvaltioiden lainsäädännön ja hallinnon koordinointi ilman, että niitä tulee yhtenäistää jonkin määräyksen mukaisesti. Yhtenäistävä sääntely voi pidemmän ajan kuluessa vaikuttaa lainsäädännön yhtenäistämiseen. Suomen sosiaaliturvaa on osakseen yritetty säännellä muiden jäsenvaltioiden työperusteisen sosiaaliturvan mukaiseksi.[25]

---

[21] Ojanen 2016, 41.
[22] Ojanen 2016, 41-42.
[23] Ojanen 2016, 42.
[24] Ojanen 2016, 42-43.
[25] Ojanen 2016, 42-43.

5.4 Asetus ja direktiivi

Asetukset ovat yleispäteviä Euroopan Unionin säännöksiä. EU-lainsäädännön mukaan asetus on sidoksissa säännöksen sisällön ominaispiirteisiin. Asetukset koskevat EU-jäsenvaltioita siinä muodossa, kuin asetus on annettu ja niitä ei tarvitse säätää osaksi jäsenvaltioiden kansalista lainsäädäntöä. Asetukset ovat EU-komission tekemiä säädöksiä, jotka koskevat usein EU:n isoa päätöksiä, kuten esimerkiksi maatalouspolitiikkaa tai kauppapolitiikkaa.[26]

Direktiivit ovat puolestaan sovellettavia jäsenvaltioiden lainsäädäntöön. Ne eivät tule voimaan sellaisenaan, vaan ne tulee liittää jäsenvaltiolle sopivalla tavalla osaksi valtion kansallista lainsäädäntöä. Direktiivi ei aina vaadi lainsäädännöllisiä toimia, vaan tulee huomioida jäsenvaltion valtiösäädön- ja hallintaoikeuden yleiset periaatteet. Jäsenvaltion tulee taata, että sen hallintoviranomaiset noudattavat direktiivin säännöksiä.[27]

6 Tietosuoja-asetus

EU:n tietosuoja-asetuksen taustalla on Euroopan Komission vuonna 2012 tekemä ehdotus tietosuojakäytäntöä kohtaan. EU:n nykyisen tietosuojalainsäädännön tavoitteena oli suojata tietosuojaa koskeva perusoikeus ja taata henkilötietojen vapaa liikkuvuus Unionin jäsenmaiden välillä. Tämä tietosuojalainsäädäntö on vuodelta 1995. Teknologian kehitys on tuonut uusia haasteita henkilötietojen suojelun kohdalla ja niitä kerätään nykyään enemmän kuin vuonna 1995, jolloin tietosuojalainsäädäntö on tullut voimaan. Uuden asetuksen taustalla on Lissabonin sopimuksessa määritetty yksilön oikeus omien henkilötietojensa suojaan sekö Euroopan Unionin perustuskirjan 8. artikla, joka määrittää henkilötietojen suojan perusoikeutena Unionin kansalaisille. Euroopan unionin perusoikeuskirjassa määritetään jokaiselle Euroopan Unionin kansalaiselle oikeus omien henkilötietojensa suojaan. Perusoikeuskirja määrittää henkilötietojen käsittelyn asianmukaisuuden ja sen tapahtumisen tiettyä henkilötietojen käsittelyn tarkoitusta varten asianomaisen henkilön suostumuksella tai jonkin muun lainmukaisen perusteen nojalla. Peruskirjan mukaisesti jokaisella on oikeus tutustua hänestä kerättyihin tietoihin ja saada tarvittaessa oikaista omia tietojaan. Näitä henkilötietojen käsittelyyn liittyviä toimien noudattamisen valvomista tulee valvoa riippumaton viranomainen Euroopan Unionin jäsenmaissa.[28]

---

[26] Raitio 2016, 203-204.
[27] Raitio 2016, 204-205.
[28] Euroopan Unionin perusoikeuskirja. Ks. myös Euroopan Komissio (2012/0011)

EU:n uusi tietosuoja-asetus sisältää päivityksiä ja uusia periaatteita vanhaan tietosuojalainsäädäntöön Euroopan Unionin alueella. Asetuksen tavoitteena on vahvistaa kansalaisten oikeuksia ja parantaa henkilötietojen liikkuvuutta Euroopan Unionin alueella. Tavoitteena on taata ihmisten henkilötietojen suoja niiden käsittelyn ja siirron aikana. Tietosuoja-asetuksen muutosten myötä on tavoitteena saada kansalaisille paremmat edellytykset kontrolloida omia tietojaan sekä päästä helpommin omiin tietoihinsa käsiksi. Uusi tietosuoja-asetus myös luo uusia velvoitteita henkilötietoja keräävälle osapuolille ja tehostaa niiden suojausvaatimuksia.[29]

7 Rekisteröidyn oikeudet

Rekisteröidyn henkilön oikeuksien perustana on henkilön yksityisyyden suojan takaaminen luvattomalta henkilötietojen käytöltä. EU:n uuden tietosuoja-asetuksen 4 artiklan mukaisesti rekisteröityä henkilöä koskevat oikeudet ovat osakseen samat, kuin nykylainsäädännössä olevat oikeudet. Tietosuoja-asetus kuitenkin tuo lisää oikeuksia rekisteröidylle, esimerkiksi oikeuden siirtää omat tietonsa toiseen järjestelmään.[30]

Uutena velvollisuutena rekisterinpitäjälle tietosuoja-asetuksen 5 artikla määrittelee ilmoitusvelvollisuuden, joka tarkoittaa velvollisuutta rekisterinpitäjältä ilmoittaa rekisterissä oleville henkilöille mahdollisista tietomurroista, jossa rekisteröityjen henkilöiden tiedot ovat vaarantuneet. Rekisterinpitäjän tulee ilmoittaa tietomurrosta, jos se todennäköisesti vaikuttaa rekisteröityjen henkilöiden henkilötietoihin.[31]

Mikäli rekisteröity henkilö haluaa päästä käsiksi omiin tietoihinsa, oikaista tai poistaa omia tietojaan rekisteristä tai siirtää omia tietojaan toiseen järjestelmään, tulee tällöin rekisterinpitäjän tunnistaa rekisteröidyn henkilön henkilöllisyys. Rekisterinpitäjän tulee suorittaa rekisteröidyn pyytämät toimenpiteet kahden kuukauden sisässä pyynnön tekemisestä ja pääsääntöisesti ilman ylimääräisiä maksuja rekisteröidylle. Tästä määritetään tietosuoja-asetuksen 5 artiklassa.[32]

---

[29] Euroopan unionin Komissio (2012/0011)
[30] EU:n yleinen tietosuoja-asetus
[31] EU:n yleinen tietosuoja-asetus
[32] EU:n yleinen tietosuoja-asetus

7.1 Rekisterinpitäjän tiedotusvelvollisuus

Uuden tietosuoja-asetuksen 6 artiklan mukaisesti rekisterinpitäjällä on velvollisuus tiedottaa henkilötietojen käsittelytoimista, ennen kuin toiminta aloitetaan. Rekisterinpitäjän tulee ennen tietojen keräämistä ilmoittaa selkeästi tietosuoja-asetuksessa määritellyt asiat. Rekisteröidyille tulee ilmoittaa rekisterinpitäjän ja tämän mahdollisen tietosuojavastaavan yhteystiedot, tietojen käsittelyn tarkoitus ja oikeusperusta, mahdolliset henkilötietojen luovutukset eteenpäin, jos sellainen on tarpeen käsittelyn aikana ja kauanko henkilötietoja säilytetään rekisterissä. Rekisterinpitäjän tulee ilmoittaa myös, mihin henkilötietojen luovutuksen pyyntö perustuu, onko rekisteröidyn henkilön pakko luovuttaa tietojaan ja mahdolliset seuraukset, mikäli rekisteröity henkilö ei luovuta tietojaan sekä mahdolliset profiloinnit tai automaattiset päätöksenteot tietojen käsittelyn yhteydessä. Profilointiin ja automaattiseen päätöksentekoon liittyy rekisteröidyn henkilön oikeus vastustaa käsittelyä.[33]

Profiloinnilla tarkoitetaan automaattista tietojenkäsittelyä, jossa muodostetaan tietojoukkoja päätöksentekoa varten. Profilointiin liittyy haasteita tietosuoja-asetuksen määräysten kannalta, koska profiloinnissa on tavoitteena kerätä mahdollisimman suuri määrä dataa, jota voidaan analysoida. Tietosuoja-asetuksessa on kuitenkin tavoitteena minimoida kerätyn datan määrä ja kerätä vain tarpeellinen data. Yksilöllä ei ole myös mahdollisuuksia osallistua mukaan omien tietojensa automaattiseen käsittelyyn.[34]

Rekisterinpitäjän tulee tietosuoja-asetuksen 6 artiklan mukaisesti pitää kuvaus tietojen käsittelystä julkisena ja helposti saatavilla, jotta rekisteröidyt henkilöt tietävät, mihin heidän tietojaan käytetään. Rekisterinpitäjien tulisi olla enemmän läpinäkyviä viestinnässään ja pitää huolta rekisteröityjen oikeuksien toteutumisesta.[35]

7.2 Käsittelyn läpinäkyvyys

Tietosuoja-asetuksen 12 artiklan mukaisesti rekisterinpitäjän tulee henkilötietojen käsittelyssä noudattaa sellaisia toimintatapoja, jotka rekisteröidylle henkilölle helposti saatavissa ja läpinäkyviä. Läpinäkyvyys on uusi rekisteröidyn henkilön oikeus, joka tulee tietosuoja-asetuk-

[33] EU:n yleinen tietosuoja-asetus.
[34] Alén-Savikko, A. 2017, 299-300.
[35] EU:n yleinen tietosuoja-asetus

sen mukana ja jota ei vielä ollut määritelty suomen henkilötietolaissa. Tietojen tulee olla rekisteröidyn henkilön osalta helposti saatavissa ja sellaisessa muodossa, että tiedot ovat helposti rekisteröidyn henkilön ymmärrettävissä. [36]

Rekisterinpitäjän tulee ilmoittaa rekisteröidylle henkilölle sellaisista toimista, jotka rekisterinpitäjä on aloittanut rekisteröidyn tekemän pyynnön perusteella. Tiedot tulee toimittaa sähköisesti rekisteröidylle henkilölle, jos rekisteröity henkilö on tehnyt sähköisesti pyynnön saada kopion omista tiedoistaan. Tiedot tulee toimittaa lähtökohtaisesti kahden kuukauden sisällä rekisteröidyn henkilön tekemästä pyynnöstä. [37]

7.3 Oikeus omiin tietoihin

Uuden tietosuoja-asetuksen 14 artiklan mukaisesti rekisteröity saa oikeuden päästä omiin tietoihinsa käsiksi. Pyydettäessä rekisterinpitäjän tulee ilmoittaa rekisteröidylle, käsitelläänkö hänen tietojansa ja toimitettava kopio rekisteröidylle tiedoistaan.[38]

Rekisterinpitäjän tulee myös ilmoittaa rekisteröidylle tietosuoja-asetuksen 13 artiklan mukaisesti edellisessä kappaleessa mainitut tietojen käsittelemiseen liittyvät määräykset. Rekisteröidyllä on myös oikeus päästä oikaisemaan omia tietojaan niin kuin nykylainsäädännönkin mukaisesti. Rekisteröidyllä on oikeus vaatia rekisterinpitäjää oikaisemaan puutteelliset tai virheelliset henkilötiedot.[39]

7.4 Oikeus poistaa tiedot

Tietojen poistamisen oikeudella tarkoitetaan tietosuoja-asetuksen 16 ja 17 artiklan mukaista rekisteröidyn oikeutta vaatia rekisterinpitäjää poistamaan rekisteröityä koskevat vanhentuneet tiedot. Rekisteröity voi esimerkiksi peruuttaa tietojen käsittelyyn liittyvän suostumuksensa ja tämän myötä vaatia rekisterinpitäjää poistamaan tiedot järjestelmistään, jonka myötä tiedot on poistettava, ellei siihen ole jokin lainmukainen peruste pitää tiedot järjestelmässä.[40] Oikeus tietojen poistamiseen pätee tietosuoja-asetuksen 17 artiklan mukaisesti silloin, kun henkilötietojen säilyttämisestä on tullut tarpeetonta, jolla tarkoitetaan tietoihin

---

[36] EU:n yleinen tietosuoja-asetus
[37] EU:n yleinen tietosuoja-asetus
[38] EU:n yleinen tietosuoja-asetus
[39] EU:n yleinen tietosuoja-asetus
[40] EU:n yleinen tietosuoja-asetus

liittyneen käsittelyn päättymistä. Oikeus pätee myös rekisteröidyn henkilön suostumuksen peruuntuessa, jos tiedot on hankittu rekisteröidyn henkilön suostumuksen perusteella ja jos käsittelylle ei ole ollut muuta perustetta tai käsittely on ollut lainvastaista.[41]

Rekisterinpitäjä voi toteuttaa tietojen poistamisen tietosuoja-asetuksen 17 artiklan mukaisesti merkitsemällä tiedot siten, ettei niitä enää käsitellä järjestelmässä, mutta tiedot voivat yhä jäädä järjestelmään sisälle. Toinen vaihtoehto on salata tiedot järjestelmässä, jotta niihin ei pääse enää käsiksi ja täten toteuttaa tietojen poistaminen. Kolmas vaihtoehto on ylikirjoittaa tiedot. Tietojen poistamisen mahdollisuutta ei kuitenkaan tule lakisääteisiin rekistereihin.[42]

7.5 Oikeus siirtää tietoja

Tietosuoja-asetuksen 20 artiklan myötä rekisteröidylle tulee uusi oikeus siirtää tietojaan järjestelmästä toiseen. Tämän myötä rekisteröidylle tulee antaa mahdollisuus saada tietonsa sellaisessa muodossa, jotta ne voidaan siirtää toiselta rekisterinpitäjältä toiselle. Tämä voidaan toteuttaa joko antamalla tiedot rekisteröidylle siirrettävässä muodossa tai tietojen siirtäminen rekisterinpitäjän toimesta toiselle rekisterinpitäjälle. Tiedonsiirron oikeus ei velvoita rekisterinpitäjiä suunnittelemaan yhteensopivia järjestelmiä, vaan on tietojen siirron tapauksessa katsottava sopiva tapa saada tiedot helposti paikasta toiseen.[43]

Siirto-oikeus pätee myös sellaisissa julkisen sektorin rekistereissä, joissa tiedot on kerätty vapaaehtoisia tehtäviä varten. Siirto-oikeus ei päde yleistä etua koskevan tehtävän suorittamisen yhteydessä tai julkisen vallan käytössä.[44]

7.6 Oikeus vastustaa käsittelyä

Rekisteröidyllä on tietosuoja-asetuksen 21 ja 22 artiklan mukaisesti oikeus vastustaa tietojensa käsittelyä erityiseen tilanteeseensa liittyvällä perustalla. Rekisterinpitäjä ei saa käsitellä tietoja, mikäli rekisteröity voi osoittaa sellaisen syyn, joka syrjäyttää rekisteröidyn

---

[41] Alén-Savikko, A. 2017, 301.
[42] EU:n yleinen tietosuoja-asetus
[43] EU:n yleinen tietosuoja-asetus
[44] EU:n yleinen tietosuoja-asetus

etuja, oikeuksia tai vapauksia. Käsittelyn vastustamisen oikeus ei päde kuitenkaan lainmukaisten rekisterien tietojen käsittelyssä.[45]

Rekisteröidyllä on oikeus olla joutumatta automaattiseen käsittelyyn. Tätä oikeutta ei sovelleta, jos päätös on välttämätön sopimuksen tekemiseen tai täytäntöön, käsittely perustuu rekisteröidyn suostumukseen tai käsittely on hyväksytty lainsäädännössä rekisteröidyn etuuksien suojaamiseksi.[46]

7.7 Oikeus saada ilmoitus tietoturvaloukkauksesta

Rekisterinpitäjän tulee tietosuoja-asetuksen 34 artiklan myötä ilmoittaa tietoturvaloukkauksesta rekisteröidylle, mikäli tietomurto koskee heidän henkilötietojaan. Oikeus pätee silloin, jos rekisteröidyn oikeudet ovat vaarantuneet esimerkiksi identiteettivarkauden riskin kohdalla. Tiedotus tulee lähtökohtaisesti antaa henkilökohtaisena ilmoituksena rekisteröidylle. [47]

Ilmoituksessa tulee kertoa lyhyt ja selkeä kuvaus tapahtuneesta tietoturvaloukkauksesta, rekisterinpitäjän tietosuojavastaavan tai muun asiaa hoitavan henkilön yhteystiedot, tiedot, millainen riski koskee rekisteröityä ja selostus, miten rekisterinpitäjä aikoo toteuttaa haittojen lieventämisen ja tilanteen ratkaisemisen. [48]

8 Rekisterinpitäjän velvollisuudet

Seuraavassa luvussa käsitellään rekisterinpitäjän velvollisuuksia kerättyä tietoa kohtaan ja velvollisuuksia rekisteröityjä henkilöitä kohtaan. Uuden EU:n tietosuoja-asetuksen 24 artikla määrittelee myös rekisteröidyn oikeuksien lisäksi rekisterinpitäjälle uusia velvollisuuksia. Tietosuoja-asetuksen mukaan rekisterinpitäjän tulee tarvittaessa pystyä osoittamaan, että pystyy ylläpitämään vaadittuja toimenpiteitä, jotka on määritelty tietosuoja-asetuksessa.[49]

---

[45] EU:n yleinen tietosuoja-asetus
[46] EU:n yleinen tietosuoja-asetus
[47] EU:n yleinen tietosuoja-asetus
[48] EU:n yleinen tietosuoja-asetus
[49] EU:n yleinen tietosuoja-asetus

8.1 Käsittelyn oikeusperusta

Rekisterinpitäjä on tietosuoja-asetuksen 28 artiklan mukaisesti vastuussa siitä, että kerättyjä henkilötietoja käsitellään tietosuoja-asetuksen määräämällä, lainmukaisella tavalla. Asetuksen mukaan lainmukaiseen käsittelyyn kuuluu, että rekisteröity henkilö on antanut vapaaehtoisen suostumuksen tietojen keräämiseen ja käsittelyyn. Tietojen keräämisen taustalla on sopimus, jossa rekisteröity henkilö on osapuolena ja tavoitteena on suojata rekisteröidyn etuja. Henkilötietojen käsittelyn tulee perustua tiettyyn tarkoitukseen, jotka on määritelty etukäteen.[50]

8.2 Tietosuojan ylläpito

Uuden tietosuoja-asetuksen 25 artikla velvoittaa rekisterinpitäjää nimeämään tietosuojavastaavan, mikäli tietojenkäsittelyä tekee jokin julkinen viranomainen tai julkisen hallinnon elin. Tietosuojavastaava tulee olla myös nimettynä, jos tietojenkäsittelyn keskeiset toimet edellyttävät rekisteröityjen seuraamista tai ne kohdistuvat rikoksia koskeviin asioihin.[51]

Nämä vaatimukset edellyttävät, että erityisesti julkisen sektorin rekisterinpitäjät nimittävät itselleen tietosuojavastaavan. Pienemmillä yrityksillä ei välttämättä tarvitse olla erillistä tietosuojavastaavaa, mutta tietosuoja-asetuksen edellyttämiä toimia tulee tällöin jonkun muun yrityksen työntekijän hoitaa.[52]

8.3 Riskinhallinta

Tietosuoja-asetuksen 35 artikla vaatii rekisterinpitäjiä arvioimaan omiin keräämiinsä tietoihinsa kohdistuvia riskejä ja valitsemaan omaan riskitasoonsa sopivat toimenpiteet. Riskienhallinta on tärkeä toimenpide rekisterinpitäjän toiminnassa ja tämä on samalla tärkeä osa rekisterinpitäjän osoitusvelvollisuutta, mikäli rekisterinpitäjän tulee näyttää toteen, että tämä noudattaa tietosuoja-asetuksen määräyksiä.[53]

---

[50] EU:n yleinen tietosuoja-asetus
[51] EU:n yleinen tietosuoja-asetus
[52] EU:n yleinen tietosuoja-asetus
[53] EU:n yleinen tietosuoja-asetus

Tietosuoja-asetuksen 35 artikla määrittelee tietosuojan vaikutustenarvioinnin pakolliseksi, sellaiselle tietojenkäsittelylle, jossa on todennäköistä, että henkilötietojen käsittelyyn liittyy erilaisia riskejä. Vaikutusarvioinnin avulla tulee pyrkiä ennaltaehkäisemään tietojenkäsittelyyn liittyviä riskejä ja varmistamaan tietosuoja-asetuksen määräyksien toteutumista. [54]

Tietosuojaa koskevalla vaikutusarvioinnilla kuvataan henkilötietojen käsittelyä, sen tarpeellisuuden arviointia ja sen tavoitteena on tukea luonnollisten henkilöiden oikeuksia ja vapauksia henkilötietojen käsittelyprosessissa. Vaikutustenarvioinnin avulla arvioidaan tietojenkäsittelyyn liittyviä riskejä ja määritellään sellaiset toimenpiteet, joiden avulla niitä voidaan ennaltaehkäistä. Vaikutustenarviointi toimii tärkeänä työkaluna rekisterinpitäjän osoitusvelvollisuuden toteen näyttämisessä. Tämän avulla rekisterinpitäjä voi osoittaa toteen, että tämä on toiminnassaan tehnyt arvion riskeistä ja varautunut toiminnassaan niihin.[55]

8.4 Oletusarvoinen tietosuoja

Tietosuoja-asetuksen 25 artikla velvoittaa rekisterinpitäjää sisäänrakennetulla ja oletusarvoisella tietosuojalla. Tällä tarkoitetaan, että rekisterinpitäjän tulee oletusarvoisesti kerätä vain sellaisia tietoja, joita välttämättä tarvitaan käsittelytarkoituksessa. Tietoja tulee kerätä vain tarpeellinen määrä ja niitä tulee säilyttää välttämättömän käsittelyn ajan, jonka jälkeen tiedot tulee poistaa. Rekisterinpitäjän tulee myös varmistaa tietosuojatoimissaan rekisteröityjen henkilöiden oikeudet ja henkilötietojen suojaamistoimet.[56]

Ennen käsittelyä rekisterinpitäjän on määritettävä omien tarpeidensa ja tietosuoja-asetuksen mukaisesti henkilötiedoille säilytysaika, eli kuinka kauan tiedot ovat rekisterinpitäjän käsiteltävänä ennen kuin ne poistetaan. Tämä aika tulee ilmoittaa rekisteröidyille, joiden tietoja ollaan käsittelemässä. Henkilötietojen säilytyksen yhteydessä tulee määrittää ne tekijät, joiden perusteella tietojen säilytysaika määräytyy. Säilytysajan jälkeen tiedot tulee poistaa tai anonymisoida tietoturvamääräysten mukaisesti, jotta tietoja ei voida tämän jälkeen yhdistää rekisteröityihin henkilöihin.[57]

Alla olevassa kuviossa on kuvattu, miten henkilötietojen käsittelijän tulisi toimia kerättyjen henkilötietojen kanssa. Tietojen keräämistä varten tulisi saada suostumus rekisteröidyltä henkilöltä, jotta tämä antaa rekisterinpitäjälle luvan tallentaa omia tietojaan rekisterinpitäjän

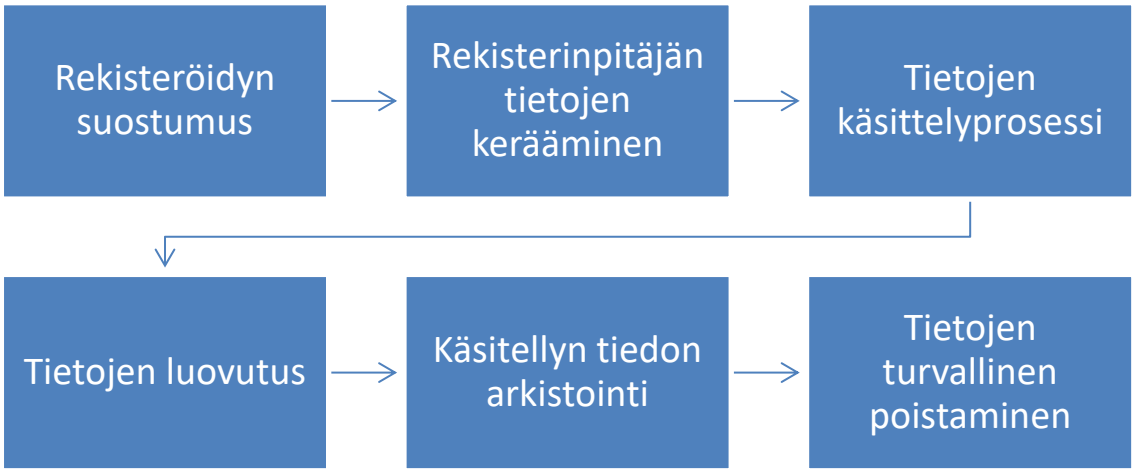
---

[54] EU:n yleinen tietosuoja-asetus
[55] Tietosuojatyöryhmä 4.10.2017.
[56] EU:n yleinen tietosuoja-asetus
[57] EU:n yleinen tietosuoja-asetus

järjestelmään. Suostumuksen antamisen jälkeen rekisterinpitäjä voi tallettaa rekisteröidyn henkilön tietoja järjestelmäänsä. Tämän jälkeen rekisterinpitäjän tulee määrittää, mitä tietoja tarvitaan kerätä rekisteröidyltä henkilöltä. Uutena määräyksenä tietosuoja-asetuksessa määritetään, että rekisterinpitäjän tulee tietojen keräämisen vaiheessa kerätä vain sellaisia tietoja, jotka ovat tarpeellisia käsittelyn kannalta ja jättää tarpeettomat tiedot keräämättä. Tällä tietojen keräämisen minimoinnilla halutaan ehkäistä mahdollisia riskejä, jotka liittyvät tarpeettomien henkilötietojen keräämiseen ja säilyttämiseen.[58]

Tietojen keräämisen jälkeen tietoja käsitellään rekisterinpitäjän toimesta. Käsittelystä tulee ilmoittaa rekisteröidylle henkilölle, mikäli se on tarpeellista ilmoittaa käsittelyn kulusta. Rekisteröidyllä henkilöllä on halutessaan oikeus tietää, mihin tarkoitukseen hänen tietojaan käsitellään ja mitä tietoja hänestä käsitellään. Rekisteröity henkilö voi tehdä pyynnön saada kopion niistä omista tiedoistaan, jotka on talletettu reksiterinpitäjälle. Rekisterinpitäjän tulee toimittaa pyynnön saadessaan kopio rekisteröidyn tiedoista ilman turhaa viivästystä tai kustannusta rekisteröidylle henkilölle. Käsittelyn jälkeen tiedot voidaan luovuttaa tarvittaessa eteenpäin toiselle rekisterinpitäjälle. Mikäli mahdollista, rekisterinpitäjä voi luovuttaa tiedot itse tarvittaessa eteenpäin toiselle reksiterinpitäjälle tai luovuttaa käsitellyt tiedot rekisteröidylle henkilölle, joka tämän jälkeen itse toimittaa tiedot eteenpäin. Tietojen käsittelyn jälkeen tiedot tulee arkistoida rekisterinpitäjän toimesta, mikäli tietojen säilyttäminen käsittelyn jälkeen on tarpeellista. Jos tietojen säilytys ei ole tarpeen, tulee tiedot poistaa sellaisella tavalla, että niihin ei poistamisen jälkeen päästä käsiksi.[59]

[58] EU:n yleinen tietosuoja-asetus
[59] EU:n yleinen tietosuoja-asetus



Kuvio 1. Tietojen keräämisprosessin elinkaari[60]

8.5 Tietoturvarikkomusten ilmoittaminen

Tietosuoja-asetuksen 33 ja 34 artikloissa määritetään rekisterinpitäjälle ilmoitusvelvollisuuden mahdollisten tietoturvarikkomusten sattuessa. Ilmoitus tulee tehdä rekisteröidyille henkilöille ja valvonnasta vastaavalle viranomaiselle 72 tunnin kuluessa tietoturvarikkomuksen havaitsemisesta. Aiemmin ei rekisterinpitäjän ole tarvinnut ilmoittaa mahdollisista tietoturvarikkomuksista. Mikäli ilmoitus täytyy tehdä, tulee rekisteröidyille ilmoittaa edellisen luvun mukaisesti. Valvontaviranomaisen ilmoitus eroaa siitä, mikä tehdään rekisteröidyille. Viranomaisille tulee ilmoittaa kuvaus tapahtuneesta ja mahdolliset rekisteröityneiden ryhmät ja lukumäärät sekä mahdolliset vaikutukset rekisteröidyille. Ilmoituksessa täytyy olla myös tietosuojavastaavan yhteystiedot sekä kuvaus toimista rekisterinpitäjän puolelta, joiden tavoitteena on ehkäistä tietorikkomuksen vaikutuksia.[61]

8.6 Sakot ja seuraukset

Valvontaviranomainen voi määrätä tietosuoja-asetuksen 83 artiklan mukaisesti rekisterinpitäjille tai henkilötietojen käsittelijöille sakkoja tai seuraamuksia, mikäli nämä eivät noudata

---

[60] EU:n yleinen tietosuoja-asetus. Ks. myös tietosuojavaltuutettu 2017.
[61] EU:n yleinen tietosuoja-asetus

tietosuoja-asetuksen velvoitteita rekisterinpitäjää kohtaan. Valvontaviranomaisen on varmistettava, että sakkojen määräämisessä noudatetaan tietosuoja-asetuksen 83 artiklan mukaisia määräyksiä oikeudenmukaisesti. Hallinnollisten sakkojen määräämisessä tulee ottaa huomioon, millainen rikkomus on ollut kyseessä sekä miten vakava kyseinen rikkomus on ollut luonteeltaan ja kauanko rikkomus on kestänyt. Rikkomuksen yhteydessä tulee myös huomioida rekisteröityjen henkilöiden määrä, joita rikkomus koskee, rekisteröidyille aiheutunut vahinko, rekisterinpitäjän vastuu rikkomuksen kohdalla ja mahdolliset lieventämistoimet, jotka rekisterinpitäjä on toteuttanut ehkäistäkseen rikkomuksesta aiheutunutta haittaa. Sakon enimmäismäärä on 20 miljoonaa euroa tai 4 % yrityksen maailmanlaajuisesta kokonaisliikevaihdosta perustuen edellisen tilikauden tilinpäätökseen. Mikäli sakkoja ei käytetä rangaistuksena, voidaan esimerkiksi laiminlyönnin seurauksena kieltää käsittely, kunnes vaadittavat toimet ovat suoritettu.[62]

9 Tietosuoja-asetuksen suhde Suomen lainsäädäntöön

EU:n tietosuoja-asetus vaikuttaa Suomen henkilötietolakiin lisäämällä jo olemassa olevaan henkilötietolakiin tietosuoja-asetuksessa tulevia säädöksiä. EU:n uusi tietosuoja-asetus on määritetty erityisesti digitaalisesti tallennettavia tietoja huomioiden. Suomen henkilötietolaki (523/1999) määrittelee ison osan EU:n tietosuoja-asetuksessa olevista säädöksistä. Suurimpana lisäyksenä tietosuoja-asetus lisää rekisteröidyille henkilöille uusia oikeuksia ja rekisterinpitäjille uusia velvoitteita.[63]

Rekisteröidyille henkilöille uusia oikeuksia ovat muun muassa rekisteröityjen henkilöiden helpompi pääsy omiin tietoihinsa ja niiden muuttaminen tai siirtäminen järjestelmästä toiseen. Rekisterinpitäjille uusia velvollisuuksia ovat muun muassa tarkemmat määräykset tallennettua tietoa kohtaan ja uudet rangaistukset lainsäädäntöä rikkomista kohtaan.[64]

9.1 Lainsäädännön valmistelu tietosuoja-asetukselle

EU:n yleistä tietosuoja-asetusta varten oikeusministeriö asetti työryhmän helmikuussa 2016. Tämän työryhmän tarkoituksena oli valmistella ehdotus lainsäädännön liikkumavaran käytöstä

[62] EU:n yleinen tietosuoja-asetus
[63] EU:n yleinen tietosuoja-asetus
[64] EU:n yleinen tietosuoja-asetus

ja Suomen lainsäädännön saattaminen asetuksen mukaisesti. Työryhmän tehtävänä oli tehdä ehdotus mahdollisesta yleislaista henkilötietolain tilalle, valmistella ehdotus kansallisesta valvontaviranomaisesta tietosuoja-asetusta varten, tehdä lakisääteiset linjaukset kansallisen lainsäädännön liikkumavarsta tietosuoja-asetusta varten ja koordinoida sekä avustaa henkilötietojen käsittelyn erityislainsäädännön tarkistamisessa.[65]

Oikeusministeriön työryhmän tavoitteena on pyrkiä yhtenäistämään Suomen lainsäädäntöä eurooppalaisen lainsäädännön mukaiseksi valtiollisen liikkumavaran suhteessa. Työryhmän tavoitteena on myös vahvistaa kansalaisten oikeuksia tietojenkäsittelyssä, varmistaa tietojen sujuva liikkuvuus viranomaisten käsittelyssä ja pyrkiä tarpeettoman eristyissääntelyn luopumiseen. Liikkumavarasta tulee säätää tarpeeksi tarkasti, jotta julkisen sektorin henkilötietojen käsittelijät pystyvät toimimaan lakisääteisten velvoitteidensa mukaisesti. Käsittely ei kuitenkaan saa olla liian yksityiskohtaista, koska tietosuoja-asetus on Euroopan Unionin asetuksen tasolla ja se tulee liittää jäsenvaltion lainsäädäntöön sellaisenaan.[66]

Työryhmä on suunnitellut uutta yleislakia, jonka tavoitteena olisi mahdollisesti korvata nykyinen henkilötietolaki, joka tulee osaltaan korvautumaan EU:n yleisen tietosuoja-asetuksen myötä. Tämä yleislaki tulee koskemana tietosuoja-asetuksen sellaisia määräyksiä, jossa kansallista liikkumavaraa tulee käyttää. Yleislain suunnitteluun käytetään nykyistä henkilötietolakia.[67]

Erityislainsäädännön kohdalla Suomessa on yksityiskohtaista eristyissääntelyä eri sektoreiden kohdalla. Työryhmän selvityksessä on löytynyt 600-700 säädöstä henkilötietojen käsittelyyn liittyen eri sektoreilla. Näitä käytiin läpi kesän 2016 aikana muiden tutkijoiden kanssa. Selvityksestä huomattiin, että nämä sääntelyt ovat muutamaa poikkeusta lukuun ottamatta tietosuoja-asetuksen mukaisia. Ongelmaksi muodostui sen sijaan säädösten määrä, koska useat yksityiskohtaisista säädöksistä olivat tarpeettoman yksityiskohtaisia ja epäyhdenmukaisia. Työryhmän olisi tarkoitus poistaa turhaa erityissääntelyä sektorikohtaisesti.[68]

9.2 Tietosuojavaltuutettu

[65] Nurmi 2017, ks. myös oikeusministeriön työryhmä. 2017, 17.
[66] Nurmi 2017, ks. myös oikeusministeriön työryhmä. 2017, 73.
[67] Nurmi 2017, ks. myös oikeusministeriön työryhmä. 2017, 119.
[68] Nurmi 2017, ks. myös oikeusministeriön työryhmä. 2017, 74.

Tietosuoja-asetus määrittää kansallisen valvontaviranomaisen tehtävät ja vastuut. Nämä vastuut valvontaviranomaiselle lisääntyvät aikaisempiin verrattuna ja valvontaviranomaiselle asetetaan myös uusia vaatimuksia, kuten riippumattomuus muista toimielimistä. Valvontaviranomaisen menettelytapoja ei kuitenkaan säädetä tietosuoja-asetuksessa, vaan nämä jäävät kansallisen lainsäädännön vastuulle. Työryhmän ehdotuksessa valvontaviranomaisena tulisi toimimaan tietosuojavaltuutettu, kuten nykytilanteessakin, mutta merkittävien päätöksien suhteen konsultoitaisiin useammasta henkilöstä koostuvasta kollegiosta. Tietosuoja-asetus määrittää myös valvontaviranomaiselle tehtävän suorittamista vaativat resurssit ja tästä tulee jokaisen EU-jäsenmaan huolehtia omalta osaltaan.[69]

Tämänhetkisen lainsäädännön mukaisesti tietosuojavaltuutetulla on oikeus tarkastaa henkilörekistereitä ja käyttää rekisterien tarkistuksessa apunaan asiantuntijoita. Tarkastuksen suorittamista varten tietosuojavaltuutetulla on oikeus päästä rekisterinpitäjän omistamiin huoneistoihin, joissa henkilötietoja käsitellään ja saada tarketukseen avuksi kaikki tietosuojavaltuutetun tarvitsemat laitteet. Kotirauhan määritelmään kuuluvaan tilaan saa tehdä tarkistuksen vain silloin, jos on syy epäillä henkilötietojen käsittelyyn liittyvien säännösten rikkomisen. Tarkastus tulee tehdä ilman suurempaa haittaa tai kustannuksia rekisterinpitäjän toiminnalle. Tarkastusoikeus ei koske elinkeinoharjoittajia yleisesti, vaan niitä huoneistoja, joissa tietojenkäsittely tapahtuu tai jossa henkilötietoja säilytetään. Esimerkiksi asianajotoimistojen kohdalla tarkastuksen kohteena voivat vain olla toimistossa säilytettävät tiedot ja laitteet, sillä asianajotoimistot eivät yleensä käsittele henkilötietoja. Jos tietosuojavaltuutettu tarkastaisi asianajotoimiston, tulisi tämä tehdä ilman tarpeetonta haittaa asianajotoimiston toiminnalle. Tarkastuksessa tulisi ottaa huomioon, että asiakastiedot pysyvät salaisena koko tarkastuksen ajan.[70]

Tietosuoja-asetuksen 58 artiklan mukaan jokaisella valvontaviranomaisella on oikeus päästä kaikkiin rekisterinpitäjän tallentamiin tietoihin, tietojenkäsittelijän tiloihin sekä oikeus päästä tietojenkäsittelyssä käytettyyn laitteistoon ja mihin tahansa tietojenkäsittelyn vaiheeseen Euroopan Unionin tai sen jäsenvaltion prosessioikeuden käsittelyn mukaisesti. Tietosuoja-asetuksen mukainen tarkastusoikeus vastaa jo olemassa olevaa tietosuojavaltuutetun tarkastusoikeutta, joten tietosuoja-asetus ei lisää valvontaviranomaisen oikeutta tarkastaa rekisterinpitäjän toimitiloja tai asianajotoimistojen toimitiloja.[71]

---

[69] Nurmi 2017, ks. myös oikeusministeriön työryhmä. 2017, 76.
[70] Ilveskero, M. 2017, 246.
[71] Ilveskero, M. 2017, 246.

10 Johtopäätökset ja tulokset

Suomen henkilötietolaki kattaa jo osaltaan EU tietosuoja-asetuksen mukana tulevia asioita, joten Suomen henkilötietolaki on EU-tasolla jo hyvin nykyaikainen. Tällä hetkellä henkilötietolaki sisältää jo osan EU tietosuoja-asetuksen määrittämistä velvollisuuksista rekisterinpitäjälle, kuten huolellisuusvelvollisuuden henkilötietojen käsittelyn yhteydessä, tietojen käsittelyn käyttötarkoitussidonnaisuuden ja ilmoitusvelvollisuuden tietosuojavaltuutetulle henkilötietojen automaattiseen käsittelyyn liittyen. Uutena velvollisuutena rekisterinpitäjälle tulee velvollisuus ilmoittaa tietoturvarikkomuksista valvontaviranomaiselle ja niille, keitä rikkomus koskee. Ilmoitusvelvollisuutta tietoturvarikkomuksista ei ole aiemmin määritetty Suomen henkilötietolaissa.

Tietosuoja-asetus määrittää myös uudenlaisia sanktioita, kuten sakkorangaistuksen, rekisterinpitäjälle tai henkilötietojen käsittelijälle, mikäli tämä ei noudata yleisen tietosuoja-asetuksen mukaisia määräyksiä tai jättää esimerkiksi ilmoittamatta määräajan kuluessa tapahtuneesta tietoturvaloukkauksesta. Rekisterinpitäjän osoitusvelvollisuus on myös uusi määräys tietosuoja-asetuksen osalta. Rekisterinpitäjän tulee tarvittaessa näyttää toteen, että on pystynyt noudattamaan ja ylläpitämään tietosuoja-asetuksen mukaisia määräyksiä henkilötietojen käsittelyn ja niiden suojaamisen suhteen toiminnassaan.

Myös osa tietosuoja-asetuksen määrittämistä rekisteröidyn henkilön oikeuksista löytyy jo olemassa olevasta Suomen henkilötietolaista. Suomen henkilötietolain mukaan rekisteröidyllä henkilöllä on oikeus saada tieto henkilötietojen käsittelijästä, rekisteröidyn tietojen käsittelyn tarkoituksesta, mahdollisesta tietojen luovutuksesta ja siitä, mitä tietoja rekisteröidystä henkilöstä käsitellään reksiterinpitäjän toimesta. Henkilötietolain mukaan rekisteröidyllä henkilöllä on myös oikeus tarkastaa ne tiedot, jotka hänestä ovat rekisterinpitäjällä ja saada oikeus oikaista virheellistä tai vanhentunutta tietoa, mikäli rekisterinpitäjällä on sellaista tietoa rekisteröidystä henkilöstä. Myös automatisoidusta päätöksenteosta on Suomen henkilötietolaissa pykälä, jonka mukaan automatisoitua päätöksentekoa saa käyttää vain, kun siihen on lakiperusteinen syy. Uusina oikeuksina rekisteröidylle henkilölle on esimerkiksi henkilötietojen käsittelyn läpinäkyvyyden parantaminen ja oikeus tietojen siirtoon rekisterinpitäjältä toiselle.

Euroopan unionin yleinen tietosuoja-asetus ylläpitää tietosuojaan ja henkilötietojen käsittelyyn liittyviä periaatteita Euroopan unionin jäsenmaissa. Tietosuoja-asetus parantaa ja nykyaikaistaa Euroopan unionin peruskirjassa määritettyä henkilötietojen suojaa käsittelevää artiklaa ja tietosuoja-asetuksen tavoitteena on ylläpitää tietosuojaa digitaalisuuden ja tietotekniikan kehittyessä.

Euroopan unionin tietosuoja-asetus yhtenäistää henkilötietojen käsittelyyn liittyviä käytänteitä koko unionin alueella ja yhtenäistämisen tavoitteena on vahvistaa rekisteröityjen henkilöiden oikeuksia ja vapauksia henkilötietojen käsittelyprosessiin liittyen sekä lisätä tietojen vapaata liikkuvuutta. Tietosuoja-asetus sisältää myös uusia vastuita ja velvollisuuksia henkilötietojen käsittelijöille ja rekisterinpitäjille, joihin tulee tietojen käsittelijöiden toimesta kiinnittää huomiota. Rekisterinpitäjien ja henkilötietojen käsittelijöiden toimintaa valvotaan ja toiminnan tulee vastata niitä määräyksiä, jotka on asetettu tietosuoja-asetuksen toimesta. Mikäli rekisterinpitäjä tai henkilötietojen käsittelijä ei noudata näitä toimia, voidaan tietojen käsittelijälle langettaa vakavan rikkomuksen kohdalla sakkorangaistus.

Euroopan unionin tietosuoja-asetuksella on vaikutus kaikkien julkisten ja yksityisen sektorin henkilötietojen kerääjiin. Vaikutukset voivat vaihdella riippuen yrityksestä ja siitä, miten tietoja kerätään. Yhtenäistä kaikille henkilötietojen kerääjille on ottaa uudet rekisteröityjen henkilöiden oikeudet henkilötietojen käsittelyn yhteydessä ja noudattaa uusia määräyksiä ja velvollisuuksia, jotka koskevat henkilötietojen kerääjiä. Eroavaisuutena on esimerkiksi tietosuojavastaavan nimittäminen yritykselle. Tietosuojavastaava tulee nimittää julkisen sektorin toimijalle tai sellaiselle toimijalle, joiden toiminta sisältää laajamittaista rekisteröityjen henkilöiden seuraamista. Vaikka erillistä tietosuojavastaavaa ei tulisikaan nimittää yritykseen, tulee silti jonkun yrityksen sisällä vastata tietosuojan toteutumisesta yrityksen sisäisen toiminnan yhteydessä.

Opinnäytetyön kohteena oleva Hyvinkääläinen mikroyritys, Neoport Oy, joutuu myös valmistautumaan tietosuoja-asetuksen uusiin määräyksiin. Yrityksessä käsiteltävät tiedot ovat asiakasrekisterin tietoja, joten tämä tulee ottaa huomioon, kun yrityksessä suunnitellaan tietosuoja-asetuksen aiheuttamia muutoksia. Tietosuojavastaavaa ei erikseen tarvitse nimittää yritykseen, vaan riittää että yrityksen toimitusjohtaja vastaa tietosuoja-asetuksen määräysten toteutumisesta ja ylläpitämisestä yrityksen toiminnassa. Kaikki uudet rekisteröityjen henkilöiden oikeudet eivät myöskään päde kyseessä olevan mikroyrityksen tapauksessa, vaan ne jotka tulee ottaa huomioon, on erikseen mainittu yrityksen suunnitelmassa.

Yritykselle toteutettiin alustava suunnitelma tietosuoja-asetusta varten, joka sisälsi pääkohdat uusista muutoksista ja miten yrityksen tulisi varautua toiminnassaan tietosuoja-asetuksen määräyksiin siirtymäajan kuluessa. Suunnitelma sai positiivista palautetta yrityksen puolelta. Yrityksen toimitusjohtajan mukaan suunnitelmasta selvisi yritystä varten, mitä muuttuu tietosuoja-asetuksen myötä ja mihin kaikkeen yrityksen tulee toiminnassaan varautua. Suunnitelma sisälsi myös tietoa uusista määräyksistä, joita ei ennen tietosuoja-asetusta tarvinnut huomioida yrityksen toiminnassa ja tämän avulla yrityksen on helpompi muuttaa toimintaansa tietosuoja-asetuksen määräysten ja velvollisuuksien mukaiseksi.

Lähteet

Kirjallisuus ja artikkelit

Alén-Savikko, A. 2017. Analyysia ja visioita EU:n tietosuojasääntelystä. Lakimies 2/2017. 299, 300, 301.

Hallberg, P., Karapuu, H., Ojanen, T., Scheinin, M., Tuori, K. & Viljanen V-P 2005. Perusoikeudet. WSOYpro: Helsinki

Hirsjärvi, S., Remes, P., Sajavaara, P. & Sinivuori, E. 2014. Tutki ja kirjoita 19. painos. Bookwell Oy: Porvoo.

Husa, J., Mutanen, A & Pohjolainen, T. 2010. Kirjoitetaan juridiikkaa 3. painos. Kariston Kirjapaino Oy: Hämeenlinna 2010.

Ilveskero, M. 2017. Eräiden viranomaisten pääsy salassa pidettäviin asiakirjoihin, Defensor Legis 2/2017. 246.

Nurmi, P. Oikeusministeriö. EU:n yleisen tietosuoja-asetuksen Suomen malli. 2017. Viitattu 28.1.2018 http://oikeusministerio.fi/blogi/-/asset_publisher/sT2AXfpZ5m0k/blog/pekka-nurmi-eu-n-yleisen-tietosuoja-asetuksen-suomen-malli

Ojanen, T. 2016. EU-oikeuden perusteita 3., uudistettu laitos. Edita: Helsinki.

Raitio, J. 2016.Euroopan Unionin Oikeus. Talentum Pro: Helsinki.

Voutilainen, T. 2012 Oikeus tietoon: informaatio-oikeuden perusteet 1.painos. Bookwell Oy: Porvoo.

Virallislähteet

EU:n yleinen tietosuoja-asetus
http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CONSIL:ST_5455_2016_INIT&from=EN

Miten valmistautua EU:n tietosuoja-asetukseen, Tietosuojavaltuutettu. 4/2017. Viitattu 7.11.2017
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

EU-tietosuojan kokonaisuudistus, Valtiovarainministeriö. Viitattu 8.11.2017

https://www.vahtiohje.fi/c/document_library/get_file?uuid=c97ee414-1fc0-4a91-969c-2ef0657605d1&groupId=10128

Euroopan Unionin perusoikeuskirja
http://www.europarl.europa.eu/charter/pdf/text_fi.pdf

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. 2017.
http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80098/OMML_35_2017_EUn_yleinen_tietosuoja.pdf

Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista, Tietosuojatyöryhmä. 10/2017.
http://tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/ibVehxmcp/Ohjeet_tietosuojaa_koskevasta_vaikutustenarvioinnista.pdf

HE 309/1993 Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta. Viitattu 29.1.2018 https://www.finlex.fi/fi/esitykset/he/1993/19930309

HE 208/2016 Hallituksen esitys eduskunnalle laiksi kirjanpitolain muuttamisesta ja eräiksi siihen liittyviksi laeiksi. Viitattu 29.1.2018 https://www.finlex.fi/fi/esitykset/he/2016/20160208

Tilastokeskuksen määritelmä mikroyrityksestä. 2016.
http://www.stat.fi/meta/kas/mikroyritys.html

Kuviot

Liitteet

Liite 1: EU-Tietosuoja-asetukseen valmistautuminen Neoport OY:lle

EU-Tietosuoja-asetukseen valmistautuminen Neoport OY:lle

EU:n uudella tietosuoja-asetuksella tarkoitetaan Euroopan unionin tietosuojalainsäädännön uudistamista, jotta tietosuojakäytäntö vastaa teknologian kehitykseen ja globalisaatioon liittyviä haasteita. Tämä uusi tietosuoja-asetus tulee voimaan 28.5.2018, johon mennessä yritysten on tullut varautua asetuksen mukana tuleviin vaatimuksiin.

Uuden tietosuoja-asetuksen tavoitteena on lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä, täten parantaen rekisteröityjen henkilöiden oikeuksien toteutumista ja henkilötietojen käsittelyn valvontaa. Tietosuoja-asetusta sovelletaan sekä yksityisellä ja julkisella sektorilla aina kun käsitellään henkilötietoja, käsittelyn laajuudesta riippumatta.

Neoport Oy kerää tietoja omaan asiakasrekisteriinsä, joka sisältää asiakkaiden nimen, osoitteen, puhelinnumeron ja mahdolliset maksutiedot. Yritys ei tallenna asiakkaiden syntymäaikoja tai henkilötunnuksia.

1. **Yrityksen henkilötietojen käsittelyn arviointi**

Kun arvioidaan tietosuoja-asetuksen vaikutuksia yrityksessä, tulisi hahmottaa millä tavalla ja millä perusteella henkilötietoja kerätään tällä hetkellä yrityksessä. Tässä tapauksessa Neoportilla voitaisiin kuvata, millaisia henkilötietoja yrityksessä kerätään, miten tietojenkeruun riskienhallinta ja suojaaminen on toteutettu ja miten rekisteröityjen oikeudet on otettu huomioon.

Tämän alustavan selvityksen jälkeen tulisi yrityksessä ottaa huomioon, millä tavalla käytäntöä tulee muuttaa, jotta se vastaisi EU-asetuksen määräyksiä. Tässä kohtaa tulisi miettiä, millä tavalla Neoportin tarvitsee mahdollisesti muuttaa nykyisiä käytänteitään. Uusia määräyksiä käsitellään tarkemmin tämän suunnitelman kappaleessa kaksi.

2. **Tietosuojaperiaatteet ja niiden toteuttaminen**

Tietosuoja-asetus määrittää tietosuojaperiaatteita, jotka koskevat henkilötietojen käsittelijän toimenpiteitä rekisteröityjen oikeudet huomioon ottaen. Periaatteet vastaavat pitkälti niitä, mitkä ovat jo Suomen henkilötietolaissa, mutta asetus tarkentaa niitä omalta osaltaan. Tietosuojaperiaatteita asetuksessa ovat:

– käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys, jolla tarkoitetaan tietojenkäsittelyn määräyksien noudattamista rekisteröidyn henkilön kannalta.

– käyttötarkoitussidonnaisuus, jolla tarkoitetaan tietojenkäsittelyyn perustuvaa käyttötarkoitusta, eli jokin lainmukainen peruste, joka on henkilötietojen käyttötarkoitukselle.

– tietojen minimointi, jolla tarkoitetaan vain sellaisten tietojen säilyttämistä, jotka ovat tietojenkäsittelijälle tarpeen. Tarpeetonta ylimääräistä tietoa ei tule kerätä.

– tietojen täsmällisyys, jolla tarkoitetaan kerättyjen tietojen ajantasaisuutta ja tietojen paikkaansa pitävyyttä.

– tietojen säilytyksen rajoittaminen, jolla tarkoitetaan tietojen säilyttämistä niin kauan kuin on tarpeellista, jonka jälkeen tiedot tulee poistaa, kun niitä ei enää tarvita.

– tietojen eheys ja luottamuksellisuus, jolla tarkoitetaan tietojenkäsittelyn luottamuksellisuutta ja tietojen salassapitoa ulkopuolisilta henkilöiltä.

– rekisterinpitäjän osoitusvelvollisuus, jolla tarkoitetaan sellaisia toimia rekisterinpitäjän puolelta, jonka avulla voidaan näyttää toteen tietosuoja-asetuksen noudattaminen. Rekisterinpitäjän tulee huolehtia näiden periaatteiden noudattamisesta tietojenkäsittelyssä. Rekisterinpitäjän osoitusvelvollisuus tarkoittaa, että rekisterinpitäjän on tarvittaessa pystyttävä osoittamaan näiden periaatteiden toteutuminen omassa toiminnassaan.

Tietosuoja-asetus edellyttää myös sisäänrakennetun tietosuojan noudattamista. Tällä tarkoitetaan aiemmin mainittujen periaatteiden noudattamista tietojenkäsittelyn yhteydessä. Tässä tapauksessa Neoport Oy:n tulee ottaa huomioon sellaiset toimenpiteet tietojenkäsittelyn yhteyteen, jotta nämä periaatteet toteutuvat henkilötietojen käsittelyssä. Yrityksen tulee itse miettiä, millä tavalla tietosuojaperiaatteet saadaan toteutettua parhaiten, ottaen huomioon yrityksen käytössä olevan teknologian ja resurssit.

Osoitusvelvollisuus tuo tietojenkäsittelijälle dokumentointivelvollisuuksia henkilötietojen käsittelyä varten. Asetuksen mukaisesti henkilötietojen käsittelijöiden on ylläpidettävä selostetta käsittelemistään henkilötiedoista. Neoport Oy:llä tämä voitaisiin toteuttaa ylläpitämällä yrityksen omaa selostetta tietojenkäsittelystä ja tällä tavoin osoittaa toiminnan olevan asetuksen mukaista.

3. Riskiperusteinen lähestymistapa

Tietosuoja-asetuksessa on määräys riskiperusteisesta lähestymistavasta, joka koskee henkilötietojen tarvittavia suojaustoimia ja rekisteröityjen oikeuksien toteutumista. Näistä riskeistä tulee tehdä arvio, minkälaisia vahinkoja voi rekisteröidyille tulla, mikäli tiedot joutuvat vaarannetuiksi. Neoport Oy:llä ei kerätä henkilötunnuksia tai syntymäaikoja, joka itsessään toimii ennaltaehkäisijänä riskien kohdalla. Yrityksen tulee kuitenkin varmistaa, että kerätyt tiedot pysyvät tallessa ja tämä voidaan näyttää tarvittaessa toteen.

4. Tietojenkäsittelyn oikeusperusteet

Tietosuoja-asetuksen mukaisesti on henkilötietojen käsittelylle oltava jokin lakisääteinen peruste. Rekisterinpitäjän tulee huomioida tietosuoja-asetuksen mahdolliset vaikutukset tietojenkäsittelyn oikeudellisiin perusteisiin. Neoport Oy:n tapauksessa tämä oikeusperusta perustuu Suomen henkilötietolain 8 § 5-momenttiin, jonka mukaan henkilötietoja saa käsitellä, jos rekisteröidyllä on asiakas- tai palvelussuhteen, jäsenyyden tai muun niihin verrattavan suhteen vuoksi asiallinen yhteys rekisterinpitäjän toimintaan, joka täyttyy tässä kohtaa Neoport Oy:n asiakasrekisterin kohdalla.

5. Rekisteröidyn oikeudet ja niiden toteutuminen

Rekisterinpitäjän tulee ottaa huomioon uudet rekisteröityjen henkilöiden oikeudet, jotka tulevat käyttöön tietosuoja-asetuksen mukana. Ne ovat suurelta osin samanlaisia, kuin nykyisen henkilötietolain määrittelyt, mutta niitä tarkennetaan tietosuoja-asetuksen yhteydessä. Käsittelyn oikeusperuste vaikuttaa osaltaan, mitä rekisteröityjen oikeuksia tulee huomioida tietojenkäsittelyssä. Rekisterinpitäjän tulee selvittää mitä oikeuksia tulee huomioida ja miten niitä toteuttaa. Neoport Oy:n kohdalla tietoja ei varsinaisesti käsitellä mitään varten ja ne ovat asiakasrekisterissä tallessa, joten kaikki rekisteröityjen henkilöiden oikeudet eivät päde tässä tapauksessa. Ne jotka tulee huomioida, ovat seuraavissa alaotsikoissa.

Rekisteröidyn oikeus omiin tietoihinsa

Rekisteröidyllä henkilöllä on oikeus esittää pyyntö rekisterinpitäjälle ja saada rekisterinpitäjältä kopio omista tiedoistaan, jotka on tallennettu rekisterinpitäjän puolelle. Rekisterinpitäjän tulee pyynnön saadessaan varmistaa tietojen saajan henkilöllisyys. Neoport Oy:n kohdalla asiakasrekisterin henkilö voi pyytää kopiota omista tallennetuista tiedoistaan, jotka tulee lähettää asiakkaalle kuukauden kuluessa pyynnön saapumisesta. Tietosuoja-asetuksen myötä rekisteröity voi pyytää oikaisemaan omia tallennettuja tietojaan tai pyytää poistamaan ne rekisteristä kokonaan.

Oikeus siirtää tietoja

Tietosuoja-asetuksen mukaan rekisteröity voi siirtää tietonsa toiselle rekisterinpitäjälle, siltä jolle tiedot on toimitettu. Tiedot tulee siirtää jäsennellyssä ja selkeässä muodossa toiselle rekisterinpitäjälle. Toisen rekisterinpitäjän on mahdollista saada tiedot suoraan siirrettynä. Oikeus tietojen siirtoon on silloin, jos tietojenkäsittely perustuu suostumukseen. Neoportin tapauksessa asiakas voi pyytää siirtämään tietojaan toiseen asiakasrekisteriin, jos asiakas on yksityisasiakas, jonka tiedot ovat Neoportilla.

6. Tietoturva

Rekisterinpitäjän on selvitettävä, vastaako tämän tietoturva tietosuoja-asetuksen periaatteita. Tietojenkäsittelyn riskit on arvioitava ja näihin varauduttava rekisterinpitäjän puolelta. Toimenpiteiden avulla varmistetaan nykyteknologiaa ja uusinta tekniikkaa vastaava tietoturvataso. Tietojen suojaamisesta on huolehdittava jokaisessa tietojenkäsittelyn vaiheessa. Neoport Oy:n kohdalla tämä tarkoittaa sitä, että kun tiedot lisätään asiakasrekisteriin, tulee huolehtia, etteivät niihin pääse ulkopuoliset henkilöt käsiksi ja että ne säilyvät suojattuna niin kauan kuin asiakas on asiakassuhteessa Neoport Oy:n kanssa.

Tietosuoja-asetukseen valmistautuessa tulee myös varautua tietoturvaloukkauksiin, jolla tarkoitetaan vahingollista tai tahallista lainvastaista toimintaa, joka kohdistuu henkilötietoihin, kuten esimerkiksi tietojen häviäminen tai tuhoutuminen taikka luvaton pääsy tietoihin. Mikäli tällainen tapahtuu, tulee rekisterinpitäjän ilmoittaa siitä valvontaviranomaiselle 72 tunnin kuluessa. Ilmoitusta ei tarvitse tehdä, mikäli on todennäköistä, ettei siitä aiheudu haittaa rekisteröidyille henkilöille. Rekisterinpitäjän tulee myös ilmoittaa rekisteröidyille henkilöille mahdollisista tietoturvarikkomuksista, mikäli rekisteröidyn oikeuksille aiheutuu korkea riski. Kaikki tietoturvaloukkaukseen liittyvät seikat tulee dokumentoida rekisterinpitäjän toimesta, sekä mahdolliset vaikutukset ja korjaustoimenpiteet. Tämän dokumentoinnin perusteella valvotaan myös ilmoitusvelvollisuuden toteutumista.

Tietosuojavastaavan nimittäminen on myös uusi määräys, joka tulee tietosuoja-asetuksen mukana. Tietosuojavastaavan nimittäminen ei ole pakollista Neoport Oy:n tapauksessa. Neoport Oy on sen verran pieni yritys, joten se ei täytä niitä vaatimuksia, jonka perusteella tulisi nimittää tietosuojavastaava. Vaikka yritykselle ei tarvitse nimittää erillistä tietosuojavastaavaa, tulee yrityksellä olla kuitenkin vastuuhenkilö tietosuoja-asetuksen asioista. Tässä tapauksessa tietosuojavastaavan toimia voi hyvin hoitaa yrityksen omistaja.

Lähde: **http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuoja-valtuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf**