EU:n yleinen tietosuoja-asetus henkilökuljetusyrityksen toiminnassa

Katja Kataja

2018 Laurea

Laurea-ammattikorkeakoulu

EU:n yleinen tietosuoja-asetus henkilökuljetusyrityksen toiminnassa

Katja Kataja
Liiketalous
Oikeudellinen osaaminen
Opinnäytetyö
Joulukuu, 2018

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

Katja Kataja

EU:n yleinen tietosuoja-asetus henkilökuljetusyrityksen toiminnassa

Vuosi 2018 Sivumäärä 90

Eurooppalainen henkilötietolainsäädäntö on suuressa muutoksessa Euroopan Unionissa käynnissä olevan tietosuojan kokonaisuudistuksen myötä. Toukokuussa 2018 sovellettavaksi tullut Euroopan Unionin yleinen tietosuoja-asetus (General Data Protection Regulation eli GDPR) on muuttanut myös suomalaisten yritysten velvollisuuksia henkilötietojen käsittelyn suhteen.

Opinnäytetyön tavoitteena oli luoda henkilökuljetuksia operoivalle kuljetusyritykselle valmius noudattaa toiminnassaan tietosuoja-asetusta ja toteuttaa asetuksen sille osoittamat velvoitteet. Yrityksen tuli voida tarvittaessa osoittaa tietosuojaperiaatteiden noudattaminen ja pystyä hallitsemaan henkilötietojen elinkaarta.

Työn tietoperustassa kuvataan tietosuoja-asetus pääpiirteittäin. Erityisesti keskitytään tietosuojaperiaatteisiin, tiedon elinkaaren hallintaan sekä asetuksen mukaisiin rooleihin. Työn keskeisinä lähteinä toimivat tietosuoja-asetus, Hallituksen esitys kansalliseksi tietosuojalaiksi (HE 9/2018), tietosuojavaltuutetun toimiston julkaisemat ohjemateriaalit sekä Valtiovarainministeriön VAHTI-työryhmän ohjeistukset.

Työn toiminnallisessa osassa esitellään kuljetusyritykselle tehty työ. Aluksi kartoitettiin kuljetusyrityksen nykytila mallintamalla henkilötiedon käsittelyn prosessit. Samalla kartoitettiin käsiteltävien henkilötietojen tyypit ja käsittelyperusteet. Prosessimallinnuksen perusteella tarkasteltiin henkilötiedon elinkaarta ja sen hallittavuutta. Henkilötiedon käsittelyn nykytilaa verrattiin tietosuoja-asetuksen edellyttämään tavoitetilaan.

Työn tuloksena syntyi materiaalia, jonka avulla yritys voi jatkossa täyttää tietosuoja-asetuksen mukaisen osoitusvelvollisuutensa. Kuljetusyritys sai työn tuloksena myös perustellun arvion tietosuojavastaavan tarpeesta ja konkreettisia kehitysehdotuksia toimintansa tehostamiseksi. Opinnäytetyöprosessin myötä yrityksen henkilökunnan kyky käsitellä henkilötietoa asetuksen edellytysten mukaisesti kasvoi. Haastetta työn toteutukseen loi lainsäädännön eräänlainen välitila, jossa kansallinen tietosuojalaki on vielä eduskunnan käsittelyssä. Näin ollen varmaa tietoa lain sisällöstä ei siis ollut saatavilla niiltä osin joissa tietosuoja-asetus jättää jäsenvaltioille kansallista liikkumavaraa.

Asiasanat: tietosuoja, GDPR, tietosuoja-asetus, osoitusvelvollisuus, henkilötiedon käsittely

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

Katja Kataja

European Union's General Data Protect Regulation and what it means to passenger transport company

Year 2018 Pages 90

European personal data legislation is undergoing a major change due to the overall revision of data protection in the European Union. The General Data Protection Regulation (GDPR), which became applicable in May 2018, has also changed the responsibilities of Finnish companies to deal with the processing of personal data.

The purpose of the thesis was to help a transport company to comply with the Data Protection Regulation in its activities and to implement the obligations imposed by the Regulation. The company should, if necessary, be able to demonstrate compliance with the data protection principles (accountability principle) and be able to control the life cycle of the personal data.

The theoretical part of the work describes the GDPR. Specific focus is on the principles relating to processing of personal data, the management of data life cycle and roles of the regulation. As a central source of work, I used the General Data Protection legislation, the Finnish Government's Proposal for a National Data Protection Act (HE 9/2018), the Guidance Documents published by the Office of the Data Protection Ombudsman and the VAHTI-guides published by the Ministry of Finance.

The functional part of the work presents the work done for the transport company. Initially, the current state of personal data managing was charted by modeling the process of processing personal data. At the same time, the types and processing criteria of the personal data processed were charted. Based on the process modeling, the life cycle of personal data and its manageability were examined. The status of data managing was compared with the target state by Data Protection Regulation.

The result of the work was a material that would enable the company to fulfill its assignment of accountability principle. After project the company's staff was able to process and handle personal data in a safe way. The company also received assessment of if they would have obligation to assign Data Protection Officer (DPO).

Keywords: data protection, data protection regulation, accountability principle

Sisällys

1 Johdanto 6
2 Tietosuoja-asetus yleisesti 8
2.1 Tietosuojaperiaatteet 12
2.2 Osoitusvelvollisuus 16
2.3 Informointivelvollisuus 20
3 Henkilötiedon käsittely 21
3.1 Henkilötiedon määritelmä ja rekisterin muodostuminen 23
3.2 Käsittelyn oikeusperuste 24
3.3 Erityiset henkilötiedot 27
3.4 Henkilötiedon elinkaari 29
3.5 Roolit 33
3.5.1 Rekisteröity 33
3.5.2 Rekisterinpitäjä 35
3.5.3 Käsittelijä 36
3.6 Sopimus henkilötietojen käsittelystä 38
3.7 Tietoturvaloukkauksesta ilmoittaminen 39
4 Sanktiot 41
5 Tietosuojavastaava 43
6 Tietosuoja-asetus henkilökuljetusyrityksen toiminnassa 45
6.1 Toimintaprosessit henkilökuljetuksissa 47
6.2 Kuvaus käsiteltävistä henkilötiedoista 50
6.3 Rekrytointi ja henkilöstön tiedot 51
6.4 Sopimukset 52
6.5 Roolit 53
7 Tulokset 54
7.1 Seloste käsittelytoimista 56
7.1.1 Käsittelyn oikeusperusteiden arviointi 57
7.1.2 Arvio tietosuojaperiaatteiden toteutumisesta 58
7.2 Henkilöstön koulutus ja ohjeistukset henkilöstölle 58
7.2.1 Salassapitosopimukset 63
7.3 Arvio tietosuojavastaavan tarpeesta 64
8 Yhteenveto 66
Lähteet 68

1 Johdanto

Henkilötietojen suojasta voidaan katsoa tulleen kansalaisen perusoikeus vuonna 2009 kun Euroopan unionin perusoikeuskirja[1] sai juridisesti sitovan aseman Lissabonin sopimuksen[2] ratifioinnin myötä. Tällöin perusoikeuskirjan 8 artiklassa mainitusta henkilötietojen suojasta tuli yksilön perusoikeus. Niin ikään Lissabonin sopimuksen myötä unionin primäärilainsäädäntöön[3] otettiin myös SEUT (Sopimus Euroopan unionin toiminnasta) 16 artikla, jonka mukaisesti jokaisella on oikeus henkilötietojensa suojaan. Samassa yhteydessä Euroopan parlamentille ja neuvostolle annetaan toimivalta säätää henkilötietojen käsittelyä määrittäviä sääntöjä henkilötietojen suojaamiseksi[4]. Euroopan unionin yleinen tietosuoja-asetus on annettu SEUT 16 artiklan 1 kohdan nojalla.[5]

Yleinen tietosuoja-asetus (GDPR)[6] tuli kaikissa EU:n jäsenmaissa sovellettavaksi oikeudeksi 25.5.2018. Sillä ajantasaistettiin ja yhtenäistettiin tietosuojasääntelyä, joka aiemmin perustui vuonna 1995 annettuun henkilötietodirektiiviin[7] sekä erinäisiin muihin EU-tasolla annettuihin säännöksiin. Yhtenäistämiselle oli tarvetta, sillä suuri osa tietosuoja-asetusta edeltävästä säätelystä oli peräisin ajalta ennen Lissabonin sopimuksen ratifiointia ja direktiivitasoisena annettua. Direktiivien implementointi eli täytäntöönpano[8] oli puolestaan johtanut jäsenvaltioissa kansallisesti hyvinkin toisistaan poikkeaviin tulkintoihin.[9]

Suomessa henkilötietodirektiivi toimeenpantiin henkilötietolailla (523/1999)[10]. Se on yleislaki, jonka lisäksi voimassa on ollut paljon erityislainsäädäntöä henkilötietojen käsittelyä koskien. Tietosuoja-asetuksen voimaanastumisen myötä Suomessa ollaan säätämässä uutta tietosuojalakia[11], joka tulee kumoamaan voimassa olleen henkilötietolain. Tietosuojalaki on sekin luonteeltaan yleislaki, mutta tulee sovellettavaksi rinnakkain tietosuoja-asetuksen kanssa.

---

[1] Euroopan unionin perusoikeuskirja, EUVL N:o C 326, 26.10.2012
[2] Lissabonin sopimus Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta, EUVL N:o C 306, 17.12.2017, s.1
[3] Finlex.fi, Lainlaatijan EU-opas 1.1, viitattu 2.11.2018
[4] Sopimus Euroopan unionin toiminnasta 16 artikla, EUVL N:o C 326, 26.10.2016, s. 47
[5] HE 9/2018, s. 27
[6] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, luonnollisen henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)
[7] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY
[8] Euroopan komissio, EU-lainsäädäntö ja sen soveltaminen, viitattu 2.11.2018
[9] HE 9/2018, s. 4
[10] HE 96/1998
[11] Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, HE 9/2018 vp

Kyseinen laki ei siis muodosta itsenäistä sääntelykokonaisuuttaan vaan täydentää ja täsmentää tietosuoja-asetusta kansalliselle lainsäätäjälle jätetyn harkintamarginaalin puitteissa mm. henkilötietojen käsittelyn oikeusperusteen osalta[12].[13]

Tietosuoja-asetuksella siis uudistetaan henkilötietojen käsittelyyn liittyvää lainsäädäntöä ja siksi sen käytännön vaikutukset ulottuvat muun muassa moneen yritykseen. Lähes kaikessa yritystoiminnassa käsitellään henkilötietoja - asiakkaiden, työntekijöiden tai usein molempien. Asetus tuo mukanaan uusi oikeuksia rekisteröidyille ja vastaavia velvoitteita rekisterinpitäjille. Uutta on mm. asetuksen mukanaan tuoma osoitusvelvollisuus[14], joka edellyttää henkilötietoihin kohdistettujen käsittelytoimien seurantaa ja dokumentointia.[15]

Tämän työn tarkoituksena on auttaa henkilökuljetuspalveluja tarjoavaa yritystä (myöhemmin kuljetusyritys) saattamaan toiminnassaan toteuttamansa henkilötietojen käsittely tietosuoja-asetuksen edellyttämälle tasolle. Työssäni pyrin antamaan lukijalle selkeän kuvan seuraavista asioista:

1. Yleiskuva tietosuoja-asetuksesta ja henkilötietojen käsittelyn määritelmästä
2. Roolien määräytyminen ja niiden oikeudet/velvoitteet[16]
3. Tietosuoja-asetuksen edellyttämä dokumentaatio
4. Kuljetusyrityksen kanssa tehty työ ja toimintamallit, jotka tukevat yritystä henkilötietojen oikeanlaisessa käsittelyssä ja osoitusvelvollisuuden täyttämisessä

Työssäni esimerkkinä käyttämäni kuljetusyritys operoi muun muassa koulukuljetuksia ja vammaispalvelulain mukaisia kuljetuksia. Yrityksen päivittäisessä toiminnassa käsitellään siis paljon henkilötietoja, joista osa kuuluu niin kutsuttuihin erityisiin henkilötietoryhmiin[17]. Toisaalta yritys tuottaa taksi- ja tilausajopalveluita, joissa liikkuvat tiedot ovat hyvin eri tyyppisiä. Lisäksi käsitellään alihankkijoiden, yhteistyökumppaneiden ja oman henkilöstön tietoja.

---

[12] Tilanteet, joissa oikeusperusteesta mahdollista säätää jäsenvaltion omassa lainsäädännössä ks. GDPR 6 artiklan 1 kohdan alakohdat c ja e
[13] HE 9/2018 s. 31
[14] GDPR 5 artikla 2 kohta
[15] Yrittäjät.fi, EU:n tietosuoja-asetus koskee kaikkia yrityksiä, viitattu 9.11.2018
[16] GDPR 4 artikla 1 ja 7-10 kohta
[17] GDPR 9 artikla

Työn aloittamisvaiheessa yrityksellä ei ole kokonaiskuvaa siitä, mitä tietosuoja-asetuksen osoitusvelvollisuus tarkoittaa käytännössä. Yrityksellä ei ole määriteltyä tietosuojapolitiikkaa, tiedon elinkaaren hallinnan mallia tai asetuksen edellyttämiä selosteita käsittelytoimista[18]. Kartoitan työssäni yrityksen nykytilan, käsiteltävät henkilötiedot, käsittelyn prosessit ja tarvittavat toimet perustuen yrityksen rooleihin tietojen käsittelyssä. Pyrin työssäni tuottamaan tuloksia, jotka ovat myös muiden tapausesimerkin kaltaisten kuljetusyritysten hyödynnettävissä joko suoraan tai pienellä soveltamisella.

Työn kirjoitusvaiheessa marraskuussa 2018 hallituksen esitys kansalliseksi tietosuojalaiksi on vielä käsittelyssä eduskunnassa. Vaikka henkilötietojen käsittelyyn sovelletaan tietosuoja-asetusta, on myös henkilötietolaki virallisesti edelleen voimassa. Henkilötietolaissa säädetään suhteellisen yksityiskohtaisesti esimerkiksi henkilötietojen käsittelyn oikeusperusteista. Henkilötietolakia ei kuitenkaan voida pitää enää ajankohtaisena lähteenä, sillä säädöshierarkiassa unionin asetuksella on etusijaperiaate suhteessa kansalliseen lakiin[19]. Asetuksen säädöstekstin lisäksi käytänkin pääasiallisena lähteenä tietosuojalain esityömateriaalia siltä osin kuin se on saatavilla[20]. Lisäksi käytän täydentävänä materiaalina asetuksen terminologian tulkinnassa Tietosuojatyöryhmän WP 29 antamia ohjeistuksia asetuksen soveltamisesta[21].

2 Tietosuoja-asetus yleisesti

Euroopan unionin yleinen tietosuoja-asetus eli GDPR (*General Data Protection Regulation)* (myöhemmin GDPR tai tietosuoja-asetus) on laki, jolla säädellään henkilötietojen käsittelyä Euroopan Unionin alueella[22]. Sillä kumottiin aiemmin voimassa ollut henkilötietodirektiivi. Tietosuoja-asetus tuli voimaan 25.5.2016, mutta soveltamisen aloittamiselle annettiin kahden vuoden siirtymäaika, joka päättyi 25.5.2018. Asetus on jäsenvaltioissa sellaisenaan sovellettavaa oikeutta, mutta tietosuojasuoja-asetus jättää direktiivinomaisesti myös kansallista liikkumavaraa. Siksi sitä tullaan täsmentämään kansallisella sääntelyllä.[23]

---

[18] GDPR 30 artikla
[19] eduskunta.fi, Lainsäädäntö, viitattu 13.11.2018
[20] eduskunta.fi, Lain säätäminen, Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, viitattu 13.11.2018
[21] Tietosuojatyöryhmä WP 29 (*Article 29 Data Protection Working Party*) oli EU-maiden tietosuojaviranomaisista koostettutyöryhmä, joka korvattiin tietosuoja-asetuksen sovellettavaksi tullessa Euroopan tietosuojaneuvostolla. Myös jälkimmäinen koostuu EU:n kansallisista tietosuojan valvonnasta vastaavista viranomaisista (Euroopan komissio, https://ec.eruopa.eu, viitattu 15.11.2018)
[22] Tietosuoja.fi, Usein kysyttyä tietosuoja-asetuksesta, viitattu 9.11.2018
[23] HE 9/2018 s. 4

Samaan aikaan tietosuoja-asetuksen kanssa hyväksyttiin rikosasioiden tietosuojadirektiivi[24], joka yhdessä asetuksen kanssa muodostaa osan EU:ssa voimaan saatettavasta tietosuojan kokonaisuudistuksesta. Tämän niin kutsutun *tietosuojapaketin* tavoitteena on yhdenmukaistaa, vahvistaa ja nykyaikaistaa EU:n henkilötietolainsäädäntöä, joka on perustunut vielä pitkälti vuoden 1995 henkilötietodirektiiviin.[25] Näkyvää uudistuksessa ovat yksilöiden oikeuksien lujittaminen ja täytäntöönpanon valvonnan tehostaminen muun muassa valvontaviranomaisen toimivaltuuksien vahvistamisella. [26]

Yhtenäistämisellä ja ajanmukaistamisella tavoitellaan myös eurooppalaisten sisämarkkinoiden vahvistamista. Valitun lainsäädäntöinstrumentin, *asetuksen,* luonne tukee tavoitetta. Toisin kuin henkilötietodirektiivi, joka on jäsenvaltioissa voitu toimeenpanna hyvinkin eri tavoin on **as**etus sellaisenaan voimassa olevaa oikeutta joka ei lähtökohtaisesti salli päällekkäistä lainsäädäntöä.[27] Direktiivin pohjalta säädettyjen lakien soveltamisessa on myös ollut eroja valtioittain. Hajanaisen tietosuojalainsäädännön on koettu muodostavan esteitä henkilötietojen liikkuvuudelle. Vaarana on kilpailun vääristyminen ja rekisteröityjen oikeuksien puutteellinen suojelu. Poistamalla henkilötietojen käsittelyn ylimääräisiä edellytyksiä asetuksella pyritään varmistamaan tietojen entistä vapaampi liikkuvuus unionin jäsenmaiden välillä ja lisäämään luottamusta tietosuojan tasoon.[28]

Suomessa henkilötietojen käsittelyä on aiemmin säädelty Henkilötietolailla (523/1999). Sillä täytäntöön pantiin vuonna 1995 annettu henkilötietodirektiivi (95/46/EY).[29] Direktiivissä ja näin henkilötietolaissa säädettiin muun muassa henkilötietojen käsittelyä koskevista yleisistä periaatteista. Digitalisaatiosta ja yhteiskunnallisesta muutoksesta huolimatta näiden periaatteiden voidaan katsoa olevan edelleen päteviä.[30]

---

[24] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikokseen liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta
[25] Lakivaliokunnan lausunto, LaVL 5/2018, s. 2
[26] HE 9/2018 s. 27
[27] HE 9/2018 s. 27
[28] HE 9/2018 s. 32
[29] HE 9/2018, s. 1
[30] HE 9/2018 s. 28

Tietosuoja-asetusta sovelletaan pääsääntöisesti kaikkeen henkilötiedon käsittelyyn niin julkisissa kuin yksityisissä organisaatioissa. Käsittely voi olla automaattista tai manuaalista[31] Varsinainen soveltamisala määritelellään tarkemmin tietosuoja-asetuksessa[32] ja se rajautuu EU:n lainsäädännön soveltamisalaan[33]. Tietosuoja-asetusta ei näin sovelleta esimerkiksi sellaiseen henkilötietojen käsittelyyn, joka liittyy kansalliseen turvallisuuteen eikä kuulu unionin oikeuden piiriin[34]. Henkilötietojen käsittelyyn rikosasioissa puolestaan sovelletaan rikosasioiden tietosuojadirektiiviä (EU 2016/680). Niin kutsutun *kotitalouspoikkeuksen* nojalla asetusta ei sovelleta kotitalouksien yksityistarkoituksessa tapahtuvaan henkilötietojen käsittelyyn[35].[36]

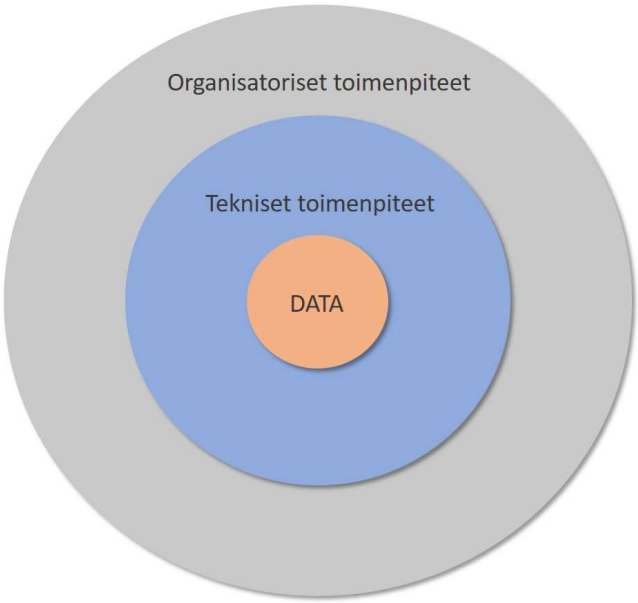
Tietosuoja-asetuksessa keskeistä on riskilähtöisyys. Kaikkea käsittelyä arvioidaan rekisteröidylle mahdollisesti aiheutuvien riskien näkökulmasta, mikä korostaa myös asetuksessa isossa asemassa olevan osoitusvelvollisuuden periaatteen merkitystä. Sen mukaisesti henkilötietojen käsittelyä suorittavan tahon tulee voida osoittaa myös käytännössä suunnitelleensa tietojen käsittelyn ja arvioineensa siihen liittyviä riskejä.[37] Riskiperusteisella lähestymistavalla pyritään toisaalta varmistamaan rekisteröidyn tietojen suoja korkeariskisessä toiminnassa ja toisaalta välttämään ylisääntelyä matalan riskin käsittelyssä.[38]

Vaikutustenarviointi (DPIA eli Data Protection Impact Assessment) on tietosuoja-asetuksen esittelemä työkalu riskien arviointiin[39]. Se tarkoittaa rekisterinpitäjän toteuttamaa arviota käsittelyn vaikutuksista rekisteröidyn oikeuksille ja vapauksille. Vaikutustenarviointi tulee tehdä ennen tietojen käsittelyn aloittamista. Se on asetuksen mukaan pakollinen silloin kun suunnitellut käsittelytoimet todennäköisesti aiheuttavat korkean riskin rekisteröidyn oikeuksille[40]. Riski voi kasvaa käsittelyn laajuuden, suunniteltujen käsittelytapojen tai käsiteltävien tietojen luonteesta johtuen.[41]

---

[31] Muuhun kuin automaattiseen käsittelyyn asetusta sovelletaan tilanteessa, jossa tiedoista muodostuu tai on tarkoitus muodostua rekisteri tai sen osa. (HE 9/2018 s. 28)
[32] ks. GDPR 2-3 artikla
[33] Soveltaminen voi tulla kyseeseen myös varsinaisesti unionin annetun toimivallan ulkopuolelle jäävissä asioissa, mikäli voidaan osoittaa asian riittävä yhteys unionin lainsäädäntöön. (HE 9/2018, s. 34)
[34] HE 9/2018 s. 33
[35] GDPR johdanto-osa 18
[36] HE 9/2018 s. 33
[37] HE 9/2018 s. 29
[38] Andreasson ym. Osaava tietosuojavastaava 2017 s. 30
[39] GDPR 35 artikla: Tietosuojaa koskeva vaikutustenarviointi
[40] GDPR 35 artikla 1 kohta
[41] Andreasson ym. Osaava tietosuojavastaava 2017 s. 60

Sekä tietosuoja että tietoturva ovat asetuksessa usein esiintyviä termejä, joiden välistä eroa lienee hyvä selventää. Tietosuojalla tarkoitetaan henkilön yksityisyyden suojaamista henkilötietojen käsittelyssä. Tietoturvaa puolestaan ovat ne keinot joilla tietosuoja käytännössä toteutetaan. Tietoturva syntyy tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistamisesta teknisten ja organisatoristen toimintojen avulla.[42]



Kuvio 1: Henkilötietojen suojaaminen[43]

Yllä olevassa kuvassa (kuvio 1) esitetty ”data” kuvaa suojattavia henkilötietoja. Sen suojaus eli tietoturva toteutuu kahdella osiolla: teknisillä- ja organisatorisilla toimenpiteillä. Teknisiä toimenpiteitä ovat esimerkiksi työtilojen lukitseminen sekä käytettävien järjestelmien suojaaminen salasanoin ja palomuurein. Organisatorisia eli hallinnollisia toimenpiteitä taas ovat esimerkiksi henkilöstön kouluttaminen ja ohjeistaminen tietosuojan toteuttamiseksi.[44] Toimenpiteitä mitoittaessa tulee arvioida datalle käsittelystä koituvan riskin määrää Vaikka tietojenkäsittelyyn liittyisi tiukkojakin rajoituksia ja erityisesti suojattavia tietoja, tulee

[42] VAHTI-raportti 1/2016, EU-tietosuojan kokonaisuudistus s. 13, viitattu 3.12.2018
[43] mukaillen VAHTI-ohje 3/2012, Teknisen ICT-ympäristön tietoturvatason ohje s. 13
[44] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Henkilötietojen käsittelijän velvollisuudet, viitattu 5.12.2018

tietosuojan ja -turvan tasoa suunniteltaessa varmistua tietoaineiston saatavuudesta ja riittävästä käytettävyydestä.[45]

Tietosuoja-asetus korostaa tiedon käsittelyn etukäteissuunnittelua, muuttaa käsittelykäytänteitä ja luo uusia velvoitteita henkilötietoa käsitteleville tahoille[46]. Se on laaja kokonaisuus, sisältäen paljon monimutkaista ja vielä kohtuu tuntematonta terminologiaa, joka ei ole tulkittavissa tai määriteltävissä kansallisella lailla. Siksi tietosuojalain (HE 9/2018) perusteluissa on pyritty avaamaan asetuksen käsitteisiin liittyvää oikeuskäytäntöä.[47] Asetus vaatii jossain määrin pois oppimista vanhasta henkilötietolain aikaisesta käsitesisällöstä esimerkiksi rekisterin ja rekisterinpitäjän määrittelyn suhteen. Asetus ei esimerkiksi edellytä enää entisen kaltaista rekisteri- ja tietosuojaselostetta mutta velvoittaa rekisteröidyn riittävään informointiin.[48]

2.1 Tietosuojaperiaatteet

Tietosuoja-asetuksen viidennessä artiklassa kuvataan henkilötietojen käsittelyä koskevat periaatteet[49]. Nämä niin kutsutut tietosuoja- tai tietojenkäsittelyperiaatteet ovat yleisperiaatteita, joiden tavoitteita asetuksen muu yksityiskohtaisempi sääntely ilmentää[50]. Periaatteet tulee huomioida ja niitä tulee noudattaa kaikessa henkilötietojen käsittelyssä[51]. Niiden tarkoituksena on taata rekisteröidyn oikeuksien toteutuminen henkilötietojen käsittelyn kaikissa vaiheissa. Periaatteiden noudattaminen tulee voida osoittaa.[52] Tietosuojaperiaatteita tulee soveltaa myös pseudonymisoituun henkilötietoon, sen voidessa muuhun tietoon yhdistettynä johtaa edelleen henkilön tunnistamiseen[53].[54]

Tietosuojaperiaatteet ovat pitkälti samanlaisia, kuin aiemmin henkilötietolailla voimaansaatetussa tietosuojadirektiivissä ilmenneet käsittelyä koskevat yleiset periaatteet.[55] Suurin ja uusin muutos on rekisterinpitäjän osoitusvelvollisuus (accountability), joka tästä syystä

---

[45] VAHTI 3/2012, Teknisen ICT- ympäristön tietoturvataso-ohje s. 13, viitattu 27.11.2018
[46] Andreasson ym. Osaava tietosuojavastaava 2017 s. 24
[47] HaVM 12/2018 vp, s. 5
[48] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Kerro käsittelystä rekisteröidylle, viitattu 5.12.2018
[49] GDPR 5 artikla
[50] Esimerkiksi rekisteröidyn oikeudet ovat pitkälti ilmentymiä tietosuojaperiaatteista
[51] Myös pseudonymisoitu henkilötieto (GDPR johdanto-osa 26)
[52] HE 9/2018, s. 29
[53] Enemmän pseudonymisoidusta henkilötiedosta luvussa 3.1. Henkilötiedon määritelmä ja rekisterin muodostuminen
[54] GDPR johdanto-osa 26
[55] HE 9/2018 s. 28

käsitellään muista periaatteista erillisessä luvussa[56]. Sen mukaan rekisterinpitäjällä on aktiivinen näyttötaakka eli käsittelyn asetuksenmukaisuus tulee voida osoittaa. Tämä edellyttää, että rekisterinpitäjä tuntee tietosuojaperiaatteet ja ymmärtää niiden sisällön asettamat käytännön vaatimukset.[57] Tietosuojaperiaatteiden noudattamatta jättäminen tahallisesti tai törkeästä huolimattomuudesta voi johtaa hallinnollisten seuraamusmaksujen ja muiden tietosuoja-asetuksen mukaisten sanktioiden määräämiseen. Vastaavasti seuraamusmaksua määrätessä viranomainen arvioi kuinka organisaatio tai yritys on pyrkinyt huolehtimaan tietosuojaperiaatteiden kautta toteutettavasta henkilötietojen suojasta.[58]

Lainmukaisen, kohtuullisen ja läpinäkyvän käsittelyn periaate[59] edellyttää, että henkilötietojen käsittely tapahtuu lainmukaisesti ja rekisteröidyn kannalta läpinäkyvällä tavalla[60]. Läpinäkyvyydellä tarkoitetaan sitä, että rekisteröidylle tulee olla selvää mitä tietoja hänestä kerätään, miten ne kerätään ja mihin tarkoitukseen niitä käsitellään. Käsittelyyn liittyvien tietojen tulee olla rekisteröidyn helposti saatavilla ja ymmärrettävällä kielellä ilmastuja[61].[62] Se millainen kieli on asetuksen tarkoittamaa ymmärrettävää ja yksinkertaista kieltä on rekisterinpitäjän itsensä arvioitavissa. Oleellista on, että käsittelyn kohderyhmän mukainen keskivertohenkilö ymmärtää hänelle käsittelystä annetun informaation.[63]

Läpinäkyvyys liittyy olennaisesti osoitusvelvollisuuden periaatteeseen. Pystyäkseen osoittamaan, että noudattaa velvollisuuksiaan tulee rekisterinpitäjän suorittaa käsittelytoimet läpinäkyvästi. Rekisteröidyn kannalta tämä tarkoittaa sitä, että hän saa jo ennen käsittelyn aiottua aloittamista aiotusta käsittelystä sellaiset tiedot, ettei esimerkiksi käsittelyn laajuus tule myöhemmin yllätyksenä. Tämä antaa rekisteröidylle mahdollisuuden valvoa henkilötietojensa käsittelyä ja käyttää oikeuksiaan tehokkaammin. Rekisterinpitäjälle ja henkilötietojen käsittelijälle läpinäkyvyyden periaate ilmenee annettuina vaatimuksina rekisteröidyn riittävästä informoinnista.[64]

---

[56] Luku 2.2 Osoitusvelvollisuus
[57] Andreasson ym. 2017, Osaava tietosuojavastaava s. 32
[58] GDPR 83 artikla
[59] GDPR 5 artikla 1 kohta a alakohta
[60] HE 9/2018 s. 28
[61] GDPR 12 artikla 1 kohta
[62] GDPR johdanto-osa 39
[63] Tietosuojavaltuutetun toimisto (Tietosuoja.fi), Kerro käsittelystä rekisteröidylle, viitattu 4.12.2018
[64] Tietosuojatyöryhmä WP29, Läpinäkyvyys s. 5, viitattu 16.11.2018

Käyttötarkoitussidonnaisuuden periaate edellyttää, että henkilötietoja kerätään ja käytetään vain ennalta määrättyä, nimenomaisia ja laillista tarkoitusta varten[65]. Tiedon sitominen johonkin käyttötarkoitukseen edellyttää, ettei tietoa saa lähtökohtaisesti hyödyntää muihin tarkoituksiin alkuperäisen tarkoituksen kanssa yhteensopimattomalla tavalla[66]. Erikseen säädetään tiedon käytöstä yleistä etua koskeviin arkistointitarkoituksiin[67] sekä käsittelystä tieteellistä, historiallista ja tilastollista tutkimusta varten. Asetuksen 89 artiklan 1 kohdan mukaan näitä ei pidetä yhteensopimattomina alkuperäisen tarkoituksen kanssa.[68] Kansallisella lainsäädännöllä täsmentää ne tarkoitukset ja tehtävät, joita varten henkilötietojen myöhempää käsittelyä voidaan pitää laillisena käsittelyn ollessa tarpeen yleisen edun tai julkisen tehtävän suorittamisen kannalta.[69]

Tietojen minimoinnin periaatteen mukaan kerättävien ja käsiteltävien henkilötietojen tulee olla asianmukaisia ja tarpeellisia käsittelytarkoituksen kannalta[70]. Tietojen keräämiselle tulee siis olla peruste. Tietoja ei näin ollen voida kerätä esimerkiksi varmuuden vuoksi jatkossa mahdollisesti eteen tulevan tarpeen varalta vaan käsiteltävien tietojen määrä tulee rajoittaa suhteessa käsittelyn tarkoituksiin[71]. Tietosuoja-asetuksen mukaisilla teknisillä ja organisatorisilla suojatoimilla pyritään erityisesti nimenomaan tiedon minimoinnin periaatteet toteuttamiseen[72]. Minimoinnin periaatetta tukee *säilytyksen rajoittamisen periaate*. Sen mukaisesti rekisterinpitäjän tulee asettaa henkilötiedoille säilytysaika, joka on mahdollisimman lyhyt käsittelyn tarkoituksen kannalta[73]. Eräissä tapauksissa tietojen säilytysaika määräytyy suoraan lain perusteella[74].

Täsmällisyyden periaate edellyttää tietojen ajantasaisuutta. Epätarkat ja virheelliset (esimerkiksi vanhat) henkilötiedot tulee oikaista tai poistaa.[75] Täsmällisyyttä ja ajantasaisuutta arvioidaan suhteessa käsittelyn tarkoituksiin[76].

---

[65] GDPR 5 artikla 1 kohta b alakohta
[66] HE 9/2018 s. 28
[67] GDPR 5 artikla 1 kohta e alakohta
[68] HE 9/2019 s. 111
[69] HE 9/2018 s. 80
[70] GDPR 5 artikla 1 kohta c alakohta
[71] HE 9/2018 s. 28, 79
[72] HE 9/2019 s. 51
[73] GDPR johdanto-osa 39
[74] esim. kirjanpitolain (1336/1997) mukaiset säilytysajat
[75] GDPR 5 artikla 1 kohta d alakohta
[76] Euroopan komissio, Mitä henkilötietoja voidaan käsitellä ja millä ehdoilla?, viitattu 5.12.2018

Eheyden ja luottamuksellisuuden periaate edellyttää henkilötietojen käsittelyä tavalla, jolla voidaan varmistaa henkilötietojen asianmukainen turvallisuus. Henkilötiedot tulee suojata lainvastaiselta ja luvattomalta käsittelyltä. Niin ikään tiedot tulee suojata vahingossa tapahtuvalta hävittämiseltä, tuhoutumiselta ja vahingoittumiselta. Suojaaminen toteutetaan suunnittelemalla tiedon käsittelyn prosessit toimiviksi ja esimerkiksi kouluttamalla henkilökuntaa riittävästä (tarpeelliset tekniset ja organisatoriset toimet).[77]

Sisäänrakennetun ja oletusarvioisen tietosuojan periaatteen[78] (privacy by design and privacy by default) mukaan tietosuojaperiaatteet tulee sisällyttää osaksi henkilötietojen käsittelyä tarvittavilla organisatorisilla ja teknisillä toimilla. Toisin sanoen, periaatteet tulee huomioida ja käsittelyn tapoja tai käsittelyyn käytettävää järjestelmää määritellessä.[79]. Sisäänrakennetun ja oletusarvioisen tietosuojan periaate kytkeytyy osoitusvelvollisuuden periaatteeseen. Sen mukaan henkilötietoja käsittelevän tahon tulee pystyä aktiivisesti osoittamaan huomioineensa tietosuojan toteutumisen kaikessa toiminnassaan ja toiminnoissaan.[80] Sisäänrakennetusta ja oletusarvoisesta tietosuojasta säädetään tarkemmin tietosuoja-asetuksen 25 artiklassa.

Asetus siis velvoittaa rekisterinpitäjän ottamaan tietosuojaperiaatteet osaksi henkilötietojen käsittelyä mahdollisimman aikaisessa vaiheessa ja suunnittelemaan toimintaansa tietosuojanäkökulma edellä. Sisäänrakennetun- ja oletusarvoisen tietosuojan vaatimuksen tavoitteena on saada tietosuoja osaksi myös sovellus- ja järjestelmäkehitystä. Sen kautta varmistutaan entistä paremmin siitä, että asetuksen velvoitteita voidaan käytännössä noudattaa.[81] Hyvin suunniteltu tietojärjestelmä ohjaa työntekijää henkilötietojen oikeanlaisessa käsittelyssä luoden toimivia prosesseja ja vähentäen työskentelyn epävarmuutta. Esimerkiksi tietojärjestelmään sisäänrakennettu tietojen näkyvyyden rajoittaminen käyttäjätasoittain, vanhentuneen tiedon poistumisen automatisointi ja tietojärjestelmien yhteensopivuus vähentävät työvaiheiden ja virheiden määrää. Tämä lisää työntekijän viihtyvyyttä ja oikeusturvaa.[82]

---

[77] GDPR 5 artikla 1 kohta f alakohta
[78] Periaatteen sijaan voidaan puhua myös sisäänrakennetun ja oletusarvoisen tietosuojan *vaatimuksesta* kyseisen periaatteen ollessa ennemmin asetuksesta johdettu
[79] VAHTI-raportti 1/2016, EU-tietosuojan kokonaisuudistus, s. 12
[80] Väestörekisterikeskus, 2018. Tietosuoja-asetuksen huomiointi sopimussuhteessa, viitattu 4.12.2018
[81] VAHTI-raportti 1/2016, EU-tietosuojan kokonaisuudistus, s. 22
[82] Andreasson ym. 2017. Osaava tietosuojavastaava s. 52

Huonosti suunniteltu tietojärjestelmä puolestaan on pahimmillaan vaara henkilötietojen suojalle[83]. Puutteet esimerkiksi asiakastietojen hallinnoinnissa voivat aiheuttaa suuren turvallisuusuhan vaikkapa turvakiellon omaavalla henkilölle. Riittämättömät tietoturvatestaukset taas altistavat tietovuodoille ja -varkauksille. Tietojärjestelmien oleelliseen roolin tietosuojan toteuttajina on kiinnitetty huomiota jo ennen tietosuoja-asetusta. Esimerkiksi Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) on laatinut useita ohjeistuksia, jotka ohjaavat erityisesti valtion tietojärjestelmähankintojen tietoturvallisuuden seurantaa.[84]

Esitettyjen lisäksi joissain yhteyksissä puhutaan myös *Tietojen siirrettävyyden periaatteesta,* joka nousee rekisteröidyn oikeudesta saada tietonsa siirrettyä järjestelmästä toiseen[85]. Sitä mitä tämä käytännössä tarkoittaa ja missä muodossa siirtäminen tapahtuu, käsitellään tarkemmin rekisteröidyn oikeuksien yhteydessä tämän työn luvussa 3.6 Roolit.

2.2 Osoitusvelvollisuus

Osoitusvelvollisuus (”accountability”) auttaa henkilötietoja käsittelevää organisaatiota tai yritystä osoittamaan koko tiedon elinkaaren ajan, että käsittelyssä noudatetaan kaikkia tietosuoja-asetuksen 5 artiklan mukaisia tietosuojaperiaatteita. [86] Se on tietosuoja-asetuksen keskeisimpiä periaatteita ja suurin muutos suhteessa aiemmin voimassa olleeseen henkilötietolainsäädäntöön. Osoitusvelvollisuus koskee kaikkea henkilötiedon käsittelyä koko tiedon elinkaaren ajan. [87]

Osoitusvelvollisuus on ensi sijaisesti rekisterinpitäjää välittömästi velvoittava periaate[88]. Rekisterinpitäjän tulee dokumentein ja erilaisin toimin osoittaa huomioineensa edellä esitellyt tietosuoja-asetuksen 5 artiklan mukaiset käsittelyperiaatteet sekä henkilötietojen käsittelyä suunnitellessaan että toteuttaessaan. Velvollisuus korostaa sisäänrakennetun- ja oletusarvoisen tietosuojan vaatimuksia sekä riskiperusteista lähestymistapaa.[89] Käsittelyperiaatteiden noudattamisen lisäksi on pystyttävä osoittamaan valittujen henkilötietojen suojatoimien oikeasuhtaisuus ja asianmukaisuus[90].

---

[83] Andreasson ym. 2017. Osaava tietosuojavastaava s. 53
[84] Vahtioje.fi, viitattu 4.12.2018
[85] GDPR 20 artikla
[86] VAHTI-raportti 1/2016, EU-tietosuojan kokonaisuudistus s. 11, viitattu 19.11.2018
[87] HE 9/2018 s. 28
[88] GDPR 5 artikla 2 kohta
[89] Andreasson ym. 2017. Osaava tietosuojavastaava s. 40
[90] HE 9/2018 s. 90

Sen lisäksi mitä osoitusvelvollisuudesta säädetään asetuksen 5 artiklassa muiden käsittelyperusteiden yhteydessä, siitä ei ole tämän löydettävissä erityisiä sääntöjä.[91] Kyseisessä kohdassa sanotaan sananmukaisesti, että ”*rekisterinpitäjä vastaa siitä ja sen on pystyttävä osoittamaan se, että 1 kohtaa* (eli henkilötiedon käsittelyä koskevia periaatteita) *on noudatettu*”. Kuten jo todettua, ensisijaisesti osoitusvelvollisuus on siis rekisterinpitäjällä suoraan tietosuoja-asetuksen nojalla. Niiltä osin kuin käsittelyä suorittaa rekisterinpitäjän lukuun ja ohjeistuksella jokin ulkopuolinen taho, tulee rekisterinpitäjän pystyä viimekädessä osoittamaan myös tämän henkilötietojen käsittelijän toimien lainmukaisuus ja tietosuojaperiaatteiden noudattaminen. Osoitusvelvollisuus vaikuttaa näin rekisterinpitäjän ja käsittelijän väliseen suhteeseen.[92] Rekisterinpitäjän tuleekin jo käsittelijää valitessaan varmistua siitä, että tämä noudattaa toiminnassaan asetuksen vaatimuksia[93]. Hallituksen esityksessä tietosuojalaiksi (HE 9/2018) osoitusvelvollisuuden katsotaan käytännössä ulottuvan myös henkilötietojen käsittelijään.[94]

Osoitusvelvollisuutta koskevia vaatimuksia on löydettävissä läpi tietosuoja-asetuksen. Näiden velvoittavuus tulee arvioida tapauskohtaisesti. Osoitusvelvollisuuden laajuus riippuu käsiteltävien henkilötietojen määrästä, tyypistä ja käsittelevän organisaation koosta. Käytännössä yrityksen tulee toiminnassaan huomioida ainakin seuraavat asiat, jotka tulee sitten voida todeksi osoittaa: [95]

- Velvollisuus ylläpitää kuvausta henkilötietojen käsittelystä (seloste käsittelytoimista)[96]
- Tietosuosuojaperiaatteiden[97] toteutuminen toiminnassa
- Tietojen käsittelyn peruste (käsittelyn oikeusperuste)[98]

---

[91] HE 9/2018 s. 28
[92] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Henkilötietojen käsittelijän velvollisuudet, viitattu 5.12.2018
[93] GDPR 28 artikla
[94] HE 9/2018 s. 90
[95] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Osoita noudattavasti tietosuojasäädöksiä, viitattu 5.12.2018
[96] GDPR 30 artikla
[97] GDPR 5 artikla ja 25 artikla
[98] GDPR artiklat 6-10

- Vaikutustenarviointia[99] ja ennakkokuulemista[100] koskeva dokumentaatio ja niiden saatavilla pidettävyys (niiltä osin kuin näitä on suoritettu)

- Tietosuojavastaavan tehtävät (näihin liittyvä dokumentaatio)[101]

- Henkilötietojen käsittelyä tulee säädellä sopimuksin (käsittelysopimukset)[102]

Osoitusvelvollisuus auttaa siis henkilötietoja käsittelevää organisaatiota tai yritystä osoittamaan koko tiedon elinkaaren ajan, että käsittelyssä noudatetaan kaikkia tietosuoja-asetuksen 5 artiklan mukaisia tietosuojaperiaatteita. Keinoja osoittaa tämä on useita[103], mutta käytännössä osoittaminen tapahtuu erilaisin dokumentein ja niihin kuvatuin toimenpitein.[104] Yksi keino osoitusvelvollisuuden toteuttamiseen on **tietotilinpäätöksen** laatiminen. Tietotilinpäätös on raportti, jolla saadaan kokonaiskuva organisaatio tai yrityksen tietojenkäsittelyn nykytilasta. Sen tarkoitus on olla dynaaminen työkalu, joka tukee organisaation tiedonhallinnan tehokkuutta. Tietotilinpäätöstä varten määritellään konkreettisia, esimerkiksi lukuihin perustuvia mittareita, jotta raprotin tuloksia voidaan hyödyntää päätöksenteossa vaivatta. Tietosuoja-asioissa säännöllisesti läpikäytäviä tunnuslukuja voivat olla esimerkiksi rekisteröidyiltä tulevien pyyntöjen määrä, havaittujen tietoturvaongelmien määrät (esim. järjestelmien käyttökatkot ja palautusajat), lokitarkastusten määrät ja henkilöstön koulutusmäärä.[105] On hyvä huomata, että tietotilinpäätöksellä ei ole asemaa virallisena dokumenttina, mutta se toimii osoitusvelvollisuuden toteuttajana avaten yrityksen toimintaa läpinäkyvästi.[106]

Käytännössä osoitusvelvollisuuden täyttämisessä pääsee pitkälle dokumentoimalla selkeästi henkilötiedon käsittelyn prosessit, käsittelyn vastuut ja tietosuojatoimet. Käytännössä tämä tarkoittaa esimerkiksi seuraavien asioiden dokumentointi:

a) Tietojen käsittelyn prosessit

b) Informointia koskevat selosteet ja ohjeet

---

[99] GDPR 35 artikla
[100] GDPR 36 artikla
[101] Jos tietosuojavastaavaa ei ole nimitetty on myös hyvä dokumentoida perusteet päätökselle. Samoin on hyvä dokumentoida tilanteet joissa organisaatio päätyy toimimaan jossakin asiassa vastoin nimitetyn tietosuojavastaavan ehdotusta.
[102] Henkilötietojen käsittelyyn liittyvät sopimukset reksiterinpitäjän ja käsittelijän välillä. Sisältävät ohjeet henkilötietojen käsittelyyn. Tulee olla kirjallisena. (GDPR 28 artikla 9 kohta)
[103] VAHTI-raportti 1/2016, EU-tietosuojan kokonaisuudistus s. 11, viitattu 19.11.2018
[104] Andreasson ym. 2017. Osaava tietosuojavastaava s. 40
[105] Andreasson ym. 2017. Osaava tietosuojavastaava s. 147
[106] Seppo, T. Tietotilinpäätös osoitusvelvollisuuden toteuttamisessa, viitattu 5.12.2018

c) Rekisteröidyn oikeuksien toteuttamiseen liittyvät prosessit ja ohjeet

d) Muut henkilöstön ohjeet

e) Henkilöstölle järjestetyt koulutukset

f) Henkilöstön salassapitosopimukset

g) Pääsynhallinnan

h) Tietoturvaloukkauksiin liittyvät ohjeet ja ilmoittamisen prosessit.[107]

On oleellista huomata, että osoitusvelvollisuus ja asetuksesta usein esiin nostettu seloste käsittelytoimista ovat kaksi eri asiaa. Seloste käsittelytoimista on edellä mainitusti vain yksi osa osoitusvelvollisuuden periaatteen mukaisesti toteen näytettävistä asioista. Velvollisuudesta pitää selostetta käsittelytoimista säädetään asetuksen 30 artiklassa. Samassa säädetään selosteen sisällöstä. Sitä tulee ylläpitää organisaatiossa tai yrityksessä, jossa on yli 250 henkilöä, kun käsittelyyn liittyy iso riski, se kohdistuu erityisiin henkilötietoryhmiin tai kun käsittely ei ole satunnaista.[108] Seloste on kirjallinen kuvaus toimijan suorittamasta henkilötietojen käsittelystä.[109]

Tietosuoja-asetuksen 58 artiklan 1 kohdassa säädetään kansallisesti asetetun valvontaviranomaisen[110] tutkintavaltuuksista. Sen perustella valvovalla viranomaisella on oikeus esimerkiksi saada pääsy rekisterinpitäjän sekä käsittelijän tiloihin. Tämä kattaa myös pääsyn laitteisiin ja tietojärjestelmiin, joilla tietojen käsittelyä suoritetaan. Tietosuojavelvoitteiden noudattamista voidaan siis myös käytännössä valvoa. Tämän takia organisaation on hyvä varmistua siitä, että se todella toteuttaa osoitusvelvollisuuden periaatetta. [111]

Osoitusvelvollisuuden täyttäminen voidaan toisaalta nähdä rekisterinpitäjää hyödyttävänä toimintana. Jos rekisterinpitäjä esimerkiksi havaitsee tieturvaloukkauksen auttaa osoitusvelvollisuus näyttämään rekisterinpitäjän aktiivisesti pyrkineen riskien vähentämiseen jo ennen käsittelyä ja toisaalta kuvaa toiminnan havainnon jälkeen. Oikein toteutettuna

---

[107] Andreasson ym. 2017. Osaava tietosuojavastaava s. 41
[108] GDPR 30 artiklan 5 kohta
[109] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Seloste käsittelytoimista, viitattu 13.12.2018
[110] Suomessa valvontaviranomaisesta säädetään tietosuojalaissa (HE 9/2018). Toimivaltaisena viranomaisena toimii tietosuojavaltuutettu toimistoineen.
[111] GDPR 58 artikla 1 kohta

osoitusvelvollisuuden toteuttaminen voidaan nähdä rekisterinpitäjän mainetta ja luottamusta kasvattavana toimintana. Se avaa läpinäkyvästi, kuinka rekisterinpitäjä huolehtii tietosuojasta ja näin kunnioittaa rekisteröidyn yksityisyyden suojaa. Osoitusvelvollisuuden laiminlyönti aiheuttaa vastaavasti maineriskin sekä mahdollisia hallinnollisia seuraamuksia kuten tietojenkäsittelyn kieltämisen.[112] Osoitusvelvollisuuden periaatteen tarkoitus onkin patistaa toimijoita tietosuojakäytäntöjensä tarkastamiseen ja tietoturvan riittävän tason varmistamiseen kokonaisvaltaisesti kaikessa toiminnassaan.[113]

2.3 Informointivelvollisuus

Rekisteröidyllä on tietosuoja-asetukseen perustuva oikeus saada riittävä informaatio henkilötietojaan koskevasta käsittelystä. Tämä synnyttää vastaavasti rekisterinpitäjälle velvollisuuden saattaa kyseinen informaatio rekisteröidyn saataville. Vastaava velvoite löytyi jo henkilötietolaista (523/1999), jonka perusajatuksena oli, että rekisteröidyn tulee saada tietää itseään koskevien tietojen käsittelystä.[114]

Aiemmin rekisterinpitäjä on voinut toteuttaa informointivelvoitteensa tietosuojaselosteella. Se on henkilötietolain (523/1999) 10§ edellyttämää rekisteriselostetta laajempi asiakirja. Tietosuoja-asetuksessa ei säädetä entisen kaltaisesta rekisteriselosteesta. Sen sijaan rekisteröidyn tulee saada selkeä ja kattava kuva hänen henkilötiedoilleen suoritettavan käsittelyn kokonaisuudesta.[115] Tiedot tulee antaa asetuksen luonnetta noudattaen selkeässä muodossa niin, että rekisteröity pystyy ne ymmärtämään.[116] Käsittelyn kohdistuessa lapseen, tulee tieto antaa niin yksinkertaisella kielellä että hän kykenee ymmärtämään sen. Tietosuoja-asetuksessa onkin kiinnitetty erityistä huomiota lapseen rekisteröitynä.[117]

Rekisteröityä tulee informoida hänen henkilötietojensa käsittelystä ensimmäisen kerran, jos silloin kun hänen tietojaan kerätään eli tiedon käsittely aloitetaan. Tarpeellinen tietosisältö on osin riippuvainen siitä mistä tiedot kerätään (rekisteröidyltä vai muualta).[118] Oleellista on, että tiedot tarjotaan tiiviisti ja läpinäkyvästi, niin että rekisteröityä ei kuormiteta tiedon

---

[112] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Osoita noudattavasti tietosuojasäädöksiä, viitattu 5.12.2018
[113] Andreasson ym. 2017. Osaava tietosuojavastaava s. 41
[114] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Kerro käsittelystä rekisteröidylle, viitattu 5.12.2018
[115] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Kerro käsittelystä rekisteröidylle, viitattu 5.12.2018
[116] HE 9/2018 s. 28
[117] HE 9/2018 s. 30
[118] vrt. GDPR 13 artikla ja 14 artikla

liiallisella määrällä. Tietosuojaan liittyvät tiedot on myös esitettävä selkeästi erillään muusta tekstistä ja johdonmukaisesti niin, että rekisteröidyn on helppo löytää haluamansa informaatio.[119] Tiedot tulee nimenomaan tarjota, eikä rekisteröidyn tule joutua niitä pyytämään.[120]

Tietosuoja-asetuksen 13 ja 14 artikoissa esitellään tarkemmin mitä tietoja rekisteröidylle on annettava, kun tiedot kerätään suoraan häneltä itseltään tai kun tiedot kerätään muualta. Tiivistettynä rekisteröidylle tulee toimittaa vähintään seuraavat tiedot:

a) rekisterinpitäjän nimi ja yhteystiedot

b) henkilötietojen käsittelyn tarkoitukset ja oikeusperuste

c) henkilötietojen mahdolliset luovutukset ja siirrot[121]

d) henkilötietojen säilytysaika tai sen määräytymisen kriteerit

e) rekisteröidyn oikeudet

f) mahdollinen tietojen jatkokäsittely

Kun henkilötiedot on kerätty muista lähteistä kuin rekisteröidyltä itseltään, tulee häntä informoida käsiteltävistä tietoryhmistä eli siitä mitä tietoja hänestä käsitellään. Mikäli rekisteröity on jo saanut kyseiset tiedot tai niiden ilmoittaminen vaatisi kohtuutonta vaivaa (esim. laajojen tietojoukkojen käsittely yleistä etua varten), voidaan informaatio jättää toimittamatta.[122]

3 Henkilötiedon käsittely

Henkilötietojen käsittelyllä tarkoitetaan kaikkia toimintoja ja toimintaa, joka kohdistuu henkilötietoihin tai sellaisiin tietojoukkoihin, jotka sisältävät henkilötietoa. Toiminta voi olla automaattista tai manuaalista. Käytännössä henkilötietojen käsittelyä ovat henkilötietojen kerääminen, tallentaminen, järjestäminen, jäsentely, säilyttäminen ja muokkaaminen. Myös tietojen poistaminen ja tuhoaminen ovat tietosuoja-asetuksessa tarkoitettuja käsittelytoimia.[123] Koska henkilötietojen suoja on perusoikeus, tulee käsittelylle löytää aina laillinen

[119] Tietosuojatyöryhmä WP 29, Läpinäkyvyys s. 7, viitattu 16.11.2018
[120] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Kerro käsittelystä rekisteröidylle, viitattu 5.12.2018
[121] vastaanottavat kolmannet tahot, luovutus EU:n ulkopuolelle
[122] GDPR artiklat 13-14
[123] GDPR 4 artikla 2 kohta

peruste[124]. Huomionarvoista toki on, että oikeus henkilötietojen suojaan ei ole täydellisen absoluuttinen ja subjektiivinen oikeus vaan sitä arvioidaan suhteellisuusperiaatteen mukaisesti[125].

Tietosuoja-asetuksessa keskeistä on riskilähtöisyys. Se millainen riski käsittelystä aiheutuu rekisteröidyn oikeuksille ja henkilötietojen suojalle tulee huomioida jo käsittelyn suunnitteluvaiheessa. Tietosuojan ja -turvan taso tulee mitoittaa oikeansuhteiseksi riskeihin nähden. Rekisterinpitäjien ja henkilötietojen käsittelijöiden velvoitteet mukautuvat siis käsittelyriskien mukaan.[126] Riskiarvioinnissa tulee pohtia kuinka todennäköisen ja vakavan uhan käsittely aiheuttaa luonnollisen henkilön oikeuksille ja vapauksille. Arvioinnissa otetaan huomioon käsittelyn luonne, laajuus, asianyhteys ja tarkoitus[127]. Riskin laukeamisesta syntyvät seuraukset voivat olla aineellisia (esimerkiksi taloudelliset menetykset) tai aineettomia (syrjintä, identiteettivarkaus, sosiaaliset vahingot)[128].

Jos käsittelystä katsotaan aiheutuvan *todennäköisesti korkea riski* rekisteröidylle, tulee rekisterinpitäjän ennen käsittelyn aloittamista tehdä tietosuojaa koskeva vaikutustenarviointi (*Data Protection Impact Assessment* eli DPIA). Arvioinnin tulee sisältää muun muassa suunniteltu kuvaus käsittelytoimista, arvio toimien tarpeellisuudesta suhteessa henkilötiedon käyttötarkoitukseen, arvio käsittelyn riskeistä rekisteröidylle sekä suunnitellut toimenpiteet näiden riskien minimoimiseksi.[129]. Vaikutustenarviointi voi koskea niin yksittäistä käsittelytointa kuin käsittelytoimien ryhmää. Kerran tehtyä vaikutustenarviointia voidaan hyödyntää muiden samankaltaisten toimien vaikutustenarvioinnissa.[130]

Henkilötiedon käsittelylle tulee olla laista löytyvä oikeusperuste minkä lisäksi tietosuoja-asetuksen 5 artiklasta löytyviä henkilötiedon käsittelyn yleisperiaatteita tulee noudattaa koko henkilötiedon elinkaaren ajan. Periaatteet velvoittavat henkilötiedon käsittelyä suorittavaa tahoa ja periaatteiden noudattaminen tulee voida osoittaa (osoitusvelvollisuus).[131]

---

[124] EU:n perusoikeusasiakirja 8 artikla
[125] GDPR johdanto-osa 4
[126] HE 9/2018 s. 29
[127] GDPR johdanto-osa 76
[128] GDPR johdanto-osa 75
[129] GDPR 35 artikla
[130] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Vaikutustenarviointi, viitattu 5.12.2018
[131] HE 9/2018 s. 28

3.1 Henkilötiedon määritelmä ja rekisterin muodostuminen

Henkilötietoa on kaikki sellainen tieto, joka koskee tunnistettavaa tai tunnistettavissa olevaa luonnollista henkilöä. Tällaisia tietoja ovat esimerkiksi nimi, henkilötunnus, kuva, sähköpostiosoite ja evästetunnus. Myös esimerkiksi kuvallinen symboli, josta henkilö voidaan tunnistaa voi olla henkilötietoa. Toisin sanoen kaikki sellainen tieto joka yksin tai yhdistettynä toiseen tietoon *voi* johtaa henkilön tunnistamiseen katsotaan henkilötiedoksi. Tällaiset tiedot kuuluvat tietosuoja-asetuksen soveltamisalaan.[132]

Pseudonymisoidulla henkilötiedolla tarkoitetaan henkilötietoja, jotka on käsitelty tunnistamattomiksi siten, ettei niitä enää voida yhdistää rekisteröityyn käyttämättä lisätietoja. Nämä lisätiedot tulee säilyttää erillään ja suojata tarvittavin teknisin ja organisatorisin toimin.[133] Pyrkimyksenä on siis varmistaa, ettei tietojen tahatonta yhdistämistä tapahdu eikä pseudonymisointi pääse näin kumoutumaan. Käytännössä henkilötietojen pseudonymisointi voidaan toteuttaa esimerkiksi kryptaamalla eli salaamalla tiedot niin ettei niitä voida yhdistää rekisteröityyn käyttämättä salausavainta. Tiedot katsotaan edelleen henkilötiedoiksi, sillä niiden palauttaminen on mahdollista ja voi johtaa henkilön tunnistamiseen. Näin ollen pseudonymisoidun tiedon käsittelyyn sovelletaan tietosuojasäännöksiä.[134] Pseudonymisoinnilla voidaan kuitenkin vähentää rekisteröityyn kohdistuvia riskejä ja auttaa rekisterinpitäjää ja henkilötietojen käsittelijää tietosuojavelvoitteidensa noudattamisessa.[135]

Anonymisointi tarkoittaa tilannetta, jossa henkilötiedon tunnistettavuus on poistettu siten, ettei tietoa ole enää mahdollista yhdistää henkilöön[136]. Tällöin tietoja ei enää katsota henkilötiedoksi eivätkä ne siten kuulu henkilötietojen soveltamisalaan. Anonymisoinnin tulee olla peruuttamaton.[137]

Entisen henkilötietolain mukainen henkilörekisteri muodostui kaikesta samaan käyttötarkoitukseen käsitellystä henkilötiedosta. Tieto on voitu tallentaa ja sitä on voitu käsitellä useissa paikoissa. Käsittelytoimien yhteydessä syntyneitä lyhytaikaisia tiedostoja tai niiden eri sukupolvia ei ole katsottu erilliseksi rekistereiksi niiden ollessa edelleen rekisterinpitäjän hallussa

---

[132] Euroopan komissio, Mitkä tiedot ovat henkilötietoja, viitattu 26.11.2018
[133] GDPR 4 artikla 5 kohta
[134] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Pseudonymisoidut ja anonymisoidut tiedot, viitattu 26.11.2018
[135] GDPR johdanto-osa 28
[136] Vahtiohje.fi, Keskeiset termit, viitattu 26.11.2018
[137] Euroopan komissio, Mitkä tiedot ovat henkilötietoja, viitattu 26.11.2018

ja palvellessa alkuperäistä käyttötarkoitusta[138]. Rekisterin muodostumisen kannalta ratkaisevaa on ollut nimenomaan käyttötarkoitus. Tämän niin kutsutun loogisen henkilörekisterikäsitteen mukaan esimerkiksi kaikki palvelussuhteen hoitamiseen liittyvät tiedot muodostavat loogisena tietokokonaisuutena yhden rekisterin (esim. työntekijärekisteri)[139]. Tietosuoja-asetuksen mukainen rekisterin käsite on laaja, mutta myötäilee loogisen henkilörekisterin käsitettä. Asetuksen 4 artiklan mukaan *rekisterillä* tarkoitetaan mitä tahansa *tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein*. Sillä kuinka tiedon jäsentely tai tallentaminen on toteutettu ei tässä yhteydessä ole merkitystä.[140]

Aiemmin rekisterinpitäjän tuli laatia rekisteriseloste erikseen jokaisesta ylläpitämästään rekisteristä. Rekisteriseloste tuli pitää kaikkien saatavilla.[141] Tietosuoja-asetus poisti tämän henkilötietolain kaltaisen määrämuotoisen rekisteriselosteen vaatimuksen. Kuten tässä työssä on aiemmin esitetty, on rekisteröidyllä kuitenkin asetuksen mukainen oikeus saada tarvittavat tiedot henkilötietojensa käsittelystä. Se kuinka rekisterinpitäjä käytännössä toteuttaa tämän on jatkossa valittavissa. Pääsääntöisesti informaatio tulee toimittaa rekisteröidylle kirjallisesti, mutta tähän voi vaikuttaa myös esimerkiksi keräämiseen käytetty laite ja tapa[142].[143]

Asetuksen estämättä rekisterinpitäjä voi myös jatkossa ryhmitellä selosteensa loogisesti henkilötietojen käyttötarkoituksen perusteella. Tällöin tulee kuitenkin arvioida sitä, onnistutaanko valitulla toimintatavalla viestimään rekisteröidylle kaikki asetuksen mukaan hänelle kuuluva tieto. Vaarana on, että rekisteröity ei saa asetuksen edellyttämää yksiselitteistä ja selkeää kokonaiskuvaa henkilötietojensa käsittelystä silloin kun tietoja käsitellään yhtä useampaan tarkoitukseen.[144]

3.2 Käsittelyn oikeusperuste

Henkilötietojen käsittelylle tulee olla aina vähintään yksi lainmukainen peruste. Käsittelyn katsotaan olevan lainmukaista, kun se täyttää jonkin tietosuoja-asetuksen 6 artiklan 1 kohdan (Käsittelyn lainmukaisuus) edellytyksistä. Näitä ovat:

---

[138] HE 96/1998, 3.1§ 3 kohta
[139] Vahtioje.fi, Säädökset 2009, viitattu 5.12.2018
[140] GDPR 4 artikla
[141] Henkilötietolaki (523/1999) 10§
[142] Esimerkiksi saavutettavuusdirektiivi (2102/2016) voi edellyttää informaation antamista äänitemuodossa (näkövammaiset) (vm.fi/saavutettavuusdirektiivi, viitattu 5.12.2018).
[143] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Kerro käsittelystä rekisteröidylle, viitattu 5.12.2018
[144] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Kerro käsittelystä rekisteröidylle, viitattu 5.12.2018

a. Rekisteröidyn suostumus

b. Sopimuksen täytäntöönpano

c. Rekisterinpitäjän lakisääteinen velvoite

d. Elintärkeiden etujen suojaaminen

e. Yleisen edun toteuttaminen tai julkisen vallan käyttäminen

f. Oikeutettujen etujen toteuttaminen

Esitellyistä käsittelyn oikeusperusteista c ja e ovat sellaisia, joista voidaan säätää kansallisessa lainsäädännössä[145]. Muissa tapauksissa käsittelyn oikeusperuste seuraa suoraan tietosuoja-asetuksesta[146]. Henkilötietolaissa käsittelyn oikeusperusteeseen on aiemmin viitattu termillä ”käsittelyn yleiset edellytykset”[147]. Kaikki tietosuoja-asetuksen 6 artiklan mukaiset käsittelyperusteet ovat tasa-arvoisia. Sillä mihin tässä esitetyistä vaihtoehdoista henkilötiedon käsittely lopulta perustuu, on kuitenkin vaikutusta siihen, millaisia oikeuksia rekisteröidyllä on.[148]

Henkilötietoja saa käsitellä, kun käsittelylle on saatu *rekisteröidyn suostumus*. Suostumus voidaan antaa yhtä tai useampaa tarkoitusta varten[149]. Jotta suostumus katsottaisiin päteväksi, tulee sen olla vapaaehtoisesti annettu, yksilöitävissä ja yksiselitteinen tahdonilmaisu[150]. Tarkemmin suostumuksesta säädetään tietosuoja-asetuksen 7 artiklassa ”Suostumuksen edellytykset”. Artiklassa 8 säädetään erikseen lapsen suostumukseen sovellettavista ehdoista. Rekisterinpitäjän tulee pystyä osoittamaan suostumuksen olemassaolo ja lainmukaisuus.[151]

Jos henkilötietoja siirretään kolmansiin maihin, tietoja käytetään profilointiin tai kun käsitellään erityisiin henkilötietoryhmiin kuuluvia tietoja (esimerkiksi terveystiedot) suostumukseen perustuen, tulee kyseisen suostumuksen olla *nimenomaisesti* annettu. Nimenomaisuuden määritelmän täyttäviä tapoja ovat allekirjoituksella, sähköisellä allekirjoituksella tai

---

145 Suomessa tietosuojalaki ja mahdollinen erityislainsäädäntö (HE 9/2918 s. 34)
146 HE 9/2918 s. 34
147 Henkilötietolaki (523/1999) 8§
148 HE 9/2018 s. 82
149 GDPR 6 artiklan 1 kohdan a alakohta
150 GDPR 4 artikla 11 kohta
151 GDPR 7 artikla 1 kohta

kaksivaiheisella varmistuksella (sähköiset palvelut) annettu suostumus.[152] Pyyntö suostumuksen antamisesta on esitettävä selvästi erottuvasti etenkin silloin kun suostumus annetaan osana muuta asiaa koskevaa kirjallista ilmoitusta. Näin pyritään varmistamaan, että rekisteröity ymmärtää antamansa suostumuksen sisällön ja kattavuuden.[153]

Suostumusta pyydettäessä rekisterinpitäjän tulee huomioida tietosuoja-asetuksen mukainen informointivelvollisuus. Käytännössä tämä tarkoittaa sitä, että kerättäessä henkilötietoja ja perustettaessa käsittely henkilön itsensä antamaan suostumukseen, tulee hänen saada tietojensa antamisen yhteydessä asetuksen 13 artiklan mukainen kuvaus niille suunnitelluista käsittelytoimista.[154] Rekisteröidyn tulee saada tämä informaatio ennen suostumuksensa antamista. Nettisivuilla yleisesti käytetty tapa onkin kerätä edellytetty informaatio esimerkiksi erilliseen liitteeseen, joka linkitetään esimerkiksi sen lomakkeen yhteyteen, jolla tietoja kerätään. Häntä voidaan pyytää hyväksymään annetut ehdot esimerkiksi klikkaamalla suostumuksensa merkiksi raksi ”suostun tietojeni käsittelyyn”-ruutuun. Suostumus voidaan pyytää samoin edellytyksin myös paperista lomaketta täytettäessä. Oleellista on, että suostumuksen osoittava ruutu tulee nimenomaisesti ruksata hyväksytyksi rekisteröidyn itsensä toimesta.[155]

Suostumus käsittelyperusteena voi joissain tilanteissa olla ongelmallinen. Rekisteröidyllä on aina mahdollisuus peruuttaa suostumuksensa henkilötietojen käsittelyyn[156] tai vaatia tietojensa siirtämistä järjestelmästä toiseen. Suostumuksen peruuttamisen tulee olla yhtä helppoa kuin antamisenkin. [157]

Henkilötietoja voidaan käsitellä *sopimuksen täytäntöönpanemiseksi,* kun se jonka henkilötietoja käsitellään (rekisteröity) on sopimuksen osapuolena[158]. Käsittelyn tarvetta ja laajuutta arvioidaan sopimuksen sisällön ja perus tavoitteen mukaan[159]. Sopimus käsittelyperusteena voi kattaa myös ne henkilötiedon käsittelytoimet, jotka on suoritettu sopimuksen synnyttämiseksi silloin kun ne on tehty rekisteröidyn pyynnöstä. Tällainen toimi on esimerkiksi rekisteröidyn luottokelpoisuuden selvittäminen.[160]

---

[152] Tietosuojavaltuutetun toimisto (Tietosuoja.fi), Rekisteröidyn suostumus, viitattu 13.11.2018
[153] GDPR johdanto-osa 42
[154] GDPR 13 artikla
[155] GDPR 7 artikla 1 kohta
[156] GDPR 7 artikla 3 kohta
[157] GDPR 7 artikla 3 kohta
[158] GDPR 6 artiklan 1 kohdan b alakohta
[159] Tietosuojavaltuutetun toimisto (Tietosuoja.fi), Milloin henkilötietoja saa käsitellä?, viitattu 13.11.2018
[160]

Henkilötietoja voidaan käsitellä myös, kun se on tarpeen *yleisen edun mukaisten tehtävien suorittamiseksi tai julkisen vallan käyttämiseksi*[161]. Siitä mitä tämä tarkoittaa ja millaisissa tapauksissa käsittely voidaan perustaa tähän, tulee säätää tarkemmin kansallisella lailla tai unionin oikeudessa[162]. Suomessa tarkempi sääntely tulee sisältymään tietosuojalakiin. Laissa täsmennetään käsittelyn oikeusperustetta esimerkiksi tilanteessa, jossa käsitellään henkilön tietoja johtuen hänen asemastaan tai hoitamistaan tehtävistä julkisyhteisössä tai vastaavassa toiminnassa. Käsittelyn tulee olla tällöin olla yleisen edun mukaista ja yleisen tietosuoja-asetuksen edellyttämällä tavalla oikeasuhtaista päämääräänsä nähden. Oikeasuhtaisuutta arvioidaan kerättyjen henkilötietojen määrän ja niille suoritettavien käsittelytoimenpiteiden perusteella. Tietosuojaperiaatteita tulee soveltaa myös yleisen edun mukaisella oikeusperusteella suoritettuun käsittelyyn. Samoin rekisteröidyn oikeudet tulevat sovellettavaksi täysmääräisesti.[163]

Oikeutetun edun toteutuminen voi muodostaa tietojen käsittelyperusteen, sillä edellytyksellä ettei se vaaranna rekisteröidyn perusoikeuksia tai -vapauksia. Oikeutettu etu voi olla esimerkiksi rekisteröidyn ja rekisterinpitäjän välinen merkityksellinen suhde kuten asiakkuus- tai palvelussuhde. Myös esimerkiksi suoramarkkinointitarkoituksessa tapahtuva käsittely voidaan perustaa oikeutettuun etuun. Ensikädessä oikeutetun edun olemassaolon arvioinnista vastaa rekisterinpitäjä[164]. Arvioinnissa tulee kiinnittää huomiota muun muassa siihen voiko rekisteröity kohtuudella odottaa tietojensa käsittelyä suunnitellussa tilanteessa ja tarkoituksessa.[165]

3.3 Erityiset henkilötiedot

Tietosuoja-asetuksen 9 artiklassa listataan niin kutsutut erityiset henkilötietoryhmät. Tällaisia ovat tiedot, joista ilmenee henkilön:

- etnisyys
- yhteiskunnallinen tai uskonnollinen vakaumus
- ammattiliittoon kuuluminen
- terveyttä koskevat tiedot
- seksuaalinen käyttäytyminen tai suuntautuminen
- geneettiset ja biometriset tiedot tunnistamista varten

---

[161] GDPR 6 artiklan 1 kohdan e alakohta
[162] GDPR 6 artiklan 3 kohta
[163] HE 9/2018 s. 79
[164] HE 9/2018 s. 49
[165] GDPR johdanto-osa 47

Erityisiin henkilötietoryhmiin kuuluvat tiedot ovat pitkälti samoja, mitä tarkoitettiin entisillä henkilötietolain ”arkaluonteisilla henkilötiedoilla”. Sisällöllisesti säädöksissä on joitain eroja[166].[167] Lähtökohtaisesti erityisiin henkilötietoryhmiin kuuluvien henkilötietojen käsittely on kielletty[168]. Kyseisten tietojen käsittelyn katsotaan sisältävän tavanomaista suuremman tietosuojariskin voidessaan vaarantaa henkilön perusoikeuksia ja -vapauksia.[169]

Ehtona mainitun kaltaisten tietojen käsittelylle on, että asetuksen 6 artiklan mukaisen käsittelyperusteen ohella myös jokin 9 artiklan 2 kohdan edellytyksistä täyttyy. Kyseisessä kohdassa esitellään tilanteet, joissa käsittely on sallittua. Osa näistä tilanteista on sovellettavissa suoraan asetuksen perusteella ja osa edellyttää kansallista lainsäädäntöä.[170] Tietosuoja-asetuksen vaatimukset ja periaatteet eivät ole tällöinkään ohitettavissa[171]. Jos käsittely mahdollistetaan kansallisella lailla, tulee säätää myös erityisistä toimenpiteistä, joilla rekisteröidyn perusoikeudet turvataan.[172]

Erityisiä henkilötietoryhmiä voidaan käsitellä esimerkiksi **rekisteröidyn nimenomaisella suostumuksella tiettyä** tarkoitusta varten[173]. Mikäli rekisteröity on fyysisesti tai juridisesti estynyt antamasta suostumustaan voidaan tietoja käsitellä, kun sen katsotaan olevan tarpeellista **henkilön elintärkeiden etujen suojaamiseksi**[174]. Niitä tietoja, jotka rekisteröity on nimenomaisesti **itse saattanut julkiseksi**, saadaan käsitellä ilman suostumustakin[175]. Käsittely on sallittua myös tilanteessa, jossa **käsittely on tarpeen rekisteröidyn tai rekisterinpitäjän velvoitteiden noudattamiseksi** sosiaaliturvan, työoikeuden tai sosiaalisen suojelun aloilla[176].

Lasten tietoja ei listata asetuksen tarkoittamiin arkaluonteisiin henkilötietoryhmiin kuuluviksi. Lasten tietoja pidetään kuitenkin erityisesti suojattavina, sillä heillä ei katsota olevan

---

[166] Esimerkiksi henkilön sosiaalihuollosta saamansa palvelut ja tukitoimet eivät tietosuoja-asetuksessa kuulu enää käsittelykiellon piiriin (Henkilötietolaki 11§ 1mom 6 kohta). Tällaiset tiedot ovat kuitenkin jatkossakin salassa pidettäviä Julkisuuslain (Laki viranomaisen toiminnan julkisuudesta 621/1999) 24§:n nojalla. (HE 9/2018 s. 39)
[167] HE 9/2018 s. 39
[168] GDPR 9 artiklan 1 kohdan nojalla
[169] Tietosuojavaltuutetun toimisto (Tietosuoja.fi), Erityisten henkilötietoryhmien käsittely, viitattu 14.11.2018
[170] HE 9/2018 s. 40
[171] EU oikeuden etusijaperiaate (Finlex.fi), Lainlaatijan EU-opas 1.2, viitattu 26.11.2018
[172] HE 9/2018 s. 84
[173] GDPR 9 artiklan 2 kohdan a alakohta
[174] GDPR 9 artiklan 2 kohdan c alakohta
[175] GDPR 9 artiklan 2 kohdan e alakohta
[176] GDPR 9 artiklan 2 kohdan b alakohta

mahdollisuutta olla perillä tietojensa käsittelyyn liittyvistä tarkoituksista ja riskeistä[177]. Lasten henkilötiedot katsotaan siinä määrin suojattavaksi, että niiden käsittelyä suunniteltaessa voidaan rekisterinpitäjältä edellyttää tietosuoja-asetuksen 35 artiklan mukaisen vaikutustenarvioinnin toteuttamista.[178]

Myöskään henkilötunnus ei kuulu asetuksen mainitsemiin erityisesti suojattaviin henkilötietoihin. Henkilötunnuksen käsittelyn edellytysten tarkempi määrittely jätetään jäsenvaltioille.[179] Suomessa henkilötunnuksen käsittelystä tullaan säätämään ensisijaisesti tietosuojalaissa ja tarkoituksena on säilyttää sääntelyn nykytila. Henkilötunnusta voidaan jatkossa käsitellä rekisteröidyn suostumuksen perusteella tai kun rekisteröidyn yksilöinti on tärkeää rekisterinpitäjän lakisääteisen velvoitteen suorittamiseksi.[180]

Erityisiin henkilötietoryhmiin liittyvästä käsittelystä säädetään ja sitä täsmennetään tietosuojalaissa[181]. Siinä säädetään esimerkiksi asetuksen edellyttämistä asianmukaisista ja erityisistä toimenpiteistä, joilla suojataan rekisteröidyn etua läpi käsittelyn. Säädöksen tarkoitus on olla kattavan ja pakottavan sijaan rekisterinpitäjien toimintaa ohjaava. Suojaustoimenpiteet tulee aina mitoittaa käsittelyn siitä rekisteröidylle aiheutuvan riskin mukaan, mutta käsiteltäessä erityisiin henkilötietoryhmiin kuuluvia tietoja on tämä riski aina jossain määrin jo oletusarvoisesti tietojen luonteesta johtuen kohonnut. Suojatoimia, joilla rekisterinpitäjä voi pienentää käsittelystä aiheutuvaa riskiä ovat etenkin käsittelyn valvontaan liittyvät toimet, kuten sen lokittaminen[182] kuka tietoa on tallentanut, muuttanut tai muutoin katsellut.[183]

3.4 Henkilötiedon elinkaari

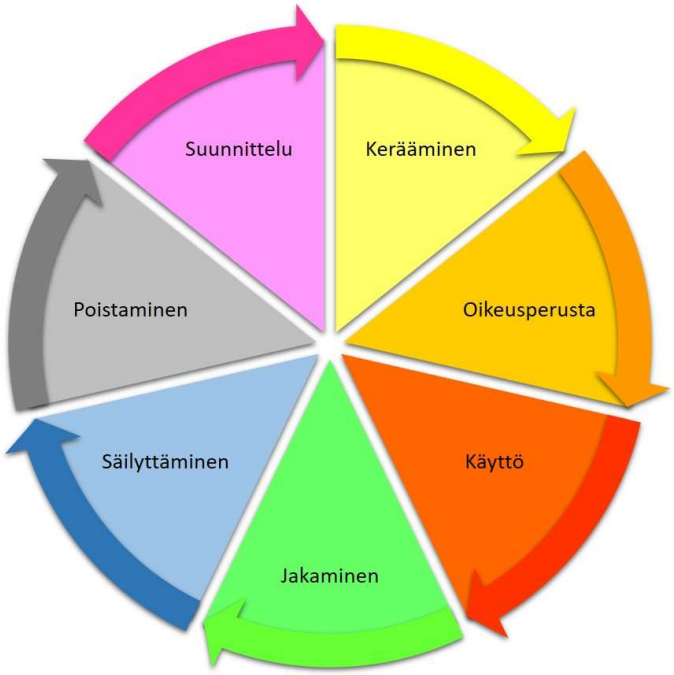
Henkilötiedon elinkaarella tarkoitetaan tiedon koko käsittelyaikaa, jolle voidaan määrittää alku ja loppu. Se alkaa käsittelyprosessin käynnistymisestä (esim. tiedon kerääminen) ja sisältää tiedon säilyttämisen (myös arkistoinnin) ja hävittämisen[184]. Käsittely päättyy, kun tieto on

---

[177] GDPR johdanto-osa 38
[178] Tietosuojatyöryhmä WP 29, Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista s. 14, viitattu 15.11.2018
[179] GDPR 87 artikla
[180] HE 9/2018 s. 113 ja Tietosuojalaki 29§
[181] HE 9/2018 s. 84: 6§ Erityisiä henkilötietoryhmiä koskeva käsittely
[182] Lokilla tarkoitetaan sähköisessä järjestelmässä tietokantaan tehtävää kronologista tapahtumatallennetta. Lokista voi selvitä esimerkiksi millaisia käsittelytoimia henkilötietoon on kohdistunut ja kenen toimesta (Viestintävirasto, Lokien keräys ja käyttö, Ohje 4/2016, viitattu 5.12.2018)
[183] Andreasson ym. Osaava tietosuojavastaava, viitattu 5.12.2018
[184] Kansallisarkisto, Sanasto: Elinkaari, viitattu 10.11.2018

hävitetty tai siitä on muutoin luovuttu[185]. Lähtökohtaisesti henkilötietojen käsittelyn tulee palvella määriteltyä tarkoitusta, jonka päättyessä henkilötietoja ei ole tarve enää säilyttää.[186] Sisäänrakennetun ja oletusarvoisen tietosuojan periaatteen mukaisesti säilytysajat tulee mahdollisuuksien mukaan määrittää järjestelmiin, joissa käsittelyä suoritetaan.[187]

Tiedon käsittelyn hallinta henkilötiedon koko elinkaaren eri vaiheissa voi olla haastavaa. Mitä pirstaloituneempaa tieto on eli mitä useammassa järjestelmässä, paikassa ja vaiheessa sitä käsitellään, sitä vaikeampaa hallinta on. Kartoittamalla tietojen sijainnit ja luomalla selkeät prosessit käsittelyyn huolehditaan henkilötiedon suojasta mutta myös tehostetaan yrityksen toimintaa.[188]



Kuvio 2: Tiedon elinkaari (esimerkki)

[185] Henkilötiedon käsittelyn elinkaari voi päättyä myös tiedon anonymisointiin. Anonyymi tieto ei ole henkilötietoa, eikä GDPR näin enää säätele sen käsittelyä. Tarkemmin ks. esim. GDPR johdanto-osa 26
[186] HE 9/2018 s. 83
[187] VAHTI-raportti 1/2016, EU-tietosuojan kokonaisuudistus s. 24, viitattu 19.11.2018
[188] Andreasson ym. 2017. Osaava tietosuojavastaava, viitattu 5.12.2018

Yllä olevassa kuvassa tiedon elinkaarta (lifecycle) kuvataan mallilla, jonka segmentit perustuvat tietosuoja-asetuksessa määriteltyihin tiedon käsittelyssä huomioitaviin vaiheisiin. Tietojen käsittely alkaa elinkaaren suunnittelulla ja päättyy henkilötiedon poistumiseen.

Elinkaarta suunniteltaessa tulee huomioida tietosuojaperiaatteet ja rekisteröidyn oikeudet. Tietojen minimoinnin periaatteen mukaisesti rekisteröidystä saadaan käsitellä ainoastaan tietoa, joka on käsittelyn tarkoituksen kannalta olennaista ja tarpeellista. Tämä voi vaihdella tiedonkäsittelyn eri vaiheissa. Niinpä tietoa pitäisi pystyä poistamaan ja tarvittaessa täydentämään dynaamisesti tarpeen mukaan. Suunnittelun yhteydessä on mahdollista tuottaa valmiiksi dokumentit, joilla rekisteröityä voidaan informoida hänestä kerätyistä tiedoista asetuksen 13 ja 14 artiklan mukaisesti. Suunnitteluvaiheessa on hyvä kiinnittää erityistä huomiota käsittelyn tarkoituksen määrittelyyn niin, että rekisteröity mutta myös käsittelijä itse tietää mihin tarkoitukseen tieto on kerätty.[189]

Koska henkilötiedon käsittely on laillista ainoastaan asetuksessa mainituin edellytyksin, tulee käsittelylle olla olemassa ainakin yksi voimassa ole käsittelyperuste (oikeusperuste). Vastuu perusteen olemassaolosta on aina rekisterinpitäjällä. Rekisterinpitäjä huolehtii myös siitä, että käyttövaiheessa tietoja käsitellään vain niille määriteltyhiin tarkoituksiin asianmukaisesti ja läpinäkyvästi.[190]

Tiedon elinkaaren mallissa jakaminen kuvaa sitä käytön vaihetta, jossa tietoa siirtyy rekisterinpitäjältä käsittelijöille ja alikäsittelijöille. Tiedon luovuttaminen käsiteltäväksi edellyttää yleensä myös sen fyysistä siirtämistä. Rekisterin tieto voi näin jakautua useisiin järjestelmiin ja monille käsittelijöille. Nämä siirrot tulee mahdollisuuksien mukaan ottaa huomioon jo henkilötietojen käsittelyä suunnitellessa. Rekisterinpitäjä on aina loppukädessä vastuussa henkilötiedon oikeanlaisesta käsittelystä ja rekisteröityjen oikeuksien toteutumisesta.

On hyvä huomioida, että myös esimerkiksi lokitiedot voivat muodostaa henkilörekisterin, jolloin myös niiden elinkaari tulee suunnitella ja ne tulee ottaa huomioon esimerkiksi tietojen poistumisen hallinnoinnissa. Tietosuoja-asetuksen käsittelyn oikeusperuste ja käsittelyn periaatteet asettavat vaatimuksia lokiin kerättäville tiedoille ja niiden säilytysajalle. Lokeja muodostuu usein ikään kuin sivutuotteena rekisterinpitäjän tai käsittelijän pyrkiessä valvomaan esimerkiksi arkaluonteisten tietojen käsittelyyn liittyvän riskin pienentämiseen[191]. Kun lokiin

---

[189] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Kerro käsittelystä rekisteröidylle, viitattu 5.12.2018
[190] Andreasson ym. 2017. Osaava tietosuojavastaava s. 77
[191] HE 9/2018 s. 91

sisältyy henkilötietoja (esimerkiksi käyttäjätunnukseen liittyvät tiedot), tulee lokistakin henkilörekisteri, joka on suojattava asetuksen edellyttämin asianmukaisin teknisin ja organisatorisin keinoin. Jos kerättyä lokia on tarkoitus käyttää henkilöstön valvontaan ja esimerkiksi selvittää sen avulla väärinkäyttötapauksia, tulee henkilöstöä informoida lokin keräämisestä asetuksen edellyttämissä määrin.[192]

Se kuinka kauan henkilötietoja säilytetään, riippuu ensisijaisesti niiden alkuperäisestä käsittelytarkoituksesta. Käyttötarkoitussidonnaisuus puolestaan estää tietojen käsittelyn muuhun kuin tähän määriteltyyn tarkoitukseen[193]. Säilytyksen rajoittamisen periaatteen mukaisesti henkilötiedot tulee poistaa alkuperäisen käsittelytarkoituksen lakattua[194]. Lähtökohtaisesti henkilötietoja saadaan siis säilyttää vain niin kauan kuin käsittelyn oikeusperuste on voimassa ja käsittelyä suoritetaan alkuperäisen tarkoituksen toteuttamiseksi.[195] Tämän jälkeen henkilötietoaineisto tulee hävittää, anonymisoida tai arkistoida, silloin kun arkistoinnille on olemassa asiallinen peruste.[196]

Joidenkin tietojen elinkaaren loppupäähän annetaan suoria aikamääreitä laissa. Esimerkiksi työsopimuslain mukaan työntekijällä on oikeus saada todistus työsuhteen keskosta ja työtehtävien laadusta 10 (kymmenen) vuotta työsuhteen päättymisestä ja tämän jälkeenkin, jos siitä ei aiheudu työnantajalle kohtuutonta vaivaa. Näin ollen mainittuja työsuhteeseen liittyviä tietoja tulee säilyttää vähintään 10 vuotta. Ylärajaa tällaisen tiedon säilyttämiselle sen sijaan ei ole asetettu, joten jää organisaation tai yrityksen omaan harkintaan, kuinka kauan säilyttäminen voi olla tarkoituksenmukaista. [197] Mikäli henkilötiedoille osataan jo sen keräämisvaiheessa antaa eksakti säilytysaika, tulee se informoida myös rekisteröidylle. Muussa tapauksessa hänelle tulee antaa tieto siitä millä perustein säilytysaika määräytyy (esim. asiakkuuden voimassaolo).[198]

Henkilötiedon elinkaari päättyy, kun henkilötietojen käsittelyn peruste lakkaa. Tällöin tiedot tulee poistaa, luovuttaa takaisin rekisterinpitäjälle tai anonymisoida peruuttamattomasti.

---

[192] Viestintävirasto, Lokien keräys ja käyttö, Ohje 4/2016 s. 6, viitattu 5.12.2018
[193] HE 9/2018 s. 28
[194] Poikkeuksena tähän on yleisen edun mukainen arkistointi (GDPR 5 artikla 1 kohta e alakohta).
[195] HE 9/2018 s. 82
[196] HE 9/2018 s. 83
[197] Työsopimuslaki (2001/55) 6 luvun 7&
[198] GDPR 13 artikla

Henkilötiedot voidaan myös arkistoida, jos arkistoinnille on asiallinen peruste. Arkistoituun henkilötietoon sovelletaan edelleen tietosuoja-asetuksen mukaisia käsittelyperusteita.[199]

3.5 Roolit

Rooleista henkilötietojen ja -rekisterien käsittelyn yhteydessä säädetään muun muassa tietosuoja-asetuksen 4 artiklan kohdissa 1 ja 7-10. Tässä luvussa esitellään tietosuoja-asetuksen mukaiset roolit. Tietosuoja-asetuksen keskiössä on rekisteröity ja hänelle tietojen käsittelystä aiheutuvien todellisten riskien arviointi. Niinpä rekisterinpitäjän ja henkilötietojen käsittelijän vastuut ja velvoitteet voivat vaihdella hyvinkin paljon käsiteltävän henkilötiedon tyypin, käsittelyn mittakaavan ja tarkoituksen mukaan.[200]

3.5.1 Rekisteröity

Rekisteröity (data subject) on se henkilö, jonka henkilötietoja käsiteltävät tiedot ovat.[201] Rekisteröidyn oikeuksien[202] vahvistaminen on tietosuoja-asetuksen keskeisimpiä tavoitteita. Asetus pyrkii varmistamaan, että rekisteröity saa selkeää ja ymmärrettävää tietoa siitä, kuinka hänen henkilötietojaan käsitellään. Oikeudet on kehitetty vastaamaan nykyistä paremmin digitalisoituneen yhteiskunnan rakenteisiin. Tavat käsitellä tietoa ja tarjota palveluita ovat muuttuneet merkittävästi sitten tietosuojadirektiivin säätämisen. Euroopassa internetiä käyttää 250 miljoonaa ihmistä päivittäin. Tietosuoja-asetus pyrkii takaamaan luonnollisille henkilöille mahdollisuuden valvoa sekä kontrolloida omien tietojensa käyttöä mahdollisimman tehokkaasti tässä jatkuvasti muuttuvassa ympäristössä.[203]

Asetuksen mukaisia rekisteröidyn oikeuksia ovat esimerkiksi:

a) tiedonsaantioikeus

b) pääsy tietoihin

c) tietojen oikaisu

d) unohdetuksi tuleminen

---

[199] HE 9/2018 s. 83
[200] esim. GDPR 28 artikla
[201] VAHTI-raportti 1/2016, s. 12, viitattu 5.12.2018
[202] GDPR 3 luku
[203] Euroopan komissio, How does the data protection reform strenghten citizens' rights? Viitattu 26.11.2018

e) käsittelyn rajoittaminen ja vastustaminen

f) tietojen siirtäminen järjestelmästä toiseen[204]

Tiedonsaantioikeus tarkoittaa, että rekisteröidyn tulee saada kaikki hänen henkilötietojensa käsittelyä koskevat tiedot selkeästi esitetyssä paketissa. Samoin hänen tulee saada riittävä informaatio ja ohjeistus oikeuksien käyttämisestä. Mikäli hän pyytää käyttää jotakin oikeuttaan kuten oikeuttaan tulla unohdetuksi tulee rekisterinpitäjän toimittaa tieto niistä toimenpiteistä, joihin se on ryhtynyt pyynnön johdosta.[205]

Rekisteröidyn oikeus päästä tietoihin takaa, että rekisteröidyllä on oikeus saada vahvistus siitä, käsitelläänkö häntä koskevia henkilötietoja. Mikäli tietoja käsitellään, hänen tulee saada pääsy tietoihinsa ja riittävä informaatio käsittelyn tarkoituksista ja tavoista. Annettavan informaation sisältö kuvataan tietosuoja-asetuksen 15 artiklassa ja se vastaa sitä, mitä tämän työn aiemmassa vaiheessa on esitetty rekisteröidyn informoinnista. Rekisterinpitäjän tulee myös toimittaa jäljennös käsittelemistään henkilötiedoista rekisteröidyn näin pyytäessä.[206] Havaitessaan, että rekisterinpitäjä käsittelee puutteellisia tai epätarkkoja henkilötietoja on rekisteröidyllä oikeus tietojensa oikaisemiseen ja täydentämiseen.[207]

Rekisteröidyllä on oikeus tietojensa poistamiseen, jota kutsutaan myös oikeudeksi tulla unohdetuksi. Oikeuden mukaisesti rekisterinpitäjä on velvollinen lopettamaan tietojen käsittelyn ja poistamaan rekisteröityä koskevat tiedot välittömästi. Tietojen poistaminen koskee myös henkilötietojen kopioita ja jäljennöksiä. Poistaminen tulee toteuttaa niin kokonaisvaltaisesti kuin mahdollista, kuitenkin teknologian ja toteuttamiskustannukset huomioon ottaen. Oikeus tulla unohdetuksi ei ole täysin subjektiivinen vaan sen käyttö edellyttää, että jokin tietosuoja-asetuksessa erikseen mainituista seikoista täyttyy. Henkilö voi vaatia tietojensa poistamista esimerkiksi tilanteessa, jossa hän peruuttaa käsittelyn perusteena toimineen suostumuksen. Mikäli käsittelyn jatkamiselle ei ole muuta laillista perustetta, tulee henkilötiedot poistaa.[208]

Rekisteröidyllä on *oikeus siirtää tietonsa järjestelmästä toiseen* (*right to data portability*)[209]. Rekisteröidyllä on oikeus saada itse rekisterinpitäjälle toimittamansa henkilötiedot

---

[204] GDPR artiklat 12-22
[205] GDPR 12 artikla
[206] GDPR 15 artikla
[207] GDPR 16 artikla
[208] GDPR 17 artikla
[209] GDPR 20 artikla

jäsennellysti yleisesti käytettävässä koneluettavassa muodossa niin, että hän voi halutessaan siirtää tiedot esimerkiksi toiselle palveluntarjoajalle rekisterinpitäjän estämättä.[210] On huomattava, että kaikki rekisteröidyn oikeudet eivät ole täysin subjektiivisia eli rekisterinpitäjää ehdottomasti velvoittavia vaan ne on sidottu käsittelyn oikeusperusteeseen. Esimerkiksi juuri oikeus siirtää tietoja järjestelmien välillä on vain tilanteissa, joissa käsittely tapahtuu rekisteröidyn suostumukseen tai sopimukseen perustuen.[211]

Mainittujen oikeuksien lisäksi rekisteröidyllä on esimerkiksi oikeus saada ilmoitus tietoturvaloukkauksesta kuten tietovuodosta. Tämä on hyvä esimerkki siitä, kuinka henkilötietojen käsittelijöiden ja rekisterinpitäjän velvoitteet heijastelevat rekisteröidyn oikeuksien toteutumista. Ilmoitus tapahtuneesta tietosuojaloukkauksesta on tehtävä rekisteröidylle silloin kun se todennäköisesti aiheuttaa korkean riskin rekisteröidyn oikeuksille.[212] Kun henkilötietojen käsittely on esimerkiksi ostopalvelusopimuksen nojalla ulkoistettu rekisterinpitäjältä käsittelijälle, tulee heidän sopia keskenään siitä, kuinka rekisteröidyn oikeuksien toteuttamisesta käytännössä huolehditaan esimerkiksi tietojen poiston, tarkastuksen tai oikaisun osalta.[213]

3.5.2 Rekisterinpitäjä

Rekisterinpitäjä (data controller) on se taho, joka määrittelee henkilötiedon käsittelyn tarkoitukset ja keinot. Rekisterinpitäjänä voi toimia luonnollinen henkilö, oikeushenkilö, julkinen viranomainen, virasto tai muu elin.[214] Kun kaksi tai useampi rekisterinpitäjä määrittää käsittelyn tarkoitukset ja keinot yhdessä, katsotaan heidät *yhteisrekisterinpitäjiksi*. Tällaisessa tilanteessa rekisterinpitäjät määrittelevät keskenään kunkin vastuualueen tietosuoja-asetuksessa säädettyjen velvoitteiden noudattamiseksi. Vastuunjaon täytyy olla läpinäkyvä ja siitä tulee ilmoittaa rekisteröidylle niin että hän ymmärtää sen sisällön.[215]

Rekisterinpitäjän tulee toteuttaa asianmukaiset toimenpiteet toteuttaakseen rekisteröityjen tietosuojaoikeuksia.[216] Käytännössä rekisteröidyn oikeudet kääntyvät velvollisuuksiksi rekisterinpitäjälle. Rekisteröidyllä tulee olla mahdollisuus oikeuksiensa käyttämiseen ja juuri rekisterinpitäjä on taho, jonka tulee mahdollisuuksien mukaan helpottaa noiden oikeuksien käyttämistä. Rekisteröidyllä on oikeus saada tieto siitä mihin toimenpiteisiin rekisterinpitäjä on

---

[210] GDPR 20 artikla
[211] HE 9/2018 s. 29
[212] VAHTI-ohje 1/2016 s. 12, viitattu 5.12.2018
[213] Nevalainen T. EU:n tietosuoja-asetus-koulutus 31.5.2016, viitattu 14.12.2018
[214] VAHTI-ohje 1/2016 s. 11, viitattu 5.12.2018
[215] Euroopan komissio, Mikä on rekisterinpitäjä tai tietojen käsittelijä?, viitattu 5.12.2018
[216] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Rekisteröidyn oikeudet, viitattu 5.12.2018

tämän pyynnöstä ryhtynyt oikeuksien toteuttamiseksi ja rekisterinpitäjää sitoo aikaraja pyynnön toteuttamisesta.[217] Rekisteröidyn oikeuksien toteuttaminen on rekisterinpitäjän päävelvoitteita. Rekisterinpitäjällä on myös velvoite tunnistaa rekisteröidyn henkilöllisyys hänen käyttäessään asetuksen mukaisia oikeuksiaan. On osa rekisteröityjen oikeusturvaa huolehtia siitä, ettei oikeuksia loukata toisen henkilön toimesta.[218]

Rekisterinpitäjän tai hänen edustajansa on ylläpidettävä asetuksen 30 artiklan mukaista selostetta (henkilötietojen) käsittelytoimista. Se on kirjallinen kuvaus siitä, kuinka organisaatio käsittelee henkilötietoja. Pakottava velvoite selosteen pitoon on vain organisaatioilla jotka työllistävät yli 250 henkeä tai joiden harjoittama tietojen käsittely on säännöllistä tai sisältää esimerkiksi erityisiin henkilötietoryhmiin kuuluvia tietoja. [219] Kuten tämän työn osoitusvelvollisuutta kuvailevassa luvussa on esitetty, seloste on organisaation oma sisäinen asiakirja, jonka tarkoitus on toimia apuna henkilötietojen käsittelyn hahmottamisessa. Se myös auttaa osoitusvelvollisuuden näyttötaakan kattamisessa. Käsittelytoimia koskeva seloste ei näin ole tarkoitettu rekisteröidyn informointiin.[220] Mikäli käsiteltävät tiedot ovat sellaisia, joista voidaan arvioida aiheutuvan merkittävä riski rekisteröidyn oikeuksille tai vapauksille, on rekisterinpitäjällä velvoite tehdä tämän lisäksi tietojen käsittelyä koskeva vaikutustenarviointi.[221]

Rekisterinpitäjänä toimivan yrityksen tai organisaation työntekijät käsittelevät henkilötietoja suorittaakseen rekisterinpitäjän tehtäviä. He eivät näin ollen siis toimi tietojen käsittelijöinä suorittaessaan konkreettia käsittelytehtäviä vaan edustavat samaa roolia jota organisaatiokin.[222] Rekisterinpitäjän tulee huolehtia siitä, että se luovuttaa tietoja muiden käsiteltäväksi ainoastaan samoihin tarkoituksiin, joihin se on ne itse kerännyt ja että näitä tarkoituksia myös noudatetaan. Tätä varten sopimus henkilötietojen käsittelystä tulee tehdä kirjallisesti.[223]

3.5.3 Käsittelijä

Henkilötietojen käsittelijän (data processor) roolista säädetään tietosuoja-asetuksen 28 artiklassa. Käsittelijällä tarkoitetaan sellaista toimijaa, joka käsittelee henkilötietoja reksiterinpitäjän lukuun. Henkilötietojen käsittelijää siis toimii rekisterinpitäjän alaisuudessa ja suorittaa

---

[217] GDPR 12 artikla
[218] VAHTI-raportti 1/2016 s. 13, viitattu 5.12.2018
[219] GDPR 30 artikla
[220] Tietosuojavaltuutetun toimisto (tietosuoja.fi), seloste käsittelytoimista, viitattu 5.12.2018
[221] GDPR 35 artikla
[222] Euroopan komissio, Mikä on rekisterinpitäjä tai tietojen käsittelijä, viitattu 14.12.2018
[223] GDPR 28 artiklan 9 kohta

käsittelyä saamiensa ohjeiden perusteella. Hän ei itse määrittele käsittelyn tarkoituksia ja keinoja.[224] Henkilötietojen käsittelijän toimet voivat olla tarkkaan rajatut sen mukaan mitä käsittelystä on sovittu. Käsittelevä taho ei voi ryhtyä käsittelemään henkilötietoja omiin tarkoituksiinsa tai ryhtyä niiden suhteen rekisterinpitäjäksi.[225] Henkilötietojen käsittelijän tulee laatia seloste käsittelytoimista samoin edellytyksin kuin rekisterinpitäjänkin[226]. Tämä kirjallinen kuvaus siitä kuinka käsittelyä suoritetaan auttaa myös rekisterinpitäjää toteuttamaan osoitusvelvollisuuden käsiteltävien henkilötietojen koko elinkaaren mitalta.[227]

Rekisterinpitäjän tulee huolehtia siitä, että se luovuttaa henkilötietoja käsiteltäviksi ainoastaan sellaiselle taholle, joka voi antaa riittävät takeet kyvystään käsitellä tietoja asetusta noudattaen. Rekisterinpitäjän tulisi varmistua käsittelevän tahon riittävästä asiantuntemuksesta, resursseista, luotettavuudesta ja tietoturvan tasosta.[228] Tietosuoja-asetusta sovelletaan myös sellaiseen henkilötietojen käsittelijään, joka on sijoittunut EU:n ja ETA-alueen ulkopuolelle, mutta käsittelee unionin kansalaisten tietoja. Tällaisia ovat tyypillisesti erilaiset pilvipalvelutarjoajat.[229] Soveltamisen tarkoituksena on taata EU-kansalaisten tietosuojaoikeudet myös globaalissa toiminnassa.[230]

Organisaatiolla voi olla myös alihankkijoita, jotka käsittelevät henkilötietoja sen lukuun. Tällöin käsittelyä suorittava alihankkija on niin sanottu alikäsittelijä ja velvoitettu sanktion uhalla noudattamaan asetuksen vaatimuksia. Yleinen esimerkki tällaisesta toimijasta ovat pilvipalveluntarjoajat ja järjestelmätoimittajat [231], jotka tarjoavat tietojen käsittelyyn käytettävän järjestelmän. Alikäsittelijän käyttäminen edellyttää rekisterinpitäjän (yleensä kirjallista) lupaa ja menettelystä sovitaan esimeriksi käsittelysopimuksen yhteydessä. Alikäsittelijään sovelletaan samoja ehtoja ja sopimuksia kuin henkilötietojen alkuperäiseen käsittelijään. Henkilötietojen käsittelijän vastuulla on huolehtia, että alikäsittelijä tuntee sopimuksen sisällön ja velvoitteet. Käsittelystä sovittaessa henkilötietojen alkuperäinen käsittelijä myös

[224] GDPR 28 artikla
[225] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Henkilötietojen käsittelijät, viitattu 5.12.2018
[226] GDPR 30 artikla 2 kohta
[227] HE 9/2018 s. 90
[228] GDPR johdanto-osa 82
[229] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Henkilötietojen käsittelijän velvollisuudet, viitattu 5.12.2018
[230] GDPR johdanto-osa 23
[231] Andreasson ym, Osaava tietosuojavastaava 2017, s. 33

vastaa siitä, että se varmistaa alikäsittelijän takaavan käsittelyn turvallisuuden ja täyttävän tietosuoja-asetuksen vaatimukset.[232]

3.6 Sopimus henkilötietojen käsittelystä

Kun henkilötietojen käsittely ulkoistetaan, tulee rekisterinpitäjän ja henkilötietojen käsittelijän laatia käsittelystä kirjallinen sopimus[233], jossa vahvistetaan käsittelyn kannalta oleelliset asiat kuten käsiteltävät tiedot, käsittelyn kesto ja tarkoitus. Samassa tulee sopia myös siitä mitä tiedolle tapahtuu sen jälkeen, kun käsittely on suoritettu loppuun. Käsittelystä voidaan sopia osana toimeksiantosopimusta[234] tai erillisellä sopimusliitteellä. [235] Liite-muotoa puoltaa se, että yksittäisen liitteen päivitys on usein koko sopimuksen päivittämistä helpompaa.[236]

Tietosuoja-asetus määrittää, mistä asioista käsittelysopimuksessa olisi hyvä vähintäänkin sopia. Tällaisia ovat[237]:

Käsittelyn yksilöinti - Mitä, minkä tyyppisiä ja mihin ryhmään kuuluvia henkilötietoja sopimuksella ulkoistetaan käsiteltäväksi

Käsittelyn tarkoitus - Mihin tai millaisiin tarkoituksiin ja missä laajuudessa tietoja saadaan käsitellä.

Ohjeistukseen sitoutuminen – Henkilötietojen käsittelijä sitoutuu suorittamaan käsittelyä vain reksiterinpitäjän dokumentoitujen ohjeistuksen mukaisesti

Salassapito – Käsittelijä vastaa siitä, että käsittelyyn oikeutetut henkilöt (esim. henkilökunta) noudattavat salassapitovelvollisuutta

Turvallisuus – Sovitaan siitä, että käsittelijä toteuttaa tarpeelliset tekniset ja organisatoriset toimet tietojenkäsittelyn turvallisuuden takaamiseksi

---

[232] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Henkilötietojen käsittelijän velvollisuudet, viitattu 5.12.2018
[233] Tarkemmin sanottuna tietosuoja-asetuksessa puhutaan ”lainsäädännön mukaisesta sopimuksesta” tai ”muusta oikeudellisesta *asiakirjasta*” (johdanto-osa 81). Muotovaatimus sopimukselle asetetaan GDPR 28 artiklan 9 kohdassa. Sen mukaan asiakirjan tulee olla kirjallinen sallien myös sähköisen muodon.
[234] HE 9/2018 s. 108
[235] GDPR johdanto-osa 81
[236] Andreasson ym. 2017. Osaava tietosuojavastaava s. 133
[237] GDPR 28 artikla 3 kohta alakohdat a-h

Sopimusta laadittaessa tulee ymmärtää missä roolissa sopijapuolet ovat henkilötietoja käsitellessään. Sopimuksin ei voida esimeriksi siirtää tietosuoja-asetuksen mukaisia vastuita vaan rekisterinpitäjän asema on ensisijaisen velvoittava käsittelyn ulkoistamisesta huolimatta. Käytännössä käsittelijä kuitenkin käsittelee tietoja hyvinkin itsenäisesti rekisterinpitäjän todellisen valvonnan ja kontrollin ulkopuolella.[238]

Käsittelysopimusta ei välttämättä tarvitse laatia alusta saakka itse. Useilla toimialoilla käytetään vakiintuneesti yleisiä sopimusehtoja (YSE) sopimuksenteon apuna.[239] Näiden yhteydessä käytettäväksi on esimerkiksi tietotekniikka-alalla laadittu lisäliite, joka vastaa asetuksen vaatimukseen kirjallisesta käsittelysopimuksesta[240]. Myös tällaisen liitteen sanamuodosta voidaan poiketa ja sopia käsittelystä toisin. Tietosuoja-asetuksen 28 artiklan pakottavat normit henkilötietojen käsittelystä kuitenkin rajoittavat osapuolten mahdollisuutta käsittelystä sopimiseen, minkä johdosta vakimalliset käsittelysopimukset voivat olla pitkälti kohtuullisen toimivia ratkaisuja.[241]

3.7 Tietoturvaloukkauksesta ilmoittaminen

Tietoturvaloukkauksella tarkoitetaan tapahtumaa, josta seuraa henkilötietojen tuhoutuminen, häviäminen, muuttuminen, luovutus tai pääsy tietoihin lainvastaisesti tai vahingossa[242]. Tietoturvaloukkausten dokumentointi on osa rekisterinpitäjään kohdistuvaa osoitusvelvollisuutta. Asetuksen 33 artiklan 5 kohdan mukaan rekisterinpitäjän tulee dokumentoida kaikki henkilötietoihin kohdistuneet tietoturvaloukkaukset, niihin liittyvät seikat ja niiden johdosta toteutetut korjaavat toimenpiteet. Rekisterinpitäjällä ja eräissä tapauksissa henkilötietojen käsittelijällä on velvollisuus ilmoittaa tietoturvaloukkauksesta valvontaviranomaiselle[243] ja rekisteröidylle[244].

Ensisijaisesti ilmoitusvelvollisuus on rekisterinpitäjällä. Tämän tulee ilmoittaa havaitsemastaan tietoturvaloukkauksesta valvontaviranomaiselle silloin kun loukkauksesta voi aiheuta riski rekisteröidyn oikeuksille ja vapauksille. Ilmoitusta ei siis tarvitse tehdä, jos se on ilmeisen aiheeton eikä vaara rekisteröidyn oikeuksille ole todellinen. Ilmoitus tulee tehdä viivytyksettä, mahdollisimman pian tietoturvaloukkauksen havaitsemisesta tai tietoon saamisesta, kuitenkin

---

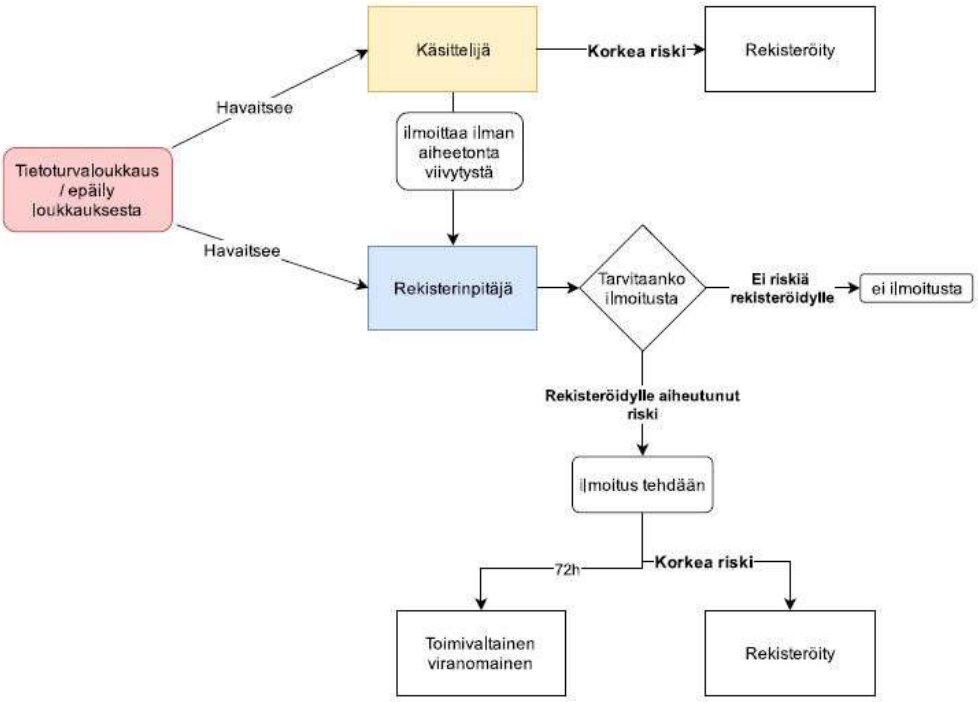
[238] Andreasson ym, s. 135
[239] Kauppakamari. Jäsentiedote 5/2017
[240] IT2018 EHK – Erityisehtoja henkilötietojen käsittelystä
[241] IT2018 EHK-ehtojen käyttö
[242] GDPR 4 artikla 12 kohta
[243] GDPR 33 artikla
[244] GDPR 34 artikla

viimeistään 72 tunnin kuluessa. Ilmoituksessa tulee kuvata, millaisiin henkilötietoryhmiin loukkaus on kohdistunut, mistä loukkauksessa on kyse, mitä siitä todennäköisesti seuraa rekisteröidylle ja mihin toimiin rekisterinpitäjä on ryhtynyt.[245]

Mikäli loukkauksen katsotaan todennäköisesti aiheuttavan korkean riskin rekisteröidyn oikeuksille, tulee tapahtuneesta ilmoittaa myös suoraan rekisteröidylle itselleen viivytyksettä. Ilmoitusta ei tarvitse tehdä, mikäli rekisterinpitäjä on toteuttanut tarvittavat tekniset ja organisatoriset keinot henkilötietojen suojaamiseksi ja niitä on sovellettu loukattuihin henkilötietoihin. Tällöin loukkauksesta aiheutuva riski rekisteröidylle on voinut pienentyä esimerkiksi, jos tiedot olivat asianmukaisesti salattu. Rekisterinpitäjä voi toteuttaa loukkauksen johdosta myös muita toimia, joilla se varmistaa, että rekisteröityyn kohdistuva riski ei enää ole todennäköinen eikä ilmoittamiselle ole näin enää perusteltua tarvetta. Valvontaviranomainen voi harkintansa mukaan vaatia ilmoituksen tekemistä rekisteröidylle tai päättää ettei ilmoitukselle ole tarvetta.[246] Hän voi myös antaa ohjeita rekisteröidylle ilmoittamista varten ja arvioida sitä mitä tietoja rekisteröidylle ilmoitetaan missäkin vaiheessa.[247]

Ilmoittamisvelvoitteen tavoitteena on vahvistaa henkilötietojen suojaa[248]. Kun tietoturvaloukkaukseen puututaan mahdollisimman nopeasti ja tehokkaasti, voidaan pienentää siitä luonnolliselle henkilölle aiheutuva vahinkoja. Tällaisia vahinkoja ovat esimerkiksi omien henkilötietojensa valvontakyvyn menettäminen, identiteettivarkaus tai salassa pidettävien tietojen luottamuksen menetys.[249] Seuraavassa kaaviossa on vielä kuvattu ilmoittamisprosessi ja toimijoiden suhteet ilmoituksen tekemisessä.

[245] GDPR 33 artikla
[246] GDPR 34 artikla
[247] GDPR johdanto-osa 86
[248] HE 9/2018 s. 61
[249] GDPR johdanto-osa 85



Kuvio 3 Tietoturvaloukkauksesta ilmoittaminen tietosuoja-asetuksen mukaan

4 Sanktiot

Mikäli tietosuoja-asetusta ei noudateta, on kansallisella valvontaviranomaisella oikeus määrätä yritykselle tai organisaatiolle hallinnollinen sakkorangaistus. Tarkemmin rangaistuksen määräämisen edellytyksistä ja perusteista säädetään asetuksen 83 artiklassa. Käytännössä rangaistuksista määrää kansallinen valvontaviranomainen. Tietosuoja-asetusta täydentävä säännös hallinnollisten seuraamusmaksujen määräytymisestä ja kansallisen viranomaisen asettamisesta tulee sisältymään kansalliseen tietosuojalakiin (HE 9/2018).[250]

Hallinnollisten sakkojen määräämisessä huomioidaan aina yksittäisen tapauksen olosuhteet. Sakon määräämistä ja suuruutta arvioitaessa valvontaviranomaisen tulee arvioida rikkomuksen luonne, vakavuus, tahallisuus ja laajuus. Näiden lisäksi tulee huomioida muun muassa ne toimet, jotka rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut henkilötietojen

[250] GDPR 83 artikla

suojaamiseksi ja esimerkiksi käsittelyvirheestä aiheutuneen vahingon pienentämiseksi. Edellisessä luvussa on esitelty rekisterinpitäjän velvoitetta ilmoittaa valvontaviranomaiselle havaitsemistaan tietoturvaloukkauksista. Huolehtimalla ilmoituksen tekemisestä ja avustamalla valvontaviranomaista tilanteen selvittämisessä yritys voi aktiivisesti itse pyrkiä vähentämään suuristakin virheistä sille aiheutuvien sakkojen määrää. Vastaavasti välinpitämättömyys tai tuottamuksellisuus voi nostaa sakkorangaistuksen määrää.[251]

Ennen hallinnollisten sakkojen määräämistä valvontaviranomaisella on mahdollisuus puuttua henkilötietojen käsittelyyn muulla tavoin ns. korjaavien toimivaltuuksien nojalla, kun katsoo tämän olevan tarpeen. Ensin rekisterinpitäjää voidaan varoittaa siitä, että käsittely on todennäköisesti asetuksen vastaista tai antaa huomautus, mikäli asetusta on jo rikottu. Jos kyse on rekisteröidyn oikeuksien käytön rajoittamisesta perusteettomasti voi valvontaviranomainen määrätä yritystä noudattamaan rekisteröidyn pyyntöjä. Tehostaakseen käsittelyn saattamista asetuksen edellyttämälle tasolle, voi valvontaviranomainen edellyttää käsittelytoimiin haluamiaan muutoksia ja asettaa muutoksille määräajan. Tarvittaessa käsittelylle voidaan asettaa määräaikainen tai pysyvä kielto.[252]

Tietosuoja-asetuksen VIII-luvussa säädetään oikeussuojakeinoista, vastuista ja seuraamuksista. Sen 84 artiklassa jäsenvaltioita edellytetään vahvistamaan säännöt seuraamusten määräämiseksi tilanteissa, jossa rikkomukseen ei sovelleta asetuksen 83 artiklan mukaisia hallinnollisia sakkoja. Jäsenvaltioiden tulee toteuttaa myös tarvittavat toimenpiteet seuraamusten täytäntöönpanon varmistamiseksi.[253] Seuraamukset voivat olla hallinnollisia tai rikosoikeudellisia. Niiden luonne on määriteltävä jäsenvaltion omassa kansallisessa lainsäädännössä.[254] Esimerkiksi tietosuoja-asetuksen 10 artiklassa säädettyä rikostuomioihin liittyvien henkilötietojen käsittelyä ei mainita asetuksen 83 artiklassa. Näin ollen 10 artiklan rikkomisesta ei ole mahdollista määrätä hallinnollista sakkoa suoraan tietosuoja-asetukseen perustuen. On siis tarpeen kansallisesti säätää toimintamallista tilanteessa.[255] [256]

---

[251] GDOR 83 artikla
[252] GDPR 58 artikla
[253] GDPR 84 artikla 1 kohta
[254] GDPR johdanto-osa 125
[255] HE 9/2018 s. 56
[256] Kyseisessä 10 artiklassa tarkoitetun rikostuomioihin liittyvät henkilötiedot ovat luoneeltaan asetuksen 9 artiklan tyylisiä erityistietoja (erityisiä henkilötietoryhmiä koskeva käsittely) ja näin suojattava samoissa määrin. Tietosuojalain esitöissä esitetäänkin 10 artiklan tarkoittamien tietojen rinnastamista tällaisiin erityisesti suojattaviin henkilötietoihin siten, että rikkomiseen sovelletaan samaa molempiin artikloihin (HE 9/2018 s. 56). Näin ollen myös 10 artiklan rikkomisesta voitaisiin määrätä hallinnollisia, korkeamman sakkoluokan mukaisia seuraamuksia (GDPR 83 artikla 5 kohdan a alakohta)

Yritys voi joutua hallinnollisen sakon maksajaksi myös välillisesti ilman suoraa omaa virhettä. Sopimuskumppanin laiminlyödessä tietosuojavelvoitteitaan voi tietosuojaviranomaisen langettama sakko tulla yrityksen maksettavaksi, jos sanktioriski on yksityisoikeudellisen sopimuksen nojalla siirretty tai jaettu.[257] Tällainen jako voi tulla osaksi sopimusta esimerkiksi yleisten sopimusehtojen mukana.[258]

Suoraan tietosuoja-asetuksesta seuraavien sanktioiden lisäksi yrityksille voi langeta seuraamuksia myös sopimusrikkomusten perusteella. Näitä voidaan pitää jopa huomattavasti todennäköisempinä kuin asetuksesta seuraavia. Vääränlaisesta henkilötietojen käsittelystä voi seurata rangaistus myös suoraan käsittelyä suorittavalle henkilölle. Rangaistus voi olla rikosoikeudellinen tai seurata salassapitosopimuksen rikkomisesta sopimussakkojen tai vahingonkorvausvelvollisuuden muodossa. Tieto- ja viestintärikoksista säädetään Rikoslain (39/1889) 38 luvussa. Esimerkiksi saman luvun 9§ mukaan henkilö, joka tahallisesta tai törkeää huolimattomuuttaan käsittelee henkilötietoja vasten käyttötarkoitussidonnaisuutta[259] voidaan tuomita sakkoon tai vankeuteen henkilörekisteririkoksesta[260]. Kyseistä rikosnimikettä ei sovelleta oikeushenkilöön vaan sen perusteella on tuomittu nimenomaan luonnollisia henkilöitä. Luvun 8§:ssä taas säädellään tietomurrosta, josta henkilö voidaan tuomita sakkoon tai vankeuteen. Tietomurrolla tarkoitetaan kyseisessä pykälässä oikeudetonta tunkeutumista järjestelmään, jossa varastoidaan tai jonka kautta siirretään dataa.[261] [262]

5 Tietosuojavastaava

Tietosuoja-asetus velvoittaa tietynlaisia rekisterinpitäjiä ja henkilötietojen käsittelijöitä tietosuojavastaavan nimittämiseen. Nimittämisvelvoite kohdistuu erityisesti julkiselle sektorille, mutta myös muille, joiden kohdalla jokin asetuksen edellytyksistä täyttyy.[263] Tietosuojavastaava on organisaation erityisasiantuntija, jonka tehtävänä on seurata henkilötietojen käsittelyä sekä auttaa organisaatiota noudattamaan tietosuojasäädöksiä. Velvollisuudesta nimittää

---

[257] HE 9/2018 s. 67
[258] esimerkiksi JIT2017
[259] Kirjoitusvaiheessa marraskuussa 2018 lain kyseinen pykälä viittaa vielä nimenomaisesti henkilötietolaissa (523/1999) säädettyyn käyttötarkoitussidonnaisuuteen.
[260] Hallituksen esityksessä tietosuojalaiksi (HE 9/2018) ehdotetaan henkilörekisteririkosta koskevan säännöksen korvaamista ”tietosuojarikosta” koskevalla säännöksellä (HE 9/2018 s. 123)
[261] HE 9/2018 s. 19
[262] Jatkossa rikoslakia tullaan luultavasti muuttamaan esimerkiksi juuri 38 luvun 9§:n mukaisen henkilörekisteririkoksen osalta, sillä suuri osa siinä käsitellyistä teoista tulee rangaistavaksi jo tietosuoja-asetuksen 83 artiklan perusteella. Rikosoikeudellisista seuraamuksista tullaan siis jatkossa säätämään kansallisesti vain niiltä osin kuin on tarpeellista eikä rangaistusta seuraa suoraan tietosuoja-asetuksen nojalla. (HE 9/2018 s. 56, viitattu 30.11.2018)
[263] VAHTI-raportti 1/2016, EU-tietosuojan kokonaisuudistus s. 18, viitattu 3.12.2018

tietosuojavastaava säädetään tarkemmin tietosuoja-asetuksen 37 artiklassa. Tietosuojavastaava tulee nimittää tilanteissa joissa organisaatio:

a) on julkishallinnon toimija (muu kuin tuomioistuin)

b) suorittaa laajamittaista, säännöllistä ja järjestelmällistä henkilöiden seurantaa

c) käsittelee arkaluontoisia tietoja laajamittaisesti[264]

Tietosuojavastaava voi olla henkilöstön jäsen tai hoitaa tehtäviään palvelusopimukseen perustuen[265]. Oleellista on, että hän on riippumaton eikä hänellä ole eturistiriitoja suhteessa tehtäviinsä. Näin ollen tietosuojavastaavana ei voi toimia sellainen henkilö, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Tietosuojavastaavaa nimittäessä tulee huomioida hänen ammattipätevyytensä ja asiantuntemuksensa tietosuojaan liittyvästä lainsäädännöstä niin, että hän voi menestyksekkäästi suorittaa hänelle tietosuoja-asetuksessa asetetut tehtävät[266].

Tietosuojavastaava voidaan nimittää myös vapaaehtoisesti ilman asetuksen nimenomaista velvoitusta. Tietosuojavastaava sujuvoittaa tietosuojatyön organisointia, työntekijöiden tietosuojataitojen ylläpitoa ja asiakaspalvelun prosesseja.[267]

Tietosuojavastaavan tehtäviin kuulu asetuksen 39 artiklan mukaan ainakin seuraavaa:

a) Sisäinen neuvonta ja ohjaus tietosuojaan liittyvissä kysymyksissä

b) Asetuksen täytäntöönpano ja soveltamisen ohjaus organisaatiossa

c) Vaikutustenarvioinnin valvonta ja ohjaus

d) Tarvittavan dokumentaation laatimisen ja saatavuuden valvonta

e) Tarvittava yhteistyö valvontaviranomaisen kanssa

f) Henkilöstön kouluttaminen

---

[264] Tietosuojavaltuutetun toimisto. Tietosuoja.fi, Tietosuojavastaavan nimittäminen, viitattu 3.12.2018
[265] GDPR 37 artikla 6 kohta
[266] GDPR 37 artikla 5 kohta
[267] Andreasson ym. Osaava tietosuojavastaava 2017 s. 41, viitattu 5.12.2018

g) Käsittelytoimiin liittyvän riskin hallinta tehtävissään [268]

Tietosuojavastaavan tehtävä on tiivistettynä valvoa, että tietosuoja-asetusta noudatetaan yrityksen tai organisaation toiminnassa. Asetus korostaa osoitusvelvollisuuden periaatetta, joten tietosuojavastaavan vastuulla on huolehtia myös siitä, että tämän periaatteen edellyttämää dokumentaatiota on tarpeeksi. Käytännössä on usein luonnollista, että valvonnan ohella tietosuojavastaava osallistuu itse tämän dokumentaation tuottamiseen. Henkilökunnan koulutukseen tietosuojavastaava voi osallistua kouluttajana. Organisaation sisäisenä erityisasiantuntijana hän on paras taho havainnoimaan koulutustarpeet ja vastaamaan henkilöstön esittämiin kysymyksiin tietosuojasta.[269]

Valvoessaan tietosuojavaatimusten noudattamaista, tietosuojavastaava valvoo myös rekisteröityjen oikeuksien toteutumista. Hänen tehtävänsä on antaa ohjausta ja neuvontaa kaikissa tietosuojaan liittyvissä kysymyksissä. Neuvontaa tulee antaa myös rekisteröidylle, etenkin hänen oikeuksiaan ja niiden käyttämistä koskevissa kysymyksissä. Tietosuojavastaavalle on tärkeää pysytellä ajan tasalla lainsäädännön, määräyksien ja ohjeiden muutoksista, jotta hän tuntee organisaatioon kohdistuvat tietosuojavaatimukset ja osaa tarjota oikeanlaista neuvontaa.[270]

6 Tietosuoja-asetus henkilökuljetusyrityksen toiminnassa

Toteutin työni kuljetusyritykselle, jolla oli tarve saada selkeä kuva tietosuoja-asetuksen sisällöstä ja sen vaatimuksista toiminnalleen. Yritys työllistää noin 50 henkilöä pääkaupunkiseudulla. Se operoi mm. koulu-, vammais- ja vanhuskuljetuksia sopimuksesta kuntien ja yksityisten toimijoiden kanssa. Se tuottaa myös taksi- ja tilausajopalveluita. Yrityksessä työskentelee omaa ja vuokrahenkilöstöä ja työtä tehdään tiiviisti yhteistyö- ja alihankkijayritysten kanssa. Näin ollen käsiteltävät henkilötiedot tulevat monesta lähteestä ja oikeus käsittelyyn perustuu moniin eri sopimuksiin. Käytännössä kaikki yrityksen päivittäiseen toimintaan osallistuvat henkilöt käsittelevät työssään henkilötietoja.

Tietosuojatyön tavoitteena oli selvittää yrityksen tietosuojaan liittyvät toiminnot ja käytännöt ja laatia suunnitelma näiden saattamisesta tietosuoja-asetuksen mukaisiksi. Lisäksi pyrin luomaan yritykselle kuvan käsittelyyn liittyvistä riskeistä ja toimintamallit näiden ehkäisemiseksi. Toiveena oli, että tuottaisin myös käytännössä tarvittavan dokumentaation ja henkilökunnan koulutuksen.

---

[268] GDPR 39 artikla 1 ja 2 kohta
[269] Andreasson ym. Osaava tietosuojavastaava 2017 s. 88, viitattu 5.12.2018
[270] Andreasson ym. Osaava tietosuojavastaava 2017 s. 87, viitattu 5.12.2018

Läpi projektin pyrin siihen, että tietosuojatyö nähtäisiin yrityksessä lain saneleman pakon sijaan ennemmin liiketoimintaa hyödyttävänä ja mahdollisuuksia luovana kokonaisuutena. Henkilötietojen käsittelyn saattaminen lain edellyttämälle tasolle oli oleellista sekä rekisteröityjen suojan että yrityksen käytännön toiminnan kannalta. Useat yrityksen operoimista kuljetuksista ovat kuntien julkisella kilpailutuksella hankkimia. Tietosuoja-asetuksen 28 artiklan mukaisesti rekisterinpitäjän eli tässä tapauksessa tilaajan tulee huolehtia siitä, että se käyttää vain sellaisia henkilötietojen käsittelijöitä joiden toiminta täyttää tietosuoja-asetuksen vaatimukset. Käytännössä tämä tarkoittaa, että jatkossa tilaaja (toimiessaan rekisterinpitäjänä) liittää hankintasopimukseen tietosuojaan liittyviä ehtoja ja ohjeita käsittelyä varten. Jotta yritys voi jatkossakin tehdä tarjouksia kyseisistä kuljetuksista, tulee sen pystyä täyttämään kilpailutuksessa mainitut ehdot.

Selkeä kuva henkilötietovarannoista ja muodostetut mallit tiedon käsittelyn apuna johtavat parhaimmillaan tehostuneisiin prosesseihin, parempaan asiakaspalveluun ja tukevat yrityksen brändin rakentumista. Henkilökunnan oikeuksien toteuttaminen ja viestiminen puolestaan voivat kasvattaa luottamusta yrityksen johtoon. Kouluttaminen tietosuoja-asetuksen vaatimaan käsittelyyn on oleellista prosessien toimivuuden ja lain noudattamisen varmistamiseksi, mutta myös henkilöstön oman oikeusturvan kannalta.

Tietosuoja-asetuksen noudattamisesta voi aiheutua yritykselle välittömiä ja välillisiä kustannuksia. Välittömiä kustannuksia ovat esimerkiksi sääntelyn noudattamisesta (tietyille toimialoille pakottavana) aiheutuva velvoite nimittää tietosuojavastaava tai tietoturvaloukkauksista ilmoittaminen. Välillisiä kustannuksia voivat olla asetuksen vaillinaisesta toteuttamisesta aiheutuva maineriski tai sopimuskumppanin toiminnan kautta aktualisoituva sanktio.[271]

Kuljetusyrityksen tilanteen kartoittaminen aloitettiin nykytila-analyysilla. Sen tarkoituksena oli saada kuva henkilötietojen käsittelyn tilasta ja nostaa esiin tarpeet, joita tietosuoja-asetuksen vaatimuksiin vastaaminen edellyttää. Prosessiin otettiin tiiviisti mukaan yrityksen toimistossa henkilötietoja käsittelevät työntekijät. Näin saatiin mahdollisimman kattava kuva yrityksen joka päiväisistä käytännöistä. Henkilökunnan tiiviillä osallistamisella pyrin myös tukemaan henkilökunnan sitouttamista tietosuojatyöhön ja mahdollisuutta tarkastella omaa rooliaan henkilötietojen käsittelyssä.

Kartoitus muodostui seuraavista asioista:

---

[271] HE 9/2018 s. 67

Toimintamallit eri kuljetusmuodoissa
Käsiteltävien henkilötietojen tyypit
Käsittelyyn vaikuttavien roolien kartoitus
Käytettävät tietojärjestelmät
Sopimustilanne
Tietosuojaperiaatteiden noudattaminen

Jotta henkilötietoja voidaan suojata tarvittavalla tavalla ja niille voidaan määritellä käsittelyprosessit, on oleellista tunnistaa mistä henkilötietoa löytyy, mistä se kerätään ja minne sitä luovutetaan. Tietosuojariskit ovat suurimmat niissä paikoissa, jossa henkilötietoa ei tunnisteta olevan eikä sen käsittelyä osata näin suunnitella ja valvoa.

Nykytila-analyysin pohjaksi tehtiin ensin vuokaaviot, joissa mallinnettiin eri tyyppisten henkilötietoryhmien käsittelyprosesseja. Henkilötiedon hallinta läpi koko elinkaarimallin on sitä haasteellisempaa mitä pienempiin kokonaisuuksiin tieto siiloutuu. Useat käsittelijät, käyttöjärjestelmät, sopimuskumppanit ja manuaaliset työvaiheet hajauttavat tietoa, mikä vaikeuttaa etenkin tiedon ajantasaisena pitämistä[272] ja poistamista[273].

6.1 Toimintaprosessit henkilökuljetuksissa

Henkilötietojen käsittelyn nykytilan hahmottamiseksi laadittiin käsittelyn prosesseja kuvaavat kaaviot. Prosessikuvasten tarkoituksena oli selvittää mistä henkilötiedot tulevat, kuka niitä käsittelee ja minne ne päätyvät. Samassa yhteydessä tehtiin riskianalyysia. Prosessista etsittiin etenkin sellaisia ongelmakohtia ja muuttujia, joilla oli vaikutusta tietojen eheyteen, salassapitoon ja elinkaaren hallintaan.

Piirretyt prosessikuvaukset auttoivat yrityksen henkilökuntaa muodostamaan kokonaiskuvan tiedonkäsittelyn prosessista. Kartoituksen alussa työntekijöillä ei ollut kaikissa tapauksissa esimerkiksi tietoa siitä, kuinka kollega suoritti vastaavan tehtävän. Näin ollen he eivät pystyneet kokonaisvaltaisesti arvioimaan minne kaikkialle tietoa päätyi eivätkä hallitsemaan sen eheyttä tai asianmukaista poistamista. Tavoitteeksi asetettiin työskentelyn yhtenäistäminen siten, että jatkossa henkilötietojen käsittelyssä noudatettaisiin ennalta määriteltyjä malleja.

Kartoituksessa keskeisiä olivat kysymykset:

---

[272] Täsmällisyyden periaate (GDPR 5 artikla 1 kohta d alakohta)
[273] Säilytyksen rajoittaminen ja tietojen minimoinnin periaate (GDPR 5 artikla 1 kohta e ja c alakohdat)

Mistä henkilötiedot tulevat, kuinka ne kerätään?
Kuka vastaanottaa tiedot?
Millä oikeudella tietoja käsitellään (käsittelyperuste)?
Mitä tietoja käsitellään (käsiteltävät henkilötietoryhmät)?
Minne henkilötietoja luovutetaan?
Ketkä kaikki osallistuvat käsittelyyn?
Minne henkilötiedot tallentuvat (tarkoituksella tai tahattomasti)?
Kuinka henkilötiedot täydentyvät/päivittyvät, kuka vastaa ylläpidosta?

Käytännössä mallinnus tapahtui ensi vaiheessa eri värisillä post-it-lapuilla seinälle yllä esitettyjä kysymyksiä apuna käyttäen. Tapa antoi mahdollisuuden hahmottaa usein abstraktisti sähköisesti liikkuvaa tietoa konkreettisemmin. Eri tyyppisille ja eri lähteistä tuleville tiedoille annettiin oman värisensä laput. Näin nähtiin missä vaiheessa tiedot mahdollisesti yhdistyivät, tuplaantuivat, minne ne jäivät ja minne ne siirtyivät. Seuraavassa vaiheessa piirsin prosessin puhtaaksi, jonka jälkeen kaavioita täydennettiin tarpeellisilta osin.

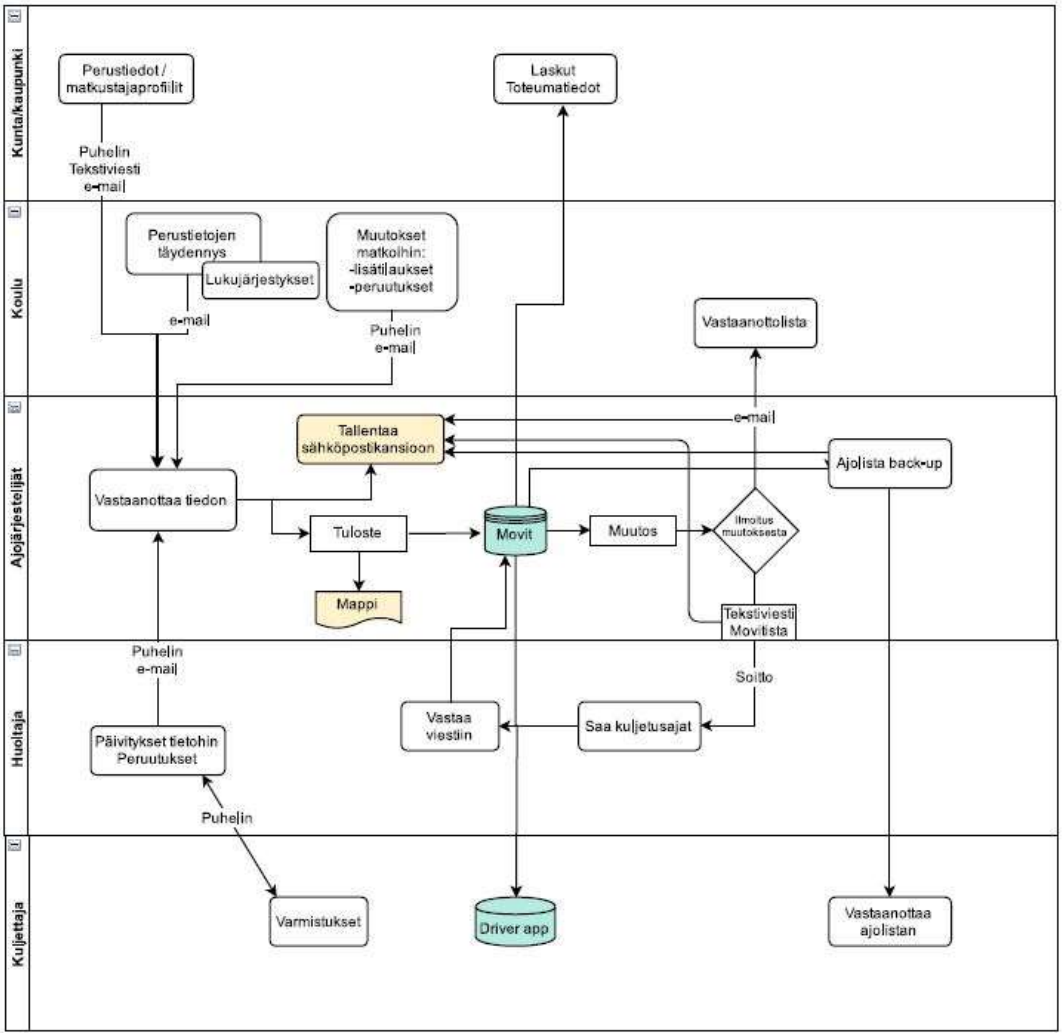
Mallintaminen onnistui paljastamaan erityisesti ne paikat, jonne henkilötietoa jäi tahattomasti. Näin sen päivittäminen, minimointi ja poistuminen on jatkossa mahdollista suunnitella. Valmiista prosessikuvista oli myös helppo nähdä ylimääräiset ja päällekkäiset työvaiheet, joita poistamalla voidaan parantaa henkilötietojen suojan lisäksi myös työskentelyn tehoa.

Yritys operoi monia erilaisia henkilökuljetuksia, joissa käsiteltävät henkilötiedot ovat peräisin moninaisista lähteistä. Käytännössä henkilökunnalle oli luonnollisinta hahmottaa tietojen käsittelyä eri kuljetustyyppien kautta. Näitä olivat:

1. Koulukuljetukset
2. Toimipaikkakuljetukset (vanhus- ja vammaispalvelukuljetukset)
3. Tilausajot (yritysten tilaamat kuljetukset)

Eri tyyppisten kuljetusten toimeksiannot ja niihin liittyvät sopimukset ovat usein hyvin samanlaisia. Esimerkiksi lakisääteisten kunnalle ostopalveluna toimitettavien kuljetusten perusteet ovat laista johtuen saman luonteisia tilaajasta riippumatta. Myös käytännössä eri kuljetustyypeissä on omat vakiintuneet piirteensä.

Kaikista kuljetustyypeistä tehtiin oma prosessimallinnuksensa. Käytännössä suuren osan yrityksen päivittäisestä henkilötietojen käsittelystä suorittaa ajojärjestelystä vastaava henkilökunta, joten he olivat mallinnuksen ensimmäisen vaiheen toteuttajia. Koska koulukuljetukset ovat yrityksen päivittäisen toiminnan keskiössä niiden suuren määrän ja niihin kohdistuvien jatkuvien muutosten myötä, avaan esimerkkinä näihin liittyvää prosessia.



Kuvio 4: Henkilötiedon käsittely koulukuljetuksissa

Käytännössä koulukuljetuksen tilaajana toimii kunta. Koulukuljetukset kuuluvat kunnan lakisääteisiin tehtäviin, joten kunta myös toimii rekisterinpitäjänä. Kuljetusyritys toimii henkilötiedon käsittelijänä. Kuviossa 3 on mallinnettu henkilötiedon kulkua. Vaakatasossa olevat altaat kuvaavat kutakin käsittelyyn osallistuvaa tahoa. Keskimmäisenä on kuljetusyrityksen ajojärjestely, joka huolehtii suurimmasta osasta tiedon käsittelyyn liittyvistä toimista. Se myös vastaa tiedon elinkaaren hallinnasta yrityksessä. Nuolet kertovat tiedon kulkusuunnan ja muodon (esim. e-mail). Keltaisella merkityt palat ovat niitä joihin tiedon huomattiin varastoituvan pitkiksi ajoiksi ja jotka tästä syystä olivat riski esimerkiksi henkilötiedon ajantasaisuuden ja laillisuuden periaatteiden näkökulmasta.

Prosessikaavion keskiössä oleva Movit on kuljetustenhallintajärjestelmä, jossa kuljetustilauksia käytännössä hallitaan. Movit toimii internet selaimella ja tallentaa tiedot pilvipalvelimelle. Se on yrityksen toiminnan kannalta keskeisin järjestelmä. Sinne tallennetaan

matkustajatiedot, jonka jälkeen aikataulujen suunnittelu, reititys ja ajolistojen välittäminen kuljettajille tapahtuu sähköisesti Movitin kautta. Jokaisella työntekijällä on pääsy Movitiin henkilökohtaisella käyttäjätunnuksella. Jokaiselle käyttäjätunnukselle on määritelty oma käyttäjärooli eli taso, joka vaikuttaa siihen mitä tietoja kukin työntekijä järjestelmässä näkee. Movit mahdollistaa matkustajatietojen hallinnoin yhdessä tietoturvallisessa paikassa. Näin matkustajien tietoja ei yrityksen sisällä tarvitse siirtää käytännössä lainkaan paperilla. Järjestelmä myös lokittaa käyttöä käyttäjätunnusten perusteella, minkä johdosta mahdollisten ongelmatilanteiden selvittäminen on helpompaa.

Huomattavaa on, että prosessikaavio ei sisällä lainkaan tietojen poistamista. Niinpä yrityksen arkistoihin ja järjestelmiin on kertynyt runsaasti vanhentunutta henkilötietoa. Jos tiedon säilyttämiselle ja käsittelylle ei ole perustetta, tulee tiedot poistaa. Suuri määrä vanhentunutta henkilötietoa on paitsi riski rekisteröidylle itselleen myös ongelma tehokkaan työskentelyn kannalta. Tietojen löydettävyys ja ajantasaisena pitäminen vaikeutuu. Selkeiden ja konkreettisten säilytysaikojen määritteleminen henkilötiedoille edesauttaa tietoaineiston säännöllistä läpikäyntiä ja hävittämistä[274]. Hallittu tietomäärä tekee työskentelystä helpompaa, kun esimerkiksi järjestelmän käyttö nopeutuu.

Pääasiassa henkilötietojen käsittely perustuu sopimukseen. Tällöin sopimuksen voimassaoloajat määrittelevät myös tietojen säilytysajat. Niissä tapauksissa, joissa yritys toimii henkilötietojen käsittelijänä, tulee huolehtia siitä, että tietojen poistamisen tapa ja aika määritellään tilaus- tai käsittelysopimuksen yhteydessä.

6.2 Kuvaus käsiteltävistä henkilötiedoista

Yritys käsittelee matkustajien, henkilöstön, yhteistyö- ja sopimuskumppaneiden tietoja. Kaikki mainitut voivat sisältää joissain määrin henkilötietoja. Tarkempi kuvaus käsiteltävistä henkilötiedoista on luettavissa tämän työn liitteenä olevasta ”Tietosuojaperiaatteemme” -selosteesta (liite 6). Siinä ilmenee mitä tietoja kustakin mainitusta ryhmästä käsitellään.

Päivittäisessä toiminnassa käsitellään joissain määrin myös henkilöiden terveydentilaan ja vammaisuuteen liittyviä tietoja. Nämä ovat oleellisia kuljetusten turvallisen ja asianmukaisen järjestämisen kannalta. Tällaiset terveyteen liittyvät tiedot luetaan asetuksen tarkoittamiin erityisiin henkilötietoryhmiin[275]. Näiden käsittelyn edellytyksiä ja rajoituksia on kuvattu tarkemmin tämän työn luvussa 3.3. Erityiset henkilötiedot.

---

[274] Kansallisarkisto, Opas säilytysaikojen määrittelyn periaatteiksi 2010, s. 3, viitattu 7.12.2018
[275] GDPR 9 artikla 1 kohta

Käsiteltävät henkilötiedot selvitettiin yrityksen käsittelyprosessien kartoituksen yhteydessä. Henkilötietoja kerätään ja käytetään lain mukaisesti ainoastaan ennalta määrättyihin tarkoituksiin. Käytännössä turvallisen kuljetuspalvelun tarjoamiseksi eli sopimuksen täyttämiseksi. Matkustajista käsitellään esimerkiksi seuraavanlaisia tietoja: nimi, osoite (kuljetuksen nouto- ja jättöpaikka), puhelinnumero ja tieto pyörätuolista. Joidenkin matkustajien osalta käsiteltiin myös esimerkiksi henkilötunnuksia ja ovikoodeja, joista jälkimmäinen ei käytännössä ole henkilötietoa. Se kuitenkin katsottiin tarpeelliseksi listata, sen ollessa tieto jota ylläpidetään henkilötietojen yhteydessä ja jonka poistumisesta tulee huolehtia henkilötietojen poistamisen yhteydessä.

Selvityksessä huomattiin, että matkustajien tietoihin liitetään yleensä myös heidän omaistensa, huoltajiensa tai muiden yhteyshenkilöiden tietoja. Tämä erityisesti tapauksissa, joissa kuljetettava on alaikäinen tai vaikeasti kehitysvammainen. Läheisten yhteystiedot ovat poikkeus- ja hätätilanteiden varalta elintärkeitä. Lisäksi ne voivat olla edellytys viestinnälle tai rekisteröidyn oikeuksien käyttämiselle silloin kun kuljetettava on alaikäinen tai muutoin holhouksen alainen. Tietojen käsittely voi niin ikään olla edellytys sopimuksen täydelle täytäntöönpanolle kuten esitän jäljempänä roolien määräytymistä pohdittaessa (6.5. Roolit). Nämä liitetyt henkilötiedot eivät varsinaisesti muodosta omaa rekisteriään vaan täydentävät asiakasrekisteriä niiden käyttötarkoituksen ollessa asiakasrekisterin käytön kanssa yhteneväinen. Tiedot on kerätty ja niitä käsitellään rekisteröidyn omalla suostumuksella ja usein heidän nimenomaisesta pyynnöstään.

6.3 Rekrytointi ja henkilöstön tiedot

Työntekijöiden henkilötietojen keräämisen tarkoitus on työsuhteeseen liittyvien velvollisuuksien ja oikeuksien hoito. Käsittely perustuu kansalliseen lainsäädäntöön. Työntekijää koskevien henkilötietojen käsittelystä säädetään laissa yksityisyyden suojasta työelämässä (759/2004). Lakia sovelletaan työsuhteiden lisäksi soveltuvin osin myös työnhakijoihin[276]. Hallituksen esityksessä tietosuojalaiksi (HE 9/2018) esitetään, että myös jatkossa henkilötietojen käsittelystä työsuhteen yhteydessä säännellään kyseisessä laissa. Kansallisessa laissa määrätään tarkemmin myös tietojen säilytys- ja vanhentumisajoista (esim. työsopimus-. työaika- ja kirjanpitolaki).

Mainitun lain nojalla työnantajalla on oikeus käsitellä työsuhteen kannalta välttämättömän tarpeellisia henkilötietoja. Tästä *tarpeellisuusvaatimuksesta* ei voida poiketa edes

[276] HE 97/2018

työntekijän suostumuksella. [277] Johtuen työsuhteiden moninaisuudesta ei ole mahdollista antaa kattavaa luetteloa siitä mitä tietoja saadaan käsitellä. Käsittelyn tarpeellisuutta arvioidaan kustakin työtehtävästä lähtien ja tarpeellisuus tulee määritellä henkilötietojen keräämisen yhteydessä. Tarpeellisuusvaatimus tulee huomioida jo työhönottotilanteessa. Työnhakijalta tulee hakemuksessa ja haastattelussa kysyä ainoastaan tietoja, jotka ovat edellytyksenä tehtävän hoitamisen kannalta. Esimerkiksi siviilisäädyn, lasten tietojen tai varusmiespalveluksen ei välttämättä katsota olevan tällaisia. Näiden kysyminen säännönmukaisesti kaikilta hakijoilta ei ole perusteltua.[278]

Henkilöstöstä käsitellään mm. seuraavanlaisia tietoja henkilöstöhallinon tarpeisiin: nimi, yhteystiedot, hetu, verokortti ja ajokortin tiedot. Henkilöstön tietoja käytetään mm. palkanmaksuun, pätevyyden tarkastukseen ja työtodistuksen antamiseksi. Rekrytoinnin yhteydessä yritys kerää haastateltavista perustiedot lomakkeella. Siinä tapauksessa kun rekrytointi päättyy palkkaamiseen, säilytetään rekrytoinnissa kerättyjä tietoja koko työsuhteen keston ajan, jonka jälkeen ne poistetaan.

Kuljetusyritys on henkilöstön tietojen suhteen rekisterinpitäjä. Näin ollen sen tulee mm. informoida rekisteröityjä eli työntekijöitään henkilötietojen käsittelystä tietosuoja-asetuksen edellyttämällä tavalla[279]. Henkilökunnan tietojen käsittelyssä tulee muutoinkin noudattaa asetusta ja sen periaatteita. Esimerkiksi vanhentuneita tietoja ei tule käsitellä.

6.4 Sopimukset

Suurin osa yrityksen suorittamasta henkilötietojen käsittelystä perustuu sopimuksiin. Henkilötietoja myös siirretään edelleen käsiteltäväksi alihankkijoille ja yhteistyökumppaneille. Tietojärjestelmät joissa henkilötietoa käsitellään, on hankittu osto- tai tilaussopimuksilla. Niihin tallennettujen tietojen osalta järjestelmätoimittaja toimii henkilötietojen alikäsittelijänä. Kuljetustenhallintajärjestelmää kehitetään jatkuvasti kuljetusyrityksen toimeksiannosta, mikä johtaa siihen, että järjestelmätoimittaja käsittelee järjestelmässä olevia henkilötietoja viikoittain osana tuki- ja päivityspalveluitaan.

Kartoituksessa huomattiin, että sopimuksissa oli paljon puutteita. Kaikkien toimien kanssa sopimuksia ei esimerkiksi ollut tehty kirjallisina. Suomessa on lähtökohtaisesti voimassa

---

[277] Laki yksityisyyden suojasta työelämässä (759/2004) 2 luvun 3§
[278] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Työelämän tietosuojan käsikirja, viitattu 12.12.2018
[279] esimerkiksi GDPR 12 artikla

sopimuksen muotovapaus, jonka mukaisesti kirjallinen sopimus ei ole edellytys sopimuksen pätevyydelle. Tietosuoja-asetus kuitenkin edellyttää, että henkilötietojen käsittelyä on määritettävä nimenomaan kirjallisella sopimuksella, jollaiseksi myös sähköinen luetaan.[280] Tarkemmin käsittelysopimuksen muotoa ja sisältöä on avattu tämän työn luvussa 3.2. Sopimus henkilötietojen käsittelystä.

Rekisterinpitäjien ja käsittelijöiden keskinäisiä vastuita ja velvoitteita ei voida sopimuksin pätevästi siirtää. Sen sijaan näiden noudattamatta jättämisestä aktualisoituvia sanktioita ja sanktioriskiä voidaan jakaa yksityisoikeudellisilla sopimuksilla[281]. Tästä voi aiheutua yritykselle merkittäviä kustannuksia. Näin ollen on suositeltavaa, että sopimukset on tehty kirjallisena asianmukaisine liitteineen, jotta yritys voi varmistua myös siitä minkälaisia sopimusehtoja sopimuksiin on liitetty.

Kuntien hankkimien kuljetuspalvelusopimusten pohjana ovat yleensä JYSE2014[282] palveluehdot. Niissä säädetään salassapidosta ja henkilötietojen käsittelystä sopimuksen piiriin kuuluvien tietojen osalta. Esimerkiksi juuri tämän sopimuksen vaateisiin vastattiin päivittämällä henkilöstön salassapitosopimuksia (liite 3). Myös järjestelmätoimittajien kanssa tehdyissä sopimuksissa oli puutteita käsittelysopimusten osalta. Näin ollen sopimuksia päivitettiin erillisillä liitteillä henkilötietojen käsittelystä.

6.5 Roolit

Jotta käsittelyn suunnittelussa ja toteutuksessa osattaisiin huomioida kaikki tarpeellinen, oli myös oleellista hahmottaa missä roolissa yritys toimi suhteessa mihinkin tietoon. Roolit vaikuttavat suoraan yrityksen velvollisuuksiin. Roolien hahmottamista vaikeuttivat tietojen moninaiset lähteet sekä päällekkäiset asiakkuudet. Henkilökunta käsittelee tietoja aina siinä roolissa, jossa yritys on suhteessa henkilötietoihin.

Rooli määräytyy sen mukaan, kuka määrittelee henkilötiedon käsittelyn tarkoitukset ja keinot. Tämä taho katsotaan rekisterinpitäjäksi. Kuten aiemmin todettua, käytännössä suurin osa yrityksessä käsiteltävistä henkilötiedoista on sellaisia, joissa rekisterinpitäjänä toimii kunta, joka antaa henkilörekisterin kuljetusyrityksen käsiteltäväksi ostopalvelusopimuksen täytäntöönpanemiseksi. Kuljetusyritys toimii rekisterinpitäjänä niiden tietojen osalta, joissa kuljetuspalvelun tilaajana toimii yksityinen yritys tai henkilö sekä henkilöstänsä tietojen suhteen.

---

[280] GDPR 28 artikla 9 kohta
[281] HE 9/2018 s. 67
[282] Julkisen hankintojen yleiset sopimusehdot palveluhankinnoissa, 2014.

Tällöin tietoja käsitellään rekisteröidyn suostumuksella palvelun tarjoamiseksi tai työsuhteen hoitamiseksi.

Roolit ilmenevät käytännössä suoraan tilaussopimuksissa ja henkilötietojen käsittelystä tehdyissä sopimuksissa. Näiden kartoittamisen apuna käytettiin VAHTI-työryhmän suunnittelemia Exel-taulukoita (liitteet 7 ja 8), jotka muodoltaan vastaavat 30 artiklan mukaista selostetta henkilötietojen käsittelystä. Tietosuoja-asetuksen mukaisesti vastuuta roolilta toiselle ei voida sopimuksin siirtää. Näin ollen rekisterinpitäjän tulee täyttää tietyt velvoitteensa silloinkin, kun se on ulkoistanut käytännössä koko rekisterin käsittelyn.

Käsittelysopimuksin voidaan kuitenkin ohjata rekisterinpitäjää esimerkiksi rekisterin ylläpitoon siten että käytännössä rekisterinpitäjältä saatuja tietoja täydennetään suoraan rekisteröidyiltä. Näin toimitaan esimerkiksi kuljetusyrityksen operoimien koulukuljetusten tapauksessa. Kuljetusten suunnittelua varten yritys saa kunnalta kuljetettavien perustiedot kuten nimen, osoitteen ja aikataulun. Koska sopimus ja kunta edellyttävät, että huoltajat saavat tiedoksi lasten kuljetusajat (nouto- ja hakuaika) tarvitsee yritys myös huoltajien yhteystiedot. Suoraan kunnalta saatavat yhteystiedot ovat usein vanhentuneita, puutteellisia tai niitä ei ilmoiteta lainkaan. Käytännössä aikojen ilmoittaminen tapahtuu tekstiviestitse, mikä ehdottomasti edellyttää ajantasaista tietoa huoltajien puhelinnumeroista. Niinpä yritys päivittää tiedot suodaan huoltajilta itseltään. Tämän lisäksi huoltajat haluavat usein päivittää myös oppilaiden tietoja esimerkiksi apuvälineiden, sairauksien tai erityistarpeiden osalta.

Paljon tietoa kerätään siis suoraan rekisteröidyiltä itseltään (tai huoltajilta kun kyseessä alaikäinen). Jos tietoa käsitellään edelleen alkuperäisen tarkoituksen eli kuljetuspalvelun suorittamiseksi voidaan ajatella, että tiedot kuuluvat samaan rekisteriin ja näin käsittelyn alkuperäisen oikeusperusteen ja käsittelysopimuksen piiriin. Toisaalta voidaan myös ajatella, että todellisuudessa erikseen kerättävien tietojen määrä on suhteellisen suuri ja käsittely kaikin puolin itsenäistä, mikä antaa kuljetusyritykselle mahdollisuuden vaikuttaa erityisesti tiedon käsittelyn keinoihin. Tämä vie yrityksen roolia rekisterinpitäjän suuntaan. Kyseenalaista on, tulisiko ostopalvelusopimuksella kunnan lakisääteisiä tehtäviä hoitava yritys katsoa käsittelijän sijaan yhteisrekisterinpitäjäksi. Jotta voidaan varmistua erityisesti rekisteröidyn oikeuksien ja tietosuojaperiaatteiden riittävästä noudattamisesta on tarkoituksenmukaista, että kuljetusyritys suhtautuu myös tällaisten henkilötietojen osalta rekisterinpitäjän tasoisen osoitusvelvollisuusdokumentaation tuottamiseen.

7 Tulokset

Nykytilakartoituksen jälkeen annoin yritykselle raportin, josta ilmenivät tarvittavat toimet, joilla yrityksen tapa käsitellä henkilötietoja saatettaisiin tietosuojan edellyttämälle tasolle. Olennaista on huomata, että tietosuojatyö on jatkuva prosessi eikä sen menestyksekäs

toteuttaminen näin toteudu yhden projektin aikana. Tietosuojatyön tulee olla osa yrityksen päivittäistä toimintaa. Myös tietosuojadokumentaatiota tulee ylläpitää ja päivittää säännöllisesti.

Työn jatkovaiheessa tuotin edellä esitettyjen selvitysten perusteella yritykselle konkreettisena tuotoksena dokumentit, joiden avulla se pystyy täyttämään tietosuoja-asetuksen mukaisen informointi- ja osoitusvelvollisuutensa[283]. Esittelen nämä dokumentit tarkemmin tässä luvussa. Ensimmäisenä esittelen sisäiseksi dokumentiksi tarkoitetun selosteen henkilötietojen käsittelytoimista. Velvollisuudesta ylläpitää tämän kaltaista selostetta säädetään tietosuoja-asetuksen 30 artiklassa. Selosteen fyysiseen yhteyteen työn yritykselle luovuttaessa liitin myös muuta dokumentaatiota, joka tukee henkilötietojen käsittelytoimien läpinäkyvää avaamista ja osoitusvelvollisuuden periaatetta. Näitä ovat kuvaus henkilöstön koulutuksesta, heille tuotetut ohjemateriaalit, aiemmassa luvussa esitelty nykytila-analyysi ja arvio tietosuojaperiaatteiden toteutumisesta käsittelyssä. Tietojen liittämistä yhteen käsittelytoimia kuvaavan selosteen kanssa perustelen sillä, että yrityksen on tällöin helpompi hahmottaa ja ylläpitää heillä olevaa henkilötietojen suojaan liittyvää materiaalia.

Lisäksi tein yritykselle ”tietosuojaperiaattemme” -selosteen, jolla se täyttää informointivelvoitettaan rekisteröidyn suuntaan (liite 6). Lopuksi annan perustellun arvion siitä, miksen katso yrityksellä tällä hetkellä olevan velvoitetta nimittää tietosuoja-asetuksen tarkoittamaa tietosuojavastaava. Käytännössä arvio on osa sisäistä selostetta käsittelytoimista, mutta selkeyden ja asian tärkeyden vuoksi esittelen sen erillisenä.

Kuten olen aiemmin tämän työn tietoperustassa esittänyt, on osoitusvelvollisuuden mukainen näyttötaakka ensi sijaisesti osoitettu rekisterinpitäjälle. Henkilötietojen käsittelijän tulee kuitenkin omilla toimillaan auttaa rekisterinpitäjää huolehtimaan rekisteröityjen oikeuksien toteutumisesta sekä henkilötietojen turvallisuudesta. Näiden toteuttamisen osoittaminen kuuluu rekisterinpitäjälle osana osoitusvelvollisuutta. Rekisterinpitäjän ja henkilötietojen käsittelijän väliseen henkilötietojen käsittelysopimukseen voidaan kirjata käsittelytoimia koskevia dokumentointivelvoitteita. Näin osoitusvelvollisuus käytännössä jalkautuu myös henkilötietojen käsittelijälle. Osoitusvelvollisuuden täyttämisen edellyttävää dokumentaatiota

Katson tuloksena syntyneen aineiston kattavan asetuksen 30 artiklan mukaisen käsittelytoimia kuvaavan selosteen vaatimukset. Tietoperustan luvussa 2.2. olen esitellyt osoitusvelvollisuuden periaatteen vaatimuksia niin rekisterinpitäjälle kuin käsittelijälle. Katson tuottamani

[283] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Osoita noudattavasi tietosuojasäännöksiä, viitattu 5.12.2018

materiaalin vastaavan näihin. Tuloksia voi pitää kuljetusyritykselle käyttökelpoisina ja toimintaan sopivina ja ne ovat työn tavoitteen mukaisesti sovellettavissa myös muihin. Valitsemani dokumentaatio on arvioni mukaan kattava ja vaikkakin jokaisen yrityksen prosessit ovat erilaiset, on ne mahdollista osoittaa asetuksen edellyttämällä läpinäkyvyydellä koostamalla toiminnasta tämän työn tuloksia vastaavat dokumentit.

7.1 Seloste käsittelytoimista

Apuna käsiteltävien rekistereiden ja tietoryhmien käsittelyn hahmottamiseen käytin apuna VAHTI-työryhmän laatimia Exel-taulukoita (liitteet 7 ja 8 [284]), joihin lisäsin ohjetekstiä jatkokäytön selkeyttämiseksi. Näitä päivittämällä yrityksen on jatkossa helppo pysyä ajan tasalla heillä käsiteltävänä olevista henkilötiedoista, rooleistaan suhteessa tietoon sekä käsittely perusteesta. Käytännössä pohjien otsikointi vastaa asetuksen 30 artiklan mukaista kuvausta käsittelytoimia dokumentoivan selosteen vaatimuksista.

Selosteet sisältävät seuraavat tiedot ja täydentävät ohjeistukset:

Käsittelyn tarkoitukset (rekisterinpitäjä kuvaa): Mihin tarkoitukseen ja millä (oikeus)perusteella käsittely tapahtuu

Kuvaus rekisteröityjen ryhmistä: Käytännössä kuvataan, kenen tietoja käsitellään (esim. kuljetusasiakkaat, henkilöstö)

Kuvaus henkilötietoryhmistä (rekisterinpitäjä kuvaa): Mitä henkilötietoja rekisteröidyistä käsitellään (esim. yhteystiedot, tieto apuvälineestä)

Vastaanottajaryhmät (rekisterinpitäjä kuvaa): Kenelle/minne henkilötietoja luovutetaan. Vastaanottajalla tulee olla lainmukainen peruste henkilötietojen käsittelylle (esim. sopimus). Kuvaa myös vastaanottajan tyyppi (viittauksella sen suorittamiin käsittelytoimiin) ja esimerkiksi toimiala (esim. pilvipalveluntarjoaja).

Tietojen säilytysajat tai määrittämisen kriteerit: Kuvataan eri henkilötietoryhmien poistamisen määräajat tai ne kriteerit joilla käsittelyn pituus määräytyy (esim. asiakkuuden voimassaolo)

*Kuvaus 32 artiklan mukaisista teknisistä ja organisatorisista turvatoimist*a: Kuvaa miten tiedot on suojattu organisaation ulkopuolisilta, miten käyttöoikeudet rajattu yrityksen sisällä,

---

[284] https://tietosuoja.fi/rekisterinpitajan-seloste-kasittelytoimista

miten käyttöoikeuksia valvotaan. Huomaa tallentaa myös tämä seloste tietoturvallisesti, mikäli tässä kohdassa kuvataan yksityiskohtaisesti yrityksen tietosuojakäytäntöjä.

Olen seuraavassa nostanut vielä erikseen käsittelyn oikeusperusteiden ja tietosuojaperiaatteiden toteutumisen arvioinnin. Käsittelyn oikeusperusteet ilmenevät selosteesta käsittelytoimista (esitellyt exelit), mutta selkeyden vuoksi avaan niitä vielä kerran tässäkin yhteydessä. Kun yrityksen suorittama henkilötietojen käsittely tapahtuu rekisterinpitäjän lukuun ei yrityksen sinänsä tarvitse miettiä mihin rekisterinpitäjän käsittelyoikeus perustuu. Kokonaisuuden kannalta ajattelen tämän hahmottamisen olevan kuitenkin hyödyllistä, johtuen osin siitä, etteivät käsittelysopimukset (kuten todettua) aina sisällä kattavaa ohjeistusta tietojen käsittelystä. Tällaisessa tapauksessa sen hahmottaminen mitä varten rekisterinpitäjä on tiedot kerännyt auttaa myös käsittelijää ymmärtämään mihin tietoja voidaan käyttää ja mitä niiden käsittelyssä tulee huomioida.

7.1.1 Käsittelyn oikeusperusteiden arviointi

Suurin osa yrityksessä tapahtuvasta henkilötiedon käsittelystä perustuu kuljetuspalvelun tilaajan kanssa tehtyyn sopimukseen, mikä huomattiin myös täyttäessä edellä esiteltyä selostetta käsittelytoimista. Käsittelyn oikeusperuste pääsääntöisesti lakkaa sopimuksen/sopimuskauden päättyessä, jollei kyse ole suoraan yksityisasiakkaan kanssa tehdystä sopimuksesta.

Käsiteltäessä henkilön terveyteen liittyviä tietoja käsittely perustuu yleisimmin sopimukseen palvelun tuottamisesta. Tällöin tiedot saadaan suoraan rekisterinpitäjältä ja yritys toimii tiedon suhteen käsittelijänä rekisterinpitäjän antamaa ohjeistusta noudattaen. Käytännössä rekisterinpitäjän oikeus käsitellä erityisiin henkilötietoryhmiin kuuluvia tietoja voi perustua esimerkiksi 9 artiklan 2 kohdan b alakohtaan, joka mahdollistaa aiemmin esitellysti (luku 3.3 Erityiset henkilötiedot) käsittelyn rekisterinpitäjän velvoitteiden tai rekisteröidyn oikeuksien noudattamiseksi. Myös jonkin asetuksen 6 artiklan mukaisista laillisuuden edellytyksistä tulee tällöin täyttyä. Tällainen on esimerkiksi vammaispalvelulain mukainen kunnan velvollisuus järjestää kuljetuspalvelu vammaiselle henkilölle[285]. Jotta palvelun tarjoamisesta vastuussa oleva julkinen toimija voi arvioida rekisteröidyn oikeuden palveluun ja tarjota lain edellyttämän palvelutason, tulee sen luonnollisesti käsitellä tietoa rekisteröidyn terveydentilasta. Sama tieto on oleellista siirtää kuljetusyritykselle palvelun tuottamisen ajaksi. Sinänsä tieto henkilön saamasta palvelusta tai etuudesta ei ole nykyisen tietosuoja-asetuksen mukaan salassa

[285] Laki vammaisuuden perusteella järjestettävistä palveluista ja tukitoimista (380/1987)

pidettävää tietoa, mutta varsinainen palvelun perusteena oleva terveystieto on. Jatkossa oikeudesta käsitellä tällaista tietoa tullaan säätämään tarkemmin tietosuojalaissa.[286]

7.1.2 Arvio tietosuojaperiaatteiden toteutumisesta

Henkilötietojen käsittelyssä huomioitavista periaatteista säädetään tietosuoja-asetuksen 5 artiklassa ja niitä on esitelty tarkemmin tämän työn luvussa 2.1 Tietosuojaperiaatteet. Kuljetusyritys pyrkii enenevissä määrin huomioimaan periaatteet toiminnassaan. Seuraavassa nostan esimerkkejä tästä.

Lainmukaista, kohtuullista ja läpinäkyvää käsittelyä toteuttamaan laadittiin ”tietosuojaperiaattemme” -seloste (liite 6). Se on hiukan entisen henkilötietolain edellyttämän rekisteriselosteen mallinen kuvaus henkilötietojen käsittelystä rekisteröidylle ja toteuttaa yrityksen informointivelvoitetta. Seloste on kuitenkin laajempi kuin rekisteriseloste ja siinä kuvataan asetuksen edellytysten mukaisesti myös rekisteröidyn asetuksenmukaiset oikeudet. Rekisteröity saa selosteesta tiedon siitä, millaisia henkilötietoja yritys toiminnassaan käsittelee ja mihin käsittely perustuu. Jälkimmäisen myötä seloste kuvaa osaltaan myös sitä, että yritys huomioi käsittelyssä tietojen *käyttötarkoitussidonnaisuuden periaatteen*.

Tehty nykytila-analyysi paljasti yrityksellä olevan kohtuullisen paljon henkilötietovarantoja, joiden säilyttämiselle ei ollut perustetta. Yritys laati sisäisen ohjeistuksen tietojen poistamiseksi ja aloitti järjestelmätoimittajan kanssa projektin, jossa se *sisäänrakennettua- ja oletusarvoista tietosuojaa* parantamalla nostaa kykyään huolehtia myös *säilytyksen rajoittamisen* sekä *tietojen minimoinnin periaatteista*.

Henkilökuntaa kouluttamalla ja oheistuksia laatimalla parannettiin organisatorisin toimin tietojen *eheydestä ja luottamuksellisuudesta huolehtimista*. Jo aiemmin käyttöönotettujen järjestelmien sisällä tehtiin vielä tarkastuksia käyttäjätasoihin ja käyttäjätunnusten hallintaan.

Kaiken kaikkiaan voidaan sanoa, että tehdyn työn myötä kuljetusyritys ymmärtää kuinka tietosuojaperiaatteet huomioidaan toiminnassa ja mikä hyöty niistä on toiminnan kokonaisuuden ohjaajina.

7.2 Henkilöstön koulutus ja ohjeistukset henkilöstölle

Kustannustehokkain tapa nostaa tietoturvan tasoa on henkilöstön kouluttaminen[287]. Ohjeistuksilla ja tietoturvatietoisuuden kehittämisellä voidaan säästyä kalliimmilta

---

[286] HE 9/2018 s. 88
[287] VAHTI 3/2012, Teknisen ICT-ympäristön tietoturvataso-ohje s. 14, viitattu 27.11.2018

järjestelmäkehitys/-hankintaprojekteilta sekä välillisesti syntyviltä kustannuksilta (virheistä aiheutuvat tietoturvapoikkeamat). Kouluttamalla henkilöstöä huolehditaan myös heidän oikeusturvastaan antamalla heille riittävät edellytykset huolehtia vastuistaan ja tehtävistään henkilötietojen käsittelyssä.

Kuvio 5: Koulutuksen suunnittelu[288]

Kuvion 2 mukaisessa lähtötilanteessa pohdin ensin koulutukseen osallistujia, käytössä olevia välineitä ja mahdollisia käytettäviä materiaaleja. Koulutuksen onnistunutta toteutusta varten päätin jakaa henkilöstön kahteen ryhmään työnkuviensa perusteella: toimisto henkilökunta ja kuljettajat. Eri tehtävissä henkilötietoja käsitellään eri laajuudessa ja tavalla, joten tiedon tarve ja esittämistapa tuli miettiä kullekin ryhmälle sopivaksi. Käytännössä koulutukset tuli toteuttaa kuljetusyrityksen toimistolla, muun työn lomassa. Hektisen arjen vuoksi kaikilla ei ollut mahdollisuutta olla koulutettavana samalla kertaa. Näin ollen koulutustilaisuuksia pidettiin useampia niin että jokainen ehti osallistua.

Toimistolla ei ollut varsinaista kokoustilaa, joten koulutukset tuli pitää toimiston aulassa, jossa ei ollut lainkaan esitystekniikkaa. Suunnittelin siis koulutukset vuorovaikutteisiksi niin että alustin aiheita hetken, jonka jälkeen keskustelimme. Näin henkilöstö pääsi kysymään heitä askarruttavia työhönsä oleellisesti liittyviä asioita ja pysyi motivoituneena läpi tilaisuuden. Koska henkilöstö tunsi toisensa hyvin en kokenut suurien ryhmäkokojen haittaavaan koulutusta vaan lopputuloksena keskustelu oli monipuolista ja kaikkia osallistavaa. Koulutuksen yhteydessä kaikki myös allekirjoittivat työsopimustensa liitteeksi salassapitosopimukset ja saivat materiaalipaketin, joka sisälsi käytännön ohjeita työarjen tilanteisiin (Liite 2: Tietosuojainfo kuljettajille). (Kuvio 2 Toimenpiteet)

[288] VAHTI-ohje, Koulutustilaisuuden suunnittelu ja toteutus. Mukaillen

Toimiston puolella henkilötietoja käsittelevät ajojärjestelijät ja palkanmaksua ynnä muita hallinnollisia toimia hoitavat henkilöt. He käsittelevät kuljetettavien, henkilökunnan ja alihankkijoiden tietoja. He olivat olleet jossain määrin (osa aktiivisesti) mukana prosessien nykytilakartoituksessa, jonka yhteydessä oli käyty läpi pääasiassa henkilökuljetuksissa liikkuvien henkilötietojen prosesseja. Varsinaista tietoa tietosuoja-asetuksen vaatimuksista heillä ei ollut. En myöskään ollut vielä kattavasti esitellyt heille ehdotuksia siitä, kuinka prosesseja tulisi muuttaa, jotta ne vastaisivat asetuksen vaatimuksiin.

Kuljettajat puolestaan käsittelevät nimenomaan matkustajatietoja. Suurimmalla osalla kuljettajista ei ollut minkäänlaista ennakkotietoa tietosuoja-asetuksesta eikä ehkä edes aiemman henkilötietolainsäädännön velvoitteista. He käsittelivät matkustajien tietoja lähinnä toimiston ohjeistuksen perusteella tai kuten katsoivat olevan työnsä puolesta tarpeellista. Toimistohenkilöstöllä oli myös kuva siitä, etteivät kuljettajat olleet sisäistäneet rooliaan henkilötietojen käsittelijöinä eivätkä olleet tietoisia siitä mitä tietosuoja käytännössä tarkoitti. Kuljettajat vaihtoivat keskenään avoimesti tietoa matkustajista ja satunnaisesti vaihdettiin myös kuljetuslistoja viestimättä tästä ensin ajojärjestelylle. Sisällön suunnittelussa pyrin huomioimaan sen, että kuljettajat saisivat riittävän tiivistetyn mutta informatiivisen käytännön ohjeistuksen henkilötietojen käsittelystä arjen tilanteissa.

Kuvion 2 mukaisesti koulutuksen tavoitteet jaettiin tiedollisiin, taidollisiin ja asenteisiin liittyviin tavoitteisiin seuraavasti:

Tiedolliset tavoitteet:
- Ymmärrys yrityksen tietosuoja-asetuksen mukaisista rooleista
- Ymmärrys rooleihin liittyvistä vastuista/velvoitteista/vaatimuksista
- Ymmärrys omista henkilökotaisista vastuista/oikeuksista henkilötietojen käsittelijänä
- Tieto rekisteröidyn oikeuksista

Taidolliset tavoitteet:
- Kyky huolehtia tietosuojasta ja -turvasta päivittäisessä työssä
- Kyky havaita tietosuojapoikkeamat ja reagoida niihin
- Kyky vastata rekisteröidyn pyyntöön liittyen asetuksen mukaisten oikeuksiensa käyttämiseen

Asenteelliset tavoitteet:
- Sitoutuminen tietosuojatyöhön
- Halu huolehtia henkilötietojen suojasta työssään
- Ymmärrys oman toiminnan merkityksestä osana tietosuojaa ja yrityksen brändiä
- Kokee tietosuojan merkitykselliseksi ja arvokkaaksi

Seuraavassa esittelen tiivistettynä koulutuksessa läpikäytyjä aiheita. Niiden lisäksi koulutuksessa käytiin läpi ja keskusteltiin tietosuoja-asetuksesta yleisesti, rekisteröidyn oikeuksista ja

henkilökunnan roolista asetuksen toteuttamisessa. Liiallisen toiston välttämiseksi jätän kertaamisen tässä yhteydessä pois.

Pääsynhallinta

Projektin aluksi yritykseltä puuttui malli käyttövaltuuksien hallintaan. Suositin keskittämään käyttövaltuuksien hallinnan parille henkilölle, jotka sitten myös huolehtisivat vanhentuneiden ja tarpeettomien käyttöoikeuksien/-tunnusten poistamisesta järjestelmistä.

Painotin henkilökohtaisten tunnusten tärkeyttä erityisesti siksi, että olimme toimintamallien kartoituksen yhteydessä havainneet riskin siihen, että oikeudetonta tietoihin pääsyä[289] voisi tapahtua ja tiedettiin aiemmin tapahtuneenkin. Esimerkiksi alihankkijayrityksillä saattoi olla kuljetustenvälitysohjelmaan käytössään vain yksi tunnus, joka oli tiedossa kaikilla kyseisen yrityksen kuljettajilla. Kuljettaja kirjautui tunnuksella puhelinsovellukseen, jonka kautta hän sai tietoonsa päivän ajolistan eli kuljetettavien tiedot. Yhden tunnuksen malli johti siihen, ettei toimeksiantajayrityksen ajojärjestelyllä ollut todellista ja reaaliaikaista tietoa siitä kuka henkilö todellisuudessa oli kulloinkin tunnusten käyttäjänä eli kuljettajana. Näin he eivät tarvittaessa pystyneet todentamaan sitä kuka henkilötietoja käsitteli, mutta myös asiakaspalvelu ja kuljettajien työsuoritteiden seuranta vaikeutuivat.

Näin asian ongelmallisena myös kuljettajien oman oikeusturvan kannalta. Kuljetustenhallintajärjestelmä lokittaa eli kerää tietoa esimerkiksi siitä millä tunnuksilla matkoja on ajettu, missä kuljettajan ajama auto liikkuu sekä kuinka monta tuntia/kilometriä ajoa on kertynyt. Näitä tietoja käytettiin työ- ja alihankintasopimusten mukaan työvelvoitteiden seurantaan kuin myös käytettiin palkan maksun perusteena. Mahdollisissa ongelmatilanteissa (koskivatpa ne sitten henkilötietojen käsittelyä tai muuta) olisi helpompaa selvittää tapahtunutta, kun jokainen kuski operoisi järjestelmässä henkilökohtaisella ja vain itsellään tiedossa olevalla tunnuksella.

Yrityksen toimintaympäristö

Yrityksessä käsitellään paljon henkilötietoja, joiden joukossa paljon myös erityisiin henkilötietoryhmiin kuuluvia tietoja. Näiden tietojen käsittelyssä tulee noudattaa erityistä tarkkuuttaa ja ymmärtää käsittelystä rekisteröidylle aiheutuva riski. Päivittäisessä työssä tietoa liikutellaan paljon henkilöltä toiselle. Useimmiten tiedon siirto tapahtuu sähköisesti joko kuljetustenhallintajärjestelmässä tai sähköpostitse. Jonkin verran tietoa liikkuu myös paperilla

[289] Tietoihin pääsyllä tarkoitetaan ”oikeutta, mahdollisuutta tai menetelmää tiedon hakemiseen, löytämiseen ja käyttämiseen” (Kansallisarkisto, Sanasto: Pääsy tietoihin”, viitattu 19.11.2018)

ajolistojen, kuittien ja ajopäiväkirjojen muodossa. Työntekijöiden kanssa keskusteltiin kuhunkin tiedonsiirto tapaan liittyvistä prosesseista, riskeistä, hyödyistä ja ongelmista.

Yrityksessä työskennellään paljon etänä yrityksen toimitilojen ulkopuolella. Ajojärjestelijät tekevät työtään pääosin toimistolla, mutta viikoittain myös etätyönä kotoa käsin. Tällöin he käyttävät yleensä omia henkilökohtaisia laitteitaan. Kuljettajat ovat työnsä luonteesta johtuen kuljettajat paljon ns. ”kentällä” eli he suorittavat suurimman osan työstään muualla kuin työnantajan tiloissa. He myös tapaavat etänä toisiaan ja keskustelevat töihin liittyvistä asioista, jolloin ulkopuolisen mahdollisuus kuulla asiakkaisiin liittyviä tietoja on hyvin realistinen. Kuljetussovelluksen avaamiseen he käyttävät satunnaisesti myös henkilökohtaisia puhelimiaan.

Keskustelimme etätyöhön liittyvistä tietosuojariskeistä. Henkilökuntaa ohjeistettiin käyttämään asiakkaiden tietojen käsittelyyn ainoastaan työantajalta saatuja tai muuten hyväksyttyjä laitteita. Työntekijän vastuulla on huolehtia, etteivät tunnukset ja salasanat päädy muiden tietoon. Niin ikään tulee varmistua siitä, etteivät esimerkiksi perheenjäsenet käytä työtehtävien hoitoon varattua työnantajan laitetta tai saa muutoin muodostettua yhteyttä yrityksen tietojärjestelmiin. Tietosuojasta tulee huolehtia myös mukana pidettävien papereiden ja etätyössä käytyjen puhelinkeskustelujen osalta. Etätyöskentelyssä on hyvä välttää tiedon tulostamista ja tallentamista tietovälineelle, etenkin jos käytössä on muu kuin työnantajan laite. Yrityksessä on käytössä Windows Sharepoint tiedoston jako, mikä mahdollistaa aineiston keskittämisen ja jakamisen kirjautuneiden käyttäjien kesken digitaalisessa ympäristössä. Sharepointiin tallennettu aineisto on siis käsiteltävissä myös etänä eikä edellytä tallentamista paikalliselle koneelle. Tämä edistää tietoturvallisen etätyöskentelyn ohella tiedon ajantasaisuutta ja löydettävyyttä. Etätyöhön viedyt ja tulostetut paperit tulee palauttaa työpaikalle tai muutoin hävittää asianmukaisesti esimerkiksi silppuamalla. Käytettäessä muita kuin työnantajan laitteita, tulee työntekijän huolehtia laitteen asianmukaisesta suojauksesta samoin periaattein kuin työnantajan laitteissa (esimerkiksi palomuuri).[290]

Tietoturvaloukkauksista ilmoittaminen

Yritys on velvollinen arvioimaan tapahtuneiden tietoturvaloukkausten vakavuus ja toimimaan sen vaatimalla tavalla. Tarvittaessa tapahtuneesta tulee ilmoittaa eteenpäin asetuksen ja erikseen laaditun mallin mukaan (liite 4). Tavoitteena on, että tietosuojaloukkauksesta mahdollisesti aiheutunut vahinko voidaan minimoida. Tietosuojaloukkaus on tilanne, jossa

[290] Opitietosuojaa.fi: Tietoturva ja tietosuoja etätyössä, viitattu 30.11.2018

henkilötietoja on voinut pääty ulkopuolisen tietoon tai niiden eheys ja luottamuksellisuus on muuten vaarantunut.

Koulutettavien kanssa keskusteltiin siitä, millaisissa tilanteissa henkilötietoja voisi kadota/muuttua/pääty oikeudettomasti ulkopuolisen tietoon. Kävimme läpi ja pohdimme toimintamallia esimerkiksi seuraavissa tilanteissa:
- ajolista on kadonnut
- henkilötietoja sisältävä laite on kadonnut, varastettu tai jäänyt lukitsematta julkisella paikalla (tiedot ovat siis käytännössä olleet kenen tahansa nähtävillä)
- tietoja on luovutettu ulkopuolisille luvattomasti

Kaikki olivat yhtä mieltä siitä, että ajojärjestelyn on tietojen ensisijaisena käsittelijänä hyvä olla tietoinen kaikista tilanteista, joissa kuljettaja epäilee tietosuojan mahdollisesti vaarantuneen. Ajojärjestely voi sitten tehdä arvion tilanteesta ja sovellettavista toimenpiteistä. Ilmoittamistarpeen harkinnassa asiaan suhtaudutaan vakavasti, mutta pienistä asioista ei ilmoiteta turhaan. Mikäli tapahtunut ei edellytä toimia, ajojärjestely kuitenkin kirjaa tapahtuneen yleiskuvauksen. Tämä antaa pidemmällä aikavälillä mahdollisuuden tarkastella tyypillisesti henkilötietojen käsittelyssä tapahtuvia ongelmia, minkä kautta käsittelyprosesseja voidaan suunnitella toimivammiksi ja edelleen turvallisimmiksi. Ajojärjestelylle laadittiin selkeä ohje tietoturvaloukkausten vakavuuden arviointiin ja ilmoittamiseen (liite 4).

7.2.1 Salassapitosopimukset

Kaikilla yrityksen henkilöstöstä ei ollut voimassa olevia salassapitosopimuksia. Jollakin salassapitolauseke oli sisällytetty työsopimuksen yhteyteen. Kaikki salassapitosopimukset päätettiin päivittää ja puuttuvat allekirjoittaa tietosuojakoulutuksen yhteydessä. Laatimani salassapitosopimus liitteessä 3. Pyrin salassapitosopimuksen laadinnassa kattavuuteen ja informatiivisuuteen niin että henkilöstö ymmärsi sopimuksen sisällön ennen allekirjoittamista. Tätä tuki samassa yhteydessä järjestetty koulutus.

Vaitiolovelvollisuudesta tullaan säätämään tarkemmin kansallisessa tietosuojalaissa. HE 9/2018 35§:ssä suunnitellaan säädettäväksi yleisestä vaitiolovelvollisuudesta, jonka piiriin kuuluvat kaikki henkilötietojen käsittelyyn liittyvät toimenpiteet. Vaitiololla tarkoitetaan sitä, ette henkilö saa oikeudettomasti ilmaista tietoonsa saamiaan vaitiolovelvollisuuden alaisia asioita sivulliselle. Vaitiolovelvollisuus koskisi paitsi henkilötietoja, myös liike- ja

ammattisalaisuuksia. Se velvoittaisi kaikkia henkilötietojen käsittelyyn osallistuvia tahoja, heidän työntekijöitään ja tietosuojavastaaviaan.[291]

Kuljetusyritys käsittelee paljon henkilötietoja perustuen sopimukseen palvelun tuottamisesta kaupunkien ja kuntien kanssa. Nämä noudattavat muun muassa julkisuuslaissa olevia salassapitoa ja yksityisyyden suojaa koskevia säännöksiä. Näin ollen myös henkilötietojen käsittelijöiden eli yrityksen työntekijöineen tulee noudattaa samoja säännöksiä käsitellessään julkishallinnon toimijoiden henkilörekistereitä.

Tietoa käsittelevät myös alihankkijat. Työnjohdon tulee yritysten välisin sopimuksin varmistua siitä, että kaikilla henkilötietoja käsittelevillä on voimassa oleva salassapitosopimus tai he ovat muutoin salassapitovelvollisia siten kuin rekisterinpitäjät edellyttävät.

7.3 Arvio tietosuojavastaavan tarpeesta

Tietosuoja-asetus edellyttää, että tietyissä tilanteissa yritys nimittää tietosuojavastaavan. Hänen tehtävänään on toimia sisäisenä asiantuntijana, joka seuraa tiedon käsittelyä ja tietosuojasäännösten noudattamista. Hän tuo esiin havaitsemansa puutteet, neuvoo henkilöstöä oikeanlaisessa tiedon käsittelyssä ja toimii yhteyshenkilönä rekisteröidyille.[292] Velvollisuudesta nimittää tietosuojavastaava säädetään tietosuoja-asetuksen 37 artiklassa. Asetuksen mukaan tietosuojavastaavan nimittäminen on pakollista kun:

a) tietojen käsittelyä suorittaa viranomainen tai julkishallinnon elin (muu kuin tuomioistuin)

b) rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät rekisteröityjen järjestelmällistä ja säännöllistä seurantaa

c) rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat *erityisiin henkilötietoryhmiin* (ja eräisin muihin ryhmiin) kuuluvien tietojen laajamittaisesta käsittelystä.[293]

Esitetyn c-kohdan mukaisilla ”ydintehtävillä” tarkoitetaan keskeisiä avaintoimintoja, jotka ovat edellytyksenä käsittelevän tahon tavoitteiden saavuttamiselle. Jotkin yrityksen suorittamista toimista voivat olla välttämättömiä, mutta niitä ei itsessään pidetä ydintehtävinä, jos

---

[291] HE 9/2018 s. 120
[292] Tietosuojavaltuutetun toimisto (tietosuoja.fi), Tietosuojavastaavat, viitattu 19.1.2018
[293] GDPR 37 artikla 1 kohta. Kohdat a-c ovat lyhennelmiä asetuksen täydestä säädöstekstistä.

ne tukevat arvoketjussa ensisijaisempien toimintojen suorittamista[294]. ”Laajamittaista” käsittelyä arvioitaessa tulee ottaa huomioon käsiteltävien henkilötietojen lukumäärä, rekisteröityjen lukumäärä ja käsittelytoiminnan kesto.[295]

Kuljetusyritys käsittelee paljon henkilötietoja, joihin sisältyy jonkin verran *myös erityisiin henkilötietoryhmiin kuuluvia tietoja* (kuljetusasiakkaat). En katso tällaisten tietojen käsittelyn kuitenkaan olevan laajamittaista siinä mielessä kuin tietosuoja-asetus määrittelee. Henkilötietoja käsitellään vain niiltä osin kuin se on välttämätöntä kuljetusten turvallisuuden varmistamiseksi ja kuljetuspalvelusopimusten täyttämiseksi. Esimerkiksi tieto pyörätuolista tai epilepsiasta voidaan katsoa erityisiin henkilötietoihin kuuluvaksi niiden kertoessa henkilön terveydestä tai vammaisuudesta. Tieto on välttämätöntä oikeanlaisen kuljetuskaluston varaamiseksi ja turvallisen kuljetuksen hoitamiseksi.

En myöskään katso kyseisten henkilötietojen käsittelyn olevan osa yrityksen *ydintehtäviä* vaan oheis- ja tukitoiminto ydintehtävän eli kuljetusten toteuttamiselle. Rekisteröityjä en katso järjestelmällisesti seurattavan, vaikka tuleekin huomioida, että kuljetusasiakkaiden matkoista jää yritykselle toteumatiedot. Nämä tiedot ovat niin ikään välttämättömiä kuljetussopimuksen täyttämiseksi.

Muutoin seurannasta: Toiminnan luonteesta johtuen, autoja seurataan niihin asennetuilla paikannuslaitteilla. Tämän lisäksi kuljettajat käyttävät työpäivänsä aikana puhelimella järjestelmää, joka suorittaa paikannusta GPS-signaaliin perustuen. Paikkatieto jää järjestelmään, jota ajojärjestelijät käyttävät ajotilausten välittämiseen kuljettajille. Käytännössä nämä signaalit kertovat työntekijän (rekisteröity) sijainnin, mutta tarkoituksena on paikantaa autoja eli kuljetuskapasiteettia. Näin ollen sijaintia ei käytetä perusteena työsuhteen ehtojen noudattamisen valvonnassa (esim. työajan seurannassa). Paikantamiseen on työntekijöiden suostumus.

Arvioni mukaan kuljetusyrityksellä ei ole yksiselitteistä velvoitetta nimittää tietosuoja-asetuksen mukaista tietosuojavastaavaa. Henkilötietojen suojan toteutumisen varmistamiseksi voisi kuitenkin olla suotavaa nimittää henkilö joka pitää pääasiallista vastuuta tietosuojatyöstä ja vastaa esimerkiksi rekisteröityjen kysymyksiin. Myös henkilökunnan asianmukaisella koulutuksella ja tietosuojataitojen ylläpidolla varmistetaan tietosuojan toteutumista. Yrityksen tietosuojan tila tulee arvioida tietyin väliajoin (esimerkiksi puolivuosittain) sekä tilanteissa, joissa tietojen käsittelyprosessit muuttavat. Tällaisia tilanteita voivat olla esimerkiksi uuden ohjelmiston käyttöönotto, uuden sopimuksen alkaminen, vanhan sopimuksen muutokset tai uusien

[294] Strategy Train, Tukitoiminnot, viitattu 19.11.2018
[295] Tietosuojatyöryhmä WP 29, Tietosuojavastaavia koskevat ohjeet s. 21, viitattu 19.11.2018

henkilötietojen käsittelyn aloitus muulla perustein. Tietosuojatyö voidaan organisoida säännölliseksi esimerkiksi vuosikellomallilla.

8 Yhteenveto

Epäselvät henkilötietojen käsittelyn prosessit johtavat tehottomaan ja pahimmillaan virheelliseen tietojen käsittelyyn. Tämä puolestaan aiheuttaa yritykselle ongelmia, jotka ilmenevät esimerkiksi työn tehottomuutena, viivästymisenä, asiakkaiden tyytymättömyytenä, lisääntyneinä selvitysprosesseina ja työntekijöiden epävarmuutena. Nämä johtavat yleensä ylimääräisiin kustannuksiin turhan työn tai jopa sakkojen ja vahingonkorvausten muodossa. Yritykselle on siis tärkeää kiinnittää huomiota henkilötietojen käsittelyyn sekä toimintansa laillisuuden että tehokkuuden takia. Tietosuojatyö on hyvä mieltää lain toteuttamista kokonaisvaltaisemmaksi tuottavan liiketoiminnan suunnitteluksi.

Työn aloitusvaiheessa kenelläkään yrityksessä ei ollut kokonaiskuvaa käsiteltävien henkilötietojen määrästä, tyypistä eikä usein edes tiedon lähteestä ja omistajasta. Vastaavasti tiedon hallinnalle, etenkään poistamiselle ei ollut mallia. Vanhentunutta henkilötietoa oli kertynyt huomattavia määriä erilaisiin epävirallisiin arkistoihin. Työntekijöillä ei ollut kuvaa omista velvollisuuksistaan, vastuistaan, roolistaan tai oikeuksistaan tiedon käsittelyssä. Epävarmuus ja osaamattomuus lisäsivät rekisteröidylle käsittelystä aiheutuvaa riskiä.

Henkilötietojen suojasta huolehditaan parhaiten viemällä tietosuoja osaksi jokapäiväisiä toimintaprosesseja. Tällöin työntekijän ei tarvitse jatkuvasti hakea vastauksia siihen, kuinka henkilötietojen suojaa toteutetaan vaan se on sisäänrakennettu koko yrityksen toimintaan. Tietoisuus oman roolin vaikuttavuudesta on kuitenkin motivoiva seikka. Tietosuojatyö on jatkuvaa tekemistä, jonka tulee jatkua myös nyt tehdyn projektin jälkeen. Toimintatavat tulee tarkastaa ja niitä tulee muuttaa sen mukaisesti millaisia palveluita, mille asiakaskunnalle ja millä järjestelmillä yritys kulloinkin tuottaa. Viime kädessä tietosuojasta huolehtiminen on johdon vastuulla.

Projektin loputtua yrityksellä oli toimintasuunnitelma mm. henkilötietojen elinkaaren hallintaan, tietoturvapoikkeamien havainnointiin ja reagointiin. Yrityksellä on tarvittava kyky tietosuoja-asetuksen mukaisten osoitus- ja informointivelvoitteidensa täyttämiseen. Vanhojen tietojen poistaminen järjestelmistä on projekti, jota jatketaan yhteistyössä järjestelmätoimittajien kanssa. Esimerkiksi kuljetustenhallintajärjestelmään toimittaja on rakentamassa erillistä näkymää tietojen säilytysaikojen hallintaa varten.

Saatavilla olevan materiaalin ja tapausesimerkkien puute vaikeutti asetuksen tulkintaa yrityksen näkökulmasta. Lainsäädännössä vallitseva välivaihe, jossa tietosuoja-asetus ohittaa henkilötietolain mutta kansallinen tietosuojalaki on vasta eduskunnan käsittelyssä tuo haastetta esimerkiksi käsittelyperusteiden laillisuuden arviointiin. Tietosuoja-asetuksen

moniulotteisuus, keskenään jossain määrin päällekkäiset säännökset sekä määrämuotoisten dokumenttimallien puuttuminen (vrt. esim. entinen rekisteriseloste) tekevät asetuksen vaatimusten ymmärtämisestä haastavaa erityisesti silloin, jos yrityksessä ei ole sisäistä juridista osaamista tai halua tämän kehittämiseen. Jatkossa tietosuojatyölle ja tulkinnalle saadaan luultavasti tukea myös kansallisen valvontaviranomaisen antamista ohjeistuksista.

Lähteet

Painetut

Andreasson, A., Rikkonen, J. & Ylipartanen, A. 2017. Osaava tietosuojavastaava. Tallinna: Printon. Tietosanoma Oy.

Sähköiset

Finlex.fi. Lainlaatijan EU-opas, Kansallisten säädösten valmistelua koskevat ohjeet 1.1. Viitattu 2.11.2018.
http://eu-opas.finlex.fi/1-eu-oikeus-osana-suomen-oikeusjarjestysta/1-1/

Eduskunta.fi. Lainsäädäntö. Viitattu 13.11.2018
https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/kotimaiset-oikeuslahteet/Sivut/Lainsaadanto.aspx

Eduskunta.fi. Lain säätäminen. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Viitattu 13.11.2018
https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_9+2018.aspx

Euroopan komissio. Mikä on rekisterinpitäjä tai tietojen käsittelijä?. Viitattu 5.12.2018.
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_fi

Euroopan komissio. Mitä tietoja voidaan käsitellä ja millä ehdoilla?. Viitattu 5.12.2018.
https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-data-can-we-process-and-under-which-conditions_fi

Euroopan komissio. Tietosuoja. Viitattu 26.11.2018.
https://ec.europa.eu/info/law/law-topic/data-protection_fi

Euroopan unioni. EU:n perussopimukset. Viitattu 2.11.2018.
https://europa.eu/european-union/law/treaties_fi

Euroopan unionin perusoikeuskirja, EUVL N:o C 326, konsolidoitu toisinto 26.10.2012, s. 391.
https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:12012P/TXT&from=fi

Euroopan unionista tehdyn sopimuksen kosolidoitu toisinto. EUVL N:o C 326, 26.10.2012, s 47.
https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:12012E/TXT&from=FI

Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin

96/46/EY kumoamisesta (yleinen tietosuoja-asetus). EUVL N:o L 119, 4.5.2016, s. 1.
https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=fi

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta. EUVL N:o 119, 4.5.2016, s. 89.
https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016L0680&from=FI

Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. EUVL N:o L 281, 23.11.1995.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fi:HTML

European Comission. How will EU's reform adapt data protection rules to new technological developments? Viitattu 26.11.2018.
https://ec.europa.eu/newsroom/just/document.cfm?doc_id=41526

European Comission. How does the data protection reform strengthen citizens' rights? Viitattu 26.11.2018.
http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41525

Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi (HE 9/2018).
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_9+2018.pdf

Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi (HE 96/1998). Viitattu 2.11.2018.
https://www.finlex.fi/fi/esitykset/he/1998/19980096

Hallituksen esitys eduskunnalle laeiksi yksityisyyden suojasta työelämässä annetun lain ja lasten kanssa työskentelevien rikostaustan selvittämisestä annetun lain 10§:n muuttamisesta (HE 97/2018)
https://finlex.fi/fi/esitykset/he/2018/20180097

Henkilötietolaki 523/1999. Viitattu 2.11.2018.
https://www.finlex.fi/fi/laki/ajantasa/1999/19990523

Kansallisarkisto. Arkistowiki, Sanasto. Viitattu 19.11.2018
http://wiki.narc.fi/arkistowiki/index.php/Luokka:Sanasto

Kauppakamari. Jäsentiedote 5/2017. Viitattu 14.12.2018
https://jasentiedote.fi/fi/jasentiedote/helsingin-seudun-kauppakamari/2017/5/mita-ovat-yleiset-sopimusehdot-yset-ja-mista-niita-saa/

Kirjanpitolaki 1336/1997. Viitattu 4.12.2018.
https://www.finlex.fi/fi/laki/ajantasa/1997/19971336

Lakivaliokunnan lausunto (LaVL) 5/2018 vp – HE 9/2018vp
https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/LaVL_5+2018.pdf

Laki yksityisyyden suojasta työelämässä 759/2004. Viitattu 7.12.2018
https://www.finlex.fi/fi/laki/alkup/2004/20040759

Lissabonin sopimus Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta. EUVL N:o C 306 17.12.2017, s. 1. (Lissabonin sopimus)
https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=OJ:C:2007:306:FULL&from=FI

Rikoslaki 39/1889. Viitattu 30.11.2018.
https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L38

Seppo, T. Tietotilinpäätös osoitusvelvollisuuden toteuttamisessa. Viitattu 5.12.2018
https://vm.fi/documents/10623/9602398/Tietoti-linp%C3%A4%C3%A4t%C3%B6s_Seppo.pdf/8a81f789-aa6d-4058-be68-24a9bf86cd17/Tietoti-linp%C3%A4%C3%A4t%C3%B6s_Seppo.pdf.pdf

Strategy Train (Multidisciplinary European Research Institute Graz). Tukitoiminnot. Viitattu 19.11.2018.
http://st.merig.eu/index.php?id=271&L=2

Tietosuojatyöryhmä WP 29. Asetuksen 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat. Viitattu 15.11.2018
https://tietosuoja.fi/documents/6927448/8316711/L%C3%A4pin%C3%A4kyvyys+fi/c102605b-e386-4661-9b51-bf427875c8db/L%C3%A4pin%C3%A4kyvyys+fi.pdf

Tietosuojatyöryhmä WP 29. Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”. Viitattu 15.11.2018.
https://tietosuoja.fi/documents/6927448/8316711/Vaikutustenarviointi+fi.pdf/af51e999-5326-4223-9deb-e21bdd2e0a63/Vaikutustenarviointi+fi.pdf.pdf

Tietosuojatyöryhmä WP 29. Tietosuojavastaavia koskevat ohjeet. Viitattu 19.11.2018. https://tietosuoja.fi/documents/6927448/8316711/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf/3aad84e5-bb59-4e64-bdaf-adc1e5f2d719/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf.pdf

Tietosuojavaltuutetun toimisto. Henkilötietojen käsittelijän velvollisuudet. Viitattu 5.11.2018. https://tietosuoja.fi/henkilotietojen-kasittelijan-velvollisuudet

Tietosuojavaltuutetun toimisto. Milloin henkilötietoja saa käsitellä?. Viitattu 13.11.2018. https://tietosuoja.fi/kasittelyperusteet#rekisteroidyn-suostumus

Työsopimuslaki 55/2001. Viitattu 19.11.2018 https://www.finlex.fi/fi/laki/ajantasa/2001/20010055

Valtiovarainministeriö. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä, VAHTI-raportti 1/2016: EU-tietosuojan kokonaisuudistus. Viitattu 19.11.2018 https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Valtiovarainministeriö. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) ohjesivusto, Vahtiohje.fi. Viitattu 26.11.2018 https://www.vahtiohje.fi/web/guest

Valtiovarainministeriö. Julkisten hankintojen yleiset sopimusehdot palveluhankinnoissa (JYSE 2014 palvelut). Tarkistettu huhtikuu 2017. Viitattu 7.12.2018 https://vm.fi/documents/10623/2291459/JYSE+palvelut+huhtikuu+2017.pdf/109174f0-f238-40aa-be5d-0b5bb9ddc440/JYSE+palvelut+huhtikuu+2017.pdf.pdf

Valtiovarainministeriö. Vahtiohje.fi. Säädökset. 2009. Viitattu 5.12.2018 https://www.vahtiohje.fi/web/guest/saadokset

Viestintävirasto. Lokien keräys ja käyttö. Ohje 4/2016. Viitattu 5.12.2018 https://www.viestintavirasto.fi/attachments/tietoturva/Lokitusohje.pdf

Väestörekisterikeskus. Tietosuoja-asetuksen huomiointi sopimussuhteessa. Viitattu 4.12.2018 https://eevertti.vrk.fi/documents/2634109/8010513/Tietosuojaliite+asiakkaille.pdf/14277b36-6f7f-4216-9e7c-a48a6fbe6f06/Tietosuojaliite+asiakkaille.pdf.pdf

Yrittäjät.fi, EU:n tietosuoja-asetus koskee kaikkia yrityksiä – Aloita valmistautuminen viimeistään nyt. Viitattu 9.11.2018.

https://www.yrittajat.fi/varsinais-suomen-yrittajat/a/uutiset/564916-eun-tietosuoja-asetus-koskee-kaikkia-yrityksia-aloita-valmistautuminen-viimeistaan

Julkaisemattomat

Nevalainen T., EU:n tietosuoja-asetus, Ohjelmistoyrittäjien koulutus 31.5.2016, viitattu 14.12.2018

Kuviot

Kuvio 1: Henkilötietojen suojaaminen 11

Kuvio 2: Tiedon elinkaari (esimerkki) 30

Kuvio 3 Tietoturvaloukkauksesta ilmoittaminen tietosuoja-asetuksen mukaan 41

Kuvio 4: Henkilötiedon käsittely koulukuljetuksissa 49

Kuvio 5: Koulutuksen suunnittelu 59

Liitteet

Liite 1: Alkukysely – Nykytilan kartoitus 75
Liite 2: Tietosuojainfo kuljettajille 76
Liite 3: Henkilökunnan salassapitosopimus 79
Liite 4: Ohjeistus, Tietoturvaloukkauksista ilmoittaminen 80
Liite 5: Ohjeistus, Rekisteröidyn oikeudet 82
Liite 6: Tietosuojaperiaatteemme -seloste 84
Liite 7: Seloste käsittelytoimista, pohja rekisterinpitäjälle 89
Liite 8: Seloste käsittelytoimista, pohja henkilötietojen käsittelijälle 90

Liite 1: Alkukysely – Nykytilan kartoitus

1. *Järjestelmät*
   a) *Listaa yrityksessä käytössä olevat järjestelmät*
   b) *Pohdi missä näistä järjestelmistä käsitellään/saatetaan käsitellä henkilötietoa*
   c) *Mistä henkilötieto järjestelmiin tulee, esim:*
      a. *Sopimuksien johdosta tilaajalta*
      b. *Työntekijöiden/asiakkaiden itsensä antamana*

2. *Käyttöoikeudet*
   a) Kenellä on pääsy järjestelmiin?
   b) Kuka hallitsee järjestelmien käyttöoikeuksia?
   c) Onko tehty kirjallisia käyttövaltuussopimuksia?

3. *Sopimukset*
   a) *Listaa kenen kaikkien kanssa sopimuksia on tehty*
      a. *Alihankkijat*
      b. *Yhteystyökumppanit*
      c. *Työntekijät (työsopimukset)*
      d. *Palvelusopimukset*
      e. *muut?*
   b) *Ovatko kaikki sopimukset kirjallisia ja ajan tasalla?*
   c) *Sisältävätkö nykyiset kuljetuspalvelusopimukset*
      a. *selkeää ohjeistusta/vaatimuksia henkilötietojen käsittelyn suhteen*
      b. *tietosuojaan ja tietoturvaan liittyviä vaatimuksia/viittauksia*

4. *Salassapito*
   a) *Onko oman henkilökunnan + kuljettajien kanssa tehty salassapitosopimukset (työsopimuksen yhteydessä tai muuten)?*

5. *Muuta*
   a) *Voiko asiakas tilata kuljetuksen netistä (esim. kotisivujen tilauslomakkeella, muusta palvelusta)?*
   b) *Jos voi, onko tilauslomakkeen yhteydessä nykyisen henkilötietolain mukaista rekisteriselostetta? / onko sitä lainkaan olemassa?*
   c) *Lähetättekö uutiskirjeitä/markkinointiviestejä?*
      i. *Missä tällaisten osoitelistat (eli rekisterit) sijaitsevat*
      ii. *Mistä tiedot näihin kerätty*
   d) *Onko yrityksellä sosiaalisen median kanavia?*

Liite 2: Tietosuojainfo kuljettajille

Euroopan unionin yleinen tietosuoja-asetus (GDPR) astui voimaan toukokuun 2018 lopussa. Sitä sovelletaan samansisältöisenä kaikissa EU-maissa ja sen tarkoituksena on luoda EU-kansalaisille paremmat mahdollisuudet vaikuttaa henkilötietojensa käsittelyyn. Henkilötietojen suoja on perusoikeus.

Tietosuoja-asetus määrittelee monenlaisia periaatteita, vaatimuksia ja rajoitteita henkilötietojen käsittelylle. Vääränlaisesta käsittelystä voidaan jatkossa rangaista suurilla sakoilla, vahingonkorvausvastuulla tai rajoittamalla yrityksen mahdollisuutta käsitellä henkilötietoja.

Suurin muutos entiseen on *osoitusvelvollisuus*. Henkilötietoja käsittelevän yrityksen tulee voida pyydettäessä osoittaa, että tietoja todella käsitellään lain edellyttämällä tavalla. Osoittamista voi pyytää viranomainen tai rekisteröity vaikka mitään virhettä käsittelyssä ei olisi havaittu. Tämän takia on tärkeää, että yrityksen koko henkilöstö on sitoutunut oikeanlaiseen tietojenkäsittelyyn.

Tietosuoja-asetuksen yhtenä tarkoituksena onkin saada yritykset ja organisaatiot käymään läpi tietosuojakäytäntönsä ja käsittelemään henkilötietoja entistä tarkemmin.

Mitä on henkilötieto?

Henkilötietoja ovat esimerkiksi

nimi

osoite

puhelinnumero

yhteyshenkilön tiedot

matkakohteet

apuväline ja sairaustiedot

ovikoodi

Myös muut tiedot**, joiden avulla henkilö voidaan tunnistaa tai yksilöidä** ovat henkilötietoa. Käytännössä voidaan todeta, että kaikki matkustajaan liittyvät tiedot ovat henkilötietoja.

Kuka saa käsitellä henkilötietoja?

Henkilötietojen keräämiselle ja käsittelylle tulee aina olla laillinen peruste. Henkilökuljetuksissa tämä tarkoittaa yleensä sopimusta asiakkaan ja kuljetusyrityksen välillä.

Kuljettajalla on oikeus käsitellä henkilötietoja hoitaessaan työtehtäviään. Henkilötietojen käsittelystä on vastuussa kuljetusyritys, jonka tulee ohjeistaa kuljettajia henkilötietojen oikeanlaiseen käsittelyyn. Yleensä kuljettajalla tulee olla tehtynä salassapitosopimus.

Henkilötietojen käsittely

Työntekijän tulee toiminnassaan ottaa huomioon tietosuoja-asetus, muu henkilötietolainsäädäntö sekä sitoutua muutoinkin käsittelemään henkilötietoja tarkasti ja hyvän tavan mukaisesti.

Henkilökuljetusten asiakkaat ovat usein henkilöitä, jotka eivät täysimääräisesti pysty huolehtimaan omasta henkilötietojensa suojasta (lapset, erityislapset, vanhukset). Tämän takia heidän henkilötietojaan tulee käsitellä **erityisellä tarkkuudella.**

Jotkin henkilötiedoista määritellään *erityisiksi henkilötiedoiksi* (eli ns. arkaluonteisiksi tiedoiksi). Tällaisia tietoja ovat esimerkiksi tieto apuvälineistä, sairaustiedot, ovikoodit ja lasten tiedot. Nämä tiedot voivat aiheuttaa henkilölle erityistä vahinkoa, jos niitä käsitellään väärin tai ulkopuolinen saa ne tiedoksi.

Käytäntö

Ajolistat

Kuljettaja saa päivittäisen ajolistan yleensä ajovälitysjärjestelmän kautta. Järjestelmän käyttäjätunnukset ovat ***henkilökohtaisia***. Niitä ei tule luovuttaa muiden tietoon tai käyttöön. Vuoron päätyttyä kuljettajan tulee kirjautua ulos järjestelmästä. Näin varmistutaan siitä, että ulkopuoliset eivät pääse näkemään järjestelmän sisältämiä tietoja luvattomasti.

Kuljettajan tulee muutoinkin pitää ajopäätettään siten, etteivät ulkopuoliset näe siinä olevan ajolistan tietoja. Järjestelmää saa käyttää ainoastaan yrityksen/alihankkijan omistamassa laitteessa tai laitteessa, jonka käytölle on muutoin saatu työnjohdon lupa.

Asiakkaan profiilissa olevista virheistä (esim. osoite, apuvälineet), tulee ilmoittaa ajojärjestelyyn, jotta tiedot saadaan pidettyä ajan tasaisina (*tietojen eheyden ja täsmällisyyden vaatimus*).

Niissä tapauksissa, kun kuljettaja saa ajolistansa sähköpostiin, tulee viesti poistaa kuljetuksen päätyttyä (myös roskapostikansiosta). Vastaavasti tulostetut ajolistat tulee hävittää asianmukaisesti. Ajolistoja ei tule jättää autoon esimerkiksi yöksi tai työvuoron päätyttyä.

Ilmoita ajojärjestelyyn viipymättä jos:

ajolista tai laite, joka sisältää asiakkaiden tietoja katoaa/varastetaan/unohtuu jonnekin

jos epäilet ulkopuolisen saaneen käsiinsä matkustajatietoja jotka eivät hänelle kuulu

Nämä ovat ns. **tietoturvaloukkaus**. Yrityksellä on velvollisuus dokumentoida ne. Jos loukkauksen katsotaan aiheuttavan riskin rekisteröidyn henkilötietojen suojalle, tehdään tästä virallinen ilmoitus. Arvion riskistä ja ilmoittamisen hoitaa ajojärjestely.

Tietojen luovutukset

Ajolistoja ja tietoa kuljetuksesta saa luovuttaa vain niille kuljettajille, joilla on voimassa oleva salassapitosopimus ja jotka tarvitsevat tietoa työnsä hoitamiseen. Muutoin kuljetettaviin liittyvistä tiedoista ei tule keskustella.

Ongelmatilanteissa kuljettaja saa lisätietoja ottamalla yhteyttä ajojärjestelyyn. Mikäli ulkopuolinen taho pyytää kuljettajalta tietoa kuljetuksista tai kuljetettavista, ohjataan hänet ottamaan yhteyttä ajojärjestelyyn.

Liite 3: Henkilökunnan salassapitosopimus

Sopimuksen tarkoitus ja salassa pidettävä tieto
Työntekijä käsittelee työtehtäviään suorittaessaan työnantajan, tämän kanssa samaan konserniin kuuluvien yhtiöiden, asiakkaiden ja yhteistyökumppaneiden liike- ja ammattisalaisuuksia sekä henkilötietoja (”salassa pidettävä tieto”). Tiedot ovat salassa pidettäviä riippumatta siitä, ovatko ne kirjallisessa, sähköisessä tai muussa vastaavassa muodossa.
Salassa pidettäviksi tiedoiksi katsotaan erityisesti:

- työntekijöiden tiedot
- yhteistyökumppaneiden tiedot
- asiakkaiden tiedot

Sopimusehdot
Työntekijä sitoutuu työsuhteensa aikana ja sen jälkeen pitämään salassa ja luottamuksellisena kaiken edellä mainitun tiedon ja olemaan sitä luvatta luovuttamatta tai paljastamatta kolmansille osapuolille. Myös tietojen luovuttaminen työyhteisön sisällä muille kuin niille, jotka tarvitsevat tiedon työtehtävien suorittamiseen ja joilla on oikeus kyseisen tiedon käsittelyyn, on kielletty.
Työntekijä sitoutuu olemaan käyttämättä salassa pidettäviä tietoja muuhun kuin työtehtäviensä hoitamiseen. Hän sitoutuu välittömästi työsuhteen päättymisen jälkeen ja milloin tahansa työnantajan sitä vaatiessa, palauttamaan kaiken hallussaan olevan salassa pidettävää tietoa sisältävän aineiston, laitteiston ja kaikki kopiot.
Työntekijä on myös välittömästi velvollinen ilmoittamaan työnantajalle, mikäli salassa pidettäviä tietoja on luvatta paljastunut tai niiden epäillään paljastuneen ulkopuolisille tai salassapito on muuten vaarantunut. Työntekijä pyrkii toimillaan minimoimaan tästä luonnollisille henkilöille aiheutuvan mahdollisen vahingon.
Työntekijä sitoutuu olemaan paljastamatta tai käyttämättä mitään salassa pidettäviä tietoja niin kauan, kun tiedolla on taloudellista merkitystä, kuitenkin vähintään kaksi vuotta työsuhteen päättymisen jälkeen. Kaikki asiakkaiden henkilötiedot ovat kuitenkin täysin salassa pidettäviä rajoittamattoman ajan.
Työntekijä sitoutuu toiminnassaan noudattamaan tietosuoja-asetusta sekä muita lakeja ja hyvää tietojen käsittelytapaa. Työntekijä huolehti siitä, että käsittelee vain sellaisia tietoja, joiden käsittelyyn hänellä on työtehtäviensä perusteella oikeus.
Työntekijä ymmärtää, että hänen työtehtäviensä hoitamiseksi käyttöönsä saamat käyttäjätunnukset eri järjestelmiin ovat henkilökohtaisia eikä niitä tule luovuttaa muiden tietoon tai käyttöön.
Edellä mainitusta poiketen työntekijällä on oikeus ilmaista tai luovuttaa salassa pidettäviä tietoja viranomaiselle, joka lakiin perustuen velvoittaa tiedonantamiseen. Työntekijä on tässä tapauksessa velvollinen ennen tiedon antamista tai mikäli tämä ei ole mahdollista niin välittömästi sen jälkeen ilmoittamaan työnantajalle tiedonantamisvelvoitteesta.
Mikäli työntekijä rikkoo tässä sopimuksessa mainittuja ehtoja ja salassa pidettävän tiedon salassapito vaarantuu, on työntekijä velvollinen korvaamaan työnantajalle sopimusrikkomuksesta aiheutuneen vahingon.

Päiväys ja allekirjoitukset

Työnantaja **Työntekijä**

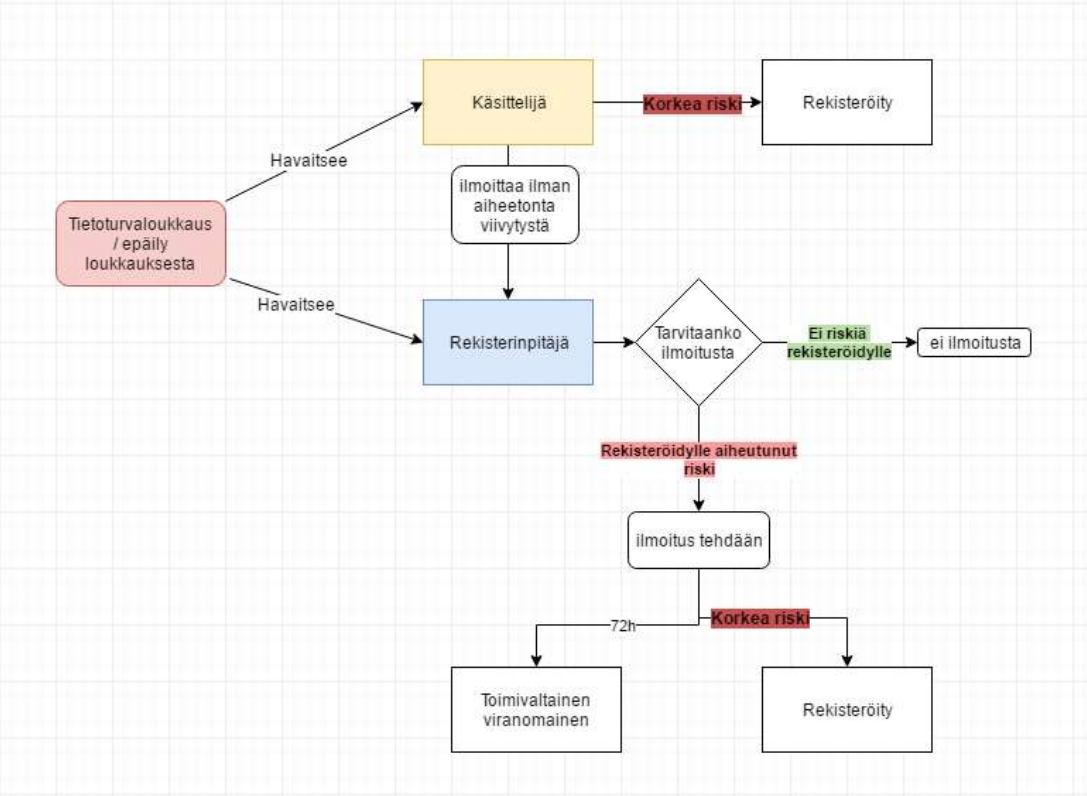
Liite 4: Ohjeistus, Tietoturvaloukkauksista ilmoittaminen

Tietoturvaloukkaukset

Henkilötietojen tietoturvaloukkaus on tilanne, jossa henkilötiedoille tapahtuu jotakin, mikä ***uhkaa rekisteröidyn yksityisyyden suojaa***. Esimerkiksi:

- tuhoutuu (tarkoitukseton poistaminen, luvaton poistaminen, haittaohjelmatartunta)
- häviää (usb-tikku, laite tai ajolista häviää)
- luovutetaan luvattomasti (lähettäminen väärälle henkilölle/väärään osoitteeseen)
- niitä käsittelee henkilö, jolla ei ollut käsittelyoikeutta tietoon (hakkerointi)

Seurauksena voi olla identiteettivarkaus, petos, tiedon valvomiskyvyn menettäminen tai muuten salassapitovelvollisuuden piiriin kuuluvien tietojen luottamuksellisuuden menetys. Tietoturvaloukkauksista tulee ilmoittaan. Se kenelle ilmoitetaan ja mitä ilmoitetaan, riippuu yrityksen roolista henkilötietojen käsittelyssä sekä tietoturvaloukkauksen vakavuudesta. Oleellista on, että loukkaukseen reagoidaan nopeasti.



Kuva 1: Henkilötietojen tietoturvaloukkauksesta ilmoittaminen

<u>Käsittelijä</u>

Ilmoita havaitusta loukkauksesta rekisterinpitäjälle viivytyksettä, kuitenkin 72h aikana huomaamisesta. ***Kuvaa ilmoituksessa*** mahdollisuuksien mukaan:

- millainen tietoturvaloukkaus on kyseessä, mistä se on aiheutunut

- ketä se koskettaa/saattaa koskettaa:
    - rekisteröityjen ryhmät (vanhukset/lapset/koulukuljetusoppilaat/jne)
    - henkilötietojen tyypit (nimi/osoite/sairastiedot)
    - arvio loukattujen henkilötietojen lukumäärästä
- arvio todennäköisistä seurauksista rekisteröidyille
- toimenpiteet, jotka on tehty ja voidaan tehdä tietoturvaloukkauksesta aiheutuneen haitan minimoimiseksi

HUOM! Jos tietoturvaloukkaus aiheuttaa todennäköisesti korkean riskin rekisteröidyille, tulee käsittelijän osana ehkäiseviä toimia ilmoittaa siitä myös suoraan henkilölle itselleen. Jos riski arvioidaan pieneksi, jää harkinta ilmoittamisesta rekisterinpitäjälle, jollei muuta ole sovittu.

Rekisterinpitäjä:

Rekisterinpitäjän tulee arvioida henkilötietojen tietoturvaloukkauksesta rekisteröidylle aiheutuvaa riskiä, jonka perusteella päättää tarvittavista toimenpiteistä.

Velvollisuus dokumentoida kaikki henkilötietoihin kohdistuneet tietoturvaloukkaukset, on osa tietosuoja-asetuksen osoitusvelvollisuutta. Dokumentointi tulee tehdä myös silloin kun tietoturvaloukkaus arvioidaan niin pieneksi, ettei muihin toimenpiteisiin ryhdytä. Dokumenteista tulee ilmetä:

- kuvaus tietoturvaloukkauksesta (ks. käsittelijän ilmoituksen sisältö)
- tietoturvaloukkauksen vaikutukset rekisteröityyn
- toteutetut korjaavat toimet

Velvollisuus ilmoittaa tietoturvaloukkauksesta toimivaltaiselle valvontaviranomaiselle on aina rekisterinpitäjällä. Ilmoitus tehdään, jos loukkauksesta voi aiheutua riski henkilöiden oikeuksille tai vapauksille, Ilmoitus tulee tehdä viivytyksettä, kuitenkin viimeistään 72h kuluttua loukkauksen havaitsemisesta. Ilmoituksessa tulee kuvata:

- tapahtunut tietoturvaloukkaus (mahdollisuuksien mukaan samat asiat kuin käsittelijän tekemässä ilmoituksessa)
- tietosuojavastaavan nimi ja yhteystiedot / muu yhteyshenkilö
- tietoturvaloukkauksesta henkilö(i)lle aiheutuvat todennäköiset seuraukset
- toimenpiteet, joita on ehdotettu tai jotka on toteutettu

Ilmoitusta **ei tarvitse tehdä jos:**

- On toteutettu ennalta suunnitellut tekniset ja organisatoriset toimet, joilla tilannetta on korjattu (esim. tietojen salaus)
- On toteutettu jatkotoimia, joilla varmistetaan, että arvioitu riski ei enää todennäköisesti toteudu
- ilmoittaminen vaatisi kohtuutonta vaivaa (riski ei ole todellinen eikä tiedetä, kehen se on kohdistunut)

Rekisteröidylle tulee ilmoittaa tietoturvaloukkauksesta silloin kun siitä voi aiheutua hänelle todennäköisiä tai vakavia seurauksia. Myös viranomainen voi vaatia ilmoituksen tekemistä.

Liite 5: Ohjeistus, Rekisteröidyn oikeudet

Rekisteröidyn oikeudet

EU:n yleinen tietosuoja-asetus antaa rekisteröidylle entistä paremmat oikeudet vaikuttaa tietojensa käsittelyyn. Vastaavasti tämä luo rekisterinpitäjälle ja käsittelijöille uusia velvollisuuksia. Oikeudet eivät ole kaikilta osin ehdottomia tai subjektiivisia.

Rekisteröidyllä on asetuksen mukaan:

1. Oikeus saada riittävästi ja läpinäkyvästi tietoa henkilötietojensa käsittelystä (tarkoitukset ja tavat)
    - rekisterinpitäjän/käsittelijän tulee avata tarvittavissa määrin tiedon käsittelyn tapoja
2. Oikeus saada pääsy omiin tietoihinsa (nähdä mitä tietoja hänestä käsitellään)
    - saada vahvistus siitä käsitelläänkö hänen tietojaan
    - mitä tietoja käsitellään
    - mistä tiedot on saatu
3. Oikeus tietojensa oikaisemiseen
    - virheelliset ja epätarkat tiedot tulee oikaista tai täydentää
4. Oikeus tulla unohdetuksi (oikeus tietojensa poistamiseen)
    - oikeus saada henkilötietonsa poistettua ilman aiheetonta viivytystä
    - poistamisoikeuden toteutumista tulee arvioida tarkkaan
    - tietojen poistamisen jälkeen kuljetuspalvelun saaminen ei ole mahdollista
5. Oikeus siirtää tietonsa toiseen järjestelmään
    - järjestelmässä henkilöstä olevat tiedot toimitetaan hänelle koneluettavassa muodossa (esim. exel)
6. Oikeus rajoittaa tietojensa käsittelyä
7. Oikeus vastustaa tietojensa käsittelyä
8. Oikeus vastusta profilointia (ja muita automatisoituja yksittäispäätöksiä
9. Oikeus saada tieto hänen tietoihinsa kohdistuneesta tietoturvaloukkauksesta
10. Oikeus tehdä valitus valvontaviranomaiselle
    - kun katsoo, että henkilötietoja ei ole käsitelty lain edellyttämällä tavalla
11. Oikeus saada vahingonkorvausta
    - aineellisista ja aineettomista vahingoista

Jos rekisteröity haluaa käyttää jotakin hänelle tietosuoja-asetuksessa asetettua oikeutta, tulee ensin varmistua rekisteröidyn henkilöllisyydestä. Tämän jälkeen on pohdittava missä määrin

oikeus voidaan toteuttaa. Tästä syystä pyynnöt kannattaa mahdollisuuksien mukaan pyytää toimittamaan kirjallisina. Niihin myös vastataan kirjallisesti, jolloin toiminnasta jää dokumentti.

HUOM! Rekisteröityjen oikeuksien toteutumisesta vastaa viimekädessä rekisterinpitäjä. Käsittelijän mahdollisuus esimerkiksi tietojen poistamiseen on sovittava erikseen. Tarkista siis kuka henkilötiedot omistaa ja mihin niiden käsittely perustuu.

Liite 6: Tietosuojaperiaatteemme -seloste

1. Tietosuojaperiaatteemme

Tässä selosteessa kuvataan yrityksemme henkilötietojen käsittelyn yleiset periaatteet, joita noudatamme kaikessa henkilötietojen käsittelyssä. Noudatamme henkilötietojemme käsittelyssä lakia ja selostetta päivitetään lainsäädännön mukaisesti.

2. Rekisterinpitäjä / henkilötietojen käsittelijä

Kuljetusyritys Oy
Katuosoite
00004 Helsinki

Y-tunnus: 123456-7

Yhteyshenkilö:

Nimi
sähköposti@mail.com
puh. 040 1234 567

3. Henkilötietojen käsittelyn oikeusperuste ja tarkoitus

Käsittelemme henkilötietoja vain niissä tarkoituksissa, joihin ne on alun perin kerätty tai johon ne on meille luovutettu. Varmistamme, että käsittelylle on aina vähintään yksi laillinen ja voimassa oleva peruste.

Käsittelemme henkilötietoja mm. seuraaviin tarkoituksiin:

Kuljetuspalvelujen tarjoaminen
Henkilötietojen käsittely perustuu sopimukseen tilaajan ja yrityksemme välillä. Asiakkuussuhteen aikana tietoja käsitellään kuljetusten toteutusta, laskutusta ja asiakaspalvelua varten.

Kun kuljetuksen tilaajana on yksityishenkilö tai yritys, toimimme rekisterinpitäjänä suhteessa meille annettuihin henkilötietoihin. Käsiteltävät henkilötiedot saadaan tilaajalta itseltään ja niitä käsitellään sopimuksen täytäntöönpanemiseksi. Luovuttaessaan käsiteltäväksemme muiden henkilötietoja (esimerkiksi yhteyshenkilö), vastaa tilaaja itse oikeudestaan näiden luovuttamiseen.

Tarjoamme kuljetuspalveluja myös ostopalvelusopimuksella kunnille, kaupungeille, yhteisöille ja yrityksille. Tällaisia palveluja ovat mm. koulu- ja toimipaikkakuljetukset. Tällöin saamme kuljetettavien henkilötiedot tilaajalta, joka toimii tietojen rekisterinpitäjänä ja vastaa oikeudestaan luovuttaa näitä tietoja. Me toimimme tietojen suhteen käsittelijöinä. Käsittely tapahtuu rekisterinpitäjän lukuun saamamme ohjeistuksen mukaisesti.

Lakisääteisten velvoitteiden täyttäminen
Lakisääteisten velvoitteiden täyttäminen voi edellyttää henkilötietojen käsittelyä, kun muut käsittelyperusteet ovat lakanneet. Noudatamme tietojen minimoinnin periaatetta ja käsittelemme aina vain tarpeellisia henkilötietoja. Lakeja, joiden perusteella henkilötietoja käsitellään ovat esimerkiksi kirjanpito- ja työsopimuslaki.

Rekrytointi
Käsittelemme henkilötietoja rekrytointien yhteydessä. Tiedot saadaan pääosin työnhakijalta itseltään. Tietojen käsittely perustuu hakijan omaan suostumukseen. Palkattujen henkilöiden hakemustietoja säilytetään koko työsuhteen ajan. Muilta osin tiedot hävitetään, jollei hakijan kanssa ole erikseen muuta sovittu.

Henkilöstöhallinto

Henkilöstöön liittyviä tietoja käsitellään molemminpuolisten työsuhteeseen liittyvien velvoitteiden ja oikeuksien toteuttamiseen, kuten:

- työnajanseuranta
- palkanmaksu
- verotus
- työtodistuksen antaminen
- muut työsuhteesta johtuvat oikeudet ja velvollisuudet

Yhteydenottopyynnöt

Meille on mahdollista antaa palautetta nettisivujen kautta. Käsittelemme tällöin tietoja henkilön suostumuksella vastaksemme yhteydenottopyyntöön tai palautteeseen.

4. Käsiteltävät henkilötiedot

Käsittelemme **kuljetettavista** esimerkiksi seuraavanlaisia tietoja:

- Kuljetettavan nimi
- Puhelinnumero
- Kotiosoite
- Noutopaikan osoite
- Matkakohteet
- Tieto apuvälineestä
- Tieto muista erityistarpeista ja -toiveista
- Yhteyshenkilön tiedot
- Sähköposti
- Laskutukseen liittyvät tiedot
    - maksajan nimi
    - y-tunnus
    - osoite
    - sähköposti
    - puhelinnumero
    - yhteyshenkilön nimi

Käsiteltävä tietosisältö riippuu siitä, millaisia tietoja meille on kuljetuksen tilaamisen yhteydessä annettu. Keräämme tiedot aina rekisteröidyltä itseltään tai saamme ne sopimuksen yhteydessä rekisterinpitäjältä.

Henkilökunnastamme käsittelemme mm. seuraavia tietoja:

- Nimi
- Osoite
- Puhelinnumero
- Sähköposti
- Tilinumero
- Henkilötunnus
- Tieto ajokorttiluokasta (kuljettajat)
- Verotuksen pidättämistä varten tarvittavat tiedot
- Työajan seuranta ja käyttö
- Sairauspoissaolotiedot
- Työsopimus
- Järjestelmien käyttäjätunnukset

Työnhakijoiden osalta käsiteltäviä tietoja ovat:

- Nimi ja yhteystiedot
- Koulutus, työhistoria
- Hakemus ja CV
- Suosittelijat (suostumuksella)
- Rikosrekisteriote (tarkastetaan, työnhakija toimittaa itse)

Käsittelemme myös **yhteistyökumppaneiden** ja **alihankkijoiden** tietoja:

- yrityksen nimi ja osoite
- y-tunnus
- yhteyshenkilön tiedot
- työntekijöiden nimet ja yhteystiedot

5. Tietojen käsittely, siirrot ja luovutukset

Henkilökuntamme käsittelee henkilötietoja työtehtäviensä yhteydessä. Heidät on perehdytetty erilaisten henkilötietoryhmien oikeanlaiseen ja tietoturvalliseen käsittelyyn. Henkilökunnallamme on voimassa olevat salassapitosopimukset ja he ovat sitoutuneet tiedon luottamukselliseen käsittelyyn.

Tuotamme kuljetuspalveluita myös alihankkijoiden ja yhteistyökumppaneiden kanssa. Näin ollen saatamme antaa henkilötietoja heidän käsiteltäväkseen niiltä osin, kuin tämä on onnistuneen ja turvallisen palvelun tarjoamisen kannalta välttämätöntä. Huolehdimme siitä, että kaikki kanssamme työskentelevät sitoutuvat noudattamaan tietosuojaperiaatteitamme ja että heillä on voimassa oleva salassapitosopimus.

Henkilötietoja ei säännönmukaisesti luovuteta eikä siirretä EU- tai ETA-alueen ulkopuolelle.

Tietoja ei käytetä profilointiin tai automaattiseen päätöksentekoon.

Voimme luovuttaa tietoja toimivaltaiselle viranomaiselle pyynnöstä lain sitä edellyttäessä.

6. Tietojen säilytys ja suojaus

Säilytämme tietoja niin kauan kuin on käyttötarkoituksesta tai sopimuksesta johtuen tarpeellista. Varmistamme aina, että meillä on tiedon käsittelylle laillinen peruste. Henkilötietojen säilytysajat vaihtelevat käsittelyperusteesta riippuen.

Henkilötietoja käsitellään ja säilytetään pääsääntöisesti sähköisessä muodossa. Käyttäjätunnuksia myöntävät ja hallinnoivat erikseen nimetyt henkilöt. Käytämme järjestelmiä, joiden toimittajien katsomme täyttävän EU:n yleisen tietosuoja-asetuksen vaatimukset ja noudattavan hyvää henkilötietojen käsittelytapaa.

Olemme kartoittaneet meillä olevat henkilötietovarannot ja käsittelyyn liittyvät riskit. Tiedämme missä tiedot sijaitsevat ja tiedon poistuessa poistamme sen myös mahdollisista paperisista arkistoista. Huolehdimme tietoturvasta myös henkilötietojen poistamisen yhteydessä. Toimitilamme ja laitteemme ovat asianmukaisesti suojatut.

7. Rekisteröidyn oikeudet

Rekisteröidylle taataan EU:n yleisen tietosuoja-asetuksen mukaiset oikeudet henkilötietojensa käsittelyssä. Pyynnöt oikeuksien käyttämiseksi pyydetään toimittamaan kirjallisena.

Niiltä osin kuin toimimme henkilötietojen suhteen käsittelijöinä, tulee rekisteröidyn osoittaa pyyntö oikeuksiensa käyttämisestä suoraan rekisterinpitäjälle. Asiakaspalvelumme vastaa rekisterien yhteyshenkilöihin liittyviin tiedusteluihin.

Oikeus tarkastaa tietonsa

Rekisteröidyllä on oikeus tarkastaa itseään koskevat henkilörekisteriintallennetut tiedot.

Oikeus peruuttaa antamansa suostumus

Kun tietoja käsitellään rekisteröidyn suostumuksella, hänellä on oikeus peruuttaa suostumuksensa ja pyytää tietojensa poistamista. Rekisterinpitäjän tulee poistaa tiedot kuukauden kuluessa niiltä osin, kun laista ei muuta johdu.

Oikeus henkilötietojen oikaisemiseen ja korjaamiseen

Rekisteröidyllä on oikeus pyytää rekisterinpitäjää oikaisemaan häntä koskevat epätarkat ja virheelliset henkilötiedot ilman aiheetonta viivytystä.

Oikeus tietojensa poistamiseen (oikeus tulla unohdetuksi)

Henkilöllä on oikeus pyytää itseään koskevien tietojen poistamista kun,

a) henkilötietoja ei enää tarvita alkuperäiseen käsittelytarkoitukseen
b) rekisteröity peruuttaa suostumuksensa tietojen käsittelyyn, eikä muuta perustetta käsittelylle ole

Henkilötietojen poistamisen mahdollisuus ja sen vaatimat toimenpiteet arvioidaan tapauskohtaisesti. Arvioinnista huolehtii tietosuoja-asioista vastaava henkilö, joka varmistaa, että poistamisen osalta menetellään laillisesti.

Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus vaatia henkilötietojensa käsittelyn rajoittamista, jos henkilötiedot eivät pidä paikkaansa, käsittely on lainvastaista tai muu lain edellyttämä peruste täyttyy.

Oikeus tietojen siirtämiseen

Rekisteröidyllä on oikeus saada rekisterinpitäjälle toimittamansa, itseään koskevat henkilötiedot jäsennellyssä, koneellisesti luettavassa muodossa ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle.

Oikeus tehdä valitus valvontaviranomaiselle

Jos henkilö katsoo, että henkilötietojen käsittelyssä rikotaan vallitsevaa lainsäädäntöä, on hänellä oikeus tehdä valitus toimivaltaiselle valvontaviranomaiselle, jona Suomessa toimii tietosuojavaltuutettu.

Liite 7: Seloste käsittelytoimista, pohja rekisterinpitäjälle

Rekisterinpitäjä					
Nimi ja yhteystiedot		Tietosuojavastaava (jos nimitetty)		Edustaja (jos tarpeen)	
Organisaation nimi		Nimi		Nimi	
Osoite		Osoite		Osoite	
Sähköposti		Sähköposti		Sähköposti	
Puhelinnumero		Puhelinnumero		Puhelinnumero	

Seloste käsittelytoimista

Käsittelyn tarkoitukset	Yhteisrekisterinpitäjän nimi ja yhteystiedot (tarvittaessa)	Kuvaus rekisteröityjen ryhmistä	Kuvaus henkilötietoryhmistä	Vastaanottajaryhmät	Viittaus (mahdolliseen) henkilötietojen käsittelijän kanssa solmittuun henkilötietojen käsittelyä koskevaan sopimukseen	Kolmannet maat ja kansainväliset järjestöt, joihin tietoja siirretään tai tieto siitä, ettei henkilötietoja siirretä kolmansiin maihin tai kansainvälisiin järjestöihin	Asianmukaisia suojatoimia koskeva dokumentaatio, jos henkilötietoja siirretään kolmansiin maihin tai kansainvälisiin järjestöihin tietosuoja-asetuksen 49 artiklan 1 kohdan toisessa alakohdassa tarkoitetulla siirrolla	Tietojen säilytysajat, tai sen määrittämisen kriteerit	Kuvaus tietosuoja-asetuksen 32 artiklan 1 kohdan mukaisista teknisistä ja organisatorisista turvatoimista

Liite 8: Seloste käsittelytoimista, pohja henkilötietojen käsittelijälle

Henkilötietojen käsittelijä					
Nimi ja yhteystiedot		Tietosuojavastaava (jos nimitetty)		Edustaja (jos tarpeen)	
Nimi	Käsittelijä Esimerkki	Nimi	Tietosuojavastaava Esimerkki	Nimi	N/A
Osoite	Postiosoite	Osoite	Postiosoite	Osoite	N/A
Sähköposti	Sähköpostiosoite	Sähköposti	Sähköpostiosoite	Sähköposti	N/A
Puhelin	Puhelinnumero	Puhelin	Puhelinnumero	Puhelin	N/A

Seloste käsittelytoimista						
Viittaus rekisterinpitäjän kanssa laadittuihin henkilötietojen käsittelyä koskeviin sopimuksiin	Rekisterinpitäjän nimi ja yhteystiedot	Rekisterinpitäjän edustajan nimi ja yhteystiedot (tarvittaessa)	Käsittelyiden ryhmät	Kolmannet maat ja kansainväliset järjestöt, joihin tietoja siirretään tai tieto siitä, ettei henkilötietoja siirretä kolmansiin maihin tai kansainvälisiin järjestöihin	Asianmukaisia suojatoimia koskeva dokumentaatio, jos henkilötietoja siirretään kolmansiin maihin tai kansainvälisiin järjestöihin tietosuoja-asetuksen 49 artiklan 1 kohdan toisessa alakohdassa tarkoitetulla siirrolla	Yleinen kuvaus tietosuoja-asetuksen 32 artiklan 1 kohdan mukaisista teknisistä ja organisatorisista turvatoimista
Viittaus	Rekisterinpitäjä A - Osoite, sähköpostiosoite, puhelinnumero	N/A	Palkanmaksu	N/A	N/A	Kryptatut tiedot
Viittaus	Rekisterinpitäjä B - Osoite, sähköpostiosoite, puhelinnumero	N/A	Palkanmaksu	N/A	N/A	Kryptatut tiedot
Viittaus	Rekisterinpitäjä B - Osoite, sähköpostiosoite, puhelinnumero	N/A	Kirjanpito	N/A	N/A	Kryptatut tiedot
Viittaus	Rekisterinpitäjä B - Osoite, sähköpostiosoite, puhelinnumero	N/A	Pilvipalvelu	Kanada	N/A	Kryptatut tiedot, pääsynvalvonta