HAAGA-HELIA
ammattikorkeakoulu

GDPR tietosuoja-asetuksen vaikutus Pk-yrityksessä

Matias Lummi

Opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

2019

HAAGA-HELIA
ammattikorkeakoulu

Tiivistelmä

20.11.2019

Tekijä tai tekijät Matias Lummi	**Ryhmätunnus tai aloitusvuosi** 2016
Koulutusohjelma Tietojenkäsittelyn koulutusohjelma	
Raportin nimi GDPR tietosuoja-asetuksen vaikutus Pk-yrityksessä	**Sivu- ja liitesivumäärä** 27 + 5

GDPR -tietosuoja-asetuksen tarkoitus on parantaa rekistereissä olevien EU:n kansalaisten henkilösuojaa ja yhtenäistää EU:n tietosuojalainsäädäntöä.

Opinnäytetyön tarkoituksena on tarkastella, miten Järvenpään Mestariasunnot Oy:ssä toteutuu GDPR -tietosuoja-asetuksen mukaiset asiat. Työn teoriaosuus koostuu tietosuoja-asetuksesta yleisesti ja varsinainen tutkimusosuus peilaa yrityksen käytäntöjä tietosuoja-asetukseen.

Tietosuoja-asetus on iso ja merkityksellinen asiakokonaisuus, jossa on paljon henkilösuojaan liittyviä asioita, jotka vaikuttavat monessa eri tilanteessa yrityselämässä. Tämän vuoksi työn teoriaosuudessa on tietosuoja-asioista kerrottu hiukan laajemmin kuin varsinaisessa tutkimusosuudessa asian käsittely olisi vaatinut.

Järvenpään Mestariasunnot Oy on yritys, joka vuokraa asuntoja Järvenpäässä. Tässä työssä selvitetään, miten yrityksessä käsitellään asukkaiden henkilötietoja eri vaiheissa asunnonhausta asumiseen ja pois muuttamiseen sekä miten näitä tietoja säilytetään. Asuntojen vuokraustoiminta on toimintaa, jossa ihmisten henkilötietoja käsitellään monessa eri tilanteessa.

Opinnäytetyötä varten laadittiin aluksi projektisuunnitelma, jonka pohjalta haastateltiin yrityksen henkilökuntaa sekä tutustuttiin muutenkin yrityksen toimintatapoihin aiheeseen liittyvien toimintojen osalta. Tutkimusta varten yritykseltä saatiin lisäksi käyttöön tarvittavia kirjallisia dokumentteja, joista myös selvisi monia käytäntöjä.

Näitä yrityksen toimintoja ja käytäntöjä siis verrataan tässä työssä suhteessa EU:n tietosuoja-asetukseen.

Asiasanat
GDPR, tietosuoja-asetus, henkilötieto

Sisällys

1 Johdanto 3
2 GDPR tietosuoja-asetus 4
2.1 Yleistä tietoa asetuksesta 4
2.2 Henkilökohtaisen tietojen määritys 5
2.3 GDPR:n vaatimat toimenpiteet yrityksen sisällä 5
2.3.1 Henkilötietojen säilytysaika 6
2.3.2 Suostumus henkilötietojen käsittelemiseen 8
2.3.3 Henkilötietojen kerääminen ja käsittely 9
2.3.4 Henkilötietojen luovutus ja arkistointi 10
2.3.5 Henkilötietojen anonymimosointi/poisto 11
2.4 Rekisteröidyn oikeudet 12
2.4.1 Henkilötietojen pyyntö rekisteristä 12
2.4.2 Tarkastusoikeus ja oikaisemisoikeus 12
2.4.3 Siirto- ja vastustamisoikeus 13
2.4.4 Henkilötietojen poisto rekisteristä 13
2.5 Rekisterinpitäjän velvollisuudet 14
2.5.1 Nykytilan arviointi 15
2.5.2 Osoitus- ja ilmoitusvelvollisuudet 15
2.5.3 Rekisteröidyn oikeuksiin vastaaminen 16
2.5.4 Rekisteri- ja tietosuojaseloste 16
2.6 Tietosuojavastaava 17
2.6.1 Tarve ja nimittäminen 18
2.6.2 Tehtävät 18
3 Tietosuoja ja -turva 18
3.1 Fyysinen turva 18
3.2 Digitaalinen turva 19
3.3 Tietotilinpäätös 20
3.4 Tietosuojaorganisaatio 21
4 Tutkimuksen toteutus ja tulokset Järvenpään Mestariasunnot Oy:ssa 22
4.1 Sähköinen asuntohakemus 22

4.2 Vuokrasopimus ja vuokrareskontra 23
4.3 Vikailmoitukset 24
4.4 Varoitukset 24
4.5 Tietotilinpäätös 25
4.6 Tietosuojaorganisaatio 26
5 Pohdinta 26
Lähteet 28
Liitteet 32

GDPR tietosuoja-asetuksen sanastoa

Anonymisointi Henkilötietojen poistaminen siten, ettei henkilöön kohdistuvaa tietoa voida enää tunnistaa rekisteristä.

Henkilötieto Tällä tarkoitetaan henkilöön kohdistuvaa tietoa, joka on tunnistettavissa esim. nimi, osoite, kuva jne.

Arkaluontoinen tieto Tällä viitataan henkilön uskontoon, rotuun tai etniseen alkuperään kohdistuvaa tietoa. Arkaluontoista tietoa on myös henkilön terveyteen liittyvät tiedot sekä henkilötiedot, joita käsitellään tilastollisia tieteellisiä tai tilastollisia tutkimuksia varten.

Henkilötietojen käsittelijä on henkilö, joka käsittelee henkilötietoja rekisterinpitäjän toimeksiannosta ja sen mukaisesti.

Kyberturvallisuus Kyberturvallisuudella pyritään tunnistamaan ja ehkäisemään yrityksen ICT-toimintoihin kohdistuvat häiriöt ja ennaltaehkäisemään niitä riskienhallinnassa koskevilla asioilla.

Lapsen henkilötietojen käsittely Tässä on huomioitava, että alle 16-vuotiaiden henkilötietoja ei saa käsitellä ilman vanhempien suostumusta.

Profilointi Tällä tarkoitetaan henkilötietojen automaattista käsittelyä, jossa esimerkiksi arvioidaan ja analysoidaan henkilötietojen avulla henkilön ominaisuuksia kuten taloudellista tilannetta, henkilökohtaisia kiinnostuksen kohteita tai terveyteen liittyviä tietoja.

Pseudonymisointi Viittaa henkilötietojenkäsittelyyn siten että, henkilöä ei pystytä enää yhdistämään rekisterissä olevaan henkilöön ilman lisätietoja.

Rekisterinpitäjä on henkilö, joka määrittelee henkilötietoihin liittyvät käsitteelliset keinot.

Rekisteriseloste, tietosuojaseloste on dokumentti, jonka rekisterinpitäjä on laatinut yleisesti saataville yrityksessä. Dokumentissa täytyy olla ymmärrettävä ja tiivis kuvaus henkilötietojenkäsittelyyn liittyen.

Rekisteröity on henkilö, jonka tietoja käsitellään.

Tietosuoja Tietosuojalla tarkoitetaan yksityisyyden säilyttämistä henkilötietoja käsiteltäessä.

Tietotilinpäätös on yrityksen laatima vapaaehtoinen raportti, joka antaa kuvaa yrityksen tietojenkäsittelyn nykyisestä tilanteesta. Raportilla on tarkoitus lisätä yrityksessä luottamusta tietojenkäsittelytavassa henkilötietojen käsittelyssä.

(EU:N Tietosuoja-asetus – sanasto 2016.)

1 Johdanto

Tämä opinnäytetyö koskee GDPR:n vaikutusta pk-yrityksen tietosuoja-asioihin yrityksen asiakkaan (tai asukkaan) tietosuojan näkökulmasta sekä yleistä taustatietoa siitä, mikä GDPR on.

Järvenpään Mestariasunnot Oy, jolle opinnäytetyö on tehty, on asuntovuokrausyritys Järvenpäästä. Työn tarkoituksena oli tutkia heidän tietosuojaansa liittyviä asioita, ovatko ne ajan tasalla ja onko korjattavaa.

Asukas lähestyy yritystä ensimmäisenä tekemällä vuokra-asunnosta sähköisen hakemuksen. Seuraavaksi asukkaan kanssa solmitaan vuokrasopimus. Asukas voi tehdä vikailmoituksen tai saada varoituksen jostakin syystä. Miten tällaiset asukkaan henkilötietoja sisältävät tiedot liikkuvat, kuinka tieto kirjataan ja kuinka kauan tällaisia tietoja voidaan säilyttää? Miten näitä käsitellään ja miten pitäisi käsitellä? Tässä työssä näihin asioihin pyritään löytämään lakiin ja asetuksiin perustuvat vastaukset teoreettisen pohjatiedon ja käytännöllisen lähestymisen kautta.

Tämän projektin tavoitteena on siis havaita ja suorittaa uuden tietosuoja-asetuksen edellyttävät toimenpiteet ja vaikutukset yrityksessä. Projektissa käydään läpi tärkeimmät tietosuoja-asetukseen liittyvät seikat asukkaan tietoturvan näkökulmasta sekä mahdolliset parannusehdotukset yrityksen käytäntöihin.

2 GDPR tietosuoja-asetus

2.1 Yleistä tietoa asetuksesta

GDPR on lyhenne, joka muodostuu sanoista General Data Protection Regulation, jolla viitataan EU:n uuteen tietosuojalakiin. (Tietosuoja 2019)
- General=yleinen
- Data Protection=tietosuoja
- Regulation=termillä viitataan EU:n kansaiseen ja yritykseen kohdistuvaan asetukseen

”Yleinen tietosuoja-asetus (GDPR) on digiajan suurin lainsäädännöllinen muutos” totesi Mark Lomas ennen tietosuoja-asetuksen astumista voimaan. (Mertaniemi 2018.)

25.5.2018 voimaan astunut EU:n yleinen tietosuoja-asetus (General Data Protection, Regulation, GDPR) on yksi merkittävämpiä muutoksia tietosuojalaissa yli kahteenkymmeneen vuoteen. Uusi tietosuoja-asetus korvaa edellisen vuodesta 1995 voimassa olleen EU:n tietosuojadirektiivin. Sen tavoitteena on tehdä tietolainsäädöstä entistä tehokkaampi ja suojata EU-kansalaisten tietosuojaa. GDPR-tietosuoja-asetuksen yleisempänä tarkoituksena on suojella rekisterissä olevien henkilöiden oikeuksia ja vapauksia sekä henkilötietojen yksityisyyttä. Asetuksen tavoitteena on tehdä henkilötietojen käsittelystä mahdollisimman yhdenmukaista. (Mertaniemi 2018.)

GDPR-tietosuoja-asetus antaa selkeämpiä sääntöjä ja ohjeistuksia rekisteröidyn oikeuksiin sekä rekisterinpitäjän velvollisuuksiin. Asetuksen astuessa voimaan ei enää riitä, jos yrityksessä sanotaan noudatettavan asetusta, vaan tästä on tehtävä yrityksen sisäinen dokumentaatio-ohje. Merkittävimpänä muutoksena asetuksessa on hallinnolliset sanktiot, jotka valvontaviranomaisella on oikeus antaa, mikäli asetusta rikotaan. Tärkeänä osana asetuksen noudattamista on, että yrityksessä henkilöt ovat tietoisia säännöksistä. Sanktio voi olla korkeimmillaan jopa 20 miljoonaa euroa tai vastaavasti neljä prosenttia yrityksen liikevaihdosta. (EU:n uusi tietosuoja- asetus koskettaa lähes jokaista yritystä ja yhdistystä 2016.)

Nykyään, kun lähes kaikkialla käsitellään henkilötietoa, on tärkeää muistaa, että asetus koskee kaikkia yrityksiä ja organisaatioita. Käsiteltävät tiedot voivat olla digitaalisessa tai fyysisessä muodossa. Kun yritys käsittelee rekisterissä olevien tietoja, on muistettava, että yrityksen henkilökunnan sisäiset dokumentit ja asiakirjat on myös suojeltava asetuksen mukaisesti.

2.2 Henkilökohtaisen tietojen määritys

Henkilökohtaisen tiedon määritelmässä EU:n asettama tietosuojadirektiivi ei varsinaisesti suoraan kerro, mikä on henkilötietoa, vaan sen sijaan kertoo tiedon olevan direktiivin alaista. Tämä puolestaan tarkoittaa, että henkilön nimen, osoitteen ja henkilötunnisteen lisäksi on muitakin tietoja, jotka voidaan katsoa henkilötiedoiksi. Näitä tietoja voivat olla esimerkiksi IP-osoitteet, MAC-osoitteet, luottokortinnumerot sekä puhelinnumerot. Direktiivi ei määrittele myöskään, mikä tallennustapa yrityksellä on. Tämä tarkoittaa, että direktiivi kattaa kaikki henkilötiedot riippumatta siitä, onko henkilötiedot tallennettu rakenteellisena tietokantoihin, tulostettuna paperille tai sitä, onko tieto Word-dokumenttina. Direktiivissä määrätään kuitenkin selkeästi, että anonymisoitu tieto ei kuulu direktiivin alaisuuteen. (Mitä jokaisen kuuluu tietää EU:N uudesta tietosuoja-asetuksesta GDPR? 2019.)

2.3 GDPR:n vaatimat toimenpiteet yrityksen sisällä

Tietosuoja-asetus edellyttää suojaamaan asianmukaisesti henkilötiedot kuten esimerkiksi yksityishenkilön nimi, syntymäaika ja osoite. Asetuksen kannalta on tärkeä osata kuvailla, mitä henkilötietoja käsitellään, millä tavalla ja minkälaiseen tarkoitukseen yrityksen sisällä. Yrityksen on tunnettava riskit henkilötietojen käsittelyyn liittyen ja pystyttävä hallitsemaan ne. Rekisteröidyn on tällöin helpompi luottaa yritykseen, jolle hän on luovuttanut henkilötietoja. Merkittävin muutos asetuksen kannalta on oikeus saada itselleen rekisterin tiedot ja tulla myös ”unohdetuksi”. GDPR-asetuksen tarkoituksena ei ole pelotella yrityksiä vaan antaa mahdollisuuksia tehokkaampaan henkilötietojen suojaamiseen. Tärkeänä asiana on ratkaista, miten asetuksen tuomat velvoitteet toteutetaan liiketoiminnassa niin ettei yrityksen liiketoiminta kärsi. Muuttuneen tietosuoja-asetuksen kannalta on hyvä tarkistaa tietosuoja vaatimukset säännöllisesti. GDPR-tietosuoja-asetuksen mu-

kaan yrityksessä on noudatettava tarkkuutta lain tuoman periaatteen mukaisesti. Henkilörekisterissä olevien tietojen tulee olla ajan tasalla ja oikeellisia. Rekisterinpitäjän työtä helpottaa paljon, jos rekisteröity tekee ajoissa oikaisupyynnön omista tiedoistaan. Tietojen ajankohtaisuus on yritykselle tärkeää. Mikäli oikaisupyynnössä ilmenee virheellisiä tietoja, on ne korjattava rekisterinpitäjän toimesta. Tiedot, joita yritys ei tarvitse, voidaan poistaa. Tällä tavalla saadaan rekisterissä olevien tieto minimoitua ja varmuus siitä, että henkilötietojen määrä on selvillä ja heistä löytyy vain tarvittavat tiedot. (Tietosuoja 2019.)

Kohdasta 3.2 alkaen käsitellään tarkemmin, mitä henkilötietojen elinkaaren määrittämiseen kuuluu. Elinkaarella tarkoitetaan ajanjaksoa henkilötietojen keräämisestä niiden anonymisointiin tai poistoon. Henkilötietojen elinkaari etenee kuvan 1. mukaisesti. (Pietikäinen 2016, kohta 5.4.3.)

Kuva 1. Henkilötietojen elinkaari

2.3.1 Henkilötietojen säilytysaika

Säilytykseen liittyvällä rajoitusperiaatteella tarkoitetaan sitä, että henkilötietoja saa säilyttää niin kauan kuin on tarpeen ja siten että, rekisteröity on tunnistettavissa. Henkilöön kohdistuvaa tietoa voi säilyttää pidempiäkin aikoja, mikäli tietoja käsitellään edun mukaisia tarkoituksia varten. Edun mukainen tarkoitus tarkoittaa asianmukaista arkistointia, tieteellistä tai historiallista tutkimusta sekä tilastointia. Henkilötietoihin kohdistuvaa elinkaarta ohjaavat erilaiset säädökset ja lait, jotka voivat mennä tietosuoja-asetuksen edelle. Erityisesti työnantajan on noudatettava erityissäännöksiä työntekijöiden henkilötietoja koskevia säilytysaikoja ajatellen. (Henkilötietojen käsittelyä koskevat periaatteet 2019.)

Alla olevassa taulukossa on listattuna keskeisimpiä asioita yrityksen aineiston säilytysaikoihin liittyen. Taulukko perustuu Finlexin arkistonmuodostusohjeistukseen. (Finlex.)

Taulukko 1. Arkistonmuodostussuunnitelma

Aineisto	**Asiakirja**	**Minimi säilytysaika**
Kirjanpito	Tilikauden tositteet Viranomaisilmoitukset Muu kirjanpitoaineisto Laskutiedot Avoimet laskut Matkalaskut	6 vuotta
	Tilinpäätösasiakirjat: Tasekirjat ja erittelyt Liitetietoerittelyt Kirjanpitokirjat Tilikartta	10 vuotta
	Kiinteistöinvestoinnit ja tositteet	14 vuotta
Kiinteistö ja materiaali hallinto	Vuokrasopimukset Siivoussopimukset Huoltosopimukset	6 vuotta sopimukset päättymisestä
Palkkakirjanpito	Palkkalaskennan muutosilmoitukset	1 vuosi
	Eläkeilmoitukset ja luettelot sekä ylityöilmoitukset ja ylityölaskut	2 vuotta
	Palkkalaskelmat Palkkaluettelut ja muut vastaavat luettelot ikilisiä koskevat asiakirjat Palkkalisiä koskevat asiakirjat irtisanomisia koskevat asiakirjat virkistyspäiviä koskevat asiakirjat	6 vuotta

	Jäsenmaksujen tilitysluettelo ulosottomääräykset Työtodistukset ja-sopimukset	10 vuotta
	Palkkoihin kohdistuvat asiakirjat	50 vuotta
	Verokortit	Verovuosi/voimassaolo-aika
	Jäsenmaksuvaltakirjat	Palvelusaika + 2 vuotta

Tietoa saa säilyttää vain sen ajan kuin sitä tarvitaan, sen jälkeen se on hävitettävä, ellei muusta lainsäädännöstä muuta johdu. Rekisteröidyn henkilön pyynnöstä tieto on poistettava, ellei sitä muun lainsäädännön vuoksi ole tarpeen säilyttää. (Finlex.)

2.3.2 Suostumus henkilötietojen käsittelemiseen

Kun yrityksen tietojenkäsittely perustuu suostumukseen, on rekisterinpitäjän pystyttävä osoittamaan se, että rekisteröidyltä on tullut suostumus henkilötietojen käsittelyä varten. Rekisteröidyn antaessa suostumuksensa kirjallisessa ilmoituksessa, jotka koskevat muita asioita, on tässä tapauksessa pyyntö esitettävä erillään muista asioista. Pyyntö tulee olla ymmärrettävässä muodossa ja se täytyy olla selkeässä muodossa sekä kirjoitettu yksinkertaisella kielellä. Rekisteröidyin oikeuteen kuuluu se, että hän voi milloin tahansa peruuttaa suostumuksensa. Kun suostumuksen peruuttaa, se ei vaikuta ennen sen peruuttamista suostumuksen perusteella suoritettuun käsittelyyn. Ennen suostumuksen antamista rekisteröidylle täytyy ilmoittaa asiasta. Suostumuksen peruuttaminen tulee tapahtua yhtä helposti kuin sen antaminenkin. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 5-7 artikla.)

> Arvioitaessa suostumuksen vapaaehtoisuutta on otettava mahdollisimman kattavasti huomioon muun muassa se, onko palvelun tarjoamisen tai muun sopimuksen täytäntöönpanon ehdoksi asetettu suostumus sellaisten henkilötietojen käsittelyyn, jotka eivät ole tarpeen kyseisen sopimuksen täytäntöönpanoa varten. (Suostumuksen edellytykset 2019.)

2.3.3 Henkilötietojen kerääminen ja käsittely

Yrityksessä pitää tietää, millaiseen tarkoitukseen henkilötietoja kerätään ja kuinka niitä käsitellään. Tietosuoja-asetuksen mukaan (Tietosuojavaltuutetun toimisto 2019.) on viisi tapaa kerätä henkilötietoja hyväksytysti:

- Henkilö on antanut suostumuksen siihen, että hänen tietojaan voidaan käsitellä.
- Sopimukseen perustuva kirjallinen dokumentaatio sopimuksesta.
- Rekisterinpitäjällä on lakiin perustuva velvoite tietojen keräämisestä viranomaistarkoituksiin.
- Rekisterinpitäjä käyttää julkista valtaa tai suorittaa yleisesti etua vaativaa tehtävää.
- Käsittely on tarpeellista rekisterinpitäjän sekä kolmannen osapuolen etujen toteuttamisesta.

Turvallinen ja luottamuksellinen henkilötietojen käsittelytapa varmistaa sen, että tiedot pysyvät suojattuina. Henkilötiedot suojataan luvattomalta ja lainvastaiselta käsittelyltä rekisterinpitäjän toimesta. Näin varmistetaan, etteivät henkilöstä olemassa olevat tiedot vahingoitu tai häviä. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 5-7 artikla.)

Tiedon käsittelyä on esimerkiksi tietojen tallentaminen, kerääminen, järjestäminen, säilyttäminen tai tietojen luovuttaminen. Käsittely voi olla automaattista tai manuaalista. Automaattisessa käsittelyssä henkilötietoja käsitellään järjestelmässä sähköisesti. Fyysisellä henkilötietojenkäsittelyllä viitataan manuaaliseen käsittelyyn, esimerkiksi yrityksen papereiden sekä mappien käsittely on manuaalista tietojen käsittelyä. Automaattisella käsittelyllä puolestaan viitataan profilointiin, jossa arvioidaan henkilöistä saatujen tietojen perusteella tämän ominaisuuksia. Arkaluontoisessa tietojenkäsittelyssä voidaan hyödyntää pseudonymisointi, jolloin henkilötietojenkäsittelystä tulee turvallisempaa. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, 5-7 artikla.)

> Arkaluonteisten henkilötietojen käsittely on pääsääntöisesti kiellettyä ja sitä säännellään erikseen. Käsittelyyn voi olla oikeus esimerkiksi silloin, kun rekisteröity on antanut siihen nimenomaisen suostumuksensa, kun henkilötietoja käsitellään tieteellistä tutkimusta tai tilastointia varten tai kun henkilötietojen käsittelystä säädetään laissa.

> Arkaluonteisista henkilötiedoista muodostettuja tietokokonaisuuksia kutsutaan EU:n yleisessä tietosuoja-asetuksessa (2016/679) erityisiksi henkilötietoryhmiksi tai henkilötietojen erityisryhmiksi. (Arkaluontoinen henkilötieto 2018.)

Termillä pseudonymisointi tarkoitetaan henkilötietojen käsittelyä siten, että rekisterissä olevaan henkilöön ei voida enää yhdistää suoraan ilman lisätietoja. Esimerkiksi henkilötiedot voidaan korvata peitenimillä tai tietokannasta henkilöön liittyvä tieto voidaan korvata toisella. Henkilötiedot voidaan myös koodata niin, että henkilön tiedot löytyvät esimerkiksi omalla koodiavaimella. Henkilötietojen koodaaminen on pseudonymisointia. (Pseudonynamisoidut ja anynomisoidut tiedot 2014.)

2.3.4 Henkilötietojen luovutus ja arkistointi

Tietoja voidaan luovuttaa niitä pyytäville viranomaisten toiminnan julkisuudesta annetun lain mukaisesti. Yrityksen tiedot ja asiakirjat ovat yleensä julkisia, ellei niitä ole erikseen nimenomaisesti säädetty salassa pidettäväksi laissa. Salassa pidettäviä tietoja voi kuitenkin luovuttaa tiettyjä tehtäviä varten, kun salassa pidettävien tietojen poistaminen niiden suuren määrän tai muun verrattavan syyn vuoksi ei ole tarkoituksenmukaista. Viranomaisen on pidettävä huoli siitä, että tietojen salassapidosta ja suojaamisesta huolehditaan asianmukaisesti. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 5-7.)

Arkistointia voidaan hyödyntää yrityksen yleisen edun mukaisia tarkoituksia varten. Muita tapauksia ovat tieteelliset ja historialliset tutkintatarkoitukset, joissa sovelletaan rekisteröidyn oikeuksia ja vapauksia koskevia suojatoimia asetuksen mukaisesti. Näillä suojatoimilla varmistetaan teknilliset ja organisatoriset toimenpiteet, tällä tavalla taataa tietojen minimointi periaatteen noudattamisessa. Pseudonymisointi kuuluu esimerkiksi tällaiseen toimenpiteeseen, jos mainitut tarkoitukset voidaan käyttää edellä mainitun tavan mukaisesti. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 5-7.)

2.3.5 Henkilötietojen anonymimosointi/poisto

Anonymisoinnilla tarkoitetaan henkilöihin liittyvän tiedon käsittelyä, ettei henkilöä pystytä enää yhdistämään tai tunnistamaan annetuista tiedoista. Tiedot on mahdollista karkeistaa yleiseen tasoon tai muuttaa tiedot esimerkiksi tilastolliseen muotoon niin, ettei henkilöstä kohdistuvia tietoja voida enää tunnistaa. Tunnistaminen täytyy tehdä niin, ettei henkilöön kohdistuva anonymisointi voi estyä peruuttamattomasti tai ettei rekisterinpitäjä tai kukaan muukaan pysty jo hallussa olevillaan tiedoilla muuttaa henkilöä tunnistettaviksi. Rekisterinpitäjän on huomioitava, että kaikki henkilöön kohdistuvat tiedot (ei pelkästään henkilötietoja, osoitetietoja vaan myös henkilöön mahdollisesti liitetyt sairaustiedot) on anonymisoitu, koska yksilöin tietojen poistaminen ei aina tarkoita, että kaikki henkilöön kohdistuvat tiedot muuttuisivat anonyymeiksi. (Pseudonymisoidut ja anonymisoidut tiedot 2014; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 17.)

Kun anonymisointia tehdään, on muistettava ottaa huomioon kaikki kohtuudella toteutettavissa olevat keinot. Esimerkiksi yrityksessä on hyvä huomioida henkilöiden tunnistamiseen vaadittavat mahdolliset kulut, aika ja käytettävissä oleva teknologia. Rekisterinpitäjän on otettava huomioon ja varauduttava siihen, että kerran tehty anonymisointi voi heiketä teknisen kehityksen ja ajan myötä. Anonymisoituja tietoja ei enää katsota henkilötiedoiksi eikä niihin enää sovelleta tietosuojasäännöksiä. Se, voidaanko tieto lopulta katsoa anonymisoinnin kannalta anonyymiksi, edellyttää tapauskohtaista arviointia. Henkilö on mahdollista tunnistaa muillakin tavoilla, kun esimerkiksi pelkästään nimen perusteella. Kerättävä aineisto voi sisältää henkilöön kohdistuvaa yksittäistä tietoa, tässä tapauksessa esimerkiksi jokin sairaus voidaan yhdistää niin, että henkilö on välillisesti tunnistettavissa. Tuloksessa olevassa aineistossa on edelleen henkilötietoja jäljellä, mikäli rekistelinpitäjä ei poista kaikkia alkuperäisiä kerättyjä aineistoja sekä henkilöstä tunnistettavissa olevia tietoja ja luovuttaa aineistosta osan edelleen. (Pseudonymisoidut ja anonymisoidut tiedot 2014; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 17.)

2.4 Rekisteröidyn oikeudet

Henkilöllä, jonka tiedot löytyvät rekisteristä, on tiedolliset oikeudet omiin henkilötietoihinsa ja oikeus tietää mitä tietoja hänestä rekisterissä on. Henkilöllä on myös valtuudet määrittää saako hänen tietojansa siirtää palveluntarjoajalta toiselle ja hänellä on myös oikeus vastustaa henkilötietojen käsittelyä ja pyytää henkilötietojen poistoa rekisteristä. (Oikeus tehdä valitus valvontaviranomaiselle 2019; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 15.)

2.4.1 Henkilötietojen pyyntö rekisteristä

Henkilöllä on oikeus pyytää omia tietoja rekisteristä. Rekisteröidyn kannalta näillä oikeuksilla tarkoitetaan parempaa tietosuojaa ja kontrollointimahdollisuutta siitä, missä yhteydessä tietoja käsitellään. Näissä tapauksissa henkilöllä, joka vastaa rekisterinpitämisestä, on kuukausi aikaa vastata rekisteröidyn pyyntöön. Jos pyyntö on monimutkainen tai tietoa ilmenee paljon, on mahdollista miettiä kahden kuukauden lisäaikaa. (Oikeus oikaista tietoa) Rekisterinpitäjän vastuulla on toimittaa rekisteröidyn haluamat tiedot sähköisessä tai kirjallisessa muodossa, jos rekisteröity niin haluaa. Rekisteröity voi halutessaan tehdä valituksen valvontaviranomaisille, jos hänen haluamissaan oikeuksien toteutumissa ilmenee ongelmia. (Oikeus tehdä valitus valvontaviranomaiselle 2019; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 15.)

2.4.2 Tarkastusoikeus ja oikaisemisoikeus

Tarkastusoikeudessa määrätään, että rekisteröidyllä on oikeus tietää, mitä henkilötietoja hänestä löytyy ja kuinka niitä säilötään. Mikäli rekisterinpitäjä kieltäytyy antamasta tietoja rekisteröidylle, tulee rekisterinpitäjän laatia selkeä kirjallinen todistus, jossa ilmenee syyt tarkastusoikeuden epäämiselle. Tietojen tarkastaminen on ilmaista kerran vuodessa kulutusasiakkaille. Oikaisupyynnöllä rekisteröity saa korjattua virheelliset henkilötietonsa oikeiksi. Rekisterinpitäjän tulee oikaista rekisteröidyn tiedot ilman aiheetonta viivytystä. Oikaisu tehdään esimerkiksi niin, että rekisteröity toimittaa lisäselvityksen epätarkoista tai virheellisistä henkilötiedoistaan rekisterinpitäjälle ja näin rekisterinpitäjä huomioi rekisterissä olevan. (Oikeus tietojen oikaisemiseen 2019; Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 16.)

2.4.3 Siirto- ja vastustamisoikeus

Rekisteröity voi siirtää omia tietojansa palveluntarjoajalta toiselle. Tiedot voidaan toimittaa automaattisesti eri järjestelmästä toiseen, mikäli se on teknisien toimenpiteiden kannalta mahdollista. Siirto voidaan tehdä myös niin, että rekisteröity pyytää tietonsa rekisterinpitäjältä ja toimittaa ne itse toiselle palveluntarjoajalle. (Oikeus siirtää tiedot järjestelmästä 2019; Euroopan parlamentin asetus (EU) 2016/679, artikla 20.)

GDPR-asetus takaa oikeuden rekisteröidylle vastustaa hänen henkilötietojensa käsittelyä. Mikäli rekisteröity käyttää vastustamisoikeuttaan, rekisterinpitäjä ei saa tämän jälkeen enää käsitellä rekisteröidyn henkilötietoja. Asetuksesta kuitenkin löytyy tietyt edellytykset käsittelykiellon poikkeamiseen. (Euroopan parlamentin asetus (EU) 2016/679, artikla 21.)

2.4.4 Henkilötietojen poisto rekisteristä

GDPR-asetuksessa on määritys siitä, että jokaisella rekisterissä olevalla on oikeus tulla ”unohdetuksi”. Tällä viitataan rekisterissä olevaan, joka voi halutessaan ilmoittaa rekisterinpitäjälle omien tietojensa poistamisesta. Tällöin rekisterinpitäjän on ilman viivästystä poistettava tiedot rekisteristä. Poistoon liittyen on olemassa lakisääteinen perusta tietojen säilyttämiseen rekisterissä. Seuraavaksi poistoa edellyttäviä perusteita, josta jokin pitää täyttyä, jotta rekisterinpitäjä pystyy poistamaan rekisterissä olevan henkilötiedot. (Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, artikla 17.)

- Henkilötietoja ei enää tarvita samoihin tarkoituksiin, joihin ne on alkuun kerätty
- Rekisteröidyn suostumuksen peruminen.
- Rekisteröity vastustaa käsittelyä ilman aiheellista syytä.
- Henkilötietojen lainvastainen käsittely.
- Henkilötiedot on poistettava jäsenvaltion lainsäädäntöön tai unionin oikeuteen perustuvan rekisterinpitäjään sovellettavan lakisääteisen velvoitteen noudattamiseksi.
- Henkilötietoja on kerätty alle 16-vuotiaalta tietoyhteiskunnan palvelujen yhteydessä.

2.5 Rekisterinpitäjän velvollisuudet

Yrityksen on oltava selvillä GDPR-asetuksen noudattamisesta, esimerkiksi tekemällä pakolliset muutokset tietosuojadokumentaatioon, joka koskee yrityksen palvelusopimuksia, asiakassopimuksia sekä muita käyttöehtoja ja tietosuojaselosteita. Kun yritys noudattaa osoitusvelvollisuutta, tulee ottaa huomioon dokumentaation, vaikutusarvioinnin ja toimintamallien käyttöönotto. Yrityksessä on hyvä pohtia, miten huomioidaan tietojärjestelmien käyttöoikeuksien jakamisesta henkilöstölle. Mikäli yritykseen kohdistuu tietoturvaloukkausta, on velvollisuus ilmoittaa yrityksen sisällä asiasta, jolloin voidaan minimoida ja ehkäistä vahinkoja. (Rekisterinpitäjän velvollisuudet 2016.)

Yrityksessä on tärkeää olla selvillä yrityksen rekisterinpitäjän ja käsittelijän vastuunjako. Rekisterinpitäjä on vastuussa siitä, mitä asiakkaiden henkilötietoja hän tallettaa rekisteriinsä. (Rekisterinpitäjän velvollisuudet 2016, kohdat 5.0-5.3.) Esimerkiksi tässä tapauksessa henkilö haluaa hakea vuokra-asuntoa yritykseltä, jolloin yritys toimii käsittelijänä. Käsittelijän tulee huomioida henkilötietoja, joita yritykseen luovutetaan, esimerkiksi nimi, puhelinnumero, henkilötunnus ja osoite. (Rekisterinpitäjän velvollisuudet 2016.)

Rekisterinpitäjän ja käsittelijän välille on tehtävä tietosuoja-asetuksen artikla 28 mukainen palvelusopimus. (Rekisterinpitäjän velvollisuudet 2016.) Sopimuksesta tulee ilmetä seuraavat asiat:

- Käsiteltävä kohde ja kesto
- Luonne ja tarkoitus
- Henkilötietojen tyyppi ja rekisteröityneet
- Rekisterinpitäjän oikeudet ja velvollisuudet

Voimassa olevia palvelusopimuksia ei tarvitse hävittää tietosuoja-asetuksen myötä. Useammissa tapauksissa GDPR:n sopimusliiteosuus liitetään valmiiseen sopimukseen. Palvelusopimus varmistaa henkilötietojen oikeanlaisen käsittelymenetelmän ja sen, että yritys käsittelee rekisterinpitäjän ylläpitämiä tietoja rekisterinpitäjän haluamalla tavalla. Mikäli yritykseltä löytyy alihankkijoita, henkilötietojen on mahdollista kulkeutua palvelun-

tarjoajalta toiselle. Näissä tapauksissa palveluntarjoaja on vastuussa siitä, miten alihankkija käsittelee henkilötietoja rekisterinpitäjältä saaneen ohjeistuksen mukaan. Yrityksessä on tärkeää tehdä ja noudattaa salassapitosopimusta, jotta saadaan väärinymmärrysriskit minimoitua. (Rekisterinpitäjän velvollisuudet 2016.)

2.5.1 Nykytilan arviointi

GDPR-tietosuoja asetuksen kannalta on tärkeää huomioida käsittelyyn liittyvät riskit rekisteröidyn oikeuksille. Yrityksen kannalta on suotavaa tehdä lähtötilanteen arviointi siitä, mikä on yrityksen nykyinen tilanne, jonka kautta yritys pystyy helpommin tutustumaan GDPR:än muihin vaatimuksiin. Lähtötilanteen arviointi eli PIA (privacy Impact assesment) on tietosuojan yksi arviointi menetelmistä. Tämän avulla yritys pystyy tekemään jonkinasteista nykytilan arviointia GDPR:n kannalta. (Tietosuoja-arviointi.)

Yrityksen on hyvä olla selvillä siitä, mitä henkilötietoja käsitellään, mitä tietoja henkilöistä löytyy ja onko käsittely GDPR-tietosuoja asetuksen mukaista. GDPR:n myötä on hyvä tietää asetuksen tuoman toimintatapojen muuttamisesta ja siitä, miten prosesseja ja dokumentteja käsitellään. (Miten vastata EU:n yleisen tietoja-asetuksen (GDPR) vaatimuksiin 2019.)

2.5.2 Osoitus- ja ilmoitusvelvollisuudet

Rekisterinpitäjän velvollisuuksiin kuuluu huolehtia tietosuoja-asetuksista siten, että kaikki siihen kuuluvat periaatteet täyttyvät henkilötietojen käsittelyssä. Jatkossa rekisterinpitäjän on pystyttävä osoitusvelvollisuudenmukaisesti toimimaan tietosuoja-asetuksen mukaisesti, kun taas ennen riitti toteaminen sanallisesti. Osoitusvelvollisuudessa edellytetään, että yrityksessä huolehditaan henkilötietoihin kohdistuvassa käsittelyssä seuraavia tärkeitä periaatteita: Luottamuksellisuus, eheys, säilytyksen rajoitus, lainmukaisuus, kohtuullisuus sekä läpinäkyvyys ja se, mihin tarkoitukseen tietoja käytetään. Edellä mainittuja osa-alueita yritys pystyy toteuttaa esimerkiksi tekemällä tietotilinpäätöksen. (Euroopan parlamentin ja neuvoston asetus EU 2016/679, artikla 33.)

Mikäli yritykseen kohdistuu tietosuojaloukkauksia, tulee rekisterinpitäjän ilmoittaa tietosuojaviranomaiselle ja sille, keneen loukkaus on kohdistunut. Ilmoitus on tehtävä 72 tunnin sisällä loukkauksen havaitsemisesta. Tärkeää on rekisteröityneen kannalta tehdä ilmoitus mahdollisimman nopeasti vakavuuden välttämiseksi ilman aiheetonta viivästystä. (Euroopan parlamentin ja neuvoston asetus EU 2016/679, artikla 33.)

2.5.3 Rekisteröidyn oikeuksiin vastaaminen

Rekisteröidyn oikeuksien toteaminen kuuluu rekisterinpitäjän tärkeimpiin tehtäviin. Jos rekisteröity tekee yritykselle tarkastuspyynnön, kuuluu rekisterinpitäjän velvollisuuksiin vastata pyyntöön viimeistään kuukauden kuluttua pyynnön jättämisestä. Pyynnöstä on mahdollisuus jatkaa määräaikaa kahteen kuukauteen, mikäli tiedoissa ilmenee monimutkaisuutta tai määrällisesti tietoa on normaalia enemmän. Pyyntö määräajan jatkamisesta kuuluu tehdä kuukauden sisällä rekisterissä olevalle. Ilmoituksessa tulee olla selkeä syy, mikäli pyyntö jätetään toteuttamatta. Rekisteröityä tulee opastaa myös tekemään valitus valvontaviranomaiselle. Ennen tietojen luovuttamista on rekisterinpitäjän varmistettava rekisteröidyn henkilöllisyys. (Läpinäkyvä informointi, viestintä ja yksityiskohtaiset säännöt rekisteröidyn oikeuksien käyttöä varten 2019.)

2.5.4 Rekisteri- ja tietosuojaseloste

Yrityksessä olevan rekisterinpitäjän on laadittava henkilötietolain mukainen tiivis ja helposti luettavissa oleva dokumentti rekisteri- tai tietosuojaselosteesta. Dokumentissa kuuluu olla muun muassa seuraavia tietoja. (Seloste käsittelytoimista 2019.)

- Kuka on rekisterinpitäjä ja kuka rekisterin yhteyshenkilö.
- Mitä tietoja rekisterissä on ja mikä on niiden käsittelyn tarkoitus.
- Miten henkilöä koskevat tiedot on suojattu.
- Kuinka pitkä on tietojen säilytysaika ja minne henkilötietoja asetuksen mukaan luovutetaan.

2.6 Tietosuojavastaava

Tietosuojavastaava toimii tietosuojan erityisasiantuntijana. Yrityksen johdon ja tietosuojavastaavan välille on hyvä muodostaa hyvä yhteystyösuhde, jotta lähestyminen on helpompaa ongelma tilanteita ajatellen. Tietosuojavastaavan tehtävänä on antaa asiantuntevaa apua yrityksen muille henkilöille ja erityisesti johtoportaaseen. Nämä säännökset koskevat myös muuta yrityksen henkilökuntaa, joiden on tärkeä noudattaa asetusta rikkomusten välttämiseksi. (Tietosuojavastaavia koskevat ohjeet 2017. kohta 3.4.; Euroopan parlamentin ja neuvoston asetus EU 2016/679, artikla 37-38.)

Tietosuojavastaava toimii asiantuntijana yrityksen tietosuoja-asioissa, vastuu asetuksen noudattamisessa on aina viimehetkillä rekisterinpitäjällä. Tietosuojavastaavalla on tärkeä rooli yrityksessä ja hänet on otettava mukaan kaikkiin tietosuojaa koskeviin asioihin ja kokouksiin mukaan. Rekisterinpitäjä tai henkilötietojen käsittelijä eivät saa erottaa eivätkä rangasta tietosuojavastaavaa tehtäviensä hoitamisen vuoksi. (Tietosuojavastaavia koskevat ohjeet 2017. kohta 3.4.; Euroopan parlamentin ja neuvoston asetus EU 2016/679, artikla 37-38.)

Tietosuojavastaava voi olla osana yrityksen henkilökuntaa tai käsittelijähenkilökuntaan. Rekisterinpitäjällä on mahdollisuus ulkoistaa tietosuojavastaavan tehtävät. Suositeltavaa kuitenkin on pitää tietosuojavastaava yrityksen omasta henkilökunnasta. Tämä siitä syystä, että tietosuojavastaavan on helpompi pysyä tietoisena yrityksen eri osa-aluista ja siitä, mitä yrityksessä tapahtuu. Mikäli yritys kuitenkin ottaa tietosuojavastaavan ulkopuolelta, voi kyseinen henkilö olla koulutukseltaan esimerkiksi tietoturva-asiantuntija tai juristi. Tietosuojavastaavan on oltava perillä tietosuojalainsäädännöstä, vaatimusten soveltamistaidoissa sekä yleinen tuntemus alan käytännöistä. Tietosuojavastaavaksi nimetyn henkilön yhteystiedot julkaistaan rekisterinpitäjän tai henkilötietoja käsittelevän toimesta. Nämä asiat on tehtävä rekisteröityjen kannalta saataviksi sekä nimitetystä tietosuojavastaavasta on ilmoitettava valvontaviranomaiselle. (Euroopan parlamentin ja neuvoston asetus EU 2016/679, artikla 37-38.)

2.6.1 Tarve ja nimittäminen

Tietosuojavastaava on aina nimitettävä rekisterinpitäjän toimesta, mikäli tietoja käsittelee jokin muu viranomainen tai julkishallinnon elin kuin lainkäyttötehtäviään toteuttava tuomioistuin. Tietosuojavastaa täytyy nimittää, mikäli rekisterinpitäjä tai käsittelijän päätoimiset tehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajempimittaista rekisteröityjen järjestelmällistä ja säännöllistä seurantaa. Mikäli käsittely kohdistuu erityisiin tietoryhmiin, rikoksiin tai tuomioihin on tärkeää yrityksen nimittää tietosuojavastaava. (Tietosuojavastaavan nimittäminen 2019; Euroopan parlamentin ja neuvoston asetus EU 2016/679, artikla 37.)

2.6.2 Tehtävät

Yleisen tietosuoja-asetuksen artikla 39 kohta 1 b alakohdan mukaan (Tietosuojavastaavia koskevat ohjeet 2017, kohta 4; Euroopan parlamentin ja neuvoston asetus EU 2016/679, artikla 39.) tietosuojavastaavan tehtäviin kuuluu muun muassa:

– Asetuksen noudattaminen ja sen seuranta.
– Rekisterinpitäjän ohjaaminen ja seuraaminen tietosuoja-asetuksessa.
– Kerätä tietoa käsittelytoimia varten ja analysoida, ovatko ne vaatimusten mukaisia.
– Yhteystyön toimiminen viranomaisten kanssa.
– Henkilökunnan kouluttaminen tietosuojaa varten.
– Valvonta rekisteröidyn oikeuksista.

3 Tietosuoja ja -turva

Tietosuojaan ja -turvaan liittyvät sekä fyysiset että digitaaliset turvat. Tässä käydään yleisellä tasolla läpi, mitä ne pitävät sisällään tietosuoja-asetuksen kannalta.

3.1 Fyysinen turva

Tärkeänä tietosuojan osa-alueena on fyysinen tietoturva siitä, miten esimerkiksi yrityksessä säilytetään henkilötietoja ja onko säilyttäminen asianmukaista. Tällä tarkoitetaan

arkistojen, asiakirjojen, mappien ja henkilöistä löytyvän tiedon oikeanlaista säilytystä, tässä tapauksessa lukollinen kaappi. Lukollisen kaapin avaimet on hyvä löytyä yrityksessä sellaiselta henkilöltä, jonka työtehtäviin kuuluu henkilötietojen käsittely. Vierailla, joilla tarkoitetaan yrityksen alihankkijoita ei ole oikeuksia päästä käsiksi henkilötietoihin. Yleisesti tilat, joihin kutsutaan vain vieraita pääsevät yritykseen vierailemaan sovitusti ja heitä on vastaanottamassa sovittu henkilö. Nämä koskevat etukäteen sovittuja tapaamisia esimerkiksi yrityksessä olevan henkilön ja alihankkijan kanssa. Sovituilla tapaamisilla estetään ulkopuolisia tahoja pääsemästä yrityksen tiloihin. (Laakso 2010.)

Käyntikortit sekä kirjepostit kuuluvat myös fyysisiin henkilötietoihin. Näissä tapauksissa tärkeä huolehtia postin kulkeutuminen lukolliseen postilokeriin ja avaimet kuuluvat asianomaiselle henkilölle. Fyysisien palvelimien kohdalla on hyvä varmistaa palvelimien löytyvän lukollisista tiloista ja avain vain niille, joilla on asiantunteva kokemus palvelimista. Yrityksessä voidaan päättää, kenelle luovutetaan pääsyoikeus palvelimille. Fyysistä turvallisuutta noudattaen kannattaa selvittää, kenelle annetaan kulkuluvat, ja miten rajataan kulkuoikeudet eri tiloihin. Tätä varten on hyvä tehdä ohjeistus turvallisuuteen liittyen, vaikka osa-asioista on itsestään selvyyksiä. (Laakso 2010.)

3.2 Digitaalinen turva

Digitaalisen turvan kannalta on tärkeää, että henkilötietoja käsiteltäessä niitä myös osataan suojata oikealla tavalla. Työpisteeltä poistuttaessa on hyvä lukita tietokone. Työtietokoneisiin tulee turvallisuuden kannalta laittaa vahva salasana. Vahvasta salasanasta pituus voi olla 12-15 merkkiä ja siinä voi olla mukana isoja ja pieniä kirjaimia, myös erikoismerkkejä ja numeroita. Tällä tavalla lisätään turvallisuutta jokaista käyttäjää kohden. Salasanan kannalta on hyvä muistaa, ettei samaa salasanaa käytetä muualla ja salasana kannattaa vaihtaa uuteen säännöllisesti. Yleensä yrityksessä on vahvat salasanat järjestelmissä, joista vastaa yrityksessä oleva henkilö. Käyttöjärjestelmiä ajatellen on hyvä kartoittaa oikeudet esimerkiksi järjestelmävalvojan ja perinteisen käyttäjän suhteen. Perinteinen käyttäjä kuuluu kuitenkin yrityksen henkilökuntaan, vaikka hänellä ei olisi järjestelmävalvojan oikeuksia. Yrityksen kannattaa myös huomioida älypuhelimen suojaus. Nykypäivänä älypuhelimalla tehdään töitä kuten kannettavalla tietokoneella. Näin ollen puhelimessa on hyvä olla suojaus kunnossa. (Laakso 2010; Asiaa tietoturvasta.)

Yrityksen jokaisessa tietokoneessa on työntekijöiden ja yleisen turvallisuuden kannalta tärkeä olla ohjelmistot ajan tasalla. Näillä ohjelmilla tarkoitetaan esimerkiksi palomuuria, virustunnisteita, käyttöjärjestelmää sekä muita yrityksen ohjelmistoja. Monella henkilökunnan työntekijällä on käytössään kannettava tietokone ja turvallisuuteen liittyen on muistettava pitää niissäkin vahvaa salasanaa. Tietojärjestelmissä on hyvä käyttää vahvoja salasanoja ja miettiä kenellä on käyttöoikeudet yrityksen tietokoneisiin ja niiden ohjelmiin. Tämä helpottaa työntekijöiden tehtäviä siinä mielessä, että jokainen yrityksessä tietää, mihin heillä on käyttöoikeus. (Laakso 2010; Asiaa tietoturvasta.)

Henkilön poistuttua yrityksen palveluksesta on äärimmäisen tärkeä muistaa kerätä avaimet, kulkuluvat ja muut käyttöoikeudet pois. Tällä estetään, ettei tieto pääse kulkeutumaan eteenpäin. (Laakso 2010; Asiaa tietoturvasta.)

3.3 Tietotilinpäätös

Tietotilinpäätöksen tarkoituksena on huolehtia siitä, että yrityksessä toimitaan henkilötietolain mukaisesti tietojenkäsittelyssä. Tietotilinpäätöksellä on mahdollista täydentää lakisääteistä tilinpäätöksiin ja toimintakertomuksiin kuuluvaa raportointia. Tietotilinpäätöksen tarkoituksena ei ole tarpeettomasti lisätä yrityksen hallinnollista taakkaa. Tietotilinpäätöksen tarkoituksena on toimia dynaamisena työkaluna, joka tukee yrityksen tehokkuutta, vaikuttavuutta ja kilpailukykyä. (Laadi tietotilinpäätös 2012.)

Yrityksen on varmistettava, että hyvä tietojenkäsittelytapa ja hyvä tiedonhallintavan toteuttamiseksi annettuja säännöksiä ja ohjeita noudatetaan sekä valvotaan. Hyvän tiedonhallintatavan edellyttämät toimenpiteet toteutetaan siten, että eri osapuolten oikeusturva toteutuu. Tietojen käsittelyn valvonta voi olla osa yrityksen muuta sisäistä valvontaa ja riskien hallintaa. Valvonnan tuloksia ja niiden perusteella tehtyjä toimenpiteitä on syytä arvioida. (Laadi tietotilinpäätös 2012.)

Tietotilinpäätöksen perusteella tehdään johtopäätöksiä siitä, onko toiminta ja tietojen käsittely ollut hyvän tietojenkäsittelytavan ja hyvän tiedonhallintatavan mukaista. (Laadi tietotilinpäätös 2012.)

- Miten henkilötiedot on suojattu?
- Millä tavalla rekisteröidyn oikeudet tietojenkäsittelyssä toteutetaan?
- Miten henkilötietojen käyttöä valvotaan?
- Mitä menettelytapoja ja periaatteita tietojenkäsittelyssä noudatetaan?

3.4 Tietosuojaorganisaatio

Tietosuoja vastaava toimii yrityksen sisäisenä asiantuntijana. Tietosuojavastaavan tehtäviin kuuluu seurata ja auttaa henkilötietojen käsittelyssä siten, että se noudattaa tietosuojasäännöstä. (Tietosuojavastaavat.) Tietosuojavastaavan tehtävät

- Seurata tietosuojasääntöjen noudattamista koko organisaatiossa ja tuoda esiin havaittuja puutteita.

- Antaa tietoja ja neuvoja tietosuojasääntöjen mukaisista velvollisuuksista johdolle ja henkilötietoja käsitteleville työntekijöille.

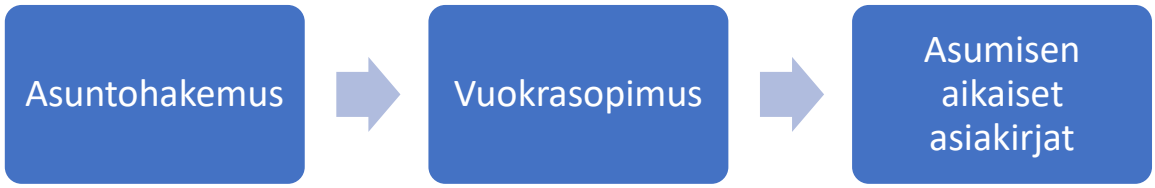
- Antaa tarvittaessa neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoo vaikutustenarvioinnin toteutusta.

- Toimia rekisteröityjen yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä asioissa.

- Toimia tietosuojavaltuutetun toimiston yhteyshenkilönä ja tehdä yhteistyötä tietosuojavaltuutetun toimiston kanssa.

4 Tutkimuksen toteutus ja tulokset Järvenpään Mestariasunnot Oy:ssa

Tutkimus on rajattu koskemaan Järvenpään Mestariasunnot Oy:n asiakkaiden henkilötietoihin kohdistuvaan tietosuojaan alla olevan kuvan mukaisista asioista. Yrityksen keräämissä tiedoissa ei ilmene arkaluontoista tietojenkäsittelyä, jolloin ei tarvita pseudonymisointia.



Kuva 2. Asukkaan henkilötietoja sisältäviä dokumentteja

4.1 Sähköinen asuntohakemus

Sähköinen asuntohakemus voidaan tehdä kahdella eri tavalla. Ensimmäinen tapa on täyttää tiedot suoraan sähköiselle lomakkeelle. Yrityksen sähköisen asuntohakemuslomakkeen tiedot lähetetään SSL-salatulla yhteydellä (SSL=Secure Sockets Layer, tietoverkkosalausprotokolla). Kun asukas tekee asuntohakemuksen, tallentuu hakemus Tampuuri -asuntohakemusrekisteriin, jossa aktiiviset hakemukset ovat voimassa kolme kuukautta. Asuntohakemukset on mahdollista uudistaa yrityksen verkkosivuilta. Asuntohakemusrekisteristä ne henkilöt, jotka saavat asunnon poimitaan rekisteristä ja heidän kanssaan solmitaan vuokrasopimus. Toinen tapa on täyttää PDF-muotoinen asuntohakemuslomake yrityksen nettisivuilla ja postittaa se Järvenpään Mestariasunnoille.

Järvenpään Mestariasunnot Oy:ssä vuokrahakemuksia käsitellään ja säilytetään seuraavilla tavoilla:

- Mikäli hakemus johtaa vuokrasopimukseen, asuntohakemus säilytetään tällöin sopimukseen liitteenä.

- Mikäli hakemus taas ei johda vuokrasopimukseen, säilytysaika on tällöin viisi (5) vuotta.
- Poikkeuksena kuitenkin tilanne, jossa kunta on osallistunut asukasvalintaan, jolloin negatiivinen päätös liitteineen on säilytettävä kymmenen (10) vuotta.

Viitaten GDPR säilytysaika liitteeseen kohtaan asuntohakemus, säilytysajat ovat huomioitu asetuksen mukaisesti viitaten Finlexin arkistomuodostus suunnitelmaan. Liitteessä on tarkemmin tietoja Järvenpään Mestariasunnot Oy:n säilytysajoista. Säilytykseen liittyvät tiedot ovat huomioitu asetuksen mukaisesti ja näihin ei tarvitse tehdä muutoksia.

4.2 Vuokrasopimus ja vuokrareskontra

Vuokrasopimus solmitaan aina kirjallisena. Vuokrasopimukset säilytetään sähköisessä muodossa ja paperiversiona. Sähköiset asuntohakemukset ovat Tampuurin asukasrekisterissä. Paperiset vuokrasopimukset säilytään toimistolla lukituissa kaapeissa. Pääsy niihin on ainoastaan henkilöillä, jotka käsittelevät vuokrasopimuksia. Tässä tapauksessa vuokravalvojalla ja asukasvalitsijalla on pääsy vuokrasopimuksiin. Vuokrareskontra eli vuokranmaksuihin liittyvät asiat käsitellään yrityksessä Tampuuri -ohjelman sisällä. Oikeus yrityksessä vuokratietojen käsittelyyn on ainoastaan vuokravalvojalla ja hänen varahenkilöllään, kuten tietosuoja-asetuksessa sanotaan.

Järvenpään Mestariasunnot Oy:ssä vuokrasopimuksia käsitellään ja säilytetään seuraavilla tavoilla:

- Jos vuokrasopimus on päättynyt ilman epäselvyyksiä (esim. riita, häätö, perintä) on säilytysaika kuusi (6) vuotta vuokrasopimuksen päättymisen jälkeen.
- Jos vuokrasopimus on päättynyt epäselvyyksien kanssa (esim. vuokravelka tai muu riita-asia) on säilytysaika tällöin kuusi (6) vuotta siitä, kunnes asia on loppukäsitelty asiakkaan ja Jma:n välillä, eikä kummallakaan ole enää vaatimuksia tai velvoitteita toista osapuolta kohtaan.

Asuntohakemuksiin kohdistuvassa henkilötietojen keräämisessä ja niiden säilyttämissä toimitaan Raklin ohjeen mukaisesti. Raklin ohjeessa on kysymys henkilötietolain ja erityislakien vaikutuksesta tietojen keräämiseen, säilyttämiseen ja niiden luovuttamiseen

vuokraustoiminnassa. Raklin ohjeessa kerrotaan esimerkiksi, miten ja missä tilanteessa henkilötunnusta sisältävää tietoa saa käsitellä. Näitä tilanteita ovat: luotonanto tai saatavan perintä, vakuutus-, luottolaitos-, vuokraus- ja lainaustoiminta, luottotietotoiminta, terveydenhuolto, sosiaalihuoltoa ja muuta sosiaaliturvaa toteutettaessa tai virka-, työ- ja muita palvelussuhteita ja niihin liittyviä etuja koskevissa asioissa. (Raklin ohje.)

Säilytysajat ovat huomioitu asetuksen mukaisesti, viitaten Finlexin arkistonmuutoksen suunnitelma taulukkoon(taulukko.1). Liitteessä on tarkemmin tietoja Järvenpään Mestariasunnot Oy:n säilytysajoista. Säilytykseen liittyvät tiedot ovat huomioitu asetuksen mukaisesti ja näihin ei tarvitse tehdä muutoksia.

4.3 Vikailmoitukset

Vikailmoitukset tallentuvat huoneistokohtaisesti Tampuurissa ja jokaisessa huoneistokohtaisessa ilmoituksessa on ilmoittajan nimi ja luonnollisesti myös osoite, sekä puhelinnumero (koska ne ovat välttämättömiä huoltotoimenpiteen suorittamiseksi) ja ne tiedot jäävät Tampuurin kantaan ikuisesti, mutta asukkaan tiedot ovat eri toiminnon alla, kuin esimerkiksi mistä asunnon vikailmoitushistorian voi nähdä.

4.4 Varoitukset

Jos asukas saa syystä tai toisesta kirjallisen varoituksen, annetaan asukkaalle ensin postitse huomautuskirje. Huomautuskirjeen kopio säilytetään palvelimella salatussa tiedostossa AES salausstandardin mukaisesti, johon käyttöoikeus on vuokravalvojalla ja isännöitsijällä. Varsinaisen varoituksen toimittaa asukkaalle haastemies. Kopio varoituksesta säilytetään palvelimella salatussa tiedostossa AES salausstandardin mukaisesti. Varsinainen varoitus sisältää asukkaan henkilötietoja. Mikäli varoitus on johtanut oikeudellisiin toimenpiteisiin niin varoitusta tulee säilyttää yhtä kauan kuin vuokrasopimusta. Kirjallista varoitusta säilytetään niin kauan kuin on saatavia.

> AES (Advanced Encryption Standard) on Rijndael-salaukseen perustuva salausstandardi, jota käytetään laajalti eri ohjelmistojen, verkkoliikenteen, henkilötietojen ja organisaatioiden IT-infrastruktuurin suojelemiseen. AES on symmetrinen lohkosalausmenetelmä, joka salaa ja purkaa tiedon useiden kierroksien läpi *(*Tietojen salaaminen.)

Kaikkien edellä mainittujen asukkaan sopimusaikaisten asioiden GDPR:n mukainen käsittely on yrityksessä otettu hyvin huomioon ja asiaan ei ole tarvetta tehdä muutosta.

4.5 Tietotilinpäätös

Tietotilinpäätös on yrityksen sisäinen dokumentti, jonka tarkoitus on toimia johdon työkaluna ja tukea tehokkuutta. Tietotilinpäätöksen avulla yritys pystyy näyttämään sen, että yrityksessä on ymmärretty tietosuoja-asetus. Tällä pystytään varmistamaan yrityksen oikea tietojenkäsittely sekä tiedonhallintatapa. Yritykseen ei ole välttämätöntä tehdä tietotilinpäätöstä, mutta se on suositeltavaa GDPR:n vähimmäisasetuksen noudattamiseksi. Yritys pysyy tietotilinpäätöksellä paremmin ajan tasalla tietosuojaa koskevien asioiden suhteen. (Mestariasunnot Oy 2018.) Tässä seuraavia esimerkkejä, mihin tietotilinpäätös vastaa:

- Mitä henkilötietoja käsitellään?
- Mihin olemassa olevia tietoja käytetään?
- Millä tavoilla ja periaatteilla noudatetaan tietojenkäsittelyä?
- Kuinka henkilötiedot on suojattu?
- Miten valvotaan tietojen käyttöä?
- Miten toteutetaan rekisteröityjen oikeudet?

Kuva 3. Yrityksen sisäisiä dokumentteja

Kuvassa on yrityksen sisäiseen käyttöön tarkoitettuja dokumentteja tietotilinpäätöksistä, yleistä ohjeistusta tietosuoja-asetuksesta ja tietoturvaan liittyvää aineistoa.

Tietotilinpäätös on huomioitu asetuksen mukaisesti, viitaten kohtaan 3.5 tietotilinpäätös teoriaosuuteen. Tietotilinpäätös on yrityskohtainen dokumentti.

4.6 Tietosuojaorganisaatio

Tietosuojan valvonnan tehostamiseksi yrityksen on hyvä muodostaa yrityksen omista henkilöistä tietosuojaorganisaatio tai tietosuojavaltuutettu. Siihen voi kuulua yksi tai useampi henkilö riippuen siitä, kuinka paljon työpisteitä yrityksessä on. Yrityksessä olevien henkilön tai henkilöiden kuuluisi olla selvillä nykyisen tietosuojan tasosta. Tietosuojavastaava voidaan valita eri yksiköistä, kuului se sitten It-yksikköön, asiakaspalveluun, henkilöstöhallintoon, palvelutuotantoon tai johonkin muuhun yksikköön. Tietosuojaorganisaation tavoitteena on varmistaa turvallinen tietosuojatyö, joka kuuluu operatiiviseen toimintaan yrityksessä. (Mestariasunnot Oy 2018.)

Viitaten tietosuojaorganisaatio -kohtaan yrityksessä, toimitaan asetuksen mukaisesti samalla tavalla, säädökset käytäntöineen ovat asianmukaisesti huomioitu ja toteutettu. Toimintaan ei ole syytä tehdä muutoksia. Yrityksestä löytyy tietosuojavaltuutettu.

5 Pohdinta

Järvenpään Mestariasunnot Oy:ssä uusi GDPR tietosuoja-asetus on omaksuttu hyvin ja asiat on järjestetty niin, että tämän työn osalta ei korjausehdotuksia yrityksen käytäntöihin tarvinnut tehdä. Työssä käytiin läpi aiheeseen liittyvät yrityksen tietoturvallisuusasiat dokumenteista, joita projektiin annettiin. Tutkimuksen kannalta erityisen tärkeää informaatiota saatiin lisäksi yrityksen tietoturva-asioista vastaavien henkilöiden haastatteluista.

Lähtökohtana tietoturva-asioihin on se, että yrityksellä on varmenteet kaikista asukkaiden henkilötiedoista omalla palvelimellaan, missä tiedot myös pysyvät tallessa. Näihin käytettävät ohjelmistot ovat sijoitettu pilvipalveluun.

Tietotilinpäätöksestä taas kävi ilmi se, että toiminta on ollut asetusten mukaista sekä tietojenkäsittelyn että tiedonhallinnan suhteen. Kaikissa yrityksen dokumenteissa, joita peilattiin tässä työssä GDPR -tietosuoja asetukseen, selvisi, että seuranta ja valvonta ovat niin ikään nykyisen lainsäädännön mukaisia. Tietotilinpäätöksistä oli tehty monta eri dokumentaatiota muun muassa henkilöstöhallinnolle, huollolle, kehityssuunnitelmalle sekä sopimushallinnalle yleisen tietotilipäätöksen lisäksi. Myös määräykset sekä sisäiset ohjeistukset olivat yrityksessä tältä osin kunnossa.

Henkilöhaastatteluissa ilmeni asiakkaiden tietojen säilytyskäytännöt kirjanpitolain mukaisiksi siten, että nämä säilytetään lukitussa huoneessa lukitussa kaapissa, kuten jo tämän työn tutkimusosiossa on mainittu. Näin on varmistettu henkilötietojen olevan myös fyysisesti oikeanlaisesti suojassa. Haastatteluissa läpikäytiin myös osittain niiden aiheeseen liittyvien dokumenttien sisältöä, joita yritykseltä saatiin tätä työtä varten. Haastatteluissa moni dokumenteissa ilmennyt asia selvisi ja auttoi ymmärtämään asetusten tekstejä paremmin, jolloin yrityksen käytäntöjen peilaus GDPR –asetukseen tuli helpommaksi.

Kaiken kaikkiaan tämän tutkimuksen perusteella kävi yksiselitteisen selväksi se, että GDPR tietosuoja-asetuksen säädökset käytäntöineen ovat asianmukaisesti huomioitu ja toteutettu Järvenpään Mestariasunnot Oy:ssä.

Lopuksi mainittakoon, että yrityksessä on myös nimetty tietosuojavastaava. Pienemmissä yrityksissä tietosuojavastaava ei ole välttämätön, mutta Järvenpään Mestariasunnot Oy:ssä on tämän asian tärkeys tiedostettu ja siihen on panostettu myös tältä osin.

Lähteet

Arkaluontoinen henkilötieto 2018. Luettavissa: https://www.tsk.fi/tsk/termitalkoot/fi/hakemistot-267.html?page=get_id&id=ID534&vocabulary_code=TSKTT. Luettu 19.9.2019.

Asiaa tietoturvasta. Järvenpään Mestariasunnot Oy 11/2018. Yrityksen tietoturvapaketti. Luettu 2.5.2019

EU:N Tietosuoja-asetus – sanasto. 2016. Luettavissa: https://gdpr.fi/sanasto/. Luettu: 15.3.2019

Euroopan parlamentin ja neuvoston asetus EU 2016/679. Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Luettavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504. Luettu: 24.10.2019.

EU:n uusi tietosuoja- asetus koskettaa lähes jokaista yritystä ja yhdistystä. Luettavissa: https://www.tietosuoja-asetus.org/. Luettu: 26.3.2019.

Finlex. Arkistonmuodostussuunnitelma. Luettavissa: https://www.finlex.fi › data › normit › arkmliit. Luettu: 6.6.2019

GDPR tulee, oletko valmis? Luettavissa: https://www.sovellin.com/gdpr-tulee-oletko-valmis/. Luettu: 25.3.2019.

Henkilötietojen käsittelyä koskevat periaatteet 2019. Luku 2, artikla 5. Luettavissa: https://tietosuojatyokalu.fi/aihealueet/periaatteet/henkilotietojen-kasittelya-koskevat-periaatteet/. Luettu: 7.5.2019.

Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaisille 2019. Luku 4, artikla 33. Luettavissa: https://tietosuojatyokalu.fi/aihealueet/rekisterinpitaja-

ja-henkilotietojen-kasittelija/henkilotietojen-tietoturvaloukkauksesta-ilmoittaminen-valvontaviranomaiselle/. Luettu: 15.4.2019.

Laadi tietotilinpäätös 24.4.2012 Luettavissa: https://tietosuoja.fi/documents/6927448/10594424/Laadi+tietotilinp%C3%A4%C3%A4t%C3%B6s.pdf/4925bd9e-d07d-82fc-3f2d-71c5955310a0/Laadi+tietotilinp%C3%A4%C3%A4t%C3%B6s.pdf. Luettu 16.11.2019

Laakso, M. 2010. Fyysinen tietoturva. Luettavissa: https://tietojesiturvaksi.fi/tietoturvasuunnitelma/fyysisessa-tietoturvassa-huomioitavaa. Luettu: 26.4.2019.

Leivonen, R. 2015. Mitä rekisteriviranomaisen pitää ottaa huomioon henkilötietoja luovuttaessaan? Luettavissa: http://stat.fi/tup/mikroaineistot/leivonen_esitys.pdf. Luettu: 12.10.2019.

Läpinäkyvä informointi, viestintä ja yksityiskohtaiset säännöt rekisteröidyn oikeuksien käyttöä varten 2019. Luku 3, artikla 12. Luettavissa: https://tietosuojatyokalu.fi/aihealueet/rekisteroidyn-oikeudet/lapinakyva-informointi-viestinta-ja-yksityiskohtaiset-saannot-rekisteroidyn-oikeuksien-kayttoa-varten/. Luettu: 29.4.2019.

Mertaniemi 2018 8 vinkkiä, joilla yrityksesi voi valmistautua yleiseen tietosuoja-asetukseen (GDPR) Luettavissa: https://www.visma.fi/blog/8-vinkkia-joilla-yrityksesi-voi-valmistautua-yleiseen-tietosuoja-asetukseen-gdpr. Luettu: 15.3.2019.

Mestariasunnot 2018. Tietotilinpäätös. Luettu: 2.5.2019

Miten vastata EU:n yleisen tietoja-asetuksen (GDPR) vaatimuksiin 2019. Luettavissa: https://ahertava.fi/tietosuoja/blogi/miten-vastata-eun-yleisen-tietosuoja-asetuksen-vaatimuksiin/. Luettu: 22.4.3019.

Oikeus oikaista tietoa. Luettavissa: https://tietosuoja.fi/oikeus-oikaista-tietoja. Luettu: 28.3.2019.

Oikeus siirtää tiedot järjestelmästä toiseen 2019. Luku 3, artikla 20. Luettavissa: https://tietosuojatyokalu.fi/aihealueet/rekisteroidyn-oikeudet/oikeus-siirtaa-tiedot-jarjestelmasta-toiseen/. Luettu: 5.4.2019.

Oikeus tietojen oikaisemiseen 2019. Luku 3 /artikla 16. Luettavissa: https://tietosuojatyokalu.fi/aihealueet/rekisteroidyn-oikeudet/oikeus-tietojen-oikaisemiseen/.Luettu: 2.4.2019.

Oikeus tietojen poistamiseen 2019. Luku 3, Artikla 17. Luettavissa: https://tietosuojatyokalu.fi/aihealueet/rekisteroidyn-oikeudet/oikeus-tietojen-poistamiseen/. Luettu: 7.4.2019.

Pietikäinen, S. 2016. Rekisterinpitäjän velvollisuudet. Kohta 5.4.3, kuva 5. Luettavissa: https://www.vahtiohje.fi/web/guest/rekisterinpitajan-velvollisuudet. Luettu: 23.5.2019.

Pseudonynamisoidut ja anonymisoidut tiedot 2014. Luettavissa https://tietosuoja.fi/pseudonymisointi-anonymisointi. Luettu 5.5.2019.

Raklin ohje Luettavissa: https://www.rakli.fi/media/asuminen/vuokrauksen-tietosuojaohje.pdf Luettu 15.11.2019

Rekisterinpitäjän velvollisuudet kohta 2016. Kohdat: 5.0-5.3, 5.5. Luettavissa: https://www.vahtiohje.fi/web/guest/rekisterinpitajan-velvollisuudet.Luettu: 10.4.2019.

Seloste käsittelytoimista 2019. Luku 4, artikla 30. Luettavissa: https://tietosuojatyokalu.fi/aihealueet/rekisterinpitaja-ja-henkilotietojen-kasittelija/seloste-kasittelytoimista/. Luettu: 16.4.2019.

Suostumuksen edellytykset 2019. Luku 2, artikla 7. Luettavissa: https://tietosuojatyokalu.fi/aihealueet/periaatteet/suostumuksen-edellytykset/. Luettu 6.5.2019.

Tietojen salaaminen luettavissa: https://www.yksityisyydensuoja.fi/tietojen-salaaminen Luettu 19.11.2019

Tietosuoja 2019. Luettavissa: https://www.secrays.com/tietosuoja/?gclid=EAIaIQobChMIgZ2T0-6N4QIVB6maCh0sTgDKEAAYAiAAEgL9ufD_BwE. Luettu: 4.4.2019.

Tietosuoja-arviointi. Luettavissa: https://privaon.fi/julkaisut/tietosuoja-arviointi/. Luettu: 25.9.2019.

Tietosuojavastaavat. Luettavissa: https://tietosuoja.fi/tietosuojavastaavat. Luettu: 25.4.2019.

Tietosuojavastaavan nimittäminen 2019. Luku 4, artikla 37. Luettavissa: https://tietosuojatyokalu.fi/aihealueet/rekisterinpitaja-ja-henkilotietojen-kasittelija/tietosuojavastaavan-nimittaminen/. Luettu: 17.4.2019.

Tietosuojavastaavia koskevat ohjeet 2017. Kohta 3.4 ja 4.0. Luettavissa: https://tietosuoja.fi/documents/6927448/8316711/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf/3aad84e5-bb59-4e64-bdaf-adc1e5f2d719/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf.pdf. Luettu: 19.4.2019.

Tietosuojavaltuutetun toimisto luettavissa: https://tietosuoja.fi/kasittelyperusteet luettu 10.11.2019

Tietosuojavastaavan tehtävät 2019. Luku 4, artikla 39. Luettavissa: https://tietosuojatyokalu.fi/aihealueet/rekisterinpitaja-ja-henkilotietojen-kasittelija/tietosuojavastaavan-tehtavat/. Luettu: 2.5.2019.

Vastustamisoikeus 2019. Luku 3, artikla 21. Luettavissa: https://tietosuojatyokalu.fi/aihealueet/rekisteroidyn-oikeudet/vastustamisoikeus/. Luettu: 5.4.2019.

Liitteet

Säilytysajat Asunnon vuokrauksessa sekä hakemukset ja vuokrasopimukset (GDPR)

Asia	kuvaus	Säilytys aika	Peruste	Muu
Asuntohakemus	Johtaa sopimukseen	Säilytetään sopimuksen liitteenä	Raklin ohje: tietosuojalainsäädänön ja erityislakien vaikutus tietojen keräämiseen, säilyttämiseen jne.	
Asuntohakemus Ara	Joka ei johtanut sopimukseen liitteineen	5 vuotta Mikäli kunta on osallistunut asukasvalintaan, päätös liitteineen säilytettävä 10 vuotta	Aran opas arava- ja korkotukivuokra-asuntojen asukasvalintoihin 2018	Mikäli kunta on osallistunut asukasvalintaan, päätös liitteineen sälytettävä 10 vuotta
Asuntohakemus Markkina/vapaarahoitteinen	Joka ei johtanut sopimukseen liitteineen	Jos hakemus sis. ainoastaan vapaarahoitteisen kohteen asuntoja. 2 vuotta viimeisestä aktivointi/muokkaus-ajankohdasta		
Vuokrasopimus, päättynyt ilman epäselvyyksiä esim. riita, häätö, perintä yms.	Vuokralainen muuttaa pois JMA:n omistamasta asunnosta.	6 vuotta vuokrasopimuksen päättymisen jälkeen.	Kirjanpitolautakunnan Yleisohje kirjanpidon menetelmistä ja aineistoista 1.2.2011. Tositteet tulee säilyttää **vähintään** 6 vuotta. Vuokrasopimus on tositteen peruste. Verottaja voi vaatia selvityksiä 5 vuoden ajan ja asukas (vuokranalennusvaatimus) 3 vuotta.	Huom. Päättyneiden sopimusten osalta tulee käyttöoikeuksia rajata siten, että ainoastaan tietyissä rooleissa olevat henkilöt näkevät sopimustiedot

Asia	kuvaus	Säilytys aika	Peruste	Muu
Vuokrasopimus, päättynyt ilman epäselvyyksiä esim. riita, häätö, perintä yms	Vuokralainen muuttaa toiseen Jma:an asuntoon	6 vuotta vuokrasopimuksen päättymisen jälkeen. Jos asiakassuhde jatkuu Jma:n kanssa, voidaan 6 vuoden jälkeen säilyttää seuraavat tiedot päättyneeltä vuokrasopimukselta: sopimuksen kesto, asunnon osoite ja pää- ja kanssavuokralaisen nimi	Asiakassuhteen hoitaminen	Huom. Päättyneiden sopimusten osalta tulee käyttöoikeuksia rajata siten, että ainoastaan tietyissä rooleissa olevat henkilöt näkevät sopimustiedot
Vuokrasopimus, päättynyt ilman epäselvyyksiä esim. riita, häätö, perintä yms	Yhteisellä vuokrasopimuksella Jmalla asuvat henkilöt muuttavat erilleen. Kuitenkin niin että toinen jää asumaan 1. yhteisellä sopimuksella olevaan asuntoon ja toinen muuttaa toiseen Jma:n asuntoon- > molemmat pysyvät Jma:n asiakkaina	6 vuotta vuokrasopimuksen päättymisen jälkeen. Jos asiakassuhde jatkuu Jma:n kanssa voidaan 6 vuoden jälkeen säilyttää seuraavat tiedot päättyneeltä vuokrasopimukselta: sopimuksen kesto, asunnon osoite ja pää- ja kanssavuokralaisen nimi.	Asiakassuhde jatkuu ja Jma seuraa asiakassuhteen kestoa. Lisäksi kyse on 1. sopimuksen osalta sopimusmuutoksesta.	Muut asiakkaaseen liittyvät henkilötiedot, jotka eivät liity asiakkuusajan todentamiseen tulee 6 vuoden jälkeen poistaa. Huom. Päättyneiden sopimusten osalta tulee käyttöoikeuksia rajata siten, että ainoastaan tietyissä rooleissa olevat henkilöt näkevät sopimustiedot
Vuokrasopimus päättynyt epäselvyyksien kanssa esim. vuokravelka, muu riita-asia yms.	Kaikki edellä mainitut tapaukset 1-3.	Säilytysaika 6 vuotta siitä kunnes asia loppukäsitelty asiakkaan ja Jma:n välillä eikä kummallakaan ole enää vaatimuksia tai velvoitteita toista osapuolta kohtaan.	Asia kesken, voidaan tarvita esim. oikeusprosessissa	Huom. Päättyneiden sopimusten osalta tulee käyttöoikeuksia rajata siten, että ainoastaan tietyissä rooleissa olevat henkilöt näkevät sopimustiedot