Tiina Oikari

Tietosuoja ja -turva tilitoimistossa

Case Tilitoimisto X Oy

Opinnäytetyö
Syksy 2019
SeAMK Liiketoiminta ja kulttuuri
Tradenomi (AMK, Liiketalous)

SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Koulutusyksikkö: SeAMK Liiketoiminta ja kulttuuri

Tutkinto-ohjelma: Liiketalouden koulutusohjelma

Tekijä: Tiina Oikari

Työn nimi: Tietosuoja ja -turva tilitoimistossa, Case Tilitoimisto X Oy

Ohjaaja: Tuulia Potka-Soininen

Vuosi: 2019 Sivumäärä: 61 Liitteiden lukumäärä: 7

Tietosuoja ja -turva on keskeinen asia ottaen huomioon hiljan voimaantulleen EU:n yleisen tietosuoja-asetuksen sekä Suomen tietosuojalain. Näiden merkitys tänä päivänä on erittäin tärkeä, kun otetaan huomioon jatkuva digitalisaation ja teknologian kehitys. Henkilötietojen oikeaan ja perusteltuun käsittelyyn on perehdytty uudistuneessa tietosuoja-asetuksessa enemmän sekä panostettu siihen, että ihmisten yksityisyys olisi turvattuna yhä paremmin.

Opinnäytetyön tavoitteena on perehtyä uudistuneeseen tietosuojaan keskittyen tarkastelemaan sitä tilitoimiston näkökulmasta. Työn teoreettisen osan aluksi perehdytään tietosuojaan ja sen keskeisimpiin käsitteisiin. Työ käsittelee muun muassa sen, mitä henkilötieto, rekisteröity, rekisterinpitäjä, tietosuojavastaava, osoitusvelvollisuus, salassapitovelvollisuus ja työntekijän yksityisyys tarkoittavat ja mitä nämä käsitteet sisältävät. Opinnäytetyö perustuu tietosuojalakiin ja EU:n yleiseen tietosuoja-asetukseen. Tietoturvaa käsitellään pääasiassa toimenpidealueiden kautta. Opinnäytetyö sisältää myös isännöintiin liittyvää tietosuojaa sekä käy läpi oleellisimmat henkilötietorekisterit tilitoimiston näkökulmasta.

Opinnäytetyön tarkoitus on myös kartoittaa Tilitoimisto X Oy:n tietosuojan ja -turvan tasoa uuden asetuksen voimaantulon jälkeen. Tämän laadullisen tapaustutkimuksen jälkeen työssä pohditaan niitä keskeisimpiä kohtia, joissa tilitoimiston tulee tehdä toimenpiteitä saavuttaakseen EU:n yleisen tietosuoja-asetuksen vaatimukset. Työ esittää toimenpide-ehdotuksia tietosuojan saattamiseksi vaaditulle tasolle.

Opinnäytetyön tapaustutkimus suoritettiin käyttämällä kyselyä. Tämän kyselyn kohteena oli Tilitoimisto X Oy:n yrittäjä. Kysely toteutettiin niin, että yrittäjä sai tarpeeksi aikaa miettiä ja pohtia vastauksiaan. Näin voidaan taata tarkempi ja yksityiskohtaisempi tulos.

Opinnäytetyö osoitti, että aihe on erittäin laaja ja vaatii paljon aikaa sen tutkimiseen ja sisäistämiseen. On olennaista osata erotella keskeisimmät asiat. Aihe on tärkeä ja erittäin ajankohtainen myös muiden tilitoimistojen ja yritysten kannalta.

Avainsanat: tietosuoja, tietoturva, EU:n yleinen tietosuoja-asetus, tietosuojalaki

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Faculty: SeAMK Business and Culture

Degree programme: Business Administration

Author: Tiina Oikari

Title of thesis: Privacy and security at the account office, Case Accounting Firm X Oy

Supervisor: Tuulia Potka-Soininen

Year: 2019 Number of pages: 61 Number of appendices: 7

Data protection and security is a key issue, given the recent entry into force of the EU General Data Protection Regulation and the Finnish Data Protection Act. They are today extremely important because of the ongoing digitalisation and technological advances. The reform of the Data Protection Regulation has focused more on the correct and justified processing of personal data and has put greater emphasis on the better protection of individuals' privacy.

The aim of this thesis is to study the renewed privacy by focusing on it from an accounting firm's perspective. The theoretical part of the thesis begins with a focus on data protection and its key concepts. This work covers, among other things, the meaning of the concepts of personal information, registered, registrar, data protection officer, duty of care, confidentiality, and employee privacy. The thesis is based on the Data Protection Act and the EU General Data Protection Regulation. Security is mainly dealt with through policy areas. The thesis also includes data protection related to hosting and reviews the most relevant personal data registers from the accounting firm's point of view.

Another aim of this thesis is to survey the level of data protection and security of Accounting firm X Oy after the entry into force of the new regulation. Following this qualitative case study, the work considers the key points where the accounting firm must take steps to meet the requirements of the EU General Data Protection Regulation. The thesis presents proposals for measures to bring the accounting firm’s level of data protection to the required level.

The thesis case study was conducted using a survey. This survey was conducted by interviewing the entrepreneur of Accounting Firm X. The respondent was given enough time to think and ponder their answers. This gives a more accurate and detailed result. The thesis showed that the topic is very broad and requires a lot of time to research and internalize. This topic is also important and very topical for other accounting firms and companies.

Keywords: Data protection, security, EU General Data Protection Regulation, Data Protection Act

SISÄLTÖ

Kuva-, kuvio- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

Rekisterinpitäjä Yritys tai taho, joka ylläpitää rekistereitä sekä määrittää tarkoitukset ja keinot henkilötietojen käsittelyyn.

Henkilötietojen käsittelijä

Ulkopuolinen taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Rekisteröity Henkilö, jonka henkilötietoja käsitellään.

GDPR General Data Protection Regulation eli yleinen tietosuoja-asetus

Osoitusvelvollisuus Rekisterinpitäjän on osoitettava noudattavansa EU:n yleisen tietosuoja-asetusta esimerkiksi asiakirjoin ja toimenpitein

Oletusarvoinen ja sisäänrakennettu tietosuoja

Teknisiä ja organisatorisia toimenpiteitä käsittelytoimenpiteiden suunnittelun alkuvaiheessa, jotta yksityisyyttä ja tietosuojaperiaatteita voidaan suojella alusta saakka. On varmistettava, että henkilötiedot käsitellään korkea yksityisyydensuoja varmistaen. Henkilötiedot eivät saa olla oletusarvoisesti rajoittamattomien henkilöiden käytössä.

1 JOHDANTO

1.1 Työn tarkoitus

Tämän opinnäytetyön tarkoituksena on selvittää muuttuneen tietosuojan keskeiset asiat ja vaatimukset, joiden perusteella yritysten ja yhteisöjen täytyy kehittää omaa tietosuojaansa. Voimaan astuneiden EU:n direktiivien ja muuttuneen tietosuojalain nojalla tämän opinnäytetyön aihe liittyy taloushallintoon ja erityisesti koskee tilitoimistoja, jotka ylläpitävät asiakasrekisteriä ja muita henkilötietoja sekä haluavat saattaa tietosuojansa vastaamaan näitä EU:n direktiivejä ja muuttunutta tietosuojalakia.

Tämän opinnäytetyö tutkii tietosuojaan ja -turvaan liittyviä asioita ja kehittää tietojen perusteella Tilitoimisto X Oy:tä ja tilitoimiston toimintaa tällä saralla. Opinnäytetyö käsittelee asiaa lähtökohtaisesti tietosuojapainotteisesti, mutta ottaa huomioon myös tietoturvan ja siihen liittyvät seikat. Yhtenä kokonaisuutena työssä on huomioitu isännöinnin merkitys tietosuojaa koskevissa asioissa, koska isännöinti kattaa monta tärkeää henkilörekisteriä, jotka täytyy huomioida. Tietosuojaa on myös käsitelty palkanlaskennan, kirjanpidon ja laskutuksen osalta. Opinnäytetyön sisältö on kartoitettu tilitoimiston näkökulmasta, eikä sisällä mahdollisia muita yleisesti tietosuojaan ja -turvaan liittyviä asioita.

Tämä opinnäytetyö saattaa lukijan ajan tasalle tietosuojaan liittyvissä asioissa yleisellä tasolla sekä syventyen kaikkine termeineen juuri taloushallinnon osalta aiheeseen. Työssä on pyritty esittelemään asiat niin, jotta lukija ymmärtää käsitellyt asiat voidakseen käyttää tietoa omiin tarpeisiinsa.

1.2 Tapaustutkimuksen kohde

Opinnäytetyö on tapaustutkimus. Tapaustutkimuksen kohteena on Tilitoimisto X Oy. Tilitoimisto X Oy tarjoaa erilaisia palveluja, kuten kirjanpitoa, palkanlaskentaa, laskutusta, isännöintiä ja muita tilitoimistopalveluja.

Tilitoimiston toimitiloissa säilytetään myös kaikki asiakkaiden aineistot ja henkilötietoja sisältävät asiakirjat. Asiakkaita on sekä liikekirjanpidon puolella, että myös isännöinnin puolella. Tilitoimiston toiminta jakautuu melko tasaisesti kummallekin toiminta-alueelle.

Tällä tutkimuksella on tärkeä merkitys kyseiselle tilitoimistolle, koska heillä hoidetaan myös taloyhtiöiden ja kiinteistöosakeyhtiöiden asioita. Taloyhtiön asiat yleensäkin sisältävät paljon henkilötietoja ja niiden käsittelyä erilaisissa tilanteissa henkilötietojen käsittelijän roolissa eri ihmisten ja tahojen kanssa. On siis oleellista ottaa asioista selvää, jotta tilitoimistolla on hyvät valmiudet jatkossakin kehittää toimintaansa ja parantaa tietosuojaansa ja -turvaansa.

1.3 Tutkimusongelman rajaus

Kehityshankkeessa keskitytään teorian tutkimiseen. Tutkimuksen pohjalta osataan määrittää ne kehityskohteet, joiden avulla kyseinen tilitoimisto saa valmiudet kehittää omaa tietosuojaansa ja -turvaansa. Viitekehyksessä käydään läpi tietosuojaa yleisesti sekä perehdytään keskeisimpiin käsitteisiin ja asioihin. Tässä työssä perehdytään tietosuojaan enemmän ottaen huomioon henkilötietojen laajuus ja merkitys nykypäivänä sekä ajankohtaisuus.

Työ sisältää haastattelun, joka on suunnattu Tilitoimisto X Oy:n yrittäjälle. Näin kartoitetaan, minkälainen tietosuojan ja -turvan taso tilitoimistossa tällä hetkellä vallitsee ja nähdään, mitkä asiat nousevat päällimmäisenä tarkastelun kohteeksi. Lisäksi tutustutaan tilitoimiston sen hetkiseen tilanteeseen tarkastelemalla itse paikan päällä tapoja, joilla työntekijät hoitavat päivittäisiä töitään sekä tutustumalla toimitiloihin.

Kun teoria ja lähtötilanne on selvitetty, suunnitellaan erilaisia toimenpiteitä ja kehitysmalleja kyseiselle tilitoimistolle, mutta itse toteutukseen ei tässä opinnäytetyössä osallistuta. Tutkimuksella pyritään löytämään myös valmiita asiakirjamalleja liittyen tietosuojaan ja -turvaan.

Opinnäytetyön sisältö on tutkittu yleisellä tasolla tilitoimiston tietosuojaa ja -turvaa koskien. Osa tutkimuksen aikana ilmenneistä tiedoista säilytetään salaisena. Perusteluna menettelylle on tilitoimiston nimettömänä pysyminen ja liiallinen tietojen yksilöinti tilitoimiston oman tietosuojan parantamiseksi.

1.4 Aineisto

Opinnäytetyössä on käytetty keskeistä alan aineistoa. Teoria perustuu kirjoihin, julkaisuihin, lakiin ja EU:n direktiiveihin sekä aiempiin tutkimuksiin ja selvitystöihin.

Tapaustutkimus pohjautuu Tilitoimisto X Oy:n tilanteeseen koskien tietosuojaa ja -turvaa. Tutkimus perehtyy nykyisin käytössä oleviin toimenpiteisiin ja tapoihin suojata asiakkaidensa ja henkilökuntansa henkilötietoja. Tapauksen lähtökohdat selvitetään konkreettisesti tilitoimistossa sekä kyselyn muodossa, jonka jälkeen teorian pohjalta suunnitellaan mahdollisia erilaisia toimenpiteitä.

Opinnäytetyössä käytetyssä aineistossa esitellään kattavasti tietosuojaan, tietoturvaan, lainsäädäntöön, isännöintiin, taloyhtiön asioihin ja muihin keskeisiin asioihin liittyvää tietoa. Vuonna 2018 voimaantulleen tietosuoja-asetuksen jälkeen on tehty tutkimuksia koskien tietosuojalakia ja EU:n yleistä tietosuoja-asetusta. Tarkasteltaessa aikaisempia tutkimuksia ja töitä huomattiin, että aiheet keskittyvät tiettyihin näkökulmiin ja aloihin, kuten sosiaali- ja terveysalaan. Muiden alojen, kuin taloushallinnon, aiemmat tutkimukset on rajattu pois tehdessä opinnäytetyön pohjatyötä.

Opinnäytetyössään Katajamäki ja Vainionpää (2019) käsittelivät lähinnä GDPR:n vaikutusta tilitoimistoihin. Opinnäytetyö perustui kyselytutkimukseen ja käsitteli pitkälti EU:n tietosuoja-asetuksen käyttöönottoa ja asetuksen sisäistämistä tilitoimistoissa. Työssä selvitettiin, millaisia toimenpiteitä ja dokumentointivaatimuksia asetus tuo tilitoimistoille sekä kartoittivat työssään, kuinka tilitoimistot olivat kokeneet ja valmistautuneet asetuksen tuomiin muutoksiin. Työssään Katajamäki ja Vainionpää tarkastelivat roolituksia, henkilötietojen käsittelyä, käytännön eri toimia ja henkilöstöhallinnon roolia ja perehdytystä asetuksen kautta. Työn kyselytutkimus oli kohdistettu suomalaisille ja ulkomailla toimiville suomalaisille tilitoimistoille.

Muun muassa Niemi (2018) käsitteli opinnäytetyössään EU:n tietosuoja-asetusta ja sen muutosten vaikutusta case-yrityksessään. Niemi (2018) käsitteli työssään henkilötietojen käsittelyyn ja rekisteröidyn oikeuksiin liittyviä asioita sekä käsitteli sanktioita ja valvontaa. Rantanen (2018) tutki myös EU:n tietosuoja-asetuksen muutoksia tilitoimistossa, mutta myös pyrki työllään helpottamaan pienten tilitoimistojen selviytymistä vaadituista tietosuojatoimenpiteistä. Tutkimuksen avulla Rantanen (2018) pystyi arvioimaan tilitoimistojen halua ja resursseja laatia tietosuojaselosteita sekä turvata oma tietosuojataso. Tilitoimiston tietosuojaan keskittyivät case-yrityksen kautta myös Vehmanen (2019) ja Hulkkonen (2018). Myös Ohtonen (2018) avasi työssään henkilötietojen käsittelyyn liittyviä asioita, joihin GDPR vaikuttaa.

Larko (2018) käsitteli opinnäytetyössään yleisen tietosuoja-asetuksen vaikutuksia isännöinti- ja kiinteistöhoitoyrityksen näkökulmasta. Opinnäytetyö keskittyi case-yritykseen. Työssä oli lähtökohtaisesti perehdytty case-yrityksen henkilötietojen käsittelyyn ja rekisterien ylläpitoon. Klemetti (2019) toi opinnäytetyössään esille tietosuojaa palkanlaskennan näkökulmasta. Hän tutki työssään, miten henkilötietojen käsittely muuttuu palkanlaskennassa. Tutkimus oli suoritettu sähköpostikyselynä palkkahallinnossa työskenteleville henkilöille. Klemetin (2019) mukaan selvisi, että suurin osa yrityksistä oli kouluttanut henkilöstönsä tietosuoja-asetusten mukaan. Tuloksista voitiin päätellä, että tietosuoja-asetuksen voimaantultua monen yrityksen tietosuoja oli parantunut.

Aiempien tutkimusten perusteella voidaan todeta, että tutkimuksia, joissa oltaisiin kartoitettu tietosuojaa ja -turvaa lähtökohtana tilitoimisto ja sen eri osa-alueet, ei olla tehty. Tämä opinnäytetyö käsittelee asiaa eri näkökulmasta kuin aiemmat tutkimukset. Tässä työssä huomioidaan muun muassa kirjanpito, palkanlaskenta, laskutus ja isännöinti. Koska tämä opinnäytetyö keskittyy myös suurelta osin case-yrityksen tietosuojan ja -turvan kartoittamiseen sekä yrityksen tietosuojan saattamiseksi vaaditulle tasolle, tuo tämä opinnäytetyö lisäarvoa case-yritykselle sekä yleiselle tasolle ollessaan yksi hyvä suunnannäyttäjä aiempien tutkimuksien rinnalla. Aiemmat tutkimukset käsittelevät aihetta yleisesti ottaen samojen näkökulmien ja kantojen kautta, mutta monista töistä jää uupumaan muun muassa isännöinnin näkökulma tietosuojaa ja -turvaa tarkasteltaessa.

2 TIETOSUOJA

2.1 Tietosuojalaki

Ehdotus tietosuojalaista (L 5.12.2018/1050) hyväksyttiin eduskunnassa marraskuussa 2018 ja laki astui voimaan 1.1.2019. Uudella tietosuojalailla kumottiin aikaisemmin käytössä ollut henkilötietolaki (EU 22.4.1999/523) sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta (L 27.5.1994/389).

Tietosuojalain (L 5.12.2018/1050) tarkoitus on täsmentää ja täydentää luonnollisten henkilöiden tietosuojaa käsitellessä henkilötietoja. Laki täsmentää myös tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annettua Euroopan parlamentin ja neuvoston asetusta (EU 27.4.2016/679) ja sen kansallista soveltamista. Lakia (L 5.12.2018/1050) sovelletaan EU:n yleisen tietosuoja-asetuksen 2 artiklan mukaisesti.

EU:n yleinen tietosuoja-asetus (EU 27.4.2016/679) säätää tietosuojaan liittyviä velvoitteita ja määräyksiä. Tietosuojalaki (L 5.12.2018/1050) on kansallisesti säädetty laki, mikä tarkoittaa sitä, että EU:n myöntämän liikkumavaran avulla lakia on voitu muokata ja soveltaa, jotta se huomioi paremmin suomalaista tietosuojaa. Tämän liikkumavaran avulla Suomi on voinut kumota tietosuojalailla entisen henkilötietolain (L 22.4.1999/523).

2.2 EU:n yleinen tietosuoja-asetus

2.2.1 Tavoitteet

Tietosuojalainsäädäntö muuttui merkittävästi uuden EU:n yleisen tietosuoja-asetuksen (EU 27.4.2016/679) astuessa voimaan 24. toukokuuta 2016, kun Euroopan parlamentti ja neuvosto uudistivat asetusta yksilöiden suojelusta henkilötietojen käsittelyssä ja vapaasta liikkuvuudesta. Uutta asetusta alettiin soveltaa vuonna 2016 ja sille annettiin joustava kansallinen siirtymäaika, jonka mukaan 25. toukokuuta 2018

henkilötietojen käsittelyn oli oltava EU:n tietosuoja-asetuksen mukainen. Tämä asetus on suoraan sovellettavaa oikeutta, joka on yleisesti pätevä sekä velvoittava kaikilta osiltaan. Uudistunutta tietosuoja-asetusta tulee soveltaa kaikissa EU:n jäsenvaltioissa ottaen huomioon myönnetyt kansalliset liikkumavarat. (Andreasson, Riikonen & Ylipartanen 2019, 27.)

Aiemmin henkilötietoja käsitellyt *Euroopan parlamentin ja neuvoston direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja tietojen vapaasta liikkuvuudesta* korvattiin EU:n yleisellä tietosuoja-asetuksella (EU 27.4.2016/679). Tämän muutoksen tarkoituksena oli päivittää nykyaikaisemmaksi henkilötietodirektiivin periaatteita, yhtenäistää tietosuojaa koskevia käytäntöjä ja vahvistaa rekisteröityjen itsemääräämisoikeutta kaikissa EU:n jäsenmaissa. Tämän lisäksi vahvistettiin yksilön oikeuksia, lujitettiin sisämarkkinaulottuvuuksia, huomioitiin tietosuojan globaalit ulottuvuudet sekä tehostettiin tietosuojasääntöjen täytäntöönpanoa. Tämä loi EU:lle kattavan, yhtenäisen vahvan ja ennen kaikkea ajanmukaisen tietosuojakehyksen. (Andreasson ym. 2019, 27.)

Andreasson ym. (2019, 27) toteavat, että asetuksen takana ovat kansainväliset ihmisoikeussopimukset ja EU:n perusoikeuskirja, jonka artiklan 7 ja 8 mukaan jokaisella on oikeus viestien, kotinsa sekä perhe-elämänsä kunnioitettavuuteen ja henkilötietojensa suojaan. Tietojen käsittely on siis tehtävä asianomaisen suostumuksella tai laissa säädetyn kohdan perusteella, jotta henkilötiedon käsittely on asianmukaista ja tapahtuu tiettyä tarkoitusta varten. Jokaisella on oikeus saada nähdä hänestä kerätty tieto. Oikeuksien olennaista sisältöä on noudatettava sekä rajoitusten oltava suhteellisuusperiaatteen mukaisia. Artiklan 52 mukaan tunnustettuja perusoikeuksia voidaan rajoittaa ainoastaan lailla. Tarkoitus on siis kunnioittaa rekisteröidyn ja sivullisten oikeuksia sekä vapauksia vastaamalla EU:n tietosuoja-asetuksen asettamia tavoitteita.

2.2.2 Riskeihin perustuva lähestymistapa

Suomessa tietosuojan yleissääntely perustuu kansalliseen lakiin ja EU:n yleiseen tietosuoja-asetukseen (EU 27.4.2016/679). On olemassa myös erityislakeja, jotka säätelevät kansallisesti henkilötietojen käsittelyä. Näistä ovat esimerkkeinä sosiaali-

ja terveydenhuolto, joissa asiakkaiden tietojen arkaluonteisuus on omaa luokkaansa. (Andreasson ym. 2019, 28.)

Kun puhutaan tietosuoja-asetuksen riskeistä, tarkoitetaan henkilötietojen käsittelyssä rekisteröidylle mahdollisesti aiheutuvia aineettomia, aineellisia taikka fyysisiä vahinkoja. Käsittely saattaa johtaa syrjintään, petokseen, taloudellisiin menetyksiin, sosiaaliseen vahinkoon, arkaluonteisten tietojen paljastumiseen sivullisille, pseudonymisoinnin kumoutumiseen taikka identiteettivarkauteen. Lasten ja muiden heikossa asemassa olevien tietoja käsitellessä riski voi olla suurempi. Suurien henkilötietomäärien ja useamman rekisteröidyn tietojen käsittely voi myös johtaa suurentuneeseen riskiin, joka täytyy huomioida. Henkilöprofilointia varten tehty analyysi sekä geneettiset ja terveyteen liittyvät tiedot sisältävät suuren riskin. Henkilötietojen käsittelijä ja rekisterinpitäjä velvoitetaankin vastaamaan EU:n yleistä tietosuoja-asetusta (EU 27.4.2016/679) ja ryhtyvän sen edellyttämiin toimiin. Suuririskisen yrityksen on tehtävä tietosuojaa koskeva vaikutustenarviointi. Yrityksen on tehtävä perusteellinen arvio riskeistä, jotka liittyvät henkilötietoihin, jotta rekisterinpitäjä voi toteuttaa oletusarvoista ja sisäänrakennettua tietosuojaa sekä muita velvoitteita. (Andreasson ym. 2019, 29–30.)

EU:n yleistä tietosuoja-asetusta (EU 27.4.2016/679) voidaan soveltaa manuaaliseen ja automaattiseen henkilötietojen käsittelyyn. Asetuksessa käytetään riskiperusteista lähestymistapaa. Asetuksen asianmukaiset suojatoimet sekä velvoitteet on henkilötietojen käsittelyssä suhteutettava rekisteröidyn vapauksille ja oikeuksille aiheutuvaan riskiin. Tällä halutaan välttää vähäriskisten toimien turhaa ylisääntelyä. Samalla varmistetaan rekisteröidyn suoja toiminnassa, jossa esiintyy suuri riski henkilötietojen väärinkäytölle. Tietojen laajuus, käsittelytarkoitus, luonne ja laatu ovat riskien arvioinnin kohteena. Asiaa voidaan siis tulkita niin, että mitä tunnistettavammassa muodossa tieto on, kuinka yksilöivää se on ja kuinka pitkään tietoa käsitellään, sitä suuremmat siihen liittyvät riskit ovat. Mitä suuremmat riskit ovat, sitä enemmän edellytetään suojakeinoilta ja velvoitteilta. Kun käsitellään korkean riskin tietoja, täytyy Andreasson ym. (2019, 28–29) mukaan arvioida erityinen riskiarvion tekemisen tarpeellisuus, esimerkiksi käsitellessä suuria määriä arkaluonteisia tietoja.

Seuraava kuva avaa kattavasti rekisteröidyn vapauksiin ja oikeuksiin kohdistuvia riskejä. Tarkastelun kohteena on luonne, laajuus, tarkoitukset ja asiayhteys.

Kuva 1. Rekisteröidyn vapauksiin ja oikeuksiin kohdistuva riski (Riskit [10.11.2019]).

Kuten yllä olevasta kuviosta voidaan nähdä, täytyy riskejä huomioida monesta eri näkökulmasta. Rekisterinpitäjän on hyvä tunnistaa jo suunnitteluvaiheessa riskianalyysin avulla ne toimenpiteet, joita on tehtävä hallitakseen riskejä ja turvatakseen asianmukaisen henkilötietojen käsittelyn. Kun riskit rekisteröidyn oikeuksille on tunnistettu, tulee arvioida riskiä ja siitä aiheutuvan haitan todennäköistä toteutumista sekä vakavuutta. (Riskit [10.11.2019].) Seuraavasta kuvasta voi nähdä, miten riskien vakavuutta voidaan arvioida.

Loukkauksen tai haitan vakavuus	Vakava	Matala riski	Korkea riski	Korkea riski
	Tunnistettuja vaikutuksia	Matala riski	Keskimääräinen riski	Korkea riski
	Vähäisiä vaikutuksia	Matala riski	Matala riski	Matala riski
		Kaukainen	Mahdollinen	Hyvin mahdollinen
		Loukkauksen tai haitan todennäköisyys		

Kuva 2. Riskien vakavuus ja todennäköisyys (Riskit [10.11.2019]).

Riskien tunnistaminen korostuu etenkin silloin, kun rekisterinpitäjä määrittää organisatorisia ja teknisiä toimenpiteitä. Toimenpiteillä halutaan varmistaa tietosuojan toteutuminen käsiteltäessä henkilötietoja. Toimenpiteitä voivat olla muun muassa henkilöstölle annetut ohjeet tietosuojaa koskevissa asioissa, käytönvalvonta omavalvonnan kautta, tietojärjestelmien tietoturva, tietojen salaus tai jokin muu suojatoimenpide. (Riskit [10.11.2019].)

Uusi tietosuoja-asetus (EU 27.4.2016/679) perustuu pitkälti tilivelvollisuus-ajatteluun. Ajattelun pohjana käytetään riskilähtöistä suunnittelua sekä kykyä todistaa tehdyt toimenpiteet. EU:n yleinen tietosuoja-asetus (EU 27.4.2016/679) sisältää oletusarvoisen ja sisäänrakennetun tietosuojan. Tietojen käsittelytavat ja prosessit tulee siis kuvata ja määritellä sekä varmistaa, että henkilötietojen käsittelyssä käsitellään vain tarpeelliseksi katsottuja henkilötietoja. Andreasson ym. (2019, 30) toteavat, että rekisterinpitäjän on toteutettava asianmukaiset hallinnolliset ja tekniset tietosuojaperiaatteen mukaiset toimenpiteet tietousoja-asetuksen täytäntöönpanoa varten. Näitä toimenpiteitä voivat olla esimerkiksi ohjeet ja määräykset henkilöstölle, tietojen salaus, tarkastus- ja valvontajärjestelmät tai omavalvonta.

Tietosuoja on otettava huomioon jo toimenpiteiden suunnitteluvaiheessa. Suunnittelu on toteutettava niin, että rekisteröityjen oikeudet ja tietosuoja-asetuksen (EU 27.4.2016/679) noudattaminen toteutuvat. Andreasson ym. (2019, 30–31) muistuttavat, että täytyy ottaa huomioon lainmukaisuus, kohtuullisuus, läpinäkyvyys, käyttötarkoitussidonnaisuus, täsmällisyys, säilytyksen rajoittaminen, eheys sekä tietojen luottamuksellisuus.

2.3 Tietosuoja

Tietosuoja turvaa ihmisten oikeuksia ja vapauksia käsiteltäessä heidän henkilötietoja. Jokaisella on oikeus yksityisyyden suojaan käsiteltäessä henkilötietoja. Tietosuojan tarkoituksen on osoittaa, miten, milloin ja miten rekisteröityjen tietojaan käsitellään. Kun henkilötietoja käsitellään, tulee käsittelyn perustua lakiin. Tätä valvoo riippumaton viranomainen. (Tietosuoja [3.9.2019].)

Riittävällä tietosuojaosaamisella voi lisätä merkittävästi organisaation tehokkuutta ja tuottavuutta sekä karsia kustannuksia. Tähän voi vaikuttaa esimerkiksi osaava henkilöstö, joka toimii toiminta- ja asiakasprosesseissa tehokkaasti sekä myös viihtyy työssään. Tietosuojassa onkin kyse henkilöstön tietosuojaosaamisesta ja asiakkaiden antamasta luottamuksesta. Asiakas luottaa siihen, että hänen tietojensa käsittely hoituu alusta loppuun saakka perustellusti, oikeaoppisesti sekä sujuvasti. Tähän elinkaareen lukeutuu Andreasson ym. (2019, 19) mukaan monia toimintoja, kuten asiakastietojen käsittely, käyttö, säilyttäminen, tallentaminen, kerääminen, hävittäminen, luovuttaminen, siirto ja yhdistäminen.

On tärkeää havaita tietosuoja-ajattelussa tapahtunut muutos. Tietosuoja-ajattelusta on yhä enemmän tulossa strategisen toiminnan keskeinen osa-alue. Tietosuojaa pidetään digitalisaation mahdollistajana. Perusteena on se, että hyvä henkilöstön tietosuojaosaaminen sekä tiedonhallinta mahdollistaisivat onnistumisen myös digimarkkinoilla, Suomessa sekä muualla Euroopassa. (Andreasson ym. 2019, 19–20.)

2.4 Henkilötieto ja niiden käsittely

Henkilötieto sisältää sellaiset tiedot, joilla henkilö voidaan tunnistaa välillisesti tai suoraan yhdistämällä muun muassa yksittäisiä tietoja johonkin toiseen tietoon, joka siten mahdollistaa tunnistamisen. Näitä ovat muun muassa nimi, henkilötunnus tai jokin tunnusomainen tekijä, jonka perusteella voidaan varmentaa henkilöllisyys. (Henkilötieto [5.9.2019].)

Tarkemmin eriteltynä henkilötieto voi olla henkilötunnus, nimi, kotiosoite, henkilökortin numero, puhelinnumero, auton rekisterinumero, sähköpostiosoite, paikannustiedot, IP-osoite, potilastiedot, isovanhempien perinnöllisistä sairauksista saatava tieto tai vaikka lemmikin eläinlääkäritiedot. (Henkilötieto [5.9.2019].)

EU:n yleisen tietosuoja-asetuksen (EU 27.4.2016/679) on tarkoitus suojata henkilötietoja. Niiden käsittelyssä tulee noudattaa tietosuoja-asetusten vaatimuksia, kun tiedot muodostavat rekistereitä. Rekisterinpitäjän pitäisi suojata henkilötietoja riippumatta siitä, millä tavalla tietoja käsitellään tai miten niitä säilytetään. Niin pitkään, kun henkilö voidaan välillisesti tai suoraan tunnistaa tietojen perusteella tai tiedot

voidaan palauttaa tunnistettaviksi tiedoiksi, on henkilötietoja suojattava oikein soveltaen tietosuoja-asetuksia. (Henkilötieto [5.9.2019].)

EU:n yleisen tietosuoja-asetuksen (EU 27.4.2016/679) artiklassa 24–36 säädetään rekisterinpitäjän ja henkilötietojen käsittelijän keskeisimmistä tehtävistä. Kumpaakin koskee vastuu varmistaa suojattavien ja käsiteltyjen henkilötietojen turvallisuustaso ja heidän on ylläpidettävä selostetta henkilötietorekisteristä, josta he ovat vastuussa. Rekisterinpitäjällä on velvollisuus ilmoittaa valvontaviranomaiselle ja rekisteröidylle tietoturvaloukkauksista, kun taas henkilötietojen käsittelijä ilmoittaa loukkauksesta rekisterinpitäjälle. (Andreasson ym. 2019, 32.)

Alihankkijat, kuten pilvipalveluntarjoajat, vastaavat myös sanktioiden uhalla asetusten noudattamisesta, kun he käsittelevät organisaation lukuun henkilötietoja. Tietosuoja-asetus (EU 27.4.2016/679) vaatii tällaisissa tilanteissa kirjalliset sopimukset osapuolien välillä, joissa sopimuksissa jaetaan muun muassa vastuut ja roolit. On huolehdittava, että vastuukysymykset on otettu huomioon sopimuksissa ja että henkilötietojen käsittelyohjeet on laadittu ajatuksella ja asianmukaisesti. Vaikka henkilötietoja ei käsiteltäisi, kannattaa sekin lisätä sopimukseen, jolloin asiaan on kuitenkin kiinnitetty huomiota. (Andreasson ym. 2019, 32–33.)

Henkilötietoja saa kerätä Andreasson ym. (2019, 34) mukaan vain tiettyyn, lailliseen sekä nimenomaiseen tarkoitukseen. Käsittelyperuste on käsite, mikä määrittää sen, mitä saa käsitellä ja miten. Esimerkiksi arkaluontoisten tietojen käsittely on tarkempaa ja ne saavatkin tietosuoja-asetuksen mukaan erityistä suojaa. Tietosuoja-asetus tarkentaa myös jo direktiivissä olevia käsittelyperusteita, joita on muun muassa julkisen vallan käyttäminen, tilastointi, tieteellinen tutkimus, suostumus ja arkistointi.

2.5 Rekisteröidyn oikeudet

Rekisteröity on henkilö, jonka henkilötietoja yritys tai taho käsittelee (Oikeudet [4.9.2019]). EU:n yleisen tietosuoja-asetuksen (EU 27.4.2016/679) mukaan rekisteröidyllä on oikeuksia koskien omia rekisterissä olevia henkilötietojaan kohtaan. Näitä oikeuksia ovat muun muassa oikeus saada pääsy tietoihinsa, oikeus oikaista tietoja, oikeus saada tietoa henkilötietojensa käsittelystä, oikeus poistaa tiedot ja

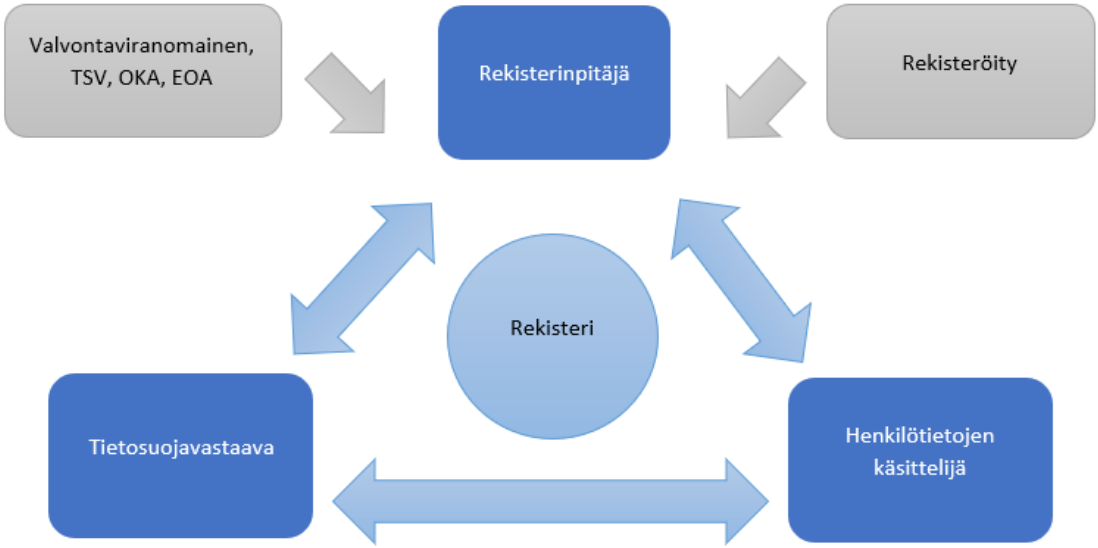
oikeus tulla unohdetuksi, oikeus rajoittaa tietojen käsittelyä, oikeus siirtää tiedot järjestelmästä toiseen, oikeus vastustaa tiedon käsittelyä sekä oikeus olla joutumatta automaattisen päätöksenteon kohteeksi. Näitä kaikkia oikeuksia ei voida kuitenkaan käyttää kaikissa tilanteissa, vaan käyttöön vaikuttaa muun muassa se, millä perusteella rekisteröityjen henkilötietojaan käsitellään. (Oikeudet [4.9.2019].)

Lisäksi on huomioitava EU:n yleisen tietosuoja-asetuksen (EU 27.4.2016/679) ja kansallisen tietosuojalain (L 5.12.2018/1050) sisältämät kohdat lasten erityisasemasta, rekisteröidyn oikeudesta luottaa tietoturvaan sekä oikeudesta saada apua valvontaviranomaiselta.

2.6 Rekisterinpitäjä

Rekisterinpitäjä on henkilö tai taho Andreassonin, Koiviston ja Ylipartasen (2013, 62) mukaan, joka käyttää henkilötietorekistereitä toimintansa ylläpitämisen vuoksi. Henkilötietorekisterit perustetaan rekisterinpitäjää varten ja rekisterinpitäjällä on myös määräysoikeus rekisterien käytöstä. Henkilötietorekisterin ylläpidosta on voitu määrätä myös lailla. Andreasson ym. (2013, 62) toteavat, että rekisterinpitäjä on vastuussa rekisterissä olevien henkilötietojen lainmukaisesta käsittelystä. Rekisterien ylläpito asettaa myös muita velvollisuuksia. Rekisterinpitäjän tulee huolehtia rekisterihallinnon järjestämisestä, lainmukaisista tietojärjestelmistä, työntekijöiden käsittelemien asiakastietojen käytön valvonnasta, tietosuojavastaavan nimittämisestä sekä tulee ohjeistaa ja kouluttaa henkilökuntaa.

Seuraavasta kuvasta voidaan nähdä, että rekisterinpitäjä ei käsittele yksinään henkilötietoja, vaan kommunikoi muiden tahojen kanssa ylläpitäessään henkilötietorekistereitä. Eniten rekisterinpitäjä kommunikoi tietosuojavastaavan ja henkilötietojen käsittelin kanssa. Henkilötietoja käsitellessä tulee huomioida myös rekisteröity sekä valvontaviranomaiset.



Kuva 3. Rekisterinpitäjän rooli (Voutilainen 2017, 3).

Rekisterinpitäjällä on oma roolinsa ja vastuunsa. Kuten yllä olevasta kuvasta voidaan todeta, on rekisterinpitäjän toimittava useiden eri toimijoiden kanssa ylläpitäessään rekisteriä. Rekisterinpitäjän on myös toteutettava organisatoriset sekä tekniset toimenpiteet, jotta voidaan osoittaa ja varmistaa käsittelyssä noudatettavan asetusta. Toimenpiteitä onkin Voutilaisen (2017, 3) mukaan jatkuvasti tarkastettava ja päivitettävä vastaamaan nykytilannetta.

2.7 Tietosuojavastaava

2.7.1 Rooli organisaatiossa

Suurelle osalle yrityksistä tietosuojavastaavan nimeäminen on vapaaehtoista. Jos yritys käsittelee ihmisten terveystietoja, tekee profilointia, seuraa liikkumista esimerkiksi matkakorttien avulla, hoitaa kameravalvontaa tai tekee seurantaa ja paikannusta, on yritys velvollinen nimeämään tietosuojavastaavan. Yritys ei voi kuitenkaan vierittää vastuuta henkilötietojen käsittelystä ja sen lainmukaisuudesta tietosuojavastaavalle. Tietosuojavastaava auttaa, tukee ja neuvoo yritystä. (Tietosuojavastaava 2018.)

Tietosuojavastaava on henkilö, joka on organisaation sisäisten asioiden asiantuntija, joka auttaa noudattamaan tietosuojasäännöksiä ja seuraa henkilötietojen käsittelyä (Tietosuojavastaavat [4.9.2019]). Hänen tehtävänsä on tuoda esiin havaitsemiaan puutteita sekä antaa neuvoa johdolle ja henkilöstölle heidän velvollisuuksistaan tietosuojasäännöksiin liittyen. Pyydettäessä hän neuvoo johtoa tietosuojan vaikutustenarvioinnin tekemisessä ja valvoo vaikutusarvioinnin toteutusta. Tietosuojavastaava toimii yhteyshenkilönä henkilötietojen käsittelyyn liittyvissä asioissa muun muassa johdon ja henkilökunnan välillä. (Tietosuojavastaavat [4.9.2019]) Tietosuojavastaavan tulee valvoa, että EU:n uutta yleistä tietosuoja-asetusta noudatetaan organisaatiossa (Andreasson ym. 2019, 133).

Vaikka tietosuojavastaava vastaa tietosuojasta, on hänen hyvä olla perillä myös tietoturvaa koskevista asioista. Monet henkilötietorekisterit toimivat nykypäivänä yhä enemmän eri ohjelmistojen kautta, jolloin tietosuojavastaavan on hyvä tietää myös niihin liittyvistä tietoturva-asioista. Karkeasti jaoteltuna tietoturva voidaan jakaa hallinnolliseen ja tekniseen tietoturvaan. Harvemmin tietosuojavastaava tuntee sekä hallinnollisen, että teknisen tietoturvan. Andreasson ym. (2019, 137) painottavat, että tietosuojavastaavan tulisi tietää myös tietoturvaloukkauksista ja siitä, miten tietoturvaloukkaustilanteissa toimitaan.

2.7.2 Tietosuojavastaavan nimittäminen

Tietosuojavastaavaa valittaessa on tärkeää huomioida tehtävälle asetetut vaatimukset. Tietosuojavastaavalla on oltava riittävästi työaikaa, välineitä sekä osaamista, jotta hän suoriutuu tehtävästään. Hänellä tulisi olla mahdollisuus myös kouluttautua tehtävää varten. (Tietosuojavastaavat [4.9.2019].)

Jos yritys haluaa nimetä tietosuojavastaavan vapaaehtoisesti, sovelletaan nimittämiseen, asemaan ja tehtäviin tietosuoja-asetuksen (EU 27.4.2016/679) tietosuojavastaavaa koskevia vaatimuksia samalla tavalla, kuin jos nimittäminen olisi pakollista. Tietosuojavastaavaa nimittäessä on otettava huomioon myös henkilön ammattipätevyys sekä erityisesti alan asiantuntemus käytänteistä ja tietosuojalainsäädännöstä. Tietosuojavastaavan työskennellessä yrityksessä, yrityksen liiketoiminnan ja organisaation asioiden tunteminen on avainasia. (Kuntaliitto 2018.)

Kun tietosuojavastaava valitaan, on siitä ilmoitettava tietosuojavaltuutetun toimistolle. Valtuutetun yhteystiedot on myös julkaistava, jotta helppo yhteydenotto on mahdollista tarvittaessa. Tietosuojavastaavaa nimettäessä on huomioitava myös yrityksen sisäinen tiedottaminen ja viestiminen. (Kuntaliitto 2018.)

2.8 Työntekijän yksityisyys

Myös työntekijöiden yksityisyys on otettava huomioon tarkasteltaessa tietosuojaa. Työntekijä voidaan lukea rekisteröidyksi henkilöksi, kun työnantaja ylläpitää työntekijöidensä henkilötietoja koskevaa rekisteriä. On yhtä tärkeää turvata työntekijöiden henkilötietojen turvallinen käsittely ja estää tietojen väärinkäytös. (Teme 2017.)

Työnantaja tarvitsee työntekijöidensä tietoja toimintansa mahdollistamiseen ja täyttääkseen lain asettamat vaatimukset henkilötietojen keräämisestä. Työntekijällä on oikeus vaikuttaa omien henkilötietojensa käsittelyyn ja hänellä on oltava mahdollisuus tulla arvioiduksi oikeiden tietojen perusteella. Tiedonsaanti perustuu aina lähtökohtaisesti rekisteröidyn suostumukseen. (Teme 2017.)

Työntekijältä kerättävät henkilötiedot, joita työnantaja tarvitsee palkatakseen työntekijän ja työsuhteen aikana kerääntyvät tiedot voivat sisältää Nyyssölän (2018, 77–78) mukaan seuraavia henkilötietoja:

- yksilöintiin perustuvat tiedot
- yhteystiedot
- tarpeelliset perhesuhteisiin perustuvat tiedot
- koulutus, aiemmat työsuhteet
- työsopimustiedot, palkkaukseen perustuvat tiedot, maksatustiedot
- karriääri-, arviointi- ja palkkakehitystiedot
- toimipistetiedot
- vakuutuksiin perustuvat tiedot
- työaikatiedot, tehtävät, joissa on toimittu työnantajan edustajana, erityistehtävät
- terveystarkastuksen mahdolliset tulokset, työkyvyn mahdolliset rajoitteet

- muut henkilökohtaiset tiedot
- työsuhteen alkaessa sekä päättyessä kerättävät tiedot

Kun työnantaja kerää työntekijänsä henkilötietoja, täytyy ne saada ensisijaisesti aina työntekijältä itseltään. Tietojen keräämisen yhteydessä on määriteltävä, mitä tietoja ylipäätänsä kerätään ja miksi niiden kerääminen on tarpeellista huomioiden työtehtävät. Työnantaja saa käsitellä vain välittömästi työsuhteen kannalta keskeisiä henkilötietoja. Vanhentuneet henkilötiedot on poistettava. Jos tarpeellisia tietoja ei saada itse työntekijältä, on työnantajan saatava työntekijältä suostumus kerätä tiedot muilta. Poikkeuksena ovat tilanteet, joissa viranomainen luovuttaa henkilötietoja lain (L 5.12.2018/1050) määräämän tehtävän suorittamiseksi tai, kun työnantaja hankkii luotto- ja rikosrekisteritietoja työntekijän luotettavuuden takaamiseksi lain mukaisilla perusteilla. (Työsuojelu 2019.)

Työntekijän arkaluonteisen henkilötiedon käsittely on pääosin kielletty. Arkaluonteisiksi henkilötiedoiksi voidaan luokitella ammattiliittoon kuuluminen, seksuaalinen suuntautuminen, terveydentilaa koskevat tiedot, uskonnollista vakaumusta koskevat tiedot tai etninen alkuperä. Jos arkaluontoisia tietoja joudutaan käsittelemään ja niiden käsittelyyn saadaan suostumus, tulee tiedot kuitenkin poistaa heti, kun asia on käsitelty. (Teme 2017.)

Työntekijän yksityisyys käsittää myös työntekijän henkilökohtaiset työn tekoon kuuluvat välineet, kuten sähköpostin ja henkilökohtaiseen käyttöön varatut tilat, kuten pukuhuone ja käymälä. Työntekijän sähköpostin lukeminen ilman lupaa on kiellettyä. On sovittava erikseen työntekijän kanssa siitä, kuka huolehtii viestien lukemisesta, kun työntekijä itse on estynyt esimerkiksi loman vuoksi. Kameravalvonta on myös otettava huomioon työtiloissa. Kameravalvontaa saa toteuttaa työtiloissa vain työntekijöiden ja muiden tiloissa oleskelevien henkilöiden toiminnan valvomiseksi ja turvallisuuden parantamiseksi. Kamera- ja kuluvalvonta muodostavat oman henkilörekisterinsä ja siksi on tärkeää suojata työntekijän yksityisyys huomioiden myös kameravalvonta. Tietosuojalaki (L 5.12.2018/150) antaa yksityiskohtaisiin edellytyksiin perustuen luvan työntekijän sähköpostiviestien hakemiselle ja avaamiselle, kun työntekijältä ei voida saada suostumusta. (Työ- ja elinkeinoministeriö [17.11.2019].)

2.9 Osoitusvelvollisuus

Osoitusvelvollisuudella tarkoitetaan sitä, että rekisterinpitäjän on pystyttävä osoittamaan noudattavansa tietosuojalainsäädäntöä (Osoitusvelvollisuus [5.9.2019]). Rekisterinpitäjä voi näyttää osoitusvelvollisuuden avulla puuttuvansa muun muassa havaitsemaansa tietoturvaloukkaukseen. Tämä tarkoittaa muun muassa sitä, että yrityksen on laadittava tietosuojaselosteet, tehtävä sopimuksiin sopimusliitteitä koskien tietosuojaa ja dokumentoida tehdyt toimenpiteet. Näiden toimenpiteiden jälkeen on näyttöä siitä, että on pyritty tunnistamaan tietosuojaan liittyviä riskejä ja ottamaan käyttöön tarvittavia toimenpiteitä. Jos taas rekisterinpitäjä ei pysty osoittamaan noudattavansa tietosuoja-asetusta (EU 27.4.2016/679) ja sen velvoitteita, voi se aiheuttaa hallinnollisia seuraamuksia, kuten sakkoja, maineen menetyksen lisäksi. (Osoitusvelvollisuus [5.9.2019].)

Osoitusvelvollisuuden tarkoitus ei ole pelkästään arvioida lakisääteisten vaatimusten toteutusta. Osoitusvelvollisuus näyttää myös sen, miten rekisterinpitäjä kunnioittaa rekisteröinnin kohteena olevien rekisteröityjen tietosuojaa. Osoitusvelvollisuus lisää luottamusta rekisterinpitäjän toimintaa kohtaan, sillä rekisterinpitäjän on toteutettava kaikki tarpeelliset organisatoriset ja tekniset toimenpiteet täyttääkseen EU:n yleisen tietosuoja-asetuksen (EU 27.4.2016/679) vaatimukset. Osoitusvelvollisuus tarkoittaa muutakin. Osoitusvelvollisuuteen kuuluu lisäksi dokumentointivelvollisuus, jonka mukaan tehdyt toimenpiteet tulee dokumentoida ja arkistoida. (Osoitusvelvollisuus [Viitattu 5.9.2019].)

Asetuksen (EU 27.4.2016/679) sisältämän ajatuksen osoitusvelvollisuudesta katsotaan vahvistavan johdon vastuuta. Jatkossa rekisterinpitäjän on osoitettava erilaisten dokumenttien ja toimenpiteiden avulla, että se on ottanut huomioon tietosuojavelvoitteet henkilötietojen käsittelyn suunnittelussa ja toteutuksessa. Andreasson ym. (2019, 43) mukaan oletusarvoisen ja sisäänrakennetun tietosuojan ja -turvan vaatimukset korostavat osoitusvelvollisuutta tukevissa toimenpiteissä, kuten suunnittelussa. On siis pystyttävä todistamaan, miten yritys noudattaa tietosuoja-asetuksen suunnittelua ja toteutusta.

Dokumentointi vie jo pitkälle tietosuoja-asetuksen osoitusvelvollisuuden noudattamista. Yritys voi Andreasson ym. (2019, 43–44) mukaan dokumentoida muun muassa tietojen käsittelyyn liittyviä prosesseja, tietoturva ja -suojaprosesseja, selosteita eri käsittelytoimista, henkilötietojen käsittelyprosesseja, informatiivisia ohjeita ja selosteita, tietoturvaloukkausten ilmoittamisen prosesseja, riskiarviointeja, henkilöstön salassapito- ja käyttäjäsitoumuksia, henkilöstölle annettuja ohjeita, koulutuksia sekä rekisteröityjen oikeuksien toteuttamisen prosesseja.

2.10 Salassapitovelvollisuus

Salassapitovelvollisuus on yksi tietosuojan käsite, joka perustuu salassapitosopimukseen tai lainsäädäntöön. Salassapitovelvollisuus velvoittaa pitämään salassa työnantajansa liike- ja ammattisalaisuudet. Tällöin salassapitovelvollisuus edistää tietosuojaa ehkäisemällä henkilötietojen joutumista vääriin käsiin. Työsopimuslaki (L 26.1.2001/55) kieltää käyttämästä hyödyksi tai kertomasta muille työnantajan liike- ja ammattisalaisuuksia työsuhteen aikana. Tämä pätee työntekijälle uskottuihin asioihin sekä muuten tietoon saatuihin asioihin. Kielto jatkuu myös työsuhteen jälkeen, jos tiedot on saatu oikeudettomasti. Organisaation sopimukset, markkinointi, hintapolitiikka ja tekniset salaisuudet kuuluvat liike- ja ammattisalaisuuksien piiriin. Salassapidolla on suuri merkitys liikesalaisuutta hallussa pitävälle organisaatiolle tai taholle, koska liikesalaisuudella voi olla huomattava vaikutus yrityksen elinkeinotoiminnalle. (Yty [5.11.2019].) Erityisesti salassapitovelvollisuus koskee tietosuojaa, kun kyseessä on muun muassa asiakkaisiin tai henkilökuntaan kohdistuvia henkilötietoja, joka voi tulla julki väärinkäytösten ja salassapitovelvollisuuden laiminlyönnin myötä.

Salassapitovelvollisuuden rikkomisella voi olla ikäviä seuraamuksia ja rangaistuksia. Rikoslain (L 19.12.1889/39) mukaan, liike- ja ammattisalaisuuden rikkominen työsuhteen aikana on kiellettyä. Tämä kielto koskee myös kahta seuraavaa vuotta työsuhteen päättymisen jälkeen. Rikkomuksesta voi saada sakkoa tai korkeintaan kaksi vuotta vankeutta. Rikoslain (L 19.12.1889/39) kielto koskee kuitenkin vain tilanteita, joissa henkilö on luovuttanut tiedot hankkiakseen itselle tai toiselle taloudellista hyötyä ja/tai vain vahingoittaakseen toista osapuolta. (Yty [5.11.2019].)

Salassapitosopimus on sopimus, jossa määritellään salassa pidettävät asiat. Sopimuksesta ei kannata tehdä liian laajaa. Olisi hyvä määritellä yksityiskohtaisesti ne asiat, joita sopimus koskee. Tietyissä tilanteissa salassapitosopimuksesta voi olla vain haittaa työnantajalle, vaikka sen tarkoitus onkin työnantajan etujen turvaaminen. Työsopimuslain (L 26.1.2001/55) asettamat rajoitukset liike- ja ammattisalaisuuksissa ovat voimassa vain työsuhteen aikana, ellei siitä ole muuta sovittu. Jos halutaan pidentää salassapitovelvollisuutta työsuhteen päättymisen jälkeiselle ajalle, on siitä tehtävä erillinen salassapitosopimus. (Yty [5.11.2019].)

3 TIETOSUOJA KÄYTÄNNÖSSÄ

3.1 Palkanlaskenta, kirjanpito ja laskutus

Palkanlaskennan kautta käsitellään muun muassa terveys- ja ay-jäsenyystietoja, jotka on huomioitava myös säilytystavoissa ja -ajoissa. Nämä henkilötiedot on Männistön (2017) mukaan suojattava huolellisesti sekä säilytettävä erillään muista aineistoista. On huomioitava rekisterinpitäjän tiedottamis- ja tiedonantovelvollisuus myös palkanlaskennassa. Rekisteröidyllä on oikeus pyytää hänestä kerätty tieto nähtäviksi ja saada nähdä hänestä kerätty tieto. Tietoihin pääsy on rajattava vain niitä käsittelevien henkilöiden saataville. Palkanlaskennan henkilötietojen käsittely käsittää sekä sähköisen-, että paperisenkin aineiston.

Fredman (2018) toteaa, että palkanlaskennassa käsiteltäviä tositteita ovat esimerkiksi palkkalaskelmat ja palkkojen yhdistelmät, lomapalkkalaskelmat, ulosotto ja ay-jäsenmaksujen tilitykset sekä lääkärintodistukset ja lausunnot. Palkanlaskennan kirjeenvaihtoa taas on palkanlaskennassa tehdyt ilmoitukset eri viranomaisille, kuten tapaturma- tai eläkevakuutusyhtiölle. Nämä tositteet ja kirjeenvaihto ovat osa kirjanpitoa. Myös kirjanpidon ja laskutuksen osalta käsitellään asiakkaiden tietoja eri aineistojen muodossa sekä lähetetään esimerkiksi laskuja ja ilmoituksia viranomaisille ja muille toimijoille.

Männistön (2017) mukaan palkanlaskennassa on huomioitava ja selvitettävä, mikä aineisto on kyseessä, miten tieto vastaanotetaan, käsitellyn tiedon luokitus (normaali vai arkaluontoinen), miten tiedot käsitellään, kenelle tietoa luovutetaan, arkistointi (miten ja missä), kauanko tietoa säilytetään sekä miten tiedot hävitetään. Henkilötietojen säilytysaika on yksi oleellisimmista asioista, jotka täytyy arvioida. Fredmanin (2019) mukaan palkanlaskennan henkilötietoihin voidaan soveltaa samoja säilytysaikoja, kuin mitä kirjanpitoonkin. Tositteet säilytetään kuusi vuotta ja tilinpäätös 10 vuotta. Palkanlaskennassa, juuri mainittuja, huomioitavia asioita voidaan soveltaa myös kirjanpitoon ja laskutukseen samalla periaatteella, kuin kirjanpidon säilytysaikoja palkanlaskentaan. Tietosuoja-asiat koskevat yleisesti kaikkia näitä palveluita.

Tietosuoja-asetuksen (EU 27.4.2016/679) mukaan palkanlaskennassa, kirjanpidossa ja laskutuksessa käytetyt henkilötiedot muodostavat asiakasrekisterin. Tämän rekisterin ylläpito perustuu asetuksen (EU 27.4.2016/679) kuudenteen artiklaan. Palkanlaskentaan, kirjanpitoon ja laskutukseen sovelletaan EU:n yleistä tietosuoja-asetusta (EU 27.4.2016/679) samalla tavalla, kuin muihinkin aineistoihin, jotka luovat henkilörekistereitä sekä käsittelevät niitä perustuen jokapäiväisten asioiden ja palveluiden ylläpitoon.

3.2 Asunto-osakeyhtiölaki

Asunto-osakeyhtiölakia (L 22.12.2009/1599) sovelletaan kaikkiin osakeyhtiöihin, jotka on rekisteröity Suomen lain mukaan asunto-osakeyhtiöiksi, ellei toisin määrätä. Laki (L 22.12.2009/1599) määrittelee asunto-osakeyhtiöstä seuraavasti: asunto-osakeyhtiö on osakeyhtiö, jonka yhtiöjärjestyksessä on määrätty tarkoitus omistaa ja hallita vähintään yhtä rakennusta tai osaa, jonka huoneiston tai huoneistojen yhteenlasketusta lattiapinta-alasta yli puolet on yhtiöjärjestyksessä määrätty osakkeenomistajien hallinnassa oleviksi asuinhuoneistoiksi. Asunto-osakeyhtiölaki määrittää myös osakeluettelon ja remonttirekisterin ylläpidon.

3.3 Isännöinti ja sen tehtävät

Isännöinti on taloyhtiön johtamista ja sen talouden hoitamista. Isännöinti tekee asumisesta helpompaa ja vaivattomampaa pitäen samalla asumiskustannukset kohtuullisella tasolla. Isännöitsijä on hallituksen tukena erilaisissa päätöksentekotilanteissa ja hankkeissa. Isännöitsijältä vaaditaankin huomattavasti kokemusta ja asiantuntemusta asioista, jotta osaa avustaa hallitusta. Asuinrakennusten ikääntyminen ja kasvava peruskorjaustarve kasvattavat isännöinnin merkitystä jatkossa. (Isännöintiliitto [12.10.2019].)

Isännöitsijän tehtäviin kuuluu huolehtia taloyhtiön päätösten lainmukaisuudesta. Hallituksen täytyy saada riittävästi tietoa sekä hallituksella tulee olla asiantuntijoita apunaan tehdessään päätöksiä. Isännöitsijä huolehtii myös siitä, että taloyhtiö pitää hallituksen kokoukset sekä yhtiökokoukset. Isännöitsijän tulee huolehtia kokousten

järjestämisestä, kokouskutsuista ja kokouksien toteuttamisesta. Isännöitsijä huolehtii taloyhtiön kirjanpidon ja tilinpäätöksen laatimisen, jos isännöitsijänsopimuksessa on sovittu asiasta. Hänen on laadittava taloyhtiön suunnitteleman strategian pohjalta talousarvio. Isännöitsijä hoitaa myös taloyhtiön jokapäiväisiä juoksevia asioita. (Isännöintiliitto [12.10.2019].)

3.4 Taloyhtiön tietosuoja

Kun käsitellään henkilötietoja, vaikka sitten taloyhtiössä, tarvitaan peruste tietojen keräämiseen. Vaatimus käsittelyperusteeseen perustuu EU:n yleiseen tietosuoja-asetukseen (EU 27.4.2016/679). Tämä käsittelyperuste vaikuttaa oleellisesti siihen, mitä eri oikeuksia rekisteröidyllä suhteessa rekisterinpitäjään on. Siksipä tietojen käsittelyn on oltava läpinäkyvää, lainmukaista ja kohtuullista. On olemassa myös käyttötarkoitussidonnaisuusvaatimus, mikä tarkoittaa sitä, että tietoja ei saa käsitellä perusteetta muussa tarkoituksessa, kuin mihin ne on alun perin kerätty. (Taloyhtiön tietosuoja [10.11.2019].)

EU:n yleisessä tietosuoja-asetuksessa (EU 27.4.2016/679) on mahdollistettu henkilötietojen käsittely kuuden (6) perusteen mukaan:

- suostumus rekisteröidyltä
- sopimus
- lakisääteinen rekisterinpitäjän velvoite
- elintärkeiden etujen suojaaminen
- tehtävä, joka koskee yleistä etua tai julkista valtaa
- rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu

Henkilötietoja saa käsitellä sopimuksen täytäntöönpanemiseksi, kun rekisteröity on myös osapuolena sopimuksessa. Rekisteröidyllä voi olla käyttöoikeus muun muassa taloyhtiön omistamaan auto- tai parkkipaikkaan. Tällöin henkilötietoja voidaan käsitellä hänen kohdallaan noudattaen esimerkiksi vuokrasopimusta. Tämän vuoksi on erittäin tärkeää määritellä tarkasti sopimuksen sisältö ja perustavoite. Sen perusteella voidaan määrittää, onko tietojen käsittely tarpeen. Henkilötietojen käsittely tuleekin rajata vain välttämättömiin tietoihin. (Taloyhtiön tietosuoja [10.11.2019].)

Sallittuna henkilötietojen käsittelynä pidetään käsittelyä, joka on tarpeen rekisterinpitäjän tai mahdollisen kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. On olemassa niin sanottu tasapainotesti, jota voidaan käyttää apuvälineenä, kun halutaan selvittää, milloin oikeutettu etu voidaan katsoa oikeutetuksi. Kun rekisteröidyn ja rekisterinpitäjän välillä on merkityksellinen suhde, voidaan katsoa edun olevan olemassa. Rekisteröity voi tässä tapauksessa olla esimerkiksi rekisterinpitäjän alainen taikka asiakas. (Taloyhtiön tietosuoja [10.11.2019].)

EU:n yleinen tietosuoja-asetus (EU 27.4.2016/679) säätelee myös tunnistetietoja. Kun tehdään osakesiirtoja, niissä tulee mainita huoneiston tunnistetiedot, ei nimiä. Nimiä ei tule myöskään mainita, kun on kyse vastikerästeistä. Tässäkin tapauksessa mainitaan vain huoneisto, jolla rästejä on. (Taloyhtiön tietosuoja [10.11.2019].)

Kun puhutaan tietosuojasta ja -turvasta, tulee huomioida myös viestintä. Taloyhtiössä sekä yleisestikin ottaen kannattaa miettiä parhaat mahdolliset viestintäkanavat. Taloyhtiön virallisia asioita ei tulisi koskaan hoitaa sosiaalisen median kautta, kuten Facebook-ryhmässä taikka WhatsApp-ryhmässä, vaikka se voisikin olla kätevä tapa. Jos tietoja jaetaan sosiaalisen median kautta, on hyvä ottaa huomioon, että näin sosiaalisen median käyttäjä luovuttaa tiedot myös sosiaalisen median kanavan omistavan tahon haltuun. Jokaisen tulee arvioida riskit käyttämässään viestintäkanavassa ja sen, takaako palvelu riittävän tietosuojan virallisille asioille. Salattu sähköposti on parempi vaihtoehto ei-salatun sijaan. Jos isännöitsijä lähettää esimerkiksi isännöitsijäntodistuksen tavallisella suojaamattomalla sähköpostilla, tulee siitä tiedottaa vastaanottajaa etukäteen. (Taloyhtiön tietosuoja [10.11.2019].)

Tietosuoja täytyy huomioida myös jokapäiväisessä toiminnassa. Taloyhtiöissä voi olla esillä asukkaista koostuva nimitaulu. Tämä nimitaulu on yksi tapa ilmoittaa muun muassa pelastushenkilöstölle, missä kukin asuu. Tämä nimitaulu ei kuitenkaan muodosta henkilörekisteriä ja saa olla esillä tavalliseen tapaan. Hallinnon hoidon oikeutettuun etuun perustuu taloyhtiöiden rappukäytävissä esillä pidettävät nimitaulut. Taloyhtiön on myös harkittava sitä, miten tarkasti tiedot kerrotaan sauna- ja pesutupavarauksissa ja -listoissa. Tarpeettomat henkilötiedot ovat kiellettyjä. Näi-

hin tarpeettomiin tietoihin voidaan lukea esimerkiksi nimi. Jos halutaan ylläpitää vuorolistoja, on niihin syytä laittaa vain huoneistonumero ja sitä voidaan käyttää perustellusti esimerkiksi laskutuksen takia. (Kiinteistöliitto [18.11.2019].)

Tietosuoja-asetus (EU 27.4.2016/679) määrittää taloyhtiön oman aineiston tarkastelua, kuten pöytäkirjojen ja tositteiden säilyttämistä. Tietosuoja-asetuksen mukaan paperista aineistoa käsitellään samalla periaatteella kuin sähköistäkin aineistoa. Säilytysajat ovat keskeinen asia huomioida. Tietosuojaselosteessa taloyhtiön tulee ilmoittaa, miten kyseisten henkilötietoja sisältävien materiaalien säilytys on toteutettu. Henkilötietojen säilytyksen tulee olla riittävää sekä tiedon käsittelyn tapahtua noudattaen EU:n yleistä tietosuoja-asetusta (EU 27.4.2016/679). Mappien ja asiakirjojen ei kuitenkaan katsota muodostavan omaa itsenäistä rekisteriä, kun tiedot ovat osa perushenkilötietorekistereitä. Perushenkilötietorekisterillä tarkoitetaan tässä yhteydessä osake- ja asukasluetteloa. Tiedot eivät siis saa olla vapaasti saatavilla, vaan säilytettävä muun muassa lukkojen takana ja pääsyä tietoihin on rajoitettava. (Kiinteistöliitto [18.11.2019].)

Taloyhtiön henkilötietoja käsitellessä on otettava huomioon myös muiden tietojen käsittely. Henkilötieto käsitteenä on erittäin laaja ja siksi on hyvä toimia varman päälle, kun on vähänkin epäselvää, onko jonkin tieto henkilötieto, josta on määrätty tietosuoja-asetuksessa (EU 27.4.2016/679). Yksi esimerkki tästä on taloyhtiöiden vesimittareiden kulutustiedot. Näiden kulutustietojen perusteella asukas on epäsuorasti yhdistettävissä ja tunnistettavissa. Sama koskee remonttitietoja. Varmin tapa on käsitellä näitä ja näiden tapaisia tietoja, kuten muitakin henkilötietoja koskevia tietoja. (Kiinteistöliitto [18.11.2019].)

4 TIETOTURVA

4.1 Yleistä

Tietoturvaa pidetään yhtenä tietosuojan toteuttamisen keinona. Tietosuoja suojaa ihmisen henkilötietoja, kun tietoturva taas suojaa pääasiassa tietoaineistoja ja tietojärjestelmiä. Tietoturva tarkoittaa erilaisia organisatorisia ja teknisiä toimenpiteitä, jotka varmistavat järjestelmän käytettävyyden, rekisteröidyn oikeuksien toteutumisen sekä tiedon eheyden ja luottamuksellisuuden. (Tietosuoja [3.9.2019].) Yhä useammin yrityksen liiketoiminnan arvo muodostuu nykypäivänä tietojenkäsittelyn hyödyntämisestä. Tämä tietojen käsittely lisää Andreasson ym. (2019, 51) mukaan digitaalisen turvallisuuden merkitystä. Tietosuojan ja -turvan riittävä taso on välttämätöntä digitalisaation jatkuvan kehityksen vuoksi.

Tietoturva jakautuu useampaan toimenpidealueeseen, joita ovat:

- hallinnollinen turvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus
- tietoliikenneturvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- tietoaineistoturvallisuus ja
- käyttöturvallisuus.

Hallinnollinen turvallisuus käsittää yrityksen johdon sitouttamisen tietoturvallisuuden kehittämiseen sekä turvallisuuden peruskäsitteiden ymmärtämiseen ja turvallisuuden toteuttamiseen. Johdon tehtävänä on suunnitella, valtuuttaa ja resursoida organisaation tietoturva ottaen huomioon riskit. (Tietoturvallisuuden johtaminen 2009.)

Henkilöstöturvallisuus pyrkii takaamaan ihmisten turvallisuuden sekä toimintakyvyn suojaamalla heitä ja toimimalla onnettomuuksia sekä rikoksia ennakoivasti. Henkilöstöturvallisuus pyrkii turvaamaan myös kriittiset henkilöresurssit organisaation toi-

minnassa. Turvallisuus voi koostua muun muassa turvallisuusohjeista, viestintäyhteyksistä, hälytys- ja päivystyspalveluista, vakuutuksista, yhteystietojen saatavuuden rajoittamisesta, hälytysmenettelyistä, turvallisuustekniikan käytöstä, salassapitosopimuksista, huumausainetestauksesta tai huolellisesta rekrytoinnista. (EK [17.11.2019].)

Fyysinen turvallisuus tarkoittaa kulunvalvontaa, kameravalvontaa ja vartiointia. Fyysisellä turvallisuudella voidaan ehkäistä muun muassa sähkö-, vesi-, palo- ja murtovahinkoja. Tarkoituksena on turvata organisaatioiden toiminta eri olosuhteissa huomioiden toiminnan riskit sekä niiden erityistarpeet. (Fyysinen turvallisuus 2009.)

Tietoliikenneturvallisuudella varmistetaan verkossa välitettävien tietojen käytettävyys, luottamuksellisuus ja eheys. Tarkoituksena on varmistaa viestien alkuperä, koskemattomuus, luotettavuus sekä todeta lähettäjä ja vastaanottaja. Uhkana voi olla muun muassa laitevika, tulipalo, vakoilu, hakkerointi tai verkon liiallinen kuormittaminen. (Kinnunen 2016, 9.)

Laitteistoturvallisuus kattaa laitteiden asennuksen, suojauksen, ylläpidon ja poiston. Laitteistoja täytyy hallinnoida, joten niille määritellään omistaja ja turvaluokat. Mietitään, miten paljon laitteilta vaaditaan ja riittääkö kapasiteetti pyörittämään ohjelmistoja ja eri toimintoja. Laitteiston elinkaari nousee esille suunnitellessa laitteistoturvallisuutta. Turvalliseen käyttöön kuuluu uusia laitteet, kun arvioitu elinkaari on tullut päätökseen tai laite ilmoittaa siitä oudolla toiminnallaan. (Laitteistoturvallisuus 2009.)

Ohjelmistoturvallisuus käsittelee käyttöjärjestelmien, tietoliikenneohjelmistojen, tietoturvaohjelmistojen, valmissovellusten, räätälöityjen valmissovellusten, teetetyiden sovellusten, itse tehtyjen sovellusten, välitason sovellusten, sovelluskehitystyökalujen ja tietoturvallisen ohjelmoinnin tietoturvaa. Näihin sovelluksiin ja ohjelmistoihin kohdistuu toimenpiteitä, joiden tunnistamista, eristämistä, pääsynvalvontaa, tarkkailua, paljastustoimenpiteitä, lokitietoja sekä laatua täytyy seurata. (Ohjelmistoturvallisuus 2009.)

Tietoaineistoturvallisuus on eri tallennusmuotojen suojausta. Se käsittää paperiset asiakirjat ja tekniset laitteet. Tietoaineistoturvallisuuden elinkaari muodostuu aineiston synnystä sen hävittämiseen. Arkistointisuunnitelmassa on huomioitava tietojen

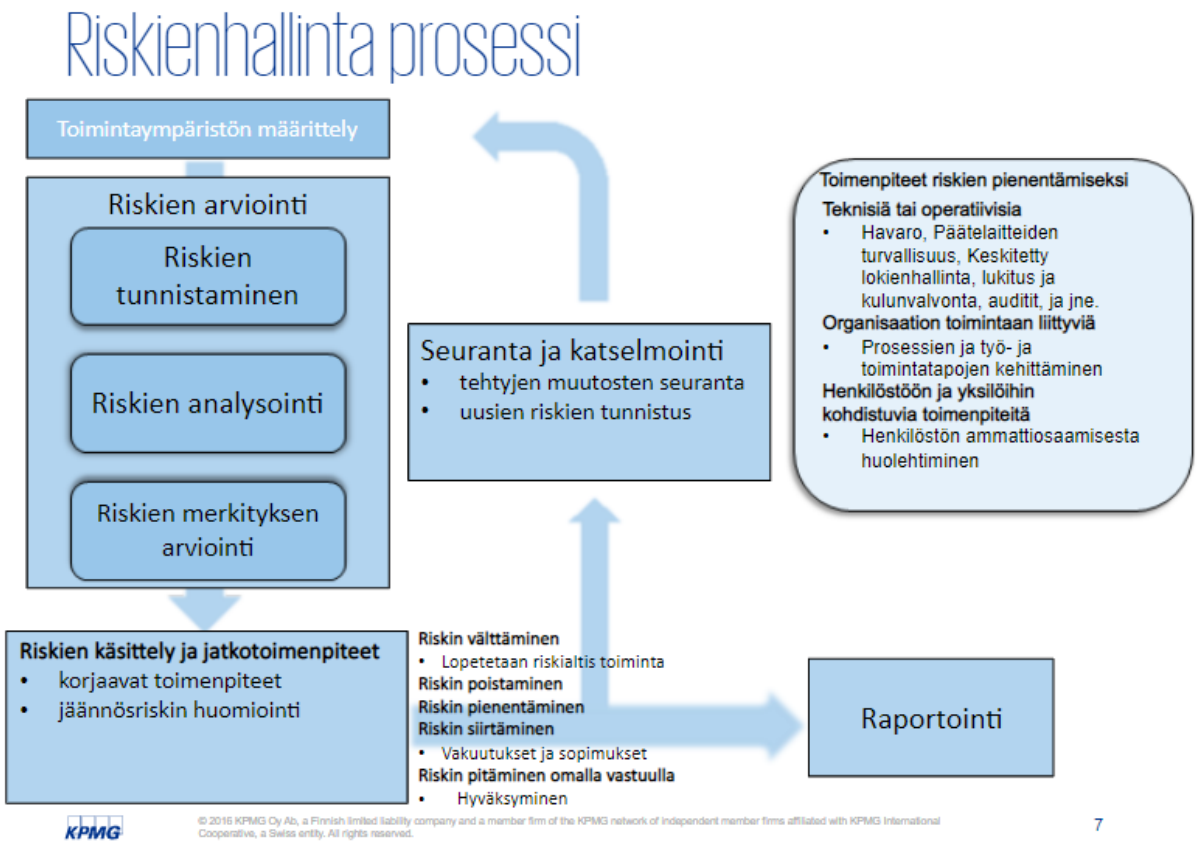
turvaluokitukset. Tiedon elinkaari voi käsittää seuraavat vaiheet: tiedon luonti ja vastaanotto, tärkeyden luokittelu ja tiedon merkintä, rekisteröinti, kopiointi, jakelu, siirto, tiedon vastaanotto, säilytys ja tallennus, arkistointi ja hävitys. Ennen tiedon hävittämistä täytyy ottaa huomioon myös se, kenellä on pääsy tietoon ja se, kenellä mahdollisesti on oikeus käsitellä kyseistä tietoa. (Tietoaineistoturvallisuus 2009.)

Käyttöturvallisuus taas käsittelee järjestelmien ylläpidon, etätyön ja -käytön, tietoteknisen valvonnan ja käyttöoikeuksien hallinnan turvallisuutta. Täytyy luoda ja ylläpitää tietotekniikan vaatimat toimintaolosuhteet, jotta taataan turvallinen käyttö. Turvallisuustoimenpiteiden on oltava ajan tasalla. Täytyy huolehtia muun muassa lokien valvonnasta, ylläpidosta, käyttöoikeuksien hallinnasta, toimivuuden valvonnasta, ohjelmatuesta ja huoltotoimenpiteistä. (Käyttöturvallisuus 2009.)

4.2 Riskienhallinta

Kun puhutaan tietoturvan riskienhallinnasta, ei pidä keskittyä yksinomaan IT-puolen asioihin. Tietoturva koskee tuotteita, tuotantolaitoksia, prosesseja, toimintapolitiikkaa, teknisiä ratkaisuja, laitteita ja verkostoja, mutta myös ihmisiä. Tietoturvatoimet tulisi kohdistaa niin sanottujen arvokkaampien tietojen sekä järjestelmien suojaamiseen. Tämä ei sulje pois muuta tietoturvaa, mutta on järkevää kartoittaa täsmällisemmin ne kohdat, jotka vaativat eniten huomiota. Olennaisuuksiin ja tärkeimpiin tietoturva-asioihin keskittyminen on sekä tehokas että toimiva käytäntö. On olemassa riskejä, joita ei voida täysin edes poistaa. Tällöin niihin riskeihin on hyvä varautua ja lieventää niitä, mutta käyttämättä niihin liikaa aikaa. Näin taataan, että tärkeimmät riskit tulee kartoitettua. (Keskuskauppakamari 2016, 8.)

Seuraava kuva avaa kattavasti riskienhallintaa. Riskien toimintaketju kattaa koko prosessin ja kuvan avulla on helpompi päästä käsiksi riskien kartoittamiseen.



Kuva 4. Riskienhallinta (KPMG 2016).

Yllä oleva kuva selventää riskienhallinnan prosessia. On hyvä huomioida jokainen vaihe. On myös syytä arvioida, millä tavalla riskiä kannattaa pienentää sen sijaan, että yrittäisi poistaa kaikki riskit kokonaan. (KPMG 2016.)

4.3 Tietoturvaloukkaukset

Tietoturvaloukkaus käsittää myös tietosuojaloukkauksen. Tietoturvaloukkauksen seuraus on tietojen siirron, tallennuksen tai muun käytön kautta tapahtunut vahinko tai lainvastainen toiminta, jonka vuoksi tieto on tuhoutunut, hävinnyt, muuttunut tai se on luvattomasti luovutettu ja annettu pääsy tietoihin. (Relipe [25.11.2019].) Koska henkilötietojen käsittely on tarkkaa ja tulee olla perusteltua, on syytä kiinnittää huomiota mahdollisiin tietoturvaloukkauksiin. On laadittava toimintaohje siitä, miten toimitaan, kun tapahtuu tietoturvaloukkaus. Andreasson ym. (2019, 172–175) mukaan tietoturvaloukkauksesta on tehtävä ilmoitus 72 tunnin kuluessa tietosuojavaltuutetulle.

5 HENKILÖTIETOREKISTERIT TILITOIMISTOSSA

5.1 Asiakasrekisteri

EU:n yleisen tietosuoja-asetuksen (EU 27.4.2016/679) artiklan kuusi perusteella palkanlaskennassa, kirjanpidossa ja laskutuksessa voidaan käyttää asiakasrekisteriä, johon henkilötietoja kerätään. Henkilötiedon käsittely on perusteltua, kun se on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi. Rekisterinpitäjänä toimiva yritys, kuten tilitoimisto, tarvitsee asiakkaidensa henkilötietoja päivittäisten toimintojen ja palveluiden toteuttamiseen. Tämä asiakasrekisteri muodostuu, kun yritys kerää asiakkaidensa henkilötietoja, joita ovat muun muassa nimi, Y-tunnus sekä muut henkilötiedot, joiden avulla tiedot ovat yhdistettävissä tiettyyn yritykseen tai henkilöön.

Yritys toimii henkilötietojen käsittelijänä myös silloin, kun henkilötietoja käsitellään toisen eli rekisterinpitäjän lukuun. Myös asiakasrekisteri kuuluu näihin rekistereihin. Esimerkiksi palkanlaskennassa palkkoja laskeva yritys toimii henkilötietojen käsittelijänä rekisterinpitäjän lukuun, kun yritys käsittelee asiakkaansa henkilökunnan tietoja. (Henkilötietojen käsittelijät [25.11.2019].)

5.2 Osakehuoneistorekisteri eli osakeluettelo

Yhtiön osakkeista sekä niiden omistajista pitää osakehuoneistorekisteriin perustuvaa osakeluetteloa Maanmittauslaitos. Osakasluettelo on luettelo, jossa on eritelty jokaisen osakkaan eli huoneiston omistaja sekä hänen tietonsa. Luetteloon merkitään asunto-osakeyhtiölain (L 22.12.2009/1599) mukaan:

- kaikki osakkeet osakeryhmittäin numerojärjestyksessä
- osakehuoneisto, jonka hallintaan osakeryhmä tuottaa oikeuden
- osakkeiden rekisteröintipäivä
- osakkeenomistajan nimi ja osoite, luonnollisesta henkilöstä syntymäaika sekä oikeushenkilöstä kotipaikka, rekisterinumero ja rekisteri, johon oikeushenkilö on merkitty

- muualla laissa osakeluetteloon merkittäväksi säädetyt tiedot
- huoneiston hallintaoikeuteen muun lain nojalla rajoitus, joka on merkitty osakehuoneistorekisteriin.

Osakeluettelon henkilötietojen käsittelyn perusteena on oltava lakisääteinen velvoite. Asunto-osakeyhtiölaki (L 22.12.2009/1599) käsittelee yhtiöjärjestystä, sen sisältöä sekä osakasluetteloa ja sitä, mitä tietoja niihin tulee kerätä. Hallituksen tehtävänä on ylläpitää tietoa yhtiönsä osakkaiden osakkeista. Osakeluettelon tulee olla kattava ja sisältää kaikki vaadittavat tiedot osakehuoneistoista aina osakkaan henkilötietoihin asti. Osakasluettelot laaditaan yhtiötä perustettaessa ja luettelo on säilytettävä myöhempää käyttöä varten. Kun osakkeen omistaja luopuu tai myy osakkeensa, on osakkaan tiedot säilytettävä vielä seuraavan 10 vuoden ajan ja merkittävä uusi osakas osakeluetteloon. (Taloyhtiön tietosuoja [10.11.2019].)

Oikeus tutustua osakeluetteloon ja saada siitä jäljennös tai osa itselleen luettavaksi on jokaisella, joka osoittaa siihen oikeuden. Osakkeenomistajilla tai entisillä osakkeenomistajilla sekä henkilöillä, jotka osoittavat oikeuden tutkia entisiä osakkeenomistajia koskevia osakasluetteloita, on oikeus saada käsiinsä jäljennös osakasluettelosta, jossa näkyy myös entiset osakkaat. Osakasluettelo ei sisällä henkilötunnusta tai muita ylimääräisiä tietoja, jolloin tietoja voidaan antaa eteenpäin. Tietojen pyytäjän on osoitettava, että hänellä on oikeus saada haltuunsa osakasluettelon sisältämät henkilötiedot. (Taloyhtiön tietosuoja [10.11.2019].)

On olemassa myös niin sanottuja julkisia osakeluetteloita, jotka ovat kaikille nähtävissä. Näissä osakeluetteloissa ei saa olla näkyvillä entisten osakkeenomistajien tietoja, vaikka tietoja pitääkin säilyttää 10 vuotta osakkeen myymisestä tai siitä luopumisesta. Maistraatti voi myös väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain (L 18.1.2019/55) perusteella rajoittaa osakkaan tietojen luovutusta. Tällöin yhtiölle annetaan tiedoksi, että osakeluetteloon merkityn osakkaan tietoja saa luovuttaa vain viranomaisille sekä osakkeenomistajille tai muille henkilöille vain, jos he ovat osoittaneet oikeuden vaatimukseensa. Henkilötietoja säilytetään 10 vuotta siitä, kun osakas on luovuttanut tai myynyt osakkeensa, mutta tämän jälkeen tietoja voidaan vielä käyttää sekä käsitellä vain tieteellistä tutkimusta, tilastointia tai yhtiön historian kirjoittamista varten. (Taloyhtiön tietosuoja [10.11.2019].)

Haarman ja Leppäsen (2018, 16) mukaan tulevaisuudessa on otettava huomioon sähköiseksi muuttuvat osakehuoneistorekisterit. Tämä tulee digitalisoimaan isännöintiä entisestään. Sähköistyminen osaltaan vähentää taloyhtiön ja isännöitsijän työtä, kun yhtiöiden ei tarvitse enää ylläpitää yhtiökohtaista osakeluetteloa. Tähän muutokseen tulee kuitenkin valmistautua ajoissa. Muutoksen vaatimukset tulee selvittää, jotta järjestelmät ehditään saada vastaamaan tietosuojaa.

5.3 Kunnossapito- ja muutostyöilmoitusrekisteri eli remonttirekisteri

Remonttirekisterin ylläpito perustuu asunto-osakeyhtiölakiin (L 22.12.2009/1599), kuten osakeluettelonkin pitäminen. Näin ollen ne ovat lakiperusteisia henkilörekistereitä. Myös tietojen säilytysaika määräytyy samoin perustein. Remonttirekisterin tietoja tulee säilyttää niin kauan kuin yhtiö on olemassa. (Taloyhtiön tietosuoja [10.11.2019].)

Remonttirekisteri sisältää seuraavia henkilötietoja (Kiinteistötili 2018):

- osakkaan nimi, osoite, sähköpostiosoite ja puhelinnumero
- mahdollisen muun yhteyshenkilön vastaavat tiedot
- työnsuorittajien (esimerkiksi suunnittelijan, urakoitsijan tai valvojan) nimi, sähköpostiosoite ja puhelinnumero

5.4 Asukasluettelo

Asukasluettelo on rekisteri, jota asunto-osakeyhtiölaki (L 22.12.2009/1599) ei vaadi ylläpidettävän. Asukasluettelo mahdollistaa taloyhtiön jokapäiväisten asioiden hoidon. Taloyhtiön oikeutettuun etuun sisältyy oikeus pitää kirjaa sen asukkaista asukasluettelon muodossa. Asukasluettelon sisältämiä henkilötietoja saa säilyttää sen ajan, jonka taloyhtiö on katsonut tarpeelliseksi. Kun kyse on henkilötiedoista, on säilytysajan oltava kuitenkin mahdollisimman lyhyt. Yleensä perusteeksi voidaan ottaa asukassuhteen kesto. Kun asukas on muuttanut pois, voidaan tietoja säilyttää vielä muun muassa laskutuksen, oikeudellisten toimenpiteiden taikka perinnän vuoksi. (Taloyhtiön tietosuoja [10.11.2019].)

Asukasluettelo sisältää seuraavia henkilötietoja (Kiinteistötili 20108):

- asukkaan nimi, syntymäaika tai henkilötunnus, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi (esimerkiksi perintä)
- osoite, sähköpostiosoite ja puhelinnumero
- muut hallinnon hoidon kannalta välttämättömät henkilötiedot

5.5 Muut rekisterit ja osarekisterit

Jos taloyhtiöön on asennettu valvontakamera, muodostaa tämä oman henkilörekisterin. Riippumatta tallennusten säilytysaikojen pituudesta, luokitellaan tallenteet henkilörekisteriksi tallentuvan luonnollisen henkilön kuvan sekä sähköisen, kulunvalvontaan perustuvan ja tallentuvan kulkutiedon perusteella. Tämän rekisterin olennainen merkitys on hyvä määritellä. Julkisissa tiloissa syy kamera- tai kulunvalvonnalle voi olla rikosten ehkäisy ja niiden selvittäminen. Täytyy ottaa huomioon, että tämä henkilörekisteri voi myös loukata jonkun yksityisyyttä tai kotirauhaa. Tallenteiden käsittelyn ja säilyttämisen pitää tapahtua huolellisesti ja suojattuna. Tallenteita ei saa säilyttää kauemmin kuin on tarpeen eikä niitä saa käyttää muihin kuin ennalta määrättyihin käyttötarkoituksiin. (Taloyhtiön tietosuoja [10.11.2019].)

5.6 Asiakirjat

EU:n yleinen tietosuoja-asetus (EU 27.4.2016/679) vaatii yhtiöt tekemään kirjallisia sopimuksia rekisterinpitäjän ja ulkoisen henkilötietoja käsittelevän palveluntarjoajan kanssa. Näitä taloyhtiössä voi olla esimerkiksi isännöitsijä ja huoltoyhtiön välillä tehdyt sopimukset. Käsiteltävät henkilötiedot tulee olla mainittuna sopimuksissa sekä käsittelyn kesto, luonne ja tarkoitus. Osapuolten oikeudet, velvollisuudet ja vastuut on hyvä olla kirjattuna myös sopimuksiin. Tärkeää on myös mainita salassapito, tietoturva sekä alihankkijoiden käyttö ja tietojen luovutukset. (Taloyhtiön tietosuoja [10.11.2019].) Näin epäselviltä tilanteilta ja ristiriidoilta voidaan välttyä.

EU:n yleisen tietosuoja-asetuksen (EU 27.4.2016/679) vaatimusten mukaan on luotava sopimusliitteitä. Tämän opinnäytetyön liitteissä on Tietosuoja taloyhtiössä – Miten taloyhtiön ja isännöitsijän tulee hallita henkilötietoja -kirjasta lainatut, muokattavat asiakirjamallipohjat taloyhtiön ja isännöinnin tietosuojasta:

- Henkilötietojen käsittely Isännöitsijäyritys A:n ja Asunto Oy B:n välillä.
- Henkilötietojen käsittely palveluntarjoaja Yritys A:n ja Asunto Oy B:n välillä.
- Tietosuoja taloyhtiössämme.
- Tietosuoja isännöintiyrityksessämme.

Koska EU:n yleisen tietosuoja-asetuksen (EU 27.4.2016/679) vaatimuksiin kuuluu laatia asiakirjoja myös muista opinnäytetyössä käsitellyistä asioista, on liitteisiin lainattu mahdollisten tietoturvaloukkausten varalle laadittu toimintaohje ja ilmoituslomake. Työn liitteenä Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus -kirjasta lainatut mallit:

- Ilmoitus tietoturvaloukkauksesta.
- Toimintaohje tietoturvaloukkaustilanteessa.

6 TILITOIMISTO X OY:N GDPR

6.1 Tutkimustapa ja sen valinta

Tämä tutkimus on luonteeltaan tapaustutkimus. Tutkimus laadittiin kyselynä, jotta vastaaja saa tarpeeksi aikaa vastatakseen kysymyksiin. Näin varmistumme siitä, että mahdollisimman paljon tärkeää ja relevanttia tietoa tulee kerättyä tutkimusta varten.

Kyselyssä kartoitettiin yrittäjän näkemystä tietosuojasta. Kysely selvitti, mitä tietosuoja tarkoittaa yrittäjälle ja kuinka tärkeänä se nähdään jokapäiväisessä toiminnassa. Tietosuojan ja -turvan taso haluttiin saada selville ja ne toimenpiteet, mitä uudistuneen tietosuoja-asetuksen voimaantulon jälkeen on tehty. Kysely oli kattava ja antoi paljon myös yksityiskohtaista tietoa, joka jouduttiin rajaamaan työstä tilitoimiston oman tietosuojan vuoksi. Kyselyn avulla saatiin selville kuitenkin paljon hyödyllistä tietoa, jota ei tarvinnut jättää pois opinnäytetyöstä. Esimerkkinä kattava listaus siitä, mitä eri ohjelmistoja ja palveluntarjoajia tilitoimisto voi toiminnassaan käyttää.

Lisäksi tutkimuksessa on käytetty muuta materiaalia, kuten tilitoimistolta saatua jo olemassa olevaa tietosuojakansiota, joka sisältää arkistoituna jo tehtyjä toimenpiteitä. Myös paikan päällä tilitoimistossa on käyty perehtymässä konkreettisesti tietosuojaan ja -turvaan, jolloin on saatu kattava kuva siitä, millaiset toimitilat ja ratkaisut yrityksessä on tehty.

Tutkimuksen kysymykset opinnäytetyön liitteissä.

6.2 Lähtötilanne

6.2.1 Tietosuojan ja -turvan merkitys ja EU:n yleiseen tietosuoja-asetukseen perehtyminen

Kyselymuotoisen haastattelun myötä selvisi, että tilitoimistossa tietosuoja ja -turva katsotaan tärkeäksi asiaksi. Ei vain sen takia, että se on lailla säädetty, vaan myös sen takia, että sillä halutaan vaikuttaa oman työn laatuun ja asiakkaiden mielikuvaan yrityksestä.

Kyseisen tilitoimiston tietosuojaan ja -turvaan ei olla vielä perehdytty niin hyvin, kuin tässä vaiheessa tulisi olla. Tämä tuli ilmi kysyttäessä, mitä toimenpiteitä uudistuneen asetuksen myötä on tehty asetuksen voimaantulon jälkeen. Yrittäjä kertoi, että toukokuussa 2018 henkilökuntaa on ohjeistettu tietosuoja-asioissa, tilitoimiston rekisteriseloste laadittu sekä tietosuojavastaava valittu ja ilmoitettu asiasta tietosuojavaltuutetulle. Tietosuojan ja -turvan riskejä on kartoitettu asetuksen tullessa voimaan ja riskit pyritty poistamaan. Uusien työntekijöiden tietosuojaan perehdyttäminen on jäänyt tekemättä. Alustavia toimenpiteitä, kuten tietosuojaselosteen laatimista, on mietitty, mutta niiden laatimista ei olla viety loppuun asti. Asia on kuitenkin katsottu ajankohtaiseksi ja tärkeäksi ja se halutaan saada ajan tasalle.

6.2.2 Tietoturva sopimuksissa ja sopimusliitteet tilitoimiston ja eri palveluntarjoajien välillä

Yrittäjältä kysyttiin myös, onko tilitoimiston ja eri palveluntarjoajien välillä sovittu tietosuojasta ja -turvasta esimerkiksi sopimuksissa tai onko niihin päivitetty myöhemmin sopimusliitteitä. Vastauksista selvisi, että joidenkin ohjelmistotoimittajien ja ulkopuolisten palveluntarjoajien kanssa asioista on sovittu jo sopimuksia laatiessa ja heiltä on saatu tietosuojaselosteet. Esimerkiksi Asterin tietosuojasta on laadittu käsittelysopimus Atsoftin kanssa sekä Procountorin tietosuojasta on tietosuojaseloste ja muita sopimuksia ja liitteitä Finacolta ohjelman hankkimisen yhteydessä. On kuitenkin käynyt ilmi, että suurimmalta osin nämä sopimusten sisäiset tietosuoja-asiat on jäänyt erittelemättä ja lisäämättä sopimuksiin muiden toimijoiden kanssa.

6.2.3 Henkilötietojen käytön seuranta

Tähän asti henkilötietojen käytön seuranta on ollut suppeaa. Ulkopuolisille toimijoille voidaan tietyin edellytyksin luovuttaa henkilötietoja, mutta sille täytyy olla hyvä peruste. Kuitenkaan tietojen käytön oikeellisuutta ei olla voitu varmistaa silloin, kun tietojen saaja on toiminut muualla, kuin tilitoimiston toimitiloissa. Luovutetuista avaimista, piirustuksista ja alkuperäisistä tiedoista pidetään kuitenkin kirjaa. Kun esimerkiksi huoltoyhtiö tarvitsee yleisavainta käydäkseen korjaamassa kohteen, josta on sovittu myös asukkaan tai tilan haltijan kanssa, kuittaa hän luovutuksen yhteydessä avaimen saaduksi ja palauttaessaan avaimen se kuitataan palautetuksi. Näin kontrolloidaan ja valvotaan kuitenkin sitä, että muun muassa avaimet eivät jää ulkopuolisille henkilöille pidemmäksi aikaa, mitä on sovittu ja sallittu. Yrittäjän mukaan tilitoimistossa kiinnitetään erityistä huomiota siihen, kenelle tietoja luovutetaan ja mitä tietoja luovutetaan.

6.2.4 Tietojen hävittäminen ja säilyttäminen

Tilitoimistolla on käytössä myös tietoturvalaatikko, mikä on todella yleinen nykypäivänä yrityksissä, joissa käsitellään asiakkaiden papereita ja halutaan myös hävittää ne oikein. Tämä ulkopuolinen palveluntarjoaja käy vaihtamassa tietyin väliajoin käytössä olevan laatikon tyhjään, avaamatta sitä matkanvarrella. Laatikon päällä on aukko, josta vain paperiset asiakirjat mahtuvat sisään. Ilman laatikon avaamista ei ole mahdollista päästä käsiksi tietoihin. Paperiset asiakirjat ja muut tulosteet, jotka sisältävät henkilötietoja, hävitetään ammattimaisesti ja tarkoituksen mukaan. Tämän palvelun avulla mahdollistetaan tietojen oikeaoppinen hävittäminen ja paperiroskan oikea lajittelu.

6.2.5 Toimitilat ja aineistojen säilytys

Kyselyn perusteella ei ole varmaa tietoa siitä, kenellä on kiinteistön omistajan puolesta käyttöoikeus yleisavaimeen tällä hetkellä. Muuten ulkopuolisilla ei ole pääsyä toimitiloihin toimiston suljettuna ollessa. Kun toimisto on auki, voivat asiakkaat käydä hoitamassa asioitaan paikan päällä. Jokaisen työpiste on suojattu sermeillä

tai korkeilla tiskeillä, jolloin asiakkailla ei ole mahdollisuutta nähdä mahdollisesti esillä olevia asiakkaiden aineistoja ja tietoja. Tämä luo myös hieman yksityisyyden-suojaa työntekijöille sekä mahdollistaa keskittymisen työhönsä. Yrittäjällä on oma työhuone. Asiakkaan saapuessa mahdollisesti esillä olevat asiakirjat ja henkilötietoja sisältävät paperit kerätään pois näkyvistä ja suojataan näin henkilön tai yrityksen yksityisyys.

Asiakkaiden aineistot säilytetään suljettujen ovien takana. Tilitoimistossa on lukoilla varusteltuja kaappeja ja säilytyspaikkoja, joissa suurin osa aineistosta säilytetään. Arkisto sijaitsee takahuoneessa, jonne ulkopuolisilla ei ole pääsyä henkilökunnan ollessa paikalla. Asiakkaalla ei ole mahdollisuutta oleskella yksin ilman henkilökuntaa toimitiloissa, vaan aina on joku varmistamassa myös tietoturvallista puolta. Arkistoa myös päivitetään jatkuvasti. Säilössä olleet kirjanpidon arkistomapit luovutetaan asiakkaalle tilinpäätöksen yhteydessä, jolloin vältytään tarpeettomalta tietojenkeruulta ja säilyttämiseltä. Näin arkisto uudistuu, siellä on tilaa muille asiakirjoille sekä riski asiakkaiden tietojen väärinkäytöstä pienenee huomattavasti myös materiaalin vähentyessä. Asiakkaan materiaalit, kuten kirjanpidon tositteet ja tilinpäätökset luovutetaan asiakkaalle, jonka jälkeen näiden aineistojen säilytys ja arkistointi ei ole enää tilitoimiston tehtävä.

6.2.6 Viestiminen asiakkaiden ja eri tahojen välillä

Yrittäjän mukaan voidaan todeta, että yritys viestii asiakkaidensa kanssa eri tavoin. Vaikka teknologia on mahdollistanut monia käteviä viestintäkanavia, käytetään tilitoimistossa viestimiseen pääsääntöisesti sähköpostia ja puhelinta. Paljon lähetetään myös perinteistä kirjepostia asiakkaille ja eri viranomaisille. Salattua sähköpostia tilitoimistossa ei ole käytössä. Viranomaisille lähetettävät asiakirjat, joita ei voida lähettää sähköisesti, laitetaan postin kautta kulkemaan. Postin käyttöä on viime aikoina hankaloittanut huomattavasti Postin työntekijöiden lakko.

6.2.7 Henkilöstön yksityisyys ja oikeudet

Henkilökunnan yksityisyys on hyvällä tasolla huomioiden kaikki siihen vaikuttavat tekijät, kuten henkilökohtaiset työpisteet. Henkilötietoihin pääsee käsiksi kuitenkin koko henkilökunta, jolla on käyttäjätunnukset Procountor-kirjanpito-ohjelmaan. Myöskään henkilöstön salassapitosopimukset eivät ole täysin ajan tasalla uuden tietosuoja-asetuksen jälkeen. Salassapitovelvollisuudesta on kuitenkin informoitu henkilöstölle vähintään palkkauksen yhteydessä. Henkilökunnan kanssa on kuitenkin sovittu muun muassa sähköpostin lukemisesta ja niihin liittyvistä toimenpiteistä työntekijän ollessa esimerkiksi lomalla.

6.2.8 Osoitusvelvollisuus

Osoitusvelvollisuus on jäänyt todentamatta. Tilitoimiston nettisivuilla ei ole tietoa yrityksen tietosuojavastaavasta tai siitä, mitä henkilötietoja käsitellään tai miten. Myöskään asiakkaita ei olla tiedotettu tietosuojan ja -turvan käytännön asioista. Tietosuojaselosteet on jäänyt antamatta sekä myös sopimusliitteet eri palveluntarjoajien ja asiakkaiden välillä on päivittämättä tai kokonaan tekemättä.

6.2.9 Käytetyt ohjelmistot ja ulkopuoliset palveluntarjoajat

Tilitoimisto käyttää useita eri ohjelmistoja asiakkaidensa aineistojen käsittelyyn ja säilyttämiseen. Osa näistä ohjelmistoista on ladattavia, jokaisella koneella sisäisen yhteyden kautta käytettäviä ja toiset taas pilvipalveluita. Käytetyimpiä ohjelmistoja ovat muun muassa Basware, Invoice, Unes, Asteri ja Procountor. Näiden avulla hoidetaan laskujen käsittelyä, isännöintiä, palkanlaskentaa, kirjanpidon hoitamista ja muita tapahtumia ja palveluita, joita tilitoimistossa tehdään.

Myös paljon ulkopuolisten tahojen palveluita ja nettisivuja käytetään jokapäiväisessä työskentelyssä. Osaan näihin palveluista työntekijöillä on henkilökohtaiset tunnukset tai tunnistautumisvälineet, toisiin taas tilitoimistokohtaiset käyttäjätunnukset. Tunnuksien käyttö määräytyy pitkälle tietojen tärkeyden perusteella ja niiden käyttäjien määrän mukaan. Tilitoimisto käyttää muun muassa seuraavia palveluita

ja palveluntarjoajien sivuja: vero.fi, ilmoitin.fi, OmaVero, tulorekisteri, Patentti- ja rekisterihallitus, Fortum, Itella Tyvi, Cash-In -Online, Nets, Paytrail, Eazybreak, Bambora, Atria, Verifone, Wisegym, Ilmarinen, Eläkevakuutusyhtiö Elo, Työllisyysrahasto, Varma, Fennia, Pohjola, Lähitapiola, Veritas ja muut palveluntarjoajat tilanteen vaatiessa. Osa näistä palveluista on jonkun tietyn asiakkaan käyttämiä palveluita, joihin tilitoimistolla on pääsy hakiessaan esimerkiksi kirjanpitoon tilitysraportteja ja muuta aineistoa.

Tilitoimiston siisteydestä huolehtii ulkopuolinen yritys, joka käy säännöllisin väliajoin. Siivooja työskentelee pääasiassa henkilöstön läsnä ollessa, jolloin voidaan taata, ettei väärinkäytöksiä tapahdu.

Myös yrityksen IT-tuki on ulkoistettu IT-palveluita tuottavalle yritykselle. Heidän kauttaan on huolehdittu, että serverillä on toimiva palomuuri ja kaikilla tietokoneilla toimiva ja jatkuvasti päivitettävä virustentorjunta-ohjelma. Myös muut mahdolliset laitteistojen turvallisuuteen liittyvät asiat on hoidettu heidän kauttaan, kuten kohta päättyvä Windows 7 -käyttöjärjestelmän päivitysten lopetus. Kaikki Windows 7 -käyttöjärjestelmän koneet, joita on vielä jonkun verran, tullaan vaihtamaan ennen päivitysten päättymistä. Koneiden vaihtoprosessi on jo aloitettu ja ensimmäiset uudet, päivitetyt koneet ovat jo käytössä. Ohjelmistoja päivitetään uusien päivitysten ilmestyessä sekä muita laitteita vaihdetaan uusiin, kun niiden elinkaari alkaa olla päättymässä tai kun laitteen toiminta muuttuu huomattavasti. Tästä hyvä esimerkki on juuri vaihdettu monitoimitulostin. Ajantasaisten ohjelmien ja laitteiden avulla tuetaan hyvää tietosuojaa ja -turvaa jokapäiväisessä toiminnassa.

6.2.10 Riskien kartoitus ja tietoturvaloukkaukset

Tilitoimistossa on yrittäjän mukaan kartoitettu tietosuojaan liittyviä riskejä asetuksen astuessa voimaan. Tällöin on myös tehty toimenpiteitä ja selvityksiä, joilla voidaan minimoida tai poistaa näitä riskejä. Sen jälkeen riskejä ei olla kartoitettu tai päivitetty. Myöskään tietoturvaloukkauksiin ei olla varauduttu sen tarkemmin. Tilitoimistolta puuttuu toimintasuunnitelma tietoturvaloukkausten varalle. Tietoturvaloukkauksille ei olla myöskään laadittu lomaketta, jolla siitä voisi ilmoittaa tietosuojavastaavalle.

6.2.11 Käytössä olevat henkilörekisterit

Tilitoimistolla on myös käytössään henkilörekisteri omista asiakkaistaan eli asiakasrekisteri. Tämä rekisteri sijaitsee sähköisessä muodossa Procountor-ohjelmistossa. Lisäksi tilitoimisto ylläpitää puhelinluetteloa sisäisellä verkkoasemallaan. Asiakasrekisterin ylläpito perustuu jokapäiväisen toiminnan hoitamiseen ja ylläpitämiseen, kuten asiakkaiden laskuttamiseen. Puhelinluettelo perustuu pitkälti samaan perusteeseen, jolloin jatkuva asiakkaiden kanssa käyty kommunikointi on sujuvampaa. Tämä henkilörekisteri sisältää asiakkaan nimen, puhelinnumeron ja joissain tapauksissa jopa sähköpostiosoitteen. Periaatteessa nämä henkilörekisterin sisältämät tiedot ovat julkisia. Useimpien asiakkaiden puhelinnumero on esimerkiksi saatavilla heidän omilla sivuillaan. Tämä henkilörekisteri on kuitenkin saatavilla vain, jos omaa salasanan jollekin työpisteelle ja tietää, millä verkkoasemalla ja missä tiedostossa puhelinluettelo sijaitsee.

Tilitoimisto käyttää ja ylläpitää myös henkilötietojen käsittelijän roolissa muita henkilöreksitereitä. Näitä ovat esimerkiksi isännöinnin kautta hoidettavat osakasluettelot, asukasrekisterit ja remonttirekisterit. Näiden rekistereiden rekisterinpitäjä on aina taloyhtiö. Tilitoimiston ja taloyhtiön välillä on solmittu isännöitsijänsopimus. Näiden rekistereiden tietosuoja on huomioitu myös päivittäisessä toiminnassa. Rekisterit sijaitsevat työntekijöiden tietokoneilla, joista jokainen on suojattu eri salasanalla, joka on vain kyseisen työpisteen käyttäjän hallinnassa. Työntekijöillä, jotka hoitavat kyseisten rekistereiden käsittelyä ja ylläpitoa, on omat käyttäjätunnukset ohjelmistoihin.

Henkilörekistereitä päivitetään jatkuvasti, kun tietoa tulee lisää tai ne muuttuvat. Kuitenkaan vanhoja tietoja ei olla poistettu, vaikka peruste niiden ylläpitämiseen olisi rauennut. Pääsääntöisesti henkilökunnalla on pääsy näihin henkilörekistereihin, mutta osaan näistä käyttäjien määrä on rajattu. Lokitietoja voidaan siltä osin tarkastella, kun ne ovat saatavilla ohjelmistoista käyttäjätunnusten myötä. Tarkempaa lokitietojen seuraamista ei olla suoritettu.

6.3 Toimenpide-ehdotukset Tilitoimisto X Oy:lle

6.3.1 Tietosuojaselosteet, sopimusliitteet sekä muut laadittavat asiakirjat ja ohjeet

Yksi oleellisin asia, joka tämän työn myötä on noussut esille, on tietosuojaselosteiden ja muiden sopimusliitteiden teko. Tutkimuksen mukaan nämä sopimusliitteet ja vastuiden jakamiset ovat jääneet kokonaan ajatuksen tasolle. On siis ensisijassa käytävä läpi eri palveluntarjoajien kanssa tehdyt sopimukset ja ryhdyttävä toimiin, mikäli tietosuojasta ei olla sovittu mitään kirjallisesti. Toinen keskeinen asia on ilmoittaa tietosuojavastaavan olemassaolosta henkilöstölle, mutta myös asiakkaille sekä laatia heille tietosuojaseloste. Tämä seloste on syytä laatia myös nähtäväksi tilitoimiston nettisivuille, jotta voidaan edesauttaa osoitusvelvollisuuden täyttämistä. Myös asiakkaille on ilmoitettava tietosuojasta sekä laadittava räätälöidyt sopimusliitteet.

Lisäksi on syytä laatia arkistointisuunnitelma. Näin osoitetaan, että tilitoimistossa ollaan perehdytty siihen, missä mitäkin tietoja säilytetään sekä samalla voidaan kartoittaa niiden mahdollisten väärinkäytösten riskit. Tämän arkistointisuunnitelman myötä tarkistetaan perusteellinen ja oikeellinen tietojen säilytys. Tilitoimiston on myös laadittava toimintasuunnitelma mahdollisia tietosuojaloukkauksia varten. Opinnäytetyön liitteissä olevaa pohjaa voidaan käyttää hyödyksi ja muokata se vastaamaan tilitoimiston tarpeita. Myös lomake tietosuojaloukkausten ilmoittamisesta on laadittava. Tietosuojapyyntöjen vastaamiseen on suunniteltava tapa, jota noudatetaan.

Tilitoimiston on huolehdittava osoitusvelvollisuuden todentamisesta. Näiden tietosuojaselosteiden, sopimusliitteiden ja muiden ohjeiden avulla voidaan osoittaa, että tietosuojaan ja -turvaan ollaan oikeasti perehdytty ja asioita mietitty syvällisemminkin. Pelkästään näiden asiakirjojen laatiminen ja räätälöiminen jokaiselle asiakkaalle on suuri työmaa. Jokainen voimassaoleva sopimus on käytävä läpi ja selvitettävä, mitä henkilötietoja kenenkin kanssa käsitellään ja miten ne säilytetään. Näillä asiakirjoilla on jo yksinään suuri vaikutus tilitoimiston tietosuojaan ja -turvaan. Näiden

toimenpiteiden avulla myös asiakkaat saattavat herätä miettimään oman yrityksensä tietosuojaa ja -turvaa, mikä on heidän kannaltaan erittäin tärkeää.

6.3.2 Henkilöstö

Henkilöstö täytyy ohjeistaa uusien ohjeiden mukaan. Henkilöstö on avainasemassa vaikuttamassa päivittäin toiminnallaan tietosuojaan ja -turvaan. Yhteisistä toimintatavoista on keskusteltava. Tulee käydä läpi EU:n yleisen tietosuoja-asetuksen oleellisimmat kohdat ja selvitettävä, mitä kyseinen asia oikeasti tarkoittaa myös käytännön kannalta. Oleellista on päivittää henkilöstön salassapitosopimukset ajan tasalle, jotta myös sen kautta voidaan turvata asiakkaiden henkilötietojen säilyminen yrityksen sisällä.

Henkilöstön yksityisyyden parantaminen on oleellista henkilötietojen käsittelyn kohdalla. Tällä hetkellä koko henkilökunnalla on pääsy kollegoidensa henkilötietoihin, jos heillä on tunnukset Procountoriin. Kun mietitään ratkaisua, millä voitaisiin parantaa tätä yksityisyyttä, täytyy ottaa huomioon monta seikkaa. Palkanlaskijalla on oikeus käsitellä henkilötietoja jo sillä perusteella, että hän tarvitsee niitä hoitaakseen työnsä. Kirjanpitäjät hoitavat myös tilitoimiston kirjanpitoa. Molemmilla kirjanpitäjillä on oltava oikeudet näihin henkilötietoihin, jotta voidaan hoitaa päivittäistä toimintaa toisen ollessa esimerkiksi sairas tai muuten estynyt. Käyttäjätunnukset ovat henkilökohtaisia, eikä niitä voi vain lainailla toisen ollessa estynyt. Myöskin varapalkanlaskijalla on oltava oikeudet käsitellä tilitoimiston henkilöstön henkilötietoja pääpalkanlaskijan ollessa estynyt. Näin ollen lähes koko henkilökunnalla on melkein pakko olla oikeudet henkilötietojen käsittelyyn, vaikka se rajaa henkilöstön yksityisyyttä huomattavasti.

Työntekijöillä on kuitenkin oikeus pyytää henkilötietojensa käsittelyn rajoittamista ja mikäli tällaisia pyyntöjä tulee, on viimeistään silloin asialle tehtävä jotain. Jokaisella on oikeus henkilötietojensa oikeaan käsittelyyn ja niiden rajaamiseen.

6.3.3 Isännöitävien taloyhtiöiden neuvonta

Isännöitsijä on sopinut isännöintisopimuksen jokaisen taloyhtiön välillä. Isännöitsijä hoitaa päivittäisiä taloyhtiön asioita ja käsittelee taloyhtiön henkilötietorekistereitä. Taloyhtiöt käsittelevät kuitenkin myös itse henkilötietojaan. Yhteisissä tiloissa voidaan säilyttää kirjanpitoaineistoja, henkilörekisterin osia ja muita virallisia asiakirjoja.

Yleisissä tiloissa, kuten kerhohuoneissa säilytettävät henkilötiedot ja asiakirjat on säilytettävä tietosuoja-asetuksen mukaisesti. Niiden tulee olla lukittujen ovien takana ja käytön oltava rajattua. Sauna- ja pesutupalistoissa ei saa enää olla asukkaiden nimiä, vaan vuorot on ilmoitettava esimerkiksi huoneiston numeron perusteella. Taloyhtiöiden ilmoitustauluilla sijaitsevat asukasluettelot ovat kuitenkin sallittuja, eivätkä ne luo uutta henkilörekisteriä. Näiden käyttö on jo pelastushenkilökunnan informoinnin myötä perusteltua.

Myös muissa keskeisissä tietosuoja-asioissa on syytä informoida ja ohjeistaa taloyhtiöitä. Heidänkin on luotava tietosuojaselosteet sekä käytävä läpi sopimukset eri palveluntarjoajien välillä. Täytyy kartoittaa järjestelmät, joissa henkilötietoja käsitellään. Rekistereiden sisältö on tarkistettava. Tietosuoja-asetuksen mukaiset roolit on tärkeä tunnistaa. Selvitetään, kuka toimii rekisterinpitäjänä, kuka on rekisteröity ja kuka on henkilötietojen käsittelijä. Taloyhtiön on nimettävä henkilö, joka vastaa tietosuoja-asioista. Sähköiseksi muuttuvan osakehuoneistorekisterin käyttöönotto ja sen riskit on hahmotettava ajoissa, jotta mahdolliset muutokset ja toimenpiteet ehditään miettimään ajoissa.

Näitä sopimuksia ja asioita yleensä hoitaa isännöitsijä, jolloin näiden muutostöiden aloittaminen ja hoitaminen kuuluu yhtenä osana isännöinnin työhön.

6.3.4 Henkilörekisterit

Jatkossakin on tärkeää miettiä sitä, mitä rekistereitä ylläpidetään ja onko vahingossa luotu tarpeettomia henkilörekistereitä, jotka eivät tämän selvityksen myötä ole nousseet esille. On tarkistettava kaikkien henkilörekistereiden sisältämät tiedot ja

poistettava sinne kuulumattomat henkilötiedot viipymättä. Perusteeton henkilötietojen käsittely on kiellettyä. Tutkimuksessa nousi esille, ettei vanhentuneita henkilötietoja olla poistettu henkilörekistereistä. Tämä tulee ehdottomasti korjata. Kun peruste vanhojen tietojen säilyttämiselle ja käsittelylle on päättynyt, on ne syytä poistaa viipymättä.

Tilitoimiston oma asiakasrekisteri on käytävä läpi, mutta myös henkilötietojen käsittelijän roolissa käytettävät osakeluettelot, asukasluettelot ja remonttirekisterit on käytävä läpi. Myös taloyhtiöiden vedenkulutusluettelot ja sauna- ja pesutupalistojen tietosuoja on taattava. Nämä luettelot ja listat on saatettava tietosuojan piiriin. Tietojen perusteella henkilöt ovat kuitenkin tunnistettavissa. Näihin luetteloihin ei tule laittaa enää nimiä esille vaan on ilmoitettava tieto pelkästään huoneiston numeron tai muun ei niin tarkan tunnisteen avulla.

6.3.5 Muut huomioitavat seikat

Rekisteröidyn on tietosuoja-asetukseen perustuen kartoitettava sekä tietosuojalliset riskit, mutta myös tietoturvaan liittyvät riskit. Riskit voivat olla henkilötietojen käsittelyssä rekisteröidylle mahdollisesti aiheutuvat aineettomat, aineelliset tai fyysiset vahingot. Myös tietoturvan riskit on kartoitettava ja päivitettävä. On otettava huomioon kaikki tietoturvan eri osa-alueet.

On selvitettävä, kuinka sitoutunut johto on tietosuojan ja -turvan ylläpitämiseen ja kehittämiseen tilitoimistossa. Henkilökunnan turvallisuus on huomioitava sekä ehkäistävä rikoksia ja onnettomuuksia, mutta myös organisaation toiminnan riskejä on ehkäistävä liittyen esimerkiksi henkilöstöpulaan. Kulunvalvonta ja vartiointi sekä vakuuttamalla ehkäistävät riskit on hyvä käydä läpi, vaikka ne eivät olisi muuttuneetkaan tai kaikki olisi kunnossa. Yleisavaimen olinpaikka on selvitettävä, jotta voidaan varmistua, ettei väärinkäyttöjä tapahdu. Tietoturvallisuuden käytettävyys ja laitteiden päivitykset sekä haavoittuvuus on tärkeää tarkastaa, jotta tietovuodot olisivat mahdollisimman hyvin estettävissä. Täytyy myös kartoittaa, kuinka todetaan viestien alkuperä, luottamuksellisuus ja eheys. Tallennustavat on kartoitettava ja saatettava vastaamaan nykyteknologiaa. Varmuuskopiot ja digitaalinen arkistointi on

oltava luettavissa ja käytettävissä nykyaikaisilla laitteilla. Tiedonkulun polku on selvitettävä. On tärkeää, että tieto kulkee oikealle henkilölle, eikä jää esimerkiksi jonkun työpöydälle ajelehtimaan. Miten jatkossa korvataan muun muassa Posti, jos kirjeiden lähetys ei ole enää luotettavaa ja nopeaa. Otettava huomioon etätyön mahdollisuus ja sen turvallisuuden turvaaminen. Mitä toimenpiteitä täytyy tehdä, jos haluaa tehdä etätöitä ja millainen työympäristö on sallittu. Miten eri laitteiden ja ohjelmien huolloista ja päivityksistä huolehditaan. Näitä tietoturvallisuuteen liittyviä asioita on useita ja ne pitää kartoittaa myös tilitoimistossa.

6.3.6 Henkilöstöpalaveri

Olisi erittäin aiheellista pitää palaveri henkilökunnan kanssa koskien tilitoimiston tietosuojaa ja -turvaa ja käydä samalla myös riskit läpi yhdessä. Tällöin kaikilla on mahdollisuus tuoda esille asioita, jotka voisivat olla merkittäviäkin tekijöitä toimintaympäristössä. Yhdessä asioiden läpikäyminen on oiva tapa sisällyttää myös henkilökunta mukaan tietosuojaa ja -turvaan. Näin jokainen henkilöstöstä sisäistää tietosuoja-asetuksen merkityksen myös omassa päivittäisessä työssään ja osaa miettiä omia työskentelytapojaan uudella tavalla. Yhteisen toimintastrategian luominen ja näistä asioista kirjallisten ohjeiden laatiminen auttaa myös tilitoimistoa toteuttamaan osoitusvelvollisuuttaan.

Tämän opinnäytetyön teoreettinen viitekehys antaa jo kattavan kuvan siitä, mitä tulee ottaa huomioon miettiessä tilitoimiston tietosuojaa. Työnantajan olisi hyvä pyytää henkilökuntaa tutustumaan tähän teokseen esimerkiksi ennen henkilöstöpalaveria, jotta henkilökunta olisi perillä käsiteltävästä asiasta sekä osaisi esittää hyödyllisiä toimintatapoja ja ratkaisuja yhteisiin kysymyksiin ja ongelmiin.

7 TULOKSET

Tapaustutkimuksen kautta on saatu selville, että tilitoimiston tietosuoja ja -turva vaatii paljon toimenpiteitä, jotta se vastaisi EU:n yleistä tietosuoja-asetusta sekä Suomen tietosuojalakia. Nämä vaadittavat toimenpiteet eivät kuitenkaan ole ylitsepääsemättömiä, vaikkakin aikaa vieviä toimenpiteitä. On kuitenkin edullisempaa käyttää työaikaa ja resursseja tietosuojaan ja -turvaan liittyvien asioiden selvittämiseksi ja ajan tasalle saattamiseksi, kuin odottaa esimerkiksi tietoturvaloukkausta ja reagoida asiaan liian myöhään. Suurin osa tietoturvaloukkauksista ja vahingoista syntyy kuitenkin vahinkojen ja erehdysten kautta, kun ei olla osattu varautua oikeisiin asioihin oikeilla tavoilla. Erityisesti koko henkilöstön informointi ja perehdyttäminen tietosuojaan ja -turvaan on oleellista. Henkilökunta on kuitenkin se, joka toimii jokapäiväisten asioiden parissa ja antavat suuren panoksen työllään yritykselle.

Keskeisimpiä asioita, jotka vaativat toimenpiteitä, ovat erilaiset laadittavat asiakirjat. Näitä on muun muassa tietosuojaseloste, sopimusliitteet, arkistointisuunnitelma, toimintasuunnitelma tietoturvaloukkauksille ja ilmoituslomake loukkauksesta. Henkilöstön salassapitosopimukset olisi hyvä päivittää, mutta niistäkin on sovittu jo työntekijää palkattaessa, jolloin asia ei ole niin kriittinen. Sen sijaan henkilörekistereiden päivittäminen, niiden sisältämien tietojen kartoittaminen sekä vanhentuneiden tietojen poistaminen nousee prioriteettilistalla kärkeen. Eikä riitä vain tilitoimiston asiakasrekisterin päivittäminen, vaan myös henkilötietojen käsittelijän roolissa taloyhtiöiden rekisterien kartoittaminen.

Tehtäviä toimenpiteitä hieman vähensi se, että tilitoimistossa on tehty tiettyjä toimenpiteitä jo vuonna 2018, kun EU:n yleinen tietosuoja-asetus astui voimaan. Tietosuojavastaava on jo nimetty. Kartoitettuja riskejä täytyy päivittää ja miettiä uudestaan niiden minimoimista, mutta alustava työ on tehty. Suurimman työn vaatii kaikkien sopimusten läpikäyminen ja useiden tietosuojaan liittyvien sopimusliitteiden tekeminen. Tilitoimiston tietosuoja ei ollutkaan aivan niin haavoittuva tutustuttaessa aineistoon, kun alkutilanne antoi olettaa. Liitteissä sijaitsee asiakirjamalleja lainattuna opinnäytetyössä käytetyistä lähteistä ja nämä antavat hyvän pohjan tietosuojan ja -turvan päivittämiselle.

8 POHDINTA

Opinnäytetyön laatiminen oli mielenkiintoinen ja opettava prosessi. Aikaa ja perehtymistä asioihin tämä vaati paljon. Lakiin ja asetuksiin perustuvaa tietoa tuli osata tulkita oikealla tavalla sekä osata poimia oleellisimmat ja keskeisimmät asiat. Työn tekemistä helpotti se, että aihe oli rajattu koskemaan nimenomaan tilitoimiston tietosuojaa ja -turvaa. Tietosuoja ja -turva on todella laaja käsite. On liki mahdottomuus käsitellä sitä kaikkea tietoa yhdessä työssä tarpeeksi laajasti. Tämä opinnäytetyö on keskittynyt niihin olennaisimpiin ja eniten huomiota vaativiin kohtiin.

Opinnäytetyön ajankohtaisuus ja tärkeys on säilynyt koko opinnäytetyöntyön teon ajan. Valittu tutkimustapa osoittautui hyväksi tiedonkeruun välineeksi ja kysymyksiin saatiin kattaviakin vastauksia yrittäjältä. Näiden vastausten analysoinnissa tuli huomioida myös tilitoimiston tietosuoja. Yksityiskohtaisimmat vastaukset ja tiedot tuli jättää avaamatta opinnäytetyöhön, jottei mahdollisuutta niiden tietojen kautta väärinkäytökselle voi syntyä. Lukijalle voi tulla mielikuva, ettei työssä ole perehdytty tarpeeksi tilitoimiston tietosuojaan ja -turvaan. Tutkimustuloksia on rajattu nimenomaan tilitoimiston tietosuojaa ja -turvaa ajatellen.

Tämä opinnäytetyö antaa kattavan tietopaketin tietosuojasta ja -turvasta kenelle tahansa. Tämä työ on hyvä lähtökohta jokaisen rekisterinpitäjän oman tietosuojan ja -turvan parantamiseen. Opinnäytetyössä esiintyvä tilitoimisto tulee hyödyntämään omalla tavallaan tätä työtä parantaen omaa päivittäistä toimintaansa ja saattamaan jo aloitettujen EU:n yleisen tietosuoja-asetuksen vaatimia toimenpiteitä ajan tasalle. On toivottavaa, että lukija havahtuu parantamaan myös omaa jokapäiväistä toimintaansa luettuaan tämän opinnäytetyön, vaikka hän ei toimisikaan rekisterinpitäjänä. Jokainen voi edistää tietosuojaa ja -turvaa omalla tavalla ja olla esimerkkinä muille.

LÄHTEET

Andreasson, A., Koivisto, J. & Ylipartanen, A. 2013. Tietosuojavastaavan käsikirja. Helsinki: Tietosanoma Oy.

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

EK. Ei päiväystä. Henkilöstöturvallisuus. [Verkkojulkaisu]. Helsinki: Elinkeinoelämän keskusliitto EK ry. [Viitattu 17.11.2019]. Saatavana: https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/henkilostoturvallisuus/

EU 27.4.2016/679. Euroopan Parlamentin ja Neuvoston Asetus.

Fredman, J. 2018. Henkilötietojen suoja ja kirjanpitolaki – Onko vaatimuksissa ristiriita?. [Verkkojulkaisu]. Helsinki: Suomen Taloushallintoliitto ry. [Viitattu 25.11.2019]. Saatavana: https://tilisanomat.fi/palkkahallinto/henkilotietojen-suoja-ja-%E2%80%A8kirjanpitolaki

Fyysinen turvallisuus. 2009. Fyysinen turvallisuus. [Verkkojulkaisu]. Helsinki: Valtiovarainministeriö. [Viitattu 17.11.2019]. Saatavana: https://www.vahtiohje.fi/web/guest/fyysinen-turvallisuus

Haarma, K. & Leppänen, T. 2018. Tietosuoja taloyhtiössä – Miten taloyhtiön ja isännöitsijän tulee hallita henkilötietoja. Helsinki: Kiinteistöalan Kustannus Oy.

Henkilötieto. Ei päiväystä. Mikä on henkilötieto?. [Verkkojulkaisu]. Helsinki: Tietosuojavaltuutetun toimisto. [Viitattu 5.9.2019]. Saatavana: https://tietosuoja.fi/mika-on-henkilotieto

Henkilötietojen käsittelijät. Ei päiväystä. Henkilötietojen käsittelijät. [Verkkojulkaisu]. Helsinki: Tietosuojavaltuutetun toimisto. [Viitattu 25.11.2019]. Saatavana: https://tietosuoja.fi/henkilotietojen-kasittelijat

Hulkkonen, J. 2018. EU:n tietosuoja-asetuksen muutokset tilitoimistossa, Case LPR Ekspertiisi Oy. [Verkkojulkaisu]. Lappeenranta: Saimaan ammattikorkeakoulu. Liiketalouden koulutusohjelma, Laskentatoimi. Opinnäytetyö. [Viitattu 11.9.2019]. Saatavana: https://www.theseus.fi/bitstream/handle/10024/156321/Hulkkonen_Jani.pdf?sequence=1&isAllowed=y

Isännöintiliitto. Ei päiväystä. Mitä on isännöinti?. [Verkkojulkaisu]. Helsinki: Isännöintiliitto. [Viitattu 12.10.2019]. Saatavana: https://www.isannointiliitto.fi/mita-on-isannointi/

Katajamäki, P. & Vainionpää, M. 2019. GDPR vaikutus tilitoimistoihin – Kyselytutkimus Euroopan Unionin uuden tietosuoja-asetuksen käyttöönottamisesta ja sisäistämisestä suomalaisissa tilitoimistoissa. [Verkkojulkaisu]. Seinäjoki: Seinäjoen ammattikorkeakoulu. Liiketalouden koulutusohjelma, Taloushallinto. Opinnäytetyö. [Viitattu 12.10.2019]. Saatavana: https://www.theseus.fi/bitstream/handle/10024/170952/Katajam%E4ki_Petra_Vainionp%E4%E4_Mari.pdf;jsessionid=72C30897F3527179EA5BF81F2290D3DE?sequence=2

Keskuskauppakamari. 2016. Tietoturvaopas yrityksille. [Verkkojulkaisu]. Suomi: Keskuskauppakamari. [Viitattu 18.11.2019]. Saatavana: https://kauppakamari.fi/wp-content/uploads/2016/11/tietoturvaopas-yrityksille.pdf

Kiinteistöliitto. Ei päiväystä. Usein kysytyt kysymykset. [Verkkojulkaisu]. Helsinki: Suomen Kiinteistöliitto ry. [Viitattu 18.11.2019]. Saatavana: https://www.kiinteistoliitto.fi/palvelut/tietosuoja/ukk/#q12

Kiinteistötili. 2018. Taloyhtiön tietosuojaseloste. [Verkkojulkaisu]. Kiuruvesi: Kiinteistötili. [Viitattu 18.11.2019]. Saatavana: https://www.kiinteistotili.fi/asukasinfo/henkilotietolaki

Kinnunen, M. 2016. Perusturvan tietoturvasuunnitelman laatiminen. [Verkkojulkaisu]. Jyväskylä: Jyväskylän ammattikorkeakoulu. Sairaanhoitaja, hoitotyö. Opinnäytetyö. [Viitattu 17.11.2019]. Saatavana: https://docplayer.fi/49138142-Perusturvan-tietoturvasuunnitelman-laatiminen.html

Klemetti, S. 2019. Tietosuoja palkanlaskennan näkökulmasta. [Verkkojulkaisu]. Rovaniemi: Lapin ammattikorkeakoulu. Kauppa ja hallinto. Opinnäytetyö. [Viitattu 25.11.2019]. Saatavana: https://www.theseus.fi/bitstream/handle/10024/167320/Klemetti_Seija.pdf?sequence=2&isAllowed=y

KPMG. 2016. Riskienhallinta STM. [Verkkojulkaisu]. Helsinki: KPMG. [Viitattu 17.11.2019]. Saatavana: https://slideplayer.fi/slide/11320253/

Kuntaliitto. 2018. Tietosuojavastaavan nimittäminen, tehtävät ja asema. [Verkkojulkaisu]. Helsinki: Kuntaliitto. [Viitattu 4.11.2019]. Saatavana: https://www.kuntaliitto.fi/yleiskirjeet/2018/tietosuojavastaavan-nimittaminen-tehtavat-ja-asema

Käyttöturvallisuus. 2009. Käyttöturvallisuus. [Verkkojulkaisu]. Helsinki: Valtiovarainministeriö. [Viitattu 17.11.2019]. Saatavana: https://www.vahtiohje.fi/web/guest/kayttoturvallisuus

L 19.12.1889/39. Rikoslaki.

L 27.5.1994/389. Laki tietosuojalautakunnasta ja tietosuojavaltuutetusta.

L 22.4.1999/523. Henkilötietolaki.

L 26.1.2001/55. Työsopimuslaki.

L 22.12.2009/1599. Asunto-osakeyhtiölaki.

L 5.12.2018/1050. Tietosuojalaki.

L 18.1.2019/55. Laki väestötietojärjestelmästä ja Väestörekisterikeskuksen varmennepalveluista annetun lain muuttamisesta.

Laitteistoturvallisuus. 2009. Laitteistoturvallisuus. [Verkkojulkaisu]. Helsinki: Valtiovarainministeriö. [Viitattu 17.11.2019]. Saatavana: https://www.vahtiohje.fi/web/guest/laitteistoturvallisuus

Larko, J. 2018. Yleisen tietosuoja-asetuksen vaikutus isännöinti- ja kiinteistöhoitoyritykseen – Case Haritun Huolto Oy. [Verkkojulkaisu]. Turku: Turun ammattikorkeakoulu. Tietojenkäsittely. Opinnäytetyö. [Viitattu 11.9.2019]. Saatavana: https://www.theseus.fi/bitstream/handle/10024/155989/juhani_larko_opari.pdf?sequence=1&isAllowed=y

Männistö, E. 2017. Miten palkkahallinnossa tulee valmistautua tietosuoja-asetukseen? [Verkkojulkaisu]. Helsinki: Suomen Taloushallintoliitto ry. [Viitattu 25.11.2019]. Saatavana: https://tilisanomat.fi/palkkahallinto/miten-palkkahallinnossa-tulee-valmistautua-tietosuoja-asetukseen

Niemi, H. 2018. EU:n tietosuoja-asetuksen muutosten vaikutukset tilitoimistossa. [Verkkojulkaisu]. Pori: Satakunnan ammattikorkeakoulu. Liiketalouden koulutusohjelma. Opinnäytetyö. [Viitattu 10.9.2019]. Saatavana: https://www.theseus.fi/bitstream/handle/10024/147435/Niemi_Hanna.pdf?sequence=1&isAllowed=y

Nyyssölä, M. 2018. Yksityisyyden suoja työsuhteessa. Helsinki: Alma Talent Oy.

Ohjelmistoturvallisuus. 2009. Ohjelmistoturvallisuus. [Verkkojulkaisu]. Helsinki: Valtiovarainministeriö. [Viitattu 17.11.2019]. Saatavana: https://www.vahtiohje.fi/web/guest/ohjelmistoturvallisuus

Ohtonen, V. 2018. GDPR:n vaikutukset yrityksen henkilötietojen käsittelyyn. [Verkkojulkaisu]. Kajaani: Kajaanin ammattikorkeakoulu. Liiketalouden koulutusohjelma, Tradenomi. Opinnäytetyö. [Viitattu 11.9.2019]. Saatavana: https://www.theseus.fi/bitstream/handle/10024/152145/Ohtonen_Veera.pdf?sequence=1&isAllowed=y

Oikeudet. Ei päiväystä. Rekisteröidyn oikeudet. [Verkkojulkaisu]. Helsinki: Tietosuojavaltuutetun toimisto. [Viitattu 4.9.2019]. Saatavana: https://tietosuoja.fi/rekisteroidyn-oikeudet

Osoitusvelvollisuus. Ei päiväystä. Osoita noudattavasi tietosuojasäännöksiä. [Verkkojulkaisu]. Helsinki: Tietosuojavaltuutetun toimisto. [Viitattu 5.9.2019]. Saatavana: https://tietosuoja.fi/osoitusvelvollisuus

Rantanen, E. 2018. EU:n tietosuoja-asetus ja sen vaatimat käytännön muutokset tilitoimistossa. [Verkkojulkaisu]. Lahti: Lahden ammattikorkeakoulu. Liiketalous, Tradenomi. Opinnäytetyö. [Viitattu 10.9.2019]. Saatavana: https://www.theseus.fi/handle/10024/158774

Relipe. Ei päiväystä. Sopimus henkilötietojen käsittelystä tilitoimistossa. [Verkkojulkaisu]. Vantaa: Relipe Oy. [Viitattu 25.11.2019]. Saatavana: https://relipe.fi/sopimus-henkilotietojen-kasittelysta-tilitoimistossa/

Riskit. Ei päiväystä. Arvioi riskit ja suunnittele toimenpiteet tietosuojan toteuttamiseksi. [Verkkojulkaisu]. Helsinki: Tietosuojavaltuutetun toimisto. [Viitattu 10.11.2019]. Saatavana: https://tietosuoja.fi/arvioi-riskit

Taloyhtiön tietosuoja. Ei päiväystä. Usein kysyttyä henkilötietojen käsittelystä taloyhtiöissä. [Verkkojulkaisu]. Helsinki: Tietosuojavaltuutetun toimisto. [Viitattu 10.11.2019]. Saatavana: https://tietosuoja.fi/usein-kysyttya-taloyhtiot

Teme. 6.9.2019. Yksityisyyden suoja työelämässä. [Verkkojulkaisu]. Helsinki: Teatteri- ja mediatyöntekijöiden liitto. [Viitattu 9.11.2019]. Saatavana: https://www.teme.fi/fi/yksityisyyden-suoja-tyoelamassa/

TE-palvelut. 2017. Työntekijän oikeudet ja velvollisuudet. [Verkkojulkaisu]. Suomi: Työ- ja elinkeinoministeriö. [Viitattu 9.11.2019]. Saatavana: http://toimistot.te-palvelut.fi/-/tyontekijan-oikeudet-ja-velvollisuudet

Tietoaineistoturvallisuus. 2009. Tietoaineistoturvallisuus – tietopääoman hallinta. [Verkkojulkaisu]. Helsinki: Valtiovarainministeriö. [Viitattu 17.11.2019]. Saatavana: https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus-tietopaaoman-hallinta

Tietosuoja. Ei päiväystä. Tietosuoja turvaa oikeutesi henkilötietoja käsiteltäessä. [Verkkojulkaisu]. Helsinki: Tietosuojavaltuutetun toimisto. [Viitattu 3.9.2019]. Saatavana: https://tietosuoja.fi/tietosuoja

Tietosuojavastaava. 2018. Toukokuussa 2018 voimaan tuleva EU:n tietosuoja-asetus laajentaa tietosuojavastaavien ammattikuntaa. [Verkkojulkaisu]. Harinjärvi: Pro PK-Pilvipalvelut. [Viitattu 10.9.2019]. Saatavana: https://www.protietosuojavastaava.fi/

Tietosuojavastaavat. Ei päiväystä. Tietosuojavastaavat. [Verkkojulkaisu]. Helsinki: Tietosuojavaltuutetun toimisto. [Viitattu 4.9.2019]. Saatavana: https://tietosuoja.fi/tietosuojavastaavat

Tietoturvallisuuden johtaminen. 2009. Hallinnollinen turvallisuus. [Verkkojulkaisu]. Helsinki: Valtiovarainministeriö. [Viitattu 17.11.2019]. Saatavana: https://www.vahtiohje.fi/web/guest/hallinnollinen-turvallisuus

Työ- ja elinkeinoministeriö. Ei päiväystä. Yksityisyyden suoja työelämässä. [Verkkojulkaisu]. Helsinki: Työ- ja elinkeinoministeriö. [Viitattu 17.11.2019]. Saatavana: https://tem.fi/tyoelaman-tietosuoja

Työsuhde. 2019. Oikeudet ja velvollisuudet työssä. [Verkkojulkaisu]. Suomi: Työsuojeluhallinto. [Viitattu 9.11.2019]. Saatavana: https://www.tyosuojelu.fi/tyosuhde/oikeudet-ja-velvollisuudet-tyossa

Työsuojelu. 2019. Yksityisyyden suoja. [Verkkojulkaisu]. Suomi: Työsuojeluhallinto. [Viitattu 6.11.2019]. Saatavana: https://www.tyosuojelu.fi/tyosuhde/oikeudet-ja-velvollisuudet-tyossa/yksityisyyden-suoja

Vehmanen, W. 2019. EU:n yleisen tietosuoja-asetuksen vaikutukset tilitoimistoon: Case X. [Verkkojulkaisu]. Pori: Satakunnan ammattikorkeakoulu. Liiketalouden koulutusohjelma. Opinnäytetyö. [Viitattu 2.11.2019]. Saatavana: https://www.theseus.fi/bitstream/handle/10024/262600/Vehmanen_Walteri.pdf?sequence=2&isAllowed=y

Voutilainen, T. 2017. Sisäänrakennettu ja oletusarvoinen tietosuoja sekä JHKA. [Verkkojulkaisu]. Helsinki: Valtiovarainministeriö. [Viitattu 10.11.2019]. Saatavana: https://slideplayer.fi/slide/13823943/

Yrittäjän kyselymuotoinen haastattelu. 2019. Tilitoimisto X Oy. 18.11.2019.

Yty. Ei päiväystä. Työsuhdeasiat. [Verkkojulkaisu]. Helsinki: Yty. [Viitattu 5.11.2019]. Saatavana: https://www.yty.fi/tyosuhdeasiat/salassapitovelvollisuus.html

LIITTEET

Liite 1. Kyselyn kysymykset.

Liite 2. Henkilötietojen käsittely Isännöitsijäyritys A:n ja Asunto Oy B:n välillä.

Liite 3. Henkilötietojen käsittely palveluntarjoaja Yritys A:n ja Asunto Oy B:n välillä.

Liite 4. Tietosuoja taloyhtiössämme.

Liite 5. Tietosuoja isännöintiyrityksessämme.

Liite 6. Ilmoitus tietoturvaloukkauksesta.

Liite 7. Toimintaohje tietoturvaloukkaustilanteessa.

Liite 1. Kyselyn kysymykset.

Haastattelukysymykset Tietosuoja ja -turva tilitoimistossa -opinnäytetyöhön

Henkilötietojen kerääminen, ylläpito ja käsittely vaativat aina perusteen, jonka vuoksi se on mahdollista ja sallittua. Tiedot tulee pääsääntöisesti saada henkilöltä itseltään tai tietojen keräämiseen on saatava lupa. EU:n direktiivi/uusi tietosuoja-asetus on siirtymäajan (2018) jälkeen astunut virallisesti sovellettavaksi. Jokaisen tahon ja yrityksen, joka täyttää asetuksen vaatimat määritykset, joutuvat nimittämään tietosuojavastaavan. Uusi asetus tiukentaa toimia, mutta sen tarkoituksena on kuitenkin suojata yhä enemmän henkilötietojen käsittelyn kohteena olevia henkilöitä sekä heidän yksityisyyttään. Tämä aiheuttaa väistämättä toimenpiteitä.

Tarkoituksena on kartoittaa tällä hetkellä tilitoimistossanne vallitseva tietosuojan ja -turvan taso.

1. Mitä tietosuoja ja -turva käsitteenä tarkoittaa sinulle ja mitä mielikuvia siitä syntyy?
2. Millainen tilitoimiston tietosuojan ja -turvan taso on mielestäsi tällä hetkellä?
3. EU:n uusi direktiivi astui voimaan, jonka myötä myös Suomen lainsäädäntö sen osalta päivittyi. Millaisia toimenpiteitä tilitoimistossa on tehty voimaantulleen uuden asetuksen jälkeen? (2016-2018 ja sen jälkeen)
4. Mitä eri palveluja/palveluntarjoajia tilitoimistossa käytetään? (IT-tuki, siivooja, ohjelmistot, pilvipalvelut, kirjautumista vaativat nettisivut yms., joihin on tunnukset ja erilliset käyttäjät, ohjelmien etäkäyttäjät)
5. Onko tilitoimiston ja palveluntarjoajien välisissä sopimuksissa sovittu tietosuojan ja -turvan asioista, vastuista ja toimintaperiaatteista? (tietosuojaliite sopimuksessa tai oma kohta sille, jokin maininta)
6. Onko ulkopuolisilla pääsy toimitiloihin, kun henkilökunta ei ole paikalla?
7. Miten henkilökuntaa on ohjeistettu tietosuojan ja -turvan asioissa?
8. Onko yleisesti nähtävissä asiakkaiden tai henkilökunnan henkilötietoja toimitiloissa, joista ulkopuoliset, esim. asiakkaat, käydessään voisi hyötyä ja käyttää väärin?
9. Miten säilytätte asiakkaiden aineistot? (kirjanpito ja isännöintiin kuuluvat asiakirjat, henkilötiedot, muu materiaali)
10. Mitä henkilörekistereitä tilitoimisto ylläpitää? Tähän lukeutuu kaikki rekisterit, jotka sisältävät henkilötietoja, joiden avulla ihmiset ovat tunnistettavissa sekä yhdistettävissä asioihin. (Kirjanpito ja isännöinti, esim. osakerekisteri, asiakasrekisteri, vedenkulutusluettelot yms.)
11. Mitä henkilötietoja näihin rekistereihin on kerätty? (luettele yleisesti kaikista, mitä tietoja niissä säilytetään)
12. Päivitetäänkö henkilörekistereitä? Kuinka usein?
13. Kuinka kauan vanhoja tietoja säilytetään? (esim. poistetaanko tiedot vasta mm. laskutuksen jälkeen, jos henkilö on muuttanut pois vai jääkö merkintä kauemmaksi aikaa)
14. Kenellä on pääsy näihin henkilötietoihin ja rekistereihin?
15. Kuinka tärkeänä pidätte tietosuojaa ja -turvaa?
16. Millainen vastuu tilitoimistolla on mielestäsi käsitellessä henkilötietoja? (omia, työntekijöiden ja asiakkaiden)

17. Miten suojaatte laitteenne tietoturvamurtojen ja haittaohjelmien ehkäisemiseksi?

18. Oletteko aiemmin kartoittaneet tietosuojaan ja -turvaan liittyviä riskejä ja tehneet toimenpiteitä niiden ehkäisemiseksi muuten, kuin vakuuttamalla?

19. Miten asioista keskustellaan ja raportoidaan asiakkaiden kanssa? Mitä kanavia käytetään? (viralliset asiakirjat, päivittäinen yhteydenpito yms.)

20. Onko käytössänne salattu sähköposti?

21. Yrityksen täytyy osoittaa perehtyneensä tietosuojaan ja -turvaan. Miten osoitusvelvollisuudesta on ilmoitettu ulkopuolisille? (kirjalliset asiakirjat, maininta nettisivuilla yms.)

22. Kuinka seurataan ja valvotaan väärinkäytöksiä? (Esim. henkilökunnan väärinkäytöksiä asiakkaiden tietojen käsittelyssä, ulkopuolisten tahojen, kuten talomiehille annetuissa tiedoissa, ulkopuolisille luovutetuissa muissa henkilötiedoissa ja niiden käytössä)

23. Miten henkilötietojen luovutusta ja palautusta kontrolloidaan? (avaimet, piirustukset, viralliset (alkuperäiset) asiakirjat, rekisterit yms.)

24. Onko henkilöstön salassapitosopimukset ajan tasalla?

25. Onko tilitoimistolla tietosuojavastaavaa?

26. Millainen rooli tietosuojavastaavalla on tällä hetkellä tilitoimistossa?

27. Oletteko harkinneet tietosuojavastaavan nimittämistä, jos teillä ei ole?

28. Onko työntekijöiden yksityisyyden oikeudet huomioitu? Kenellä on pääsy henkilötietoihin?

29. Toteutetaanko tietosuojaa ja -turvaa jokapäiväisessä työssä? Kuinka se huomioidaan?

Vapaa sana. Mitä muuta huomioitavaa nousi esille? Onko jokin asia, johon pitäisi erityisesti kiinnittää huomiota? Mitä muutoksia odotatte opinnäytetyön tuovan?
V:

Liite 2. Henkilötietojen käsittely Isännöintiyritys A:n ja Asunto Oy B:n välillä.

Henkilötietojen käsittely Isännöintiyritys A:n ja Asunto Oy B:n välillä

Tarkoitus

Sopimusliitteen tarkoituksen on sopia soveltuvan tietosuojalainsäädännön edellyttämällä tavalla henkilötietojen käsittelystä isännöintisopimuksessa sovittujen palveluiden tuottamiseksi. Sopimusliite täydentää [xx.xx.xxxx] allekirjoitettua isännöintisopimusta, ja se tulee voimaan xx.xx.xxxx. Mikäli isännöitsijäsopimuksen sopimusehdot ovat ristiriidassa tämän sopimusliitteen kanssa, sovelletaan tässä sopimusliitteessä sovittua.

Tietosuoja-asetuksen mukaisesti reksiterinpitäjällä tarkoitetaan taloyhtiöitä ja käsittelijällä isännöintiyritystä.

Isännöintiyritys huolehtii rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamisesta taloyhtiön henkilötietojen käsittelyssä siinä määrin kuin sovittujen palveluiden laatu ja laajuus edellyttävät. Isännöintiyritys huolehtii suorittamaansa henkilötietojen käsittelyyn liittyvän, käsittelytoimia koskevan tietosuojaselosteen laatimisesta ja ylläpidosta.

Taloyhtiön hallitus vastaa siitä, että taloyhtiöllä olevien henkilötietojen käsittely on lainmukaista. Taloyhtiön hallitus myötävaikuttaa isännöintiyrityksen käsittelijätehtävien hoitamiseen (esimerkiksi rekisteröidyn oikeuksien toteuttaminen) ja saattaa havaitsemansa käsittelyn riskit viipymättä isännöintiyrityksen tietoon.

Käsiteltävät henkilötiedot

Isännöintiyrityksessä käsitellään seuraavia taloyhtiön keräämiä henkilötietoja ja rekisteröityjen ryhmiä:

- osakeluettelo: omistajan nimi ja postiosoite, luonnollisen henkilön syntymäaika, mahdollisen muun huoneiston hallintaoikeuden haltijan nimi (esimerkiksi lesken asumisoikeus)
- remonttirekisteri: osakkaan nimi, osoite, sähköpostiosoite ja puhelinnumero, mahdollisen muun yhteyshenkilön vastaavat yhteystiedot, työnsuorittajien (esimerkiksi suunnittelija, urakoitsija, valvoja) nimi, sähköpostiosoite ja puhelinnumero
- asukasluettelo: asukkaan nimi, syntymäaika tai henkilötunnus, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi (esimerkiksi perintä), osoite, sähköpostiosoite ja puhelinnumero ja muut hallinnon hoidon kannalta välttämättömät henkilötiedot.
- tallentava valvontakamera/sähköinen kulunvalvonta/muu henkilörekisteri.

Henkilötietojen käsittely ja palauttaminen

Isännöintiyritys käsittelee henkilötietoja vain isännöintisopimuksen mukaisten velvoitteiden täyttämiseksi ja sovittujen palveluiden tuottamiseksi huomioiden tämä sopimusliite sekä muut taloyhtiön hallituksen mahdolliset kirjallisesti toimittamat ohjeet. Isännöintiyritys käsittelee henkilötietoja soveltuvan tietosuojalainsäädännön ja tämän sopimusliitteen mukaisesti. Isännöintiyrityksellä on oikeus mukauttaa henkilötietojen käsittely myöhemmin syntyvää vakiintunutta tietosuojalainsäädännön tulkintaa vastaavaksi kohtuullisen ajan kuluessa.

Isännöintipalvelun laadun, luotettavuuden ja jatkuvan kehittämisen varmistamiseksi henkilötietoja saatetaan käsitellä ISA- tai muun vastaavan auditoinnin yhteydessä.

Palvelun päättyessä isännöintiyritys luovuttaa kaikki edellä mainitut henkilötiedot taloyhtiölle sekä poistaa tiedot huomioiden laista mahdollisesti seuraavat säilyttämisvelvoitteet. Isännöintiyritys voi kuitenkin omien oikeuksiensa ja velvollisuuksiensa toteuttamiseksi (esim. huolellisuusvelvoitteensa toteennäyttämiseksi) säilyttää henkilötietoja tämä jälkeenkin tarpeellisin osin.

Salassapito ja tietoturva

Isännöintiyritys varmistaa, että henkilötietoja käsittelevät vain sellaiset henkilöt, joilla on oikeus käsitellä henkilötietoja ja jotka ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus, ja että tietoja luovutetaan vain sellaisille henkilöille, jotka täyttävät edellä mainitut velvoitteet.

Isännöintiyritys toteuttaa henkilötietojen käsittelyssä tarpeelliset tekniset ja organisatoriset toimenpiteet, kuten ohjeistaa henkilöstönsä ja huolehtii käyttämiensä järjestelmien tietoturvasta.

Alihankkijat ja henkilötietojen siirto Euroopan unionin ulkopuolelle

Isännöintiyrityksellä on oikeus käyttää alihankkijoita (alikäsittelijä) henkilötietojen käsittelyssä. Isännöintiyritys ei siirrä käsittelemiään henkilötietoja Euroopan unionin ulkopuolelle.

Tarkastusoikeus

Taloyhtiöllä on oikeus omalla kustannuksellaan suorittaa auditointi arvioidakseen tämän liitteen mukaisten tietosuojavelvoitteiden täyttäminen ja henkilötietojen käsittelyssä noudatettava tietoturvan taso.

Rekisterinpitäjän avustaminen

Isännöintiyritys auttaa taloyhtiötä rekisteröityjen oikeuksien toteuttamisessa.

Vastuu

Kumpikin osapuoli vastaa kaikilta osin omista, mukaan lukien alihankkijoidensa, toimista ja laiminlyönneistä.

Sopimusliitteen voimassaolo

Tämä sopimusliite on voimassa isännöintisopimuksen päättymisen jälkeen niin kauan kuin on tarpeellista henkilötietojen käsittelyyn liittyvän toiminnan loppuunsaattamiseksi, kuten sen ajan, joka on tarpeen henkilötietojen palauttamiseksi taloyhtiölle ha henkilötietojen poistamiseksi, tai kauemmin, mikäli soveltuva lainsäädäntö niin määrää.

Allekirjoitukset

(Haarma ym. 2018, 61–65.)

Liite 3. Henkilötietojen käsittely palveluntarjoaja Yritys A:n ja Asunto Oy B:n välillä.

Henkilötietojen käsittely palveluntarjoaja Yritys A:n ja Asunto Oy B:n välillä

Tarkoitus

Sopimusliitteen tarkoituksena on sopia soveltuvan tietosuojalainsäädännön edellyttämällä tavalla henkilötietojen käsittelystä. Sopimusliite täydentää [xx.xx.xxxx] allekirjoitettua [sopimuksen nimi] (jäljempänä sopimus), ja se tulee voimaan 25.5.2018. Mikäli sopimuksen ehdot ovat ristiriidassa tämän sopimusliitteen kanssa, sovelletaan tässä liitteessä sovittua.

Tietosuoja-asetuksen mukaisesti rekisterinpitäjällä tarkoitetaan taloyhtiötä ja käsittelijällä [yritys].

[Palveluntarjoaja] huolehtii reksiterinpitäjän oikeuksien ja velvollisuuksien toteuttamisesta taloyhtiön henkilötietojen käsittelyssä siinä määrin kuin sopimuksessa sovittujen palveluiden laatu ja laajuus edellyttävät.

Taloyhtiö vastaa siitä, että taloyhtiöllä olevien henkilötietojen käsittely on lainmukaista. Taloyhtiö myötävaikuttaa [palveluntarjoajan] käsittelijätehtävien hoitamiseen (esimerkiksi rekisteröidyn oikeuksien toteuttaminen) ja saattaa havaitsemansa käsittelyn riskit [palveluntarjoajan] tietoon.

Käsiteltävät henkilötiedot

[Palveluntarjoaja] käsittelee seuraavia taloyhtiön keräämiä henkilötietoja ja rekisteröityjen ryhmiä:

[Tähän luettelo henkilötietoryhmistä, jotka palveluntarjoajalle siirretään käsiteltäväksi].

Henkilötietojen käsittely ja palauttaminen

[Palveluntarjoaja] käsittelee henkilötietoja vain toimeksiantosopimuksen mukaisten velvoitteiden täyttämiseksi ja sovittujen palveluiden tuottamiseksi. [Palveluntarjoaja] käsittelee henkilötietoja soveltuvan tietosuojalainsäädännön ja tämän sopimusliitteen sekä taloyhtiön mahdollisten kirjallisten ohjeiden mukaisesti.

[Palveluntarjoajan] tulee saattaa reksiterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen rekisterinpitäjän osoitusvelvollisuuden täyttämiseksi.

Sopimuksen päättyessä [palveluntarjoaja] luovuttaa kaikki edellä mainitut henkilötiedot taloyhtiölle sekä poistaa tiedot huomioiden laista mahdollisesti seuraavat säilyttämisvelvoitteet. [Palveluntarjoaja] voi kuitenkin omien oikeuksiensa ja velvollisuuksiensa toteuttamiseksi säilyttää henkilötietoja tämänkin jälkeen tarpeellisin osin.

Salassapito ja tietoturva

[Palvelutarjoaja] varmistaa, että henkilötietoja käsittelevät vain henkilöt ja niitä luovutetaan vain henkilöille, joilla on oikeus käsitellä henkilötietoja ja jotka ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus.

[Palveluntarjoaja] toteuttaa henkilötietojen käsittelyssä tarpeelliset tekniset ja organisatoriset toimenpiteet, kuten ohjeistaa henkilöstönsä ja huolehtii käyttämiensä järjestelmien tietoturvasta.

Alihankkijat ja henkilötietojen siirto Euroopan unionin ulkopuolelle

[Palveluntarjoajalla] on oikeus käyttää alihankkijoita (alikäsittelijä) henkilötietojen käsittelyssä, ja tällöin palveluntarjoaja tiedottaa asiasta riittävän ajoissa taloyhtiölle. [Palveluntarjoaja] ei siirrä käsittelemiään henkilötietoja Euroopan unionin ulkopuolelle.

Tarkastusoikeus

Taloyhtiöllä on oikeus kustannuksellaan suorittaa auditointi arvioidakseen tämän liitteen mukaisten tietosuojavelvoitteiden täyttäminen ja henkilötietojen käsittelyssä noudatettava tietoturvan taso.

Rekisterinpitäjän avustaminen

[Palveluntarjoaja] auttaa taloyhtiötä rekisteröityjen oikeuksien toteuttamisessa.

Vastuu

Kumpikin osapuoli vastaa kaikilta osin omista, mukaan lukien alikäsittelijöidensä, toimista ja laiminlyönneistä.

Sopimusliitteen voimassaolo

Tämä sopimusliite on voimassa toimeksiantosopimuksen päättymisen jälkeen niin kauan kuin on tarpeellista henkilötietojen käsittelyyn liittyvän toiminnan loppuunsaattamiseksi, kuten sen ajan, joka on tarpeen henkilötietojen palauttamiseksi taloyhtiölle ja henkilötietojen poistamiseksi, tai kauemmin, mikäli soveltuva lainsäädäntö niin määrää.

Allekirjoitukset

(Haarma ym. 2018, 66–69.)

Liite 4. Tietosuoja taloyhtiössämme.

Tietosuoja taloyhtiössämme

xx.xx.xxxx

Asunto-osakeyhtiö A:n henkilötietojen käsittelyyn liittyvissä kysymyksissä voitte olla yhteydessä henkilöön xx.

Taloyhtiössämme kerätään henkilötietoja kolmeen eri käyttötarkoitukseen. Osakasluettelon pitämine ja velvollisuus kerätä tietoja osakkaiden tekemistä muutostöistä (remonttirekisteri) perustuvat asunto-osakeyhtiölakiin, ja asukasluetteloa pidämme yllä, jotta saamme taloyhtiömme arjen pyörimään. Taloyhtiössämme muodostuu lisäksi henkilörekisteri tallennettavasta valvontakamerasta sekä sähköisestä kulunvalvonnasta, joita käytetään ihmisten ja omaisuuden turvaksi. Rekistereihin on kirjattu seuraavia henkilötietoja:

- osakasluettelo: omistajan nimi ja postiosoite, luonnollisen henkilön syntymäaika, mahdollisen muun huoneiston hallintaoikeuden haltijan nimi (esimerkiksi lasken asumisoikeus)
- remonttirekisteri: osakkaan nimi, osoite, sähköpostiosoite ja puhelinnumero, mahdollisen muun yhteyshenkilön vastaavat yhteystiedot, työnsuorittajien (esimerkiksi suunnittelija, urakoitsija, valvoja) nimi, sähköpostiosoite ja puhelinnumero
- asukasluettelo: asukkaan nimi, syntymäaika tai henkilötunnus, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi (esimerkiksi perintä), osoite, sähköpostiosoite ja puhelinnumero ja muut hallinnon hoidon kannalta välttämättömät henkilötiedot
- tallentava valvontakamera/sähköinen kulunvalvonta/muu henkilörekisteri.

Kerätyt henkilötiedot saamme yhtiömme osakkailta ja asukkailta itseltään, ja niitä voidaan lisäksi päivittää viranomaislähteistä tai muilta palveluntarjoajilta, millä varmistamme reksitereissä olevan tiedon ajantasaisuuden.

Osakeluettelon ja remonttireksiterin tietoja säilytämme asunto-osakeyhtiölain määrittelemän ajan. Asukasreksiterin henkilötietoja säilytämme niin kauan kuin asukas tai osakas asuu taloyhtiössä. Poismuuton jälkeen henkilötietoja voidaan kuitenkin säilyttää ja käyttää sen ajan ja siinä laajuudessa kuin se on tarpeellista laskutuksen, perinnän ja oikeudellisten toimenpiteiden takia. Tallentavan valvontakameran, sähköisen kulunvalvonnan tai muun henkilörekisterin sisältämiä henkilötietoja säilytämme…

Henkilötietoihin on pääsy yhtiömme hallituksella, toiminnantarkastajalla ja/tai tilintarkastajalla omien tehtäviensä hoitamiseksi sekä mahdollisesti perintäyhtiöllä vastike- tai muiden vastaavien saatavien perinnän toteuttamiseksi. Lisäksi tietoja voidaan luovuttaa talon asukkaalle, osakkaalle tai viranomaiselle lainsäädännön edellyttämällä tavalla. Tallentavan valvontakameran sekä sähköisen kulunvalvonnan henkilötietoja voivat tarkastella vain esitutkintaviranomaiset. Kaikki henkilötietojen käsittely tapahtuu kunnioittaen rekisterissä olevien henkilöiden yksityisyyttä ja saadut tiedot pidetään salassa.

Taloyhtiömme varmistaa, että yhtiön tiedossa olevat henkilötiedot suojataan asianmukaisesti, ja edellyttää tätä myös omilta alihankkijoiltaan, joille tietoa luovutetaan. Käytännössä taloyhtiön käsittelemät henkilötiedot voivat sijaita ulkopuolisten palveluntarjoajien palvelimilla tai laitteilla, jotta voimme turvata riittävän tietoturvatason toteutumisen. Paperiset asiakirjat säilytämme paloturvallisessa ja lukitussa tilassa. Rekisteröidylle kuuluvat oikeudet turvaamme kaikille rekisteröidyille.

(Haarma ym. 2018, 69–71.)

Liite 5. Tietosuoja isännöintiyrityksessämme.

Tietosuoja isännöintiyrityksessämme

xx.xx.xxxx

Taloyhtiönne hankkii isännöintipalvelut yritykseltämme, joten käsittelemme taloyhtiön asukkaiden ja osakkaiden henkilötietoja. Tarvitsemme näitä tietoja, jotta voimme tuottaa sopimuksemme mukaista isännöintipalvelua sekä muita asumisen palveluita taloyhtiössänne. Tietosuoja on meille tärkeää ja huomioimme sen päivittäisessä työssämme.

Henkilötietojen käsittelyä koskevissa kysymyksissä voitte olla yhteydessä henkilöön xx.

Isännöintiyrityksessä säilytämme henkilötietoja omassa asiakasrekisterissämme. Asiakasrekisterimme sisältää seuraavia henkilötietoja isännöimiemme taloyhtiöiden asukkaista ja osakkaista:

- tähän lista henkilötiedoista, joita käsitellään. Käsiteltävät henkilötiedot on kartoitettu osana tietosuojaprojektia.

Säilytämme henkilötietoja asiakasrekisterissämme sen ajan, kun asukas/osakas asuu taloyhtiössä tai taloyhtiö on isännöintiyrityksemme asiakas. Tämän jälkeen säilytämme tietoja vain niin kauan ja siinä laajuudessa kuin se on tarpeellista laskutuksen, perinnän ja oikeudellisten toimenpiteiden takia.

Henkilötiedot saamme kerättyä pääasiassa taloyhtiöön muuton yhteydessä yhtiön osakkailta ja asukkailta itseltään eri viestintäkanavissamme, kuten puhelimitse, postitse, sähköpostitse tai vastaavalla tavalla. Lisäksi henkilöön liitettävissä olevia tietoja kertyy taloyhtiösivuille kirjautumisen yhteydessä sekä niitä käytettäessä. Varmistaaksemme tiedon ajantasaisuuden päivitämme tietoja viranomaislähteistä tai muilta palveluntarjoajilta.

Tarvitsemme osakkaan ja asukkaan henkilötietoja, jotta voimme tunnistaa asiakkaamme tämän asioidessa isännöintiyrityksessämme tai sähköisissä palveluissamme. Käytämme tietoja taloyhtiön vastike- ja vuokravalvonnassa, saatavien perinnässä, asukastiedottamisessa sekä taloyhtiölle hankittujen palvelujen järjestämisessä. Lisäksi tietoja voidaan käsitellä valvottaessa isännöintiyrityksen ja taloyhtiön etua. Näiden ohella henkilötietoja voidaan luovuttaa viranomaiselle, joka esittää lakiin perustuvan tietopyynnön.

Henkilötietoja luovutetaan taloyhtiönne virallisille edustajille näiden tehtävien hoitamiseksi sekä taloyhtiön käyttämille palveluntarjoajille, kuten huolto- ja perintäyhtiöille. Lisäksi tietoja voidaan luovuttaa talon asukkaalle, osakkaalle tai viranomaiselle lainsäädännön edellyttämällä tavalla. Kaikki henkilötietojen käsittely tapahtuu kunnioittaen rekisterissä olevien henkilöiden yksityisyyttä.

Isännöintiyrityksessämme käsiteltävät henkilötiedot säilytetään tietoturvallisessa ympäristössä, ja niitä käyttävät ainoastaan isännöintiyrityksemme työntekijät suojatuilla työasemillaan, joihin työntekijät pääsevät kirjautumaan henkilökohtaisella käyttäjätunnuksellaan. Käytännössä henkilötiedot voivat sijaita ulkopuolisten palveluntarjoajien palvelimilla tai laitteilla, jotta voimme turvata riittävän tietoturvatason toteutumisen. Paperiset asiakirjat säilytämme paloturvallisessa ja lukitussa tilassa.

Rekisteröidylle kuuluvat oikeudet turvaamme kaikille rekisteröidyille voimassa olevan tietosuojalainsäädännön mukaisesti. Näitä oikeuksia ovat oikeus pyytää isännöintiyritykseltä pääsy häntä koskeviin tietoihin, oikeus pyytää häntä itseään koskevien tietojen oikaisemista tai poistamista taikka käsittelyn rajoittamista, oikeus vastustaa häntä itseään koskevien tietojen käsittelyä sekä oikeus tehdä valitus valvontaviranomaiselle.

(Haarma ym. 2018, 73–75.)

Liite 6. Ilmoitus tietoturvaloukkauksesta.

Tietoturvaloukkauksen raportointi -lomake

Ilmoittajan nimi, yhteystiedot sekä toimipaikka: _____

_____

Henkilötietojen tietoturvaloukkaus/epäily tapahtui (pvm ja klo): _____

Loukkauksesta saatiin tieto (pvm ja klo): _____

Mahdollisimman tarkka kuvaus tapahtumasta: _____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Loukkauksen laajuus: _____

_____

_____

Tehdyt alustavat korjaavat toimenpiteet: _____

_____

_____

_____

_____

_____

_____

Lisätietoa tietoturvaloukkauksesta antaa: _____

_____

Ilmoitus annettu:

(Andreasson ym. 2019, 173.)

Liite 7. Toimintaohje tietoturvaloukkaustilanteessa.

Toimenpiteet tietoturvaloukkauksen sattuessa

1. Loukkauksen havainnointi
   - tehdään ilmoitus tietoturvaloukkauksesta esimiehelle valmiiksi suunnitellun lomakkeen mukaan

2. Loukkauksen laadun selvittäminen ja korjaavat toimenpiteet
   - otetaan selvää loukkauksen laadusta ja laajuudesta
   - selvitetään, voidaanko korjata tietosuojaloukkauksen aiheuttamat vahingot
   - ollaan yhteydessä esim. IT-asiantuntijoihin tai muihin asiantuntijoihin
   - arvioidaan, aiheutuuko loukkauksesta luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuvaa vahinkoa
   - arvioidaan tietoturvaloukkauksen aiheuttamaa riskiä (korkea, keskiverto tai matala)

3. Ilmoitus tietoturvaloukkauksesta tietosuojavaltuutetulle 72 tunnin kuluessa
   - annetaan asia tiedoksi tietosuojavaltuutetulle

4. Ilmoitus tietoturvaloukkauksesta rekisteröidylle
   - ilmoitetaan tapahtuneesta tietoturvaloukkauksesta rekisteröidylle
   - päätöksen ilmoituksesta tekee johto ja rekisterin vastuuhenkilö

5. Koordinointiryhmän perustaminen tarvittaessa
   - vakavan ja laajan loukkauksen ollessa kyseessä, perustetaan koordinointiryhmä

6. Rikosilmoitus poliisille
   - rikollisen teon yhteydessä tehdään rikosilmoitus

7. Ilmoitus Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskukselle
   - kalastelun tai palvelunestohyökkäyksen ollessa kyseessä, ilmoitus Kyberturvallisuuskeskukselle

8. Tietoturvaloukkauksen tai -poikkeaman jälkiarviointi
   - käydään dokumentaatio läpi
   - arvioidaan työmäärä ja aiheutuneet kustannukset
   - opitaan tapahtuneesta, varaudutaan paremmin

9. Raportointi ja tilastointi
   - kaikki tietoturvaloukkaukset on tilastoitava
   - yhteenveto puolivuosittain johdolle
   - seurataan trendejä ja ennakoidaan tulevaa

(Andreasson ym. 2019, 173–175.)