Tampereen ammattikorkeakoulu

Tietosuojan hallintamallin kehittäminen

Lasse Kammonen

OPINNÄYTETYÖ
Toukokuu 2024

Hyvinvointiteknologian YAMK

Sisällys

TIIVISTELMÄ

Tampereen ammattikorkeakoulu

Hyvinvointiteknologia/Tradenomi (YAMK)

KAMMONEN, LASSE

Tietosuojan hallintamallin kehittäminen

Opinnäytetyö 80 sivua

Toukokuu 2024

Sain inspiraation tähän opinnäytteeseen työskennellessäni tietosuojavastaavana organisaatiossa, joka toimi rekisterinpitäjänä useissa hyvin erilaisissa henkilörekistereissä. Käytänteet, menettelyt ja jopa rekisteröinnin perusteet vaihtelivat voimakkaasti ja teki kokonaisuuden hallinnasta haastavaa. Esille nousi usein ajatus toimintamallien yhdenmukaistamisesta. Vaatimukset jo lainsäädännön minimi tason täyttämisellekin kuitenkin poikkesivat toisistaan merkittävästi. Kaikki vaatimukset eivät koske kaikkia henkilörekistereitä ja ajatus, että pienimpiäkin sisäiseen käyttöön tarkoitettuja rekistereitä hallittaisiin samoin menettelyin kuin suurimpia tuntui tarpeettoman raskaalta. Pitäisi siis luoda malli, jota voi skaalata kohteen mukaan.

Työssä käydään läpi keskeisimmät tietosuojaa säätelevät normit ja niiden valvonta. Työssä keskitytään kuitenkin pääasiassa niihin menettelyihin ja toimintamalleihin, joilla nämä saadaan toteutettua käytännössä.

Työ luo kuvan tietosuojan kokonaisuudesta ja antaa mallin sen hallitsemiseksi. Malli soveltuu useimpien organisaatioiden käyttöön riippumatta sen toimialasta tai koosta. Malli on muokattavissa kunkin organisaation tarpeiden mukaiseksi.

Asiasanat: tietosuoja, tietosuojavastaava, hallintamalli

ABSTRACT

Tampereen ammattikorkeakoulu

Tampere University of Applied Sciences

Master of Business Administration in well-being technology

KAMMONEN, LASSE

Privacy Protection Management Model

Masters thesis 80 pages

May 2024

Inspiration to this Masters thesis came when I worked as Data Protection Officer in an organization that was data controller in multiple very different personal registers. Practices, procedures and even the basis for registrations varied widely and made management difficult. The idea of making these as similar as possible in all the personal registers came up. Even minimum requirements to obey the law were very different between registers. All the requirements do not affect all the registers and the idea that even the smallest internal registers would require the same procedures as the large ones seemed unnecessarily difficult. The model that could be scaled in every register to meet the requirements and best practices was needed.

This Masters thesis introduces essential norms in data protection and how they are governed. It concentrates mainly in practical procedures and practices that should be done to meet the criteria described in these norms.

This thesis gives you big picture of data protection and a model to manage it. This model suits to most organizations no matter the field or size. The introduced model can be scaled to fit each organizations needs.

Key words: data protection, data protection officer, management model

1. JOHDANTO

Tässä opinnäytetyössä käsitellään Tietosuojan hallintamallin kehittämistä. Malli on sovellettavissa varsin laajasti erilaisiin toimijoihin sillä tietosuojaa ja rekisterinpitäjää säätelevä normisto ei juurikaan poikkea eri toimialoilla.
Tietosuoja nähdään usein asioita hankaloittavana ja monimutkaisena asiana, jopa toimintaa rajoittavana ja estävänä asiana. Osaltaan tämä pitää paikkansa, rekistereillä ja rekisteröityjen tiedoilla ei saa tehdä mitä tahansa.
Itse näen tietosuojan pikemminkin mahdollistajana. Kun tietosuoja on hoidettu hyvin, se on myös merkittävä osa vastuullista toimintaa, julkisuuskuvaa ja työpaikan maineenhallintaa. Viime vuosina on julkisuudessa ollut useita laajaa mediahuomiota saanutta tapausta, joissa rekisteröityjen tietoja on käytetty väärin. Nämä ovat aiheuttaneet mainehaittaa ja suuren yleisön luottamus organisaatiota kohtaan on heikentynyt. Luottamusta voi olla erittäin vaikea palauttaa, kun se on kerran menetetty.

Itselleni mielenkiinto tietosuojaan heräsi katsottuani dokumentin Edward Snowdenista (https://www.youtube.com/watch?v=9g_sqKH2z4I) . Dokumentissa kuulin ensimmäistä kertaa lauseen: ”*If you are not paying for the product, You are the product*”. Tämän lauseen tarkka alkuperä ei ole tiedossa, mutta se liitetään usein amerikkalaiseen insinööriin, Andrew Lewisiin. Yksityisyyden suoja ei kaikkialla maailmassa ole samalla tasolla kuin Suomessa tai EU:ssa. Ihmisistä verkossa kerättyjä tietoja käytetään hyväksi monilla eri tavoilla ja valtaosa heistä suhtautuu tähän hyvin kevyesti. Tämä johtuu pääosin tietämättömyydestä. Ei tunneta miten laajoja vaikutuksia tällä voi yksilön elämään olla. Tässä työssä pyrin osin myös avaamaan tätä ongelmakenttää.

Rajauksena tein viranomaisrekisterit ja muut rekisterit, joissa rekisteröity on ns. tahdosta riippumatta (esim. luottotiedot, terveydenhuollon järjestelmät). Nämä sisältävät osin merkittävästi poikkeavia menettelyjä ja perustuvat osin eri lainsäädäntöön.

2. Työn tavoite, tarkoitus ja tutkimuskysymykset

Tämän työn tarkoituksena on luoda organisaatiolle malli tietosuojan hallintaan. Siinä on tarkoitus käydä läpi tietosuojaan liittyvä asiat. Tietosuojaa voi lähestyä usealta eri näkökannalta.

1. **Lainsäädännöllinen lähestymistapa** keskittyy siihen, että toiminta on vallitsevan lainsäädännön, hyvien käytänteiden ja viranomaisohjeistuksen mukaista.
2. **Tekninen lähestymistapa** keskittyy henkilötietojen käsittelyn tekniseen toteutukseen ja turvallisuuteen. Tekniseen tiedon turvaamiseen liittyvät kysymykset ovat erottamaton osa tätä lähestymistapaa
3. **Hallinnollinen lähestymistapa** tähtää toiminnan toteuttamiseen ja organisointiin siten, että edelliset on huomioitu riskienarviointiin perustuen riittävällä tasolla. Hallinnollisessa lähestymistavassa keskeistä on kuitenkin kokonaisuuden hallinta. Tässä varmistutaan, että henkilötietojen käsittely on koko ajan vallitsevan normiston mukaista ja tekniseltä turvallisuustasoltaan asianmukaista mutta ennen kaikkea kiinnitetään huomiota organisaation ja tietoja käsittelevien henkilöiden toimintaan.

Tässä työssä keskitytään erityisesti hallinnolliseen lähestymistapaan ja tavoitteena on luoda mahdollisimman selkokielinen ja hallittavissa olevissa malli tietosuoja-asioiden hallintaan.
Tutkimuskysymyksenä onkin, mitä asioita tällaisen hallintamallin pitää sisältää ja ottaa huomioon?
Työn tarkoituksena on selkeyttää tietosuojan usein hieman hämmentävältä vaikuttavaa kenttää siten, että henkilötietoja käsittelevät henkilöt ja rekisterinpitäjät kykenevät toimimaan asianmukaisesti.

2.1 Työn taustaa

Itselläni aktiivinen työskentely tietosuojan parissa alkoi vuonna 2018 kun minut nimettiin tietosuojavastaavaksi. Silloisessa työpaikassani ei aiemmin tietosuojavastaavaa ollut ja tietosuoja-asiat nousivat esille, kun sinne valittiin uusi viestintäjohtaja, joka nosti asian esille.
Vuonna 2022 toteutimme koko organisaation kattavan vaikutusten arvioinnin.

Tässä esiin nousi käytänteiden ja toimintamallien suuret eroavaisuudet. Erilaisten tahojen hallinnoimia rekistereitä on paljon ja niiden koko, käyttötarkoitus ja henkilötietojen keräämisen perusteet vaihtelevat voimakkaasti. Pienimmissä sisäisissä rekistereissä oli vain joitakin kymmeniä rekisteröityjä, suurimmassa yksittäisessä rekisterissä taas yli miljoona rekisteröityä.

Samoin perusteet rekistereiden olemassaololle vaihtelevat voimakkaasti. Näitä ovat mm.

- Sisäiseen käyttöön (rekisteröidyt lähinnä työntekijöitä)
- Lainsäädäntöön perustuva velvoite (mm. monet julkishallinnon rekisterit)
- Verkkopalveluita ja -työkaluja (palvelun käyttäjät)
- Maksulliset (kaupalliset) palvelut
- Laajat sidosryhmiin liittyvät rekisterit

Koska perusteet rekisterien olemassaololle vaihtelevat voimakkaasti ovat käytännöt aikojen saatossa muuttuneet toisistaan poikkeaviksi. Tämä johtaa siihen, että kokonaisuuden hallinta vaikeutuu ja aina kun tulee tarvetta luoda uusi henkilörekisteri (esimerkiksi uuden palvelun avaamisen yhteydessä) joudutaan tietosuojan näkökulmasta aloittamaan alusta.

Tarve menettelyjen yhdistämiselle oli selkeä ja sen keskeisimmät tavoitteet olivat:

- Mahdollistaa kokonaisuuden hallinta
- Parantaa rekisteröityjen oikeuksien toteutumista
- Vähentää ja yhdenmukaistaa ohjeistusta
- Helpottaa henkilöstön työtä
- Vähentää virheiden mahdollisuuksia

Työ silloisessa työpaikassani käynnistyi vuonna 2022 henkilöstön koulutuksella tietosuojan perusteista. Tämän yhteydessä kävi myös selväksi, että tietosuojan perusteita on hyvä jatkossa kouluttaa vielä enemmän. Seuraava vaihe oli kartoittaa kaikki rekisterit, jotka täyttävät henkilörekisterin kriteerit. Eli sisältävät henkilötietoja, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön. Henkilötietoja ovat kaikki tiedot, jotka liittyvät henkilöön, kuten nimi, henkilötunnus, osoite, puhelinnumero, sähköpostiosoite, ammatti, harrastukset, terveystiedot ja taloudelliset tiedot. Näiden lisäksi selvitettiin rekisterit, löytyykö niistä ”erityisiä henkilötietoryhmiä” eli:

- rotu tai etninen alkuperä
- poliittisia mielipiteitä
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- terveyttä koskevia tietoja
- seksuaalinen suuntautuminen tai käyttäytyminen
- geneettisiä ja biometrisia tietoja henkilön tunnistamista varten.

Lähde: Tietosuojavaltuutetun toimisto (https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely)

Näitäkin löytyi. Perustelut näille olivat kunnossa mutta nämä asettavat tietojenkäsittelylle omia vaatimuksiaan. Lähes poikkeuksetta organisaatioilla on useita henkilörekisterejä, joiden olemassaolon tulee kestää myös kriittinen tarkastelu.

Erityinen huolenaihe, joka nousee usein esiin myös vaikutusten arvioinneissa, ovat erilaiset verkkopalvelut ja -työkalut. Vaikka pääsy näiden sisältämiin tietoihin ei pääsääntöisesti ole mahdollista tuovat nämä mukanaan kolme uutta ulottuvuutta tietosuojan hallintaan, kolmannen osapuolen (eli käytännössä teknisen palvelun tarjoajan), tietojen siirron ja työkalujen vapaa kenttä -osiot.

Teknisestä toteutuksesta vastaa usein ulkopuolinen palveluntarjoaja ja he tarvitsivat käytännössä laajan pääsyn sovelluksiin ja niiden dataan. Heidän kanssaan tulee laatia tietojenkäsittelysopimukset.

Tietojen siirrossa tulee kiinnittää huomiota siihen, että tieto ei saa missään vaiheessa ylittää EU/ETA rajoja, sekä siihen, että tiedon liikuttelu on turvallista. Käytännössä tämä tarkoittaa suojattuja yhteyksiä ja tiedon liikkumista salattuna.

Verkkosovellusten ”vapaa kenttä” -osiot ovat nousevat verkkopalveluiden kehittämisessä usein esiin ongelmallisina. Vapaa kentissä rekisterinpitäjällä ei ole käytännössä mitään tapaa hallita käyttäjän sovellukseen syöttämää tietoa. Käyttäjiä tulee ohjeistaa siihen, millaista tietoa ei tule sovellukseen kirjata mutta käytännössä tämän valvonta on mahdotonta. Tähän ongelmaan tekoälyn kehitys voi tuoda tulevaisuudessa helpotusta. Vastuu rekisterin sisällöstä säilyy kuitenkin aina oletusarvoisesti rekisterinpitäjällä, vaikka oikeustapauksia tästä ei vielä toistaiseksi ole tiedossani.

Maineen ja julkisuuskuvan hallinta ovat keskeinen, mutta usein unohdettu, osa tietosuojaa nykyaikaisessa mediaympäristössä. Tietosuojakäytännöt ja -vaatimukset ovat kiristyneet merkittävästi viime vuosina, erityisesti Euroopan unionin GDPR:n ja kansallisen lainsäädännön myötä. Uutta sääntelyä, joka koskee henkilötietojen käsittelyä, valmistellaan ja tulee voimaan lähes jatkuvasti.

Tietoa ja tutkimusta tietosuojan ja maineenhallinnan välisestä yhteydestä on olemassa vain vähän. Maineenhallinnan vaikeutta kuvaa hyvin Yhdysvaltalaisen sijoittajan Warren Buffetin lause: ”Maineen rakentaminen kestää 20 vuotta ja tuhoaminen viisi minuuttia”. Aula & Mantere määrittää maineenhallinnan ”Maineenhallinta on hyvän tekemistä, hyvän viestimistä ja hyviä suhteita”.

(Aula, P. & Mantere, S. 2005. Hyvä yritys: Strateginen maineenhallinta. Helsinki. WSOY). Tietoturvapoikkeamissa ollaan usein tilanteessa jossa, aiheutettiin vahinkoa, joudutaan viestimään negatiivisista tapahtumista ja hyvät suhteet vaarantuvat.

Tietosuojaa koskevat rikkomukset voivat aiheuttaa vakavia mainehaittoja organisaatioille. Maineen ja julkisuuskuvan hallinta on tärkeää tietosuojan näkökulmasta. Seuraavassa lueteltuna maineenhallinnan kannalta keskeisiä tietosuojassa huomioitavia asioita Valtionvarainministeriön julkaisun Tietoturvapoikkeamatilanteiden hallinta (https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79258/VM_8_2017.pdf?sequence=6&isAllowed=y) mukaan:

Luottamuksen rakentaminen: Tehokas tietosuojakäytäntöjen noudattaminen auttaa rakentamaan luottamusta asiakkaiden ja sidosryhmien keskuudessa. Kun asiakkaat tietävät, että heidän henkilötietojaan käsitellään asianmukaisesti ja turvallisesti, se vahvistaa organisaation mainetta luotettavana toimijana. Luottamus toiseen osapuoleen on usein edellytys yhteistoiminnalle.
Maineenhallinta kriisitilanteissa: Tietovuodot ja tietoturvaloukkaukset voivat aiheuttaa vakavia mainevahinkoja. Nopeat ja avoimet toimet kriisin hallinnassa voivat auttaa lieventämään vahinkoja ja säilyttämään luottamuksen sidosryhmiin.
Vastuullinen tietojenkäsittely: Organisaatioiden on oltava vastuullisia henkilötietojen käsittelijöitä. Tämä sisältää tietojen keräämisen, käsittelyn ja säilyttämisen vain tarpeellisessa laajuudessa, sekä tiedon turvallisen asianmukaisen poistamisen, kun sitä ei enää tarvita.
Läpinäkyvyys ja viestintä: Organisaatioiden tulisi olla avoimia tietosuojakäytännöistään ja informoida asiakkaita selkeästi siitä, miten heidän tietojaan käsitellään. Nämä seikat tulee käydä selkeästi ilmi tietosuojaselosteesta.
Sidosryhmäsuhteiden hallinta: Tehokas sidosryhmäviestintä voi auttaa organisaatioita osoittamaan sitoutumistaan tietosuojakäytäntöihin ja vastaamaan sidosryhmien huoliin ja odotuksiin.

Yhteenvetona todettakoon, että maineen ja julkisuuskuvan hallinta on olennainen osa tietosuojaa. Organisaatioiden on ymmärrettävä, että vastuullinen tietojenkäsittely ja avoin viestintä edistävät luottamusta ja vahvistaa niiden mainetta.

Tietosuojaan liittyvät riskit on otettava vakavasti, ja organisaatioiden on pyrittävä jatkuvasti parantamaan tietosuojakäytäntöjään säilyttääkseen kilpailukykynsä ja luottamuksensa asiakkaiden keskuudessa.

2.1 Työssä käytetyt menetelmät ja aineiston kerääminen

Työ pohjautuu vuosina 2021-2023 tietosuojavastaavana toimiessani kerättyyn aineistoon ja tietoon. Näitä ovat mm.

- Tehdyt vaikutusten arvioinnit
- Poikkeamaraportit
- Epäilyt tietosuojaloukkauksista
- Pitämäni koulutukset ja niiden aikana saatu tieto
- Keskustelut työntekijöiden kanssa
- Henkilöstölle tehdyt kyselyt ja heidän tekemänsä kehittämisehdotukset

Työhön käytetyt tiedot on kerätty työpaikalta ja sen työntekijöiltä. Työ on kvalitatiivinen tapaustutkimus, jossa on käytetty sekä dokumentointia, että havainnointia tiedonhankinta keinoina.

Keskeisimpinä menetelminä tässä oli, erilaisten tietosuojaan liittyvien dokumenttien käyttö sekä havainnot toiminnasta.
Dokumentteihin minulla oli erittäin hyvä pääsy ja ison osan näistä kirjoitin itse (raportit, selvitykset, yms.) ja osan sain muilta työntekijöiltä. Suurimmassa roolissa dokumenteista oli vuonna 2022 tehty tietosuojan vaikutusten arviointi. Tämä toteutettiin laajasti, siihen osallistui käytännössä kaikki henkilötietoja työssään käsittelevät henkilöt. Se antoi varsin kattavan kuvan kehittämiskohteista ja niiden priorisoinnista.

Havaintoja kehittämiskohteista sain useaa kautta. Näistä keskeisin ja järjestelmällisin oli tietosuojan poikkeamailmoitukset. Toinen merkittävä havaintojen lähde oli erilaissa tilanteissa (kokoukset/keskustelut/esitetyt kysymykset) tehdyt havainnot. Työssä käytettiin siis sekä systemaattista havainnointia, että osallistuvaa havainnointia tiedonhankinnassa.
Kirjassa Tutki ja kirjoita (Hirsjärvi, S., Remes, P., & Sajavaara, P. 2016. Tutki ja kirjoita. Porvoo: Bookwell Oy.) mainitaan useita havainnointiin liittyviä huomion arvoisia seikkoja. Näitä ovat:

- Havainnoijan vaikutus
- Havainnoijan emotionaalinen sitoutuminen
- Havainnoijan objektiivisuus

Havainnoijalla (tekijällä) on melko varmasti ollut vaikutusta kohdehenkilöihin. Työntekijät olivat ainakin osin tietoisia siitä, millaisiin asioihin tullaan huomiota kiinnittämään ja he olivat usein raportointivastuussa tekemisistään tai tekemättä jättämisistään. Iso osa havainnoista syntyi juuri erilaisten ongelmatilanteiden yhteydessä, joissa he epäilivät tehneensä virheen tai olivat sellaisen tehneet. Toinen usein toistunut havaintojen teko hetki oli, kun he tulivat kysymään neuvoa tai hyväksyntää jollekin menettelylle.
Havaintojen tekijä on myös työskennellyt pitkään kyseisten henkilöiden kanssa ja siten muodostanut väkisinkin kuvan henkilöistä ja heidän tavoistaan toimia. Tämä vaikuttaa myös siihen, miten tulkitsen heitä ja heidän kysymyksiään. Tästä syystä havaintojen objektiivisuuteen ei myöskään voi täysin luottaa. Rinnakkaishavainnoijaa ei ollut käytössä.

Systemaattisen havainnoinnin kriteerejä ovat havainnointitavan systemaattisuus ja se, että havainnoija on ulkopuolinen toimija. Systemaattista havainnointia käytettiin ennen kaikkea ulkopuolisten sidosryhmien toiminnan tarkasteluun sekä erilaisissa tehtävissä työskentelevien työntekijöiden tarkasteluun. Luokitteluskeemana tässä käytettiin erilaisia auditointimalleja sekä vaikutusten arvioinnin työskentelytapoja. Osin oli käytössä myös erilaisia tarkastuslistoja.

Osallistuva havainnointi oli kuitenkin selvästi suuremmassa roolissa. Osallistuva havainnointi on tilanteessa vapaasti muotoutuvaa ja havainnoija on osa ryhmän toimintaa ja toimii ryhmässä jäsenenä.
Osallistumisen asteeni oli pääsääntöisesti täydellinen osallistuminen, eli työskentelin samassa ryhmässä työntekijöiden kanssa. Eettisiä ongelmia tämä ei aiheuttanut, sillä osallistujat olivat tietoisia asemastani tietosuojavastaavana. Toiminta oli siten läpinäkyvää ja monessa työryhmässä olin mukana juuri tässä roolissa.
Oli myös tilanteita, joissa oma roolini oli enemmän havainnoiva osallistuja. En niinkään osallistunut itse työhön vaan seurasin sen etenemistä tietosuojan näkökulmasta ja tarvittaessa nostin esille mahdollisia kehittämiskohteita tai esitin

tarkentavia kysymyksiä. Nämä perustuivat tulkintaani asian etenemisestä ja sen yhteensopivuudesta vallitsevan tietosuojan normiston kanssa.
Työskentelymallina tämä havaittiin yleisesti varsin tehokkaaksi. Tämä mahdollisti jo asian valmistelun alkuvaiheessa mahdollisten ongelmien ennakoinnin.

2.2 Lähteet

Tietosuojaan liittyvät kirjallisuuslähteet voidaan jakaa karkeasti kolmeen eri luokkaan: tietosuojan juridiikkaan keskittyviin, tietoturvallisuuden johtamiseen liittyviin tai tekniseen tietoturvallisuuteen keskittyviin lähteisiin.
Näistä etenkin juridiikkaan keskittyvää kirjallisuutta on saatavilla erittäin hyvin. Jopa yksittäisistä juridisista kysymyksistä on julkaistu omia kirjojaan. Näiden lähteitä on tässä työssä hyödynnetty lähinnä yksittäisissä asioissa, joissa sääntely on erityisen monimutkaista, kuten esimerkiksi tietopyyntöjä käsittelevässä osassa. Näissä pyrin löytämään uusimman saatavilla olevan kirjan.

Tietoturvallisuuden johtamiseen (ml. riskienhallinta, hallinnolliset menettelyt) on kirjallista materiaali saatavilla melko rajoitetusti. Tähän liittyvä kirjallisuus ja tieto on käytännössä siirtynyt verkkoon suurelta osin. Koska työni keskittyy ennen kaikkea tietosuojan hallintaan (johtamiseen) on tämä kuitenkin työni kannalta keskeisin osa-alue. Tässä käyttämäni lähteet ovat vanhoja mutta niistä otetut asiat eivät sinällään ole muuttuneet miksikään. Juha E. Miettisen Tietoturvallisuuden johtaminen (. Miettinen Juha. E, Tietoturvallisuuden johtaminen, Gummerus, 1999, Jyväskylä) ja Yritysturvallisuuden käsikirja (Miettinen Juha. E, Yritysturvallisuuden käsikirja, Kauppakaari. 2002. Helsinki) sekä Juha Leppäsen Yritysturvallisuus käytännössä (Leppänen, J. 2006. Yritysturvallisuus käytännössä. Jyväskylä. Gummerus kirjapaino Oy) sisältävät käytännössä samat asiat kuin nykyisin riskienhallinnan (turvallisuusjohtamisen) tämän hetkinen ”ykkösteos” Paul Hopkinin Fundamentals of risk management (Hopkin P. Fundamentals of risk management 5th edition, 2018, Kogan page limited, USA). Itselläni oli käytössä tuo viides painos. Tästä on julki jo kuudeskin painos mutta siinä isoimmat muutokset liittyivät lähinnä COVID-19 pandemian hallintaan. Joulukuussa 2024 on tulossa laajemmin päivitetty seitsemäs painos kirjasta. Se ei ollut tätä kirjoitettaessa siis vielä saatavilla. Käytin siis lähteinä näitä minulle tuttuja kirjoja ja tarkistin asioiden paikkansa pitävyyden ristiin vertailemalla asiaa saatavilla oleviin uudempiin lähteisiin (uudemmat kirjat, verkkolähteet).

Suurin osa tiedosta tähän työhön löytyi verkosta. Tässä pyrin tietoisesti rajaamaan kaikkea saatavilla olevaa tietoa viranomaisiin sekä muuten luotettaviin lähteisiin. Tietosuojasta löytyy hyvää ja tarkkaa tietoa paljon, mutta monen sivuston ongelmana on, että lähdettä tai tiedon alkuperää tai oikeellisuutta ei pysty varmistamaan. Blogit, yksityisten tahojen verkkosivustot, keskustelupalstat ja erilaiset foorumit ovat mainio tapa hankkia paljon tietoa jostain asiasta lyhyessä ajassa. Näissä kuitenkin tiedon oikeellisuuden varmistaminen (onko kysymys faktasta vai henkilön omasta tulkinnasta? disinformaatio, jne.), konteksti ja lähtökohdat ratkaisulle jäävät usein mahdottomiksi selvittää. Näistä syistä tein tiedonhaussa rajauksen ja käytin vain ns. luotetun tahon lähteitä.
Muutamia mediassa olleita uutisia käytin lähinnä esimerkkeinä tietoturvapoikkeamista soveltuvissa kohdin.

Olen kouluttautunut tietosuojan saralla aiemmin Turun yliopiston Snellman -kesäyliopistossa (Tietosuojavastaavan peruskoulutus), Itä-Suomen yliopistossa (Osaava tietosuojavastaava erikoistumisopinnot) sekä viimeisimpänä Jyväskylän yliopistossa (Johdatus tiedusteluun) sekä useisiin seminaareihin ja ajankohtaispäiviin. Näistä koulutuksista on kertynyt paljon luennoitsijoiden materiaalia ja hyödynsin myös näitä työssäni soveltuvin osin. Nämä materiaalit katson luotettaviksi lähteiksi.

Theseuksesta löysin hakusanalla tietosuoja 14 opinnäytetyötä. Tietosuojan hallintamallia ei tämän haun mukaan oltu aiemmin käsitelty. Muutamassa opinnäytteessä oli hyviä asiaan liittyviä seikkoja ja käytin näitä työssäni.

3 Miksi tietosuojasta tulee huolehtia?

Tietoja henkilöistä rekisteriin keräävä taho on lähtökohtaisesti vastuussa siitä, että hän kerää vain niitä tietoja, joita hän on oikeutettu keräämään ja käyttämään keräämiään tietoja vain niihin tarkoituksiin, joihin rekisteröity on antanut hyväksyntänsä. Tietosuojavaltuutetun toimisto määrittelee tietosuojan seuraavasti:

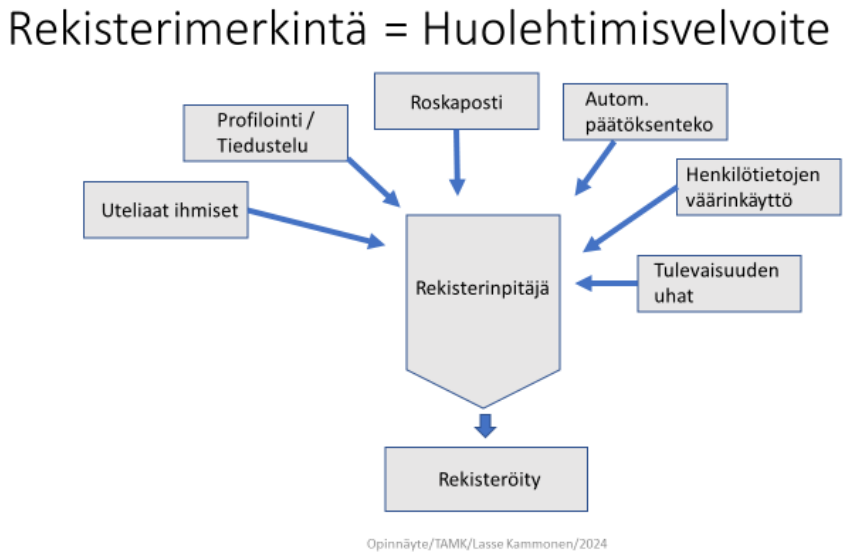
” *Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä. Tietosuojan tarkoituksena on osoittaa, milloin ja millä edellytyksillä henkilötietoja voidaan käsitellä.”*
(https://tietosuoja.fi/tietosuoja)

Tietosuojalaki (5.12.2018/1050) ja Laki yksityisyyden suojasta työelämässä (13.8.2004/759) säätelee työntekijän, työnhakijan ja virkasuhteisen henkilön asemassa olevien henkilötietojen käsittelyä huomattavasti yksityiskohtaisemmin. Näiden lisäksi Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, josta yleisemmin käytetään nimitystä tietosuoja-asetus asettaa omalta osaltaan vaatimuksia henkilötietojen käsittelylle.

Rekisterinpitäjän näkökulmasta kysymys on kuitenkin, paitsi lain noudattamisesta myös toiminnan jatkuvuuden turvaamisesta ja maineenhallinnasta. Erilaiset tietosuojaloukkaukset tai tietosuojaan liittyvät häiriötilanteet voivat aiheuttaa merkittäviä keskeytyksiä toimintaan. Nämä kiinnostavat myös mediaa ja vaikuttavat merkittävästi siihen, miten luotettavana tahona rekisteriä ylläpitävää organisaatiota pidetään. Vakavan mainehaitan toteutuminen tietosuojassa vaikeuttaa usein organisaation toimintaa pitkään monella eri tavalla. Laajoissa, paljon julkisuutta saaneissa tapauksissa maineen luotettavana tahona palauttaminen voi olla erittäin vaikea ja pitkä prosessi. Jopa koko toiminnan jatkuvuus voi olla vaakalaudalla. Tästä esimerkkinä Psykoterapiakeskus Vastaamon tapaus (https://fi.wikipedia.org/wiki/Vastaamon_tietomurto) joka oli jopa maailmanlaajuisesti poikkeuksellisen laaja. Tietosuojaloukkaukset tapahtuivat vuosina 2018-2020. Tapauksen oikeudenkäynnit jatkuvat edelleen tätä kirjoitettaessa, itse yritys on selvitystilassa ja kaikkia vahinkoja, joita tapahtunut aiheutti ei varmasti koskaan tulla saamaan selville.

4. Miltä uhilta rekisteröityä suojellaan?

Kun rekisterinpitäjä päättää perustaa rekisterin tulee hänen tiedostaa, että samalla hän ottaa myös vastuun rekisteröityjen yksityisyydensuojasta. Epäonnistuminen tämän vastuun hoitamisessa voi johtaa merkittäviin oikeudellisiin vastuisiin, vahingonkorvauksiin ja vahingoittaa rekisterinpitäjän mainetta pitkäksi ajaksi eteenpäin. Vastaavasti onnistuminen luo luotettavaa kuvaa rekisterinpitäjästä. Alla olevassa kuvassa on koottu niitä asioita, joilta rekisterinpitäjän tulee rekisteröityä suojella.



Kuvio 1. Rekisterinpitäjän huolehtimisvelvoitteet

4.1 ”Uteliaat ihmiset”

Valitettavasti kaikki ihmiset, joilla on pääsy henkilörekistereihin eivät omaa riittävän korkeaa moraalia ja ammattietiikkaa käyttääkseen tietoja vain niihin tarkoituksiin, joihin ne on kerätty. Inhimillinen uteliaisuus on yleisin motiivi, mutta nämä voivat joskus olla epäselviä. Tästä esimerkkinä silloisen pääministeri Marinin tietojen katselu Helsingin ja Uudenmaan sairaanhoitopiirissä kaksoiskansalaisen toimesta (https://www.mtvuutiset.fi/artikkeli/sk-marinin-hallituksen-ministerin-terveystietoja-urkittu-husissa-epailty-on-suomen-ja-venajan-kaksoiskansalainen/8689902). Tämä ongelma on erityisen hankala järjestelmissä, jotka eivät pidä yllä lokia tapahtumista. Jos henkilöstö tietää tämän se tietää myös, että rekisterin käyttö omiin tarkoituksiin on käytännössä mahdollista. Kiinnijäämisen riski oikeudettomasta tietojenkatselusta on pieni ja se on erittäin vaikea näyttää

toteen myöhemmin. Rekistereissä tulee olla automaattinen logitus järjestelmä tämän riskin hallitsemiseksi. Se ei vielä tee järjestelmästä aukotonta mutta helpottaa asioiden selvittelyä jälkikäteen merkittäväksi. Asian selvittelylle on ainakin jokin lähtökohta. Tehokkainta on rajata käyttöoikeuksia siten, että rajaavat saatavilla olevan tiedon määrää tai sen hakemista.

4.2 Profilointi ja tiedustelu

Kuluttajien profilointi on yleistynyt digitaalisten alustojen kasvun ja kehityksen myötä. Data-analytiikka ja tekoäly ovat mahdollistaneet massiivisen datan keräämisen ja analysoimisen. Erilaisista rekistereistä on saatavilla tietoa esimerkiksi kuluttajien kulutustottumuksista ja mieltymyksistä, joiden perusteella voidaan profiloida kuluttajia. Tämä voi osaltaan asettaa kuluttajia eriarvoiseen asemaan.

Vakuutusyhtiöt käyttävät melko laajasti profilointia vakuutusriskin arvioimiseen, tätä tutki Mikael Nuotio kandidaatin työssään Aalto yliopistolle. (Mikael Nuotio, Profilointi ja vakuutusriskin arviointi, Aalto-yliopisto, 2023). Tämä on pääsääntöisesti sallittua mutta kovin moni ei ole tästä tietoinen. Tietosuojavaltuutetun toimisto on kiinnittänyt huomiota tähän toimintaan. Hiljattain tuli ulos Hallinto-oikeuden päätös koskien vakuutusyhtiöiden oikeutta käsitellä ja saada haltuunsa terveystietoja vakuutuksen hakemisvaiheessa (https://tietosuoja.fi/-/hallinto-oikeus-piti-voimassa-tietosuojavaltuutetun-paatokset-vakuutusyhtioiden-terveystietojen-kasittelysta).

Profilointia käytetään laajasti kaikessa liiketoiminnassa ja eri hallinnonaloilla mitä erilaisimpiin tarkoituksiin. Myös käytettävät menetelmät ja niiden laajuus vaihtelevat eri toimijoiden ja profiloinnin tarkoitusperien mukaan. Profiloinnille ja tiedustelulle yhteistä on kerätä tietoa kohteesta, analysoida kyseinen tieto käytettävään muotoon ja käyttää sitä apuna päätöksenteossa. Rekisterinpitäjän kannalta on erityisen tärkeää varmistaa, että rekisteröidyn tiedot eivät joudu sellaisten käsiin, jotka eivät ole siihen oikeutettuja tai, että tietoa käytettäisiin muuhun tarkoitukseen kuin mihin rekisteröity on antanut suostumuksensa (ellei muuta oikeutusperustetta ole). Erityistä huomiota on kiinnitettävä, jos kerätään erityisen arkaluonteista tietoa, rekisteröityjen joukossa on henkilöitä, jotka voivat

asemansa puolesta olla median kiinnostuksen, vihamielisen vaikuttamisen tai mahdollisen hyväksikäytön kohteena.

4.3 Roskaposti

Rekisteröityjen sähköpostiosoitteet, profiilitiedot, puhelinnumerot sekä sijainti tiedot kiinnostavat monia kaupallisia toimijoita. He käyttävät näitä eri tavoin markkinoinnissaan ja nämä tiedot ovat varsin yleistä kauppatavaraa. Samoin verkkoalustojen ylläpitäjät keräävät näitä tietoja käyttäjistään ja mahdollistavat siten kohdennetun markkinoinnin käyttäjäprofiiliin perustuen alustoillaan. Isolle osalle ilmaisien verkkoalustojen ylläpitäjistä tämä on merkittävä tulonlähde. Rekisterinpitäjän olisi hyvä tiedottaa tästä avoimesti mutta valitettavasti näin ei usein ole. Etenkin EU/ETA alueen ulkopuoliset toimijat tiedottavat siitä, mihin tietoja itse asiassa käyttävät vaihtelevasti.

4.4 Automaattinen päätöksenteko

Automaattinen päätöksenteko on prosessi, jossa päätökset tehdään ilman ihmisen aktiivista osallistumista, käyttämällä erilaisia teknologioita, kuten tekoälyä (AI), koneoppimista ja sääntöpohjaisia järjestelmiä. Tämä on usein nopeampaa, tarkempaa ja objektiivisempaa verrattuna perinteisiin, manuaalisiin menetelmiin. Siinä päätöksentekoon liittyy kiinteästi myös jonkinlainen profilointi eli päätöksenteon kohteesta kerätään tarvittava informaatio ja tämän informaation pohjalta tehdään päätös siten, että ihminen ei ole mukana ratkaisussa.

Tietosuojavaltuutetun toimiston kriteerit (päätöksillä ei ole merkittäviä oikeusvaikutuksia tai muita vaikutuksia kohteelle) automaattiselle päätöksenteolle eivät toistaiseksi tarkastelemissani rekistereissä täyttyneet. Asiasta on ollut tosin keskustelua lähinnä markkinointiin ja muuhun viestintään liittyen, mutta toistaiseksi sen suhteen ei ole ryhdytty toimenpiteisiin. Mikäli automaattista päätöksentekoa aiotaan ryhtyä ottamaan käyttöön, tulee se toteuttaa normien ja suositusten mukaisesti. Tietosuojavaltuutetun sivuilla (https://tietosuoja.fi/automaattinen-paatoksenteko-profilointi) on tähän hyvät ohjeet. Huomioitavia seikkoja ovat:

- Välttämättömyyskriteeri
- Rekisteröidyn suostumus
- Rekisteröidyn informointi tämän oikeuksista

- Vaihtoehtoisten menetelmien tarjoaminen
- Valitusten mahdollistaminen
- Käytettävien tietojen oikeellisuuden varmistaminen ja algoritmien säännöllinen seuranta
- Mahdollistettava lisäselvitysten toimittaminen

Edellä mainittujen lisäksi on erityisesti markkinointiin liittyvässä automaattisessa päätöksenteossa ja profiloinnissa kiinnitettävä huomiota profilointimenetelmien tunkeilevuuteen.
Toinen huomioitava seikka, johon kyseisessä yhdistyksessä on syytä kiinnittää erityistä huomiota, on valittavien algoritmien tasapuolisuus kaikkia kohtaan. Algoritmi ei saa asettaa rekisteröityjä eriarvoiseen asemaan tai syrjiä ketään.

4.5 Tietosuoja ja avointen lähteiden tiedustelu (OSINT, SOCMINT)

Monilla eri tahoilla on intressejä hankkia tietoa jostain henkilöstä. Nämä tarkoitusperät voivat olla esimerkiksi kaupallisia, ne voivat liittyä jonkin työtehtävän suorittamiseen tai vaikkapa työnhakijan taustojen selvittämiseen. Erityisesti työnhakijaan kohdistuva tiedonhaku Internetistä on juridisesti hieman ristiriitaista erityisesti, jos hausta saaduista tiedoista ei muodosteta rekisteriä vaan käytetään ainoastaan päätöksenteon tukena.
Valitettavasti tiedonhaku jostain henkilöstä voi olla myös pahantahtoista eli tarkoituksena on löytää henkilöstä tietoa, jota voidaan käyttää hänen vahingoittamisekseen tavalla tai toisella. Nämä voivat liittyä esimerkiksi yksityiselämän ristiriitatilanteisiin, henkilön painostamiseen tai kiristämiseen tai muuhun epäasialliseen käytökseen sekä maalittamiseen. Tämä voi joskus olla huomattavasti perinteistä hakukoneiden palveluja laajempaa ja ammattimaisempaa toimintaa. Tällaisesta toiminnasta käytetään termejä OSINT ja SOCMINT.

4.5.1 Avointen lähteiden tiedustelu (OSINT)

Avointen lähteiden tiedustelu (OSINT, engl. Open Source Intelligence) on prosessi, jossa kerätään ja analysoidaan julkisesti saatavilla olevaa tietoa eri lähteistä (Johdatus tiedusteluun. 2024. Verkkokoulutus 2op. Jyväskylän yliopisto. 5.1.2024. Koulutusmateriaali). Tällainen tieto voi sisältää verkkosivustoja, sosiaalisen median sisältöä, julkisia rekistereitä, tiedotusvälineitä, akateemisia julkaisuja ja muita julkisia tietolähteitä. Avointen lähteiden tiedustelu on tärkeä osa

tiedustelutoimintaa, ja sitä käytetään laajasti niin valtiollisissa kuin ei-valtiollisissa organisaatioissa erilaisiin tarkoituksiin, kuten turvallisuus- ja tiedustelutehtävissä, liiketoimintatiedustelussa, journalistisessa tutkimuksessa ja akateemisessa tutkimuksessa.

Avointen lähteiden tiedustelun merkitys on kasvanut merkittävästi internetin ja sosiaalisen median yleistymisen myötä. Tietoa on nyt saatavilla valtavia määriä eri lähteistä, ja asianmukaisella analyysillä voidaan saada arvokasta tietoa erilaisiin tarkoituksiin. Avoin tiedonkeruu voi olla erityisen hyödyllistä tilanteissa, joissa muut tiedustelu keinot ovat rajallisia tai hankalia toteuttaa.
Avointen lähteiden tiedustelu voi kuitenkin herättää myös eettisiä kysymyksiä, erityisesti yksityisyydensuojan ja tietoturvan näkökulmasta. On tärkeää varmistaa, että tiedonkeruu ja -analyysi toteutetaan lain ja eettisten periaatteiden mukaisesti, ja että kerättyä tietoa käytetään vain asianmukaisiin tarkoituksiin. Lisäksi on tärkeää olla tietoinen siitä, että julkisesti saatavilla oleva tieto voi olla virheellistä tai harhaanjohtavaa, joten tiedon arviointi ja tulkinta ovat keskeisiä osia avointen lähteiden tiedusteluprosessia.

4.5.2 Sosiaalisen median tiedustelu (SOCMINT, SMT)

Sosiaalisen median tiedustelu on prosessi, jossa kerätään, analysoidaan ja hyödynnetään sosiaalisen median alustoilla ja verkostoissa jaettua tietoa (Johdatus tiedusteluun. 2024). Se mielletään useimmiten osaksi avointen lähteiden tiedustelua, mutta sen merkitys on kasvanut niin suureksi, että se on mielekästä eriyttää jo omaksi osakseen. SOCMINT:stä on tullut oleellinen osa tiedustelutoimintaa, markkinointia, maineen hallintaa sekä turvallisuutta aloilla, jotka hyötyvät julkisesta tiedosta, joka jaetaan sosiaalisessa mediassa. Sosiaalisen median tiedustelu on voimakkaasti kasvava ala, joka tarjoaa valtavia mahdollisuuksia monille eri organisaatioille ja toimialoille. On kuitenkin tärkeää käyttää sitä vastuullisesti ja kunnioittaen yksityisyyttä ja muita eettisiä periaatteita. Lisäksi on olennaista kehittää jatkuvasti tietoturvakäytäntöjä ja -tekniikoita vastatakseen yhä monimutkaisempiin verkkouhkiin.
Nämä ovat usein tietoja, jotka henkilö itse jakaa erilaisilla sosiaalisen median alustoilla mutta eivät aina. Erityisesti erilaiset henkilöön yhdistettävät aika- ja paikkatiedot, verkkokauppojen markkinoinnissa käytettävät ”asiakkaiden suositukset” ostetuista tuotteista, jne. voivat olla erinomainen tiedonlähde henkilöä

profiloivalle tai muuhun tarkoitukseen tietoja keräävälle taholle. Tällaista toimintaa ylläpitävän tulee huolehtia siitä, että käyttäjä on ainakin tietoinen siitä mihin hänen tietojaan julkaistaan. Valitettavasti näin ei aina ole.

5 Tietosuoja osana organisaation turvallisuuden kokonaisuutta

Organisaation turvallisuuden kokonaisuuden hallintaa kutsutaan monilla nimillä. 90 -luvun loppupuolella oli vallalla Elinkeinoelämän keskusliiton käyttämä termi yritysturvallisuus. Tätä käytetään edelleen varsin laajalti, mutta termi rajaa tarpeettomasti pois organisaatiot, jotka eivät ole yrityksiä. Juha Leppänen käytti kirjassaan Yritysturvallisuus käytännössä (Leppänen, J. 2006. Yritysturvallisuus käytännössä. Jyväskylä. Gummerus kirjapaino Oy) organisaatioturvallisuus. Tämä termi kattaa laajemman piirin. Se soveltuu yhdistyksille ja yhteisöille, julkishallinnon organisaatioille ja vastaaville paremmin ja on nykyään yleisesti käytössä.

Näillä kaikilla kuitenkin tarkoitetaan käytännössä samaa asiaa. Luodaan kokonaiskuva organisaation turvallisuudesta ja siten mahdollistetaan turvallisuuden johtaminen.

Kuvio 2. Yritysturvallisuus (https://ek.fi/hyotytietoa-yrityksille/yritysturvallisuus/ 1.4.2024)

Kuvassa 2 on Elinkeinoelämän keskusliiton kuva yritysturvallisuuden osa-alueista. Se miten eri turvallisuuden osa-alueet painottuvat missäkin organisaatiossa vaihtelee voimakkaasti, mutta käytännössä lähes kaikissa organisaatioissa on otettava huomioon ja arvioitava kaikki turvallisuuden osa-alueet.

Menettelyä, jossa eri turvallisuuden osa-alueiden painopisteitä arvioidaan, kutsutaan riskienhallinnaksi. Juha Leppänen (Leppänen. J., 2006) määrittelee riskienhallinnan kokonaisvaltaiseksi prosessiksi, jonka tavoitteena on hallita tunnistettuja riskejä.

On tärkeää huomata, että turvallisuuden osa-alueet organisaatiossa ovat usein riippuvaisia toisistaan. Turvallisuutta ei voi hallita tai johtaa tarkastelemalla vain sen yksittäisiä osia, vaan on huomioitava kokonaisuus ja asioiden joskus monimutkaiset sidonnaisuudet ja riippuvuudet.
Tietosuoja on suoraan sidoksissa seuraaviin osa-alueisiin:

- Tietoturvallisuuteen
- Toimitila- ja kiinteistöturvallisuuteen
- Väärinkäytösten ja poikkeamien hallintaan
- Henkilöstöturvallisuuteen
- tuotannon- ja toiminnan turvallisuuteen

Lisäksi välillisiä vaikutuksia voi olla työturvallisuudessa (ilmapiiri, juoruilu, kiusaaminen) sekä varautumisessa ja kriisinhallinnassa (henkilöiden sijoitukset ja tehtävät poikkeus oloissa). Kun tietosuojan toimintatapoja ja menettelyjä kehitetään työpaikalla on tärkeää huomioida miten, tietosuoja osaltaan tukee muita osa-alueita ja miten muut osa-alueet puolestaan tukevat tietosuojaa.

6 Vaikutusten arviointi eli DPIA

Tietosuoja vaikutusten arviointi (DPIA, Data Protection Impact Assesment) on prosessi, jonka tarkoituksena on auttaa organisaatioita tunnistamaan ja minimoimaan hankkeen tietosuojaan liittyvät riskit. DPIA on tärkeä silloin, kun hanke sisältää henkilötietojen käsittelyä, joka voi aiheuttaa suuria riskejä yksilöiden oikeuksille ja vapauksille.
Pohjimmiltaan vaikutusten arviointi on riskienarviointia, jossa tarkastellaan henkilötietojen keräämiseen, käsittelyyn ja käyttöön liittyviä riskejä. Tarkastelu tapahtuu sekä organisaation, että rekisteröidyn näkökulmasta.

Ensimmäinen vaihe DPIA -menettelyssä on tunnistaa tilanteet, joissa se on tehtävä. Mikäli rekisteri, jota ollaan tekemässä täyttää lainsäädännön määrittämät reunaehdot henkilörekisterille, on lähtökohtaisesti vaikutusten arviointi hyvä toteuttaa. Tällä organisaatio voi myös osoittaa tahtotilaansa suojata rekisteröityjen tietoja ja toimia hyvän tavan mukaisesti. Tietosuojavaltuutetun toimisto (https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista), edellyttää vaikutusten arviointia, vaikka muut kriteerit eivät täyttyisikään jos käsiteltävät tiedot ovat biometrisiä, geneettisiä tai sijaintitietoja tietyin edellytyksin. Samoin jos rekisteröidyn informoinnista poiketaan on vaikutusten arviointi laadittava.

Toisessa vaiheessa kuvataan tietojenkäsittelyn luonne, laajuus, konteksti ja tarkoitukset. Tähän sisällytetään yksityiskohdat kerättävistä tiedoista, rekisteröidyistä henkilöistä ja siitä, miten tietoja käsitellään.

Kolmas vaihe on kuulla sidosryhmiä ja yhteistyötahoja. Osallistutaan sisäisiin ja ulkoisiin sidosryhmiin, mukaan lukien rekisteröidyt henkilöt ja tietosuojavaltuutetut ja kerätään näkemyksiä suunnitelluista tietojenkäsittelytoimenpiteistä.

Neljäntenä on välttämättömyyden ja suhteellisuuden arviointi. Organisaation täytyy kyetä perustelemaan miksi se kerää tietoja ja miksi juuri näiden tietojen kerääminen on välttämätöntä. Tietojen keräämisen ja käsittelyn täytyy olla oikeassa suhteessa rekisteröidyille koituviin mahdollisiin haittoihin. Perusteluista on

myös selvittävä olisiko muita, rekisteröidylle vähemmän haitallisia tapoja mahdollista käyttää.

Viides vaihe on riskien tunnistaminen ja arviointi. Tietosuojaan liittyvä lainsäädäntö edellyttää arvioimaan rekisteröidyille aiheutuvia riskejä. Tässä kohtaa on perusteltua arvioida samalla myös organisaatiolle rekisterinpidosta aiheutuvat riskit. Tähän on saatavilla ohjeita Tietosuojavaltuutetun toimiston sivuilta (https://tietosuoja.fi/vaikutustenarviointi) ja erilaisia kaupallisia menetelmiä. Kohde organisaatiossa tämä tehtiin osin omin voimin, osin käytettiin ulkopuolista asiantuntija apua.
Tunnistetut riskit arvioidaan kahden ulottuvuuden kautta, riskin toteutumisen todennäköisyyden ja riskin mahdollisten seurausten yhdistelmän avulla. Tähän on olemassa useita eri työkaluja ja tapoja. Olennaista on, että käytössä on työkalu joka tarkastelee näitä molempia ulottuvuuksia.

Kuudentena vaiheena on päättää toimenpiteistä tunnistettujen ja arvioitujen riskien hallitsemiseksi. Tässä keinoina voi olla:

- Tietojen minimointi
- Pseudonymisointi tai anonymisointi
- Salaus ja pääsyoikeuksien hallinta
- Kerättävän tiedon rajaaminen tai muuttaminen vähemmän haitalliseksi

Toimenpiteiden tulee olla sellaisia, että jäännösriski jää hyväksyttävälle tasolle.

Seitsemäs vaihe on DPIA-prosessin dokumentointi. Kirjaa ylös jokaisen vaiheen tulokset, mukaan lukien tunnistetut riskit, lieventämistoimenpiteet ja mahdolliset päätökset. Tämä dokumentointi on olennaista vastuullisuuden kannalta ja tietosuojaviranomaiset saattavat pyytää sitä nähtäväkseen.

DPIA tulee pitää ajan tasalla. DPIA:n suorittaminen ei ole vain oikeudellinen vaatimus asetuksissa kuten GDPR, vaan myös paras käytäntö varmistaaksesi, että tietosuojaan liittyvät riskit hallitaan ennakoivasti. Se on yksi tapa osoittaa organisaation sitoutuneen henkilötietojen suojaamiseen ja yksilöiden yksityisyyden kunnioittamiseen.

7 Keskeiset käsitteet

7.1 Tietosuoja

Tietosuoja on perusoikeus, joka koskee yksilön oikeutta hallita henkilökohtaisia tietojaan ja suojella niiden luottamuksellisuutta. Se on keskeinen käsite nykyaikaisessa yhteiskunnassa, jossa teknologian kehitys ja digitaalisen tiedon kasvava käyttö lisäävät yksityisyyden haavoittuvuutta. Tietosuoja liittyy myös ihmisten perusoikeuksiin ja yksityisyyden suojaan. Sitä säädellään lailla ja määräyksillä, jotka pyrkivät varmistamaan, että henkilökohtaiset tiedot säilytetään turvallisesti ja niitä käsitellään asianmukaisesti. Tietosuojavaltuutetun toimisto määrittelee tietosuojan seuraavasti: ”Tietosuoja on perusoikeus, joka turvaa rekisteröidyn oikeuksien ja vapauksien toteutumisen henkilötietojen käsittelyssä” (**https://tietosuoja.fi/tietosuoja**).

Teknologian kehitys on tehnyt henkilökohtaisten tietojen keräämisestä, tallentamisesta ja jakamisesta helpompaa kuin koskaan aiemmin. Digitaaliset alustat, älylaitteet ja verkkopalvelut keräävät jatkuvasti tietoa käyttäjistään, kuten sijainti tietoja, ostoskäyttäytymistä, terveystietoja ja henkilökohtaisia viestejä. Tämä tieto voi olla arvokasta sekä yrityksille että rikollisille.

Tietosuoja on tärkeä yhteiskunnassa, jossa digitalisaatio on laajentunut kaikille elämänalueille, mukaan lukien terveydenhuolto, talous, viestintä ja viranomaistoiminta. Esimerkiksi terveysalan digitalisaatio on tuonut mukanaan mahdollisuuksia kerätä ja analysoida suuria määriä potilastietoja, mikä voi parantaa hoitotuloksia ja terveydenhuollon tehokkuutta. Samalla se kuitenkin herättää kysymyksiä siitä, miten näitä tietoja käytetään, ja miten varmistetaan, että ne säilyvät turvassa ja että potilaiden yksityisyys säilyy.

7.2 Henkilötieto

Tietosuojavaltuutetun toimisto (https://tietosuoja.fi/mika-on-henkilotieto) määrittelee henkilötiedon seuraavasti:

”Henkilötietoja ovat sellaiset tiedot, joiden perusteella henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistämällä yksittäinen tieto johonkin toiseen tietoon, joka mahdollistaa tunnistamisen.”

Tietosuojavaltuutetun toimisto listaa esimerkkeinä seuraavat:

- Nimi

- Osoite
- etunimi.sukunimi tyyppinen sähköposti osoite
- Puhelinnumero
- Henkilökortin numero
- Ajoneuvon rekisteritunnus
- Paikannustiedot
- IP -osoite
- Potilastiedot
- Lemmikin eläinlääkäritiedot
- Perinnöllisiä sairauksia koskevat tiedot

Henkilötietoja ovat siis kaikki tiedot, jotka liittyvät yksilöön ja joista voidaan päätellä hänen henkilöllisyytensä tai joista johtaa hänet voidaan tunnistaa

Henkilötiedon käsite on siis laaja, ja sen soveltaminen käytännössä voi olla monimutkaista, erityisesti tilanteissa, joissa tietoja yhdistellään tai käsitellään eri tavoin. Tärkeää onkin ymmärtää, että henkilötietoja ei ole pelkästään perinteisissä asiakirjoissa tai tietokannoissa, vaan niitä voi olla myös digitaalisissa järjestelmissä, verkkopalveluissa, älylaitteissa ja muilla alustoilla.

Organisaatiot ja yritykset, jotka käsittelevät henkilötietoja, ovat velvollisia noudattamaan GDPR:n vaatimuksia, kuten tietosuojaperiaatteita, turvallisuusvaatimuksia ja yksilön oikeuksia koskevia säännöksiä. Tämän tarkoituksena on varmistaa, että henkilötietoja käsitellään asianmukaisesti ja että yksilöiden yksityisyys ja oikeudet turvataan.

7.3 Tietosuojavastaava

Tietosuojavastaavalla on keskeinen rooli tietosuojan hallinnassa. Tietosuojavastaavan tehtävänä on toimia sisäisenä asiantuntijana organisaatiossa tietosuoja asioissa sekä toimia myös yhteyshenkilönä viranomaisiin päin. Tietosuojavastaavan nimike on hieman harhaanjohtava. Tietosuojavastaavalla ei ole juridista vastuuta tietosuojasta. Tämä vastuu on aina organisaatiolla ja rekisterinpitäjällä.

Tietosuojavaltuutetun toimisto (https://tietosuoja.fi/tietosuojavastaavat) listaa tietosuojavastaavan tehtävät seuraavasti:

- seuraa tietosuojasääntöjen noudattamista koko organisaatiossa ja tuo esiin havaitsemiaan puutteita
- antaa tietoja ja neuvoja tietosuojasääntöjen mukaisista velvollisuuksista johdolle ja henkilötietoja käsitteleville työntekijöille
- antaa pyydettäessä neuvoja tietosuojan vaikutustenarvioinnin tekemisestä ja valvoo vaikutustenarvioinnin toteutusta
- on rekisteröityjen yhteyshenkilö henkilötietojen käsittelyyn liittyvissä asioissa
- on tietosuojavaltuutetun toimiston yhteyshenkilö ja tekee yhteistyötä tietosuojavaltuutetun toimiston kanssa.

Harto Pönkä listaa luennollaan Tietosuojavastaavien peruskoulutuksessa (Pönkä, H. Innowise. 2020. Tietosuojavastaavan tehtävä ja henkilötietojen käsittelyn perusteita. Luento. Tietosuojavastaavien peruskoulutus. Snellman -kesäyliopisto. 3.12.2020. Verkkoluento) tietosuojavastaavan nimeämisestä, että sellainen on nimettävä kun:

- Rekisterinpitäjä on julkishallinnon toimija
- Tietojen käsittely on laajamittaista tai kohdistuu erityisiin henkilötietoryhmiin
- Organisaatio niin haluaa

GDPR määrittelee tietosuojavastaavan roolin organisaation tietosuojakulttuurin ja -käytäntöjen kehittämisessä ja ylläpidossa. Tietosuojavastaava toimii linkkinä organisaation ja tietosuojaviranomaisten välillä ja vastaa tietosuojan valvonnasta ja toteuttamisesta organisaatiossa. Tässä muutamia keskeisiä tehtäviä, joita tietosuojavastaavalla voi olla:

- Tietosuojakäytäntöjen kehittäminen ja valvonta. Tietosuojavastaavan tehtäviin kuuluu tietosuojakäytäntöjen kehittäminen ja niiden valvonta organisaatiossa.
- Tietosuojakoulutus ja -ohjaus. Tietosuojavastaava vastaa usein myös tietosuojakoulutuksesta ja -ohjauksesta organisaatiossa.
- Tietosuojaselosteiden ja -sopimusten hallinta. Tietosuojavastaava vastaa tietosuojaselosteiden ja -sopimusten hallinnasta. Tämä voi sisältää tieto-

suojaselosteiden laatimisen ja ylläpidon sekä tietosuojasopimusten tekemisen ja valvonnan kolmansien osapuolten kanssa, kuten alihankkijoiden ja palveluntarjoajien kanssa.

- Tietoturvan ja tietosuojan valvonta. Tietosuojavastaava seuraa ja valvoo organisaation tietoturvan ja tietosuojan tilannetta. Tämä voi sisältää tietoturva- ja tietosuoja-asioiden seurannan, tietoturvaloukkausten raportoinnin ja niihin vastaamisen sekä riskienhallinnan ja -arvioinnin suorittamisen.
- Yhteydenpito tietosuojaviranomaisiin. Tietosuojavastaava toimii yhteyshenkilönä tietosuojaviranomaisiin. Hän vastaa tietosuojaviranomaisten tiedusteluihin ja tiedonantovelvollisuuksiin ja toimii tarvittaessa yhteistyössä viranomaisten kanssa.

Tietosuojavastaavan tehtävään ei ole määritetty koulutusvaatimusta. Käytännössä tehtävän hoitaminen vaatii kuitenkin huomattavaa perehtyneisyyttä tietosuojaan liittyvään sääntelyyn, tietosuojan toimintamalleihin sekä organisaation toimintaan. Tietosuojavastaavan tehtävä on varsin itsenäinen ja hänellä ei ole velvoitetta ottaa ohjeita vastaan. Tietosuojavastaava ei voi olla organisaatiossa asemassa, jossa hän tekee päätöksiä tai on muuten vastuullinen rekisterin normien mukaisuudesta.

7.4 Rekisterinpitäjä

Rekisterinpitäjä on vastuussa tietosuoja- asetuksen mukaisesta toiminnasta. Hänen roolina on huolehtia, että henkilötietoja käsitellään lainmukaisesti organisaatiossa koko sen elinkaaren ajan.

Tietosuojavaltuutetun toimisto (https://tietosuoja.fi/henkilotietojen-kasittelyn-roolit-ja-vastuut) määrittelee rekisterinpitäjäksi sen, joka määrittelee henkilötietojen käsittelyn perusteet, tarkoitukset ja keinot. Rekisterinpitäjä voi olla organisaatio tai luonnollinen henkilö. Rekisterinpitäjän vastuulla on GDPR:n mukaan:

Tietosuojaperiaatteiden noudattaminen**:** Rekisterinpitäjänä organisaation tulee noudattaa GDPR:n tietosuojaperiaatteita, kuten oikeudenmukaisuutta, läpinäkyvyyttä, tarkoitussidonnaisuutta ja tietojen minimointia. Tämä tarkoittaa muun

muassa sitä, että rekisterinpitäjän on kerättävä henkilötietoja laillisesti ja oikeudenmukaisesti ja käytettävä niitä vain määriteltyihin tarkoituksiin.

Tietojen suojaaminen: Rekisterinpitäjänä organisaation tulee varmistaa henkilötietojen asianmukainen suojaaminen ja turvallisuus. Tämä sisältää tietojen turvallisen säilyttämisen, käyttöoikeudet, tietoturvaloukkausten ehkäisyn ja tietojen salauksen tarvittaessa. Rekisterinpitäjän on myös varmistettava, että henkilötietoja käsitellään vain niillä henkilöillä, joilla on tarve käsitellä niitä.
Tietosuojaselosteiden laatiminen: Rekisterinpitäjänä organisaation tulee laatia ja ylläpitää tietosuojaselosteita, jotka kertovat henkilötietojen käsittelyyn liittyvistä asioista, kuten käsittelyn tarkoituksesta, käsittelyn perusteista ja käsittelyyn liittyvistä oikeuksista. Tietosuojaselosteiden avulla rekisterinpitäjä voi täyttää läpinäkyvyyttä koskevat vaatimukset ja antaa asianmukaiset tiedot rekisteröidyille henkilöille.
Rekisteröityjen oikeuksien kunnioittaminen: Rekisterinpitäjänä organisaation tulee kunnioittaa rekisteröityjen oikeuksia GDPR:n mukaan. Tämä sisältää muun muassa oikeuden saada tietoa henkilötietojen käsittelystä, oikeuden saada pääsy omiin tietoihinsa, oikeuden korjata virheelliset tiedot ja oikeuden pyytää tietojensa poistamista.
Yhteistyö tietosuojaviranomaisten kanssa: Rekisterinpitäjänä organisaation tulee toimia yhteistyössä tietosuojaviranomaisten kanssa ja noudattaa heidän antamiaan ohjeita ja suosituksia. Tämä sisältää muun muassa tietosuojaviranomaisten tiedusteluihin vastaamisen ja tietosuojaviranomaisten valvonta- ja tarkastustoimien tukemisen.

7.5 Henkilötietojen käsittelijä ja käsittelytoimet

Tietosuojavaltuutetun toimiston mukaan henkilötietojen käsitelijä on taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijä voi olla esimerkiksi yritys, yksityinen elinkeinonharjoittaja, viranomainen tai yhdistys (https://tietosuoja.fi/henkilotietojen-kasittelijat). Heidän roolinsa perustuu rekisterinpitäjän antamiin ohjeisiin ja GDPR:n vaatimuksiin. Tärkeimmät velvoitteet ja vastuut sisältävät:

Sopimukset ja vastuunselvitys: Käsittelijän ja rekisterinpitäjän välillä on solmittava kirjallinen sopimus, jossa määritellään käsittelyn tarkoitus, laajuus ja vastuut.
Tietoturvatoimenpiteet: Käsittelijän on toteutettava asianmukaiset tekniset ja muut ohjeistetut toimenpiteet henkilötietojen suojaamiseksi. Näihin kuulu tietojen salaus, pääsynvalvonta ja ohjeistuksen sekä tietoturvakäytänteiden noudattaminen.
Yhteistyö rekisterinpitäjän kanssa: Käsittelijän tulee toimia yhteistyössä rekisterinpitäjän kanssa ja auttaa tietosuojavaatimusten noudattamisessa. Heidän on myös varmistettava rekisterinpitäjän tukeminen tietosuojaviranomaisten kanssa.

Käsittelijän suorittamat käsittelytoimet vaihtelevat organisaatiosta ja toiminnasta riippuen. Ne voivat olla mm.

Tietojen kerääminen ja tallentaminen: Käsittelijä voi kerätä ja tallentaa henkilötietoja rekisterinpitäjän ohjeiden mukaisesti esimerkiksi asiakasrekistereihin.
Tietojen käsittely ja analysointi: Käsittelijä voi käsitellä ja analysoida henkilötietoja rekisterinpitäjän antamien ohjeiden pohjalta.
Tietojen siirto ja jakaminen: Käsittelijä voi siirtää ja jakaa henkilötietoja rekisterinpitäjän luvalla esimerkiksi alihankkijoiden kanssa.
Tietojen poisto ja hävittäminen: Käsittelijä voi poistaa ja hävittää henkilötietoja rekisterinpitäjän ohjeiden mukaisesti esimerkiksi säilytysajan päätyttyä.

Henkilötietojen käsittelijän rooli ja suorittamat toimet ovat olennaisia GDPR:n vaatimusten noudattamisessa ja henkilötietojen asianmukaisessa käsittelyssä.

7.6 Rekisteröity

Rekisteröity on luonnollinen henkilö, jonka henkilötietoja käsitellään. Tietosuojavaltuutetun toimisto (https://tietosuoja.fi/rekisteroidyn-oikeudet) listaa rekisteröidyn oikeuksiksi Tietosuojalain mukaan:

- saada tietoa henkilötietojensa käsittelystä
- saada tutustua tietoihin
- oikaista tietoja

- poistaa tiedot ja tulla unohdetuksi
- rajoittaa tietojen käsittelyä
- siirtää tiedot järjestelmästä toiseen
- vastustaa tietojen käsittelyä
- olla joutumatta automaattisen päätöksenteon kohteeksi.

Nämä oikeudet ovat rekisteröidyllä aina oletusarvoisesti olemassa. Tietojenkäsittelyn peruste saattaa kuitenkin rajata joissain tapauksissa rekisteröidyn oikeuksia. Tällaisia perusteita voivat liittyä esimerkiksi viranomaistoimintaan tai rahoitukseen.
Henkilötietojen käsittelyn edellytyksenä on pääsääntöisesti rekisteröidyn suostumus, jonka tulee olla yksilöity, tietoinen, aidosti vapaaehtoinen ja yksiselitteinen tahdonilmaisu (https://tietosuoja.fi/rekisteroidyn-suostumus).

7.7 Tietoturvaloukkaus

Euroopan komissio (https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_fi) määrittelee tietoturvaloukkauksen seuraavasti: ” Kyse on tietoturvaloukkauksesta, kun yrityksesi/organisaatiosi vastuulla olevien tietojen salassapito, saatavuus tai eheys vaarantuvat.”. Tästä samasta asiasta käytetään myös usein termiä tietosuojaloukkaus. Käytännössä tämä tarkoittaa, että tietoja on päässyt sellaisten käsiin joilla ei ole niihin oikeutta, tietojen hallinta on tavalla tai toisella menetetty tai tiedot ovat hallitsemattomasti muuttuneet. Myös rekisteriin kirjattu virheellinen tieto voidaan katsoa tietoturvaloukkaukseksi sillä tieto ei ole enää eheä. Tietosuojavaltuutetun toimisto (https://tietosuoja.fi/tietoturvaloukkaukset) Suomessa käyttää hieman tarkempaa määritelmää: ” Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtumaa, jonka seurauksena henkilötietoja tuhoutuu, häviää, muuttuu, henkilötietoja luovutetaan luvattomasti tai niihin pääsee käsiksi taho, jolla ei ole käsittelyoikeutta.”.

Kun rekisterinpitäjä saa tietoonsa tietoturvaloukkauksen tapahtuneen on hänen viipymättä, mutta viimeistään 72h kuluessa ilmoitettava siitä Tietosuojavaltuutetun toimistolle. Jos tietoturvaloukkauksen havaitsee ensin tietojenkäsittelijä, tulee tämän ilmoittaa tapahtumasta rekisterinpitäjälle, ellei asiasta ole muuta sovittu. Vastuu ilmoituksen tekemisestä määräajassa on kuitenkin rekisterinpitäjällä riippumatta mahdollisista sovituista muista menettelytavoista.

Rekisterinpitäjän on arvioitava tietoturvaloukkauksen vakavuus rekisteröidyn näkökulmasta. Mikäli tietoturvaloukkauksella voi olla merkittäviä seurauksia rekisteröidylle tulee rekisterinpitäjän ilmoittaa tästä rekisteröidylle. Tämä voi olla erityisen haastavaa, jos rekisteröityjä on suuri määrä. Esimerkiksi Helsingin kaupungin Kasvatuksen ja koulutuksen toimialan tietomurron epäillään loukanneen yli 100 000 ihmisen yksityisyyttä. Helsingin kaupunki julkaisi sivuillaan tiedotteen (https://www.hel.fi/fi/paatoksenteko-ja-hallinto/tietomurto) asiasta. Asia on ollut myös esillä julkisuudessa huomattavan paljon.
Rekisteröityjen informointiin liittyy monia käytännön ongelmia. Kaikkia ei välttämättä tavoiteta kovin hyvin ja usein ilmoitus tietoturvaloukkauksesta herättää rekisteröidyissä kysymyksiä, joihin he haluavat vastauksia. On tärkeää varata riittävästi resursseja vastaamaan rekisteröityjen kysymyksiin. Laajojen tietomurtojen tai muiden isompien tietojenkäsittelyn häiriötilanteiden selvittely voi kestää kauan ja informointi vaiheessa ei useinkaan ole kaikkea tarvittavaa tietoa käytettävissä. Rekisteröityjen informoinnissa on tällaisissa tapauksissa hyvä käyttää apuna viestinnän ammattilaisia jos sellaisia on käytettävissä.

Tietoturvaloukkauksen tapahtuessa on rekisterinpitäjä lähtökohtaisesti epäonnistunut rekisteröityjen tietojen suojaamisessa ja tällä voi olla myös oikeudellisia ja hallinnollisia seuraamuksia. Erilaiset sakot, toiminnan rajoitukset ja keskeyttämiset ovat yleisimpiä. Myöskään mahdollisia vahingonkorvauksia rekisteröidyille ei voi unohtaa, jos heille on aiheutettu tietoturvaloukkauksella vahinkoa tai muuta haittaa.

7.8 Tietopyyntö

Tietopyyntö käsitteenä ei perustu lakiin vaan se vakiintunut nimitys toimelle, jolla yksilö voi toteuttaa tiedonsaantioikeuttaan asioista jotka ovat julkisia, henkilön tiedonsaantioikeuden piirissä tai joissa hän on itse asiaan osallisena. Tietopyyntö käsitettä käytetään myös julkisuuslain mukaisissa tietopyynnöissä, mutta tässä työssä se rajataan koskemaan vain GDPR:n ja Tietosuojalain mukaista rekisteröidyn oikeutta saada tietoja itseään koskevista rekisterimerkinnöistä.

Tietopyyntö on yksilön oikeuden pyytää tietoja hänestä tallennetuista henkilötiedoista toteuttamista. Tämä tapahtuu siten, että rekisteröity esittää rekisterinpitäjälle tietopyynnön ja yksilöi siinä mitä tietoja hän haluaa selvittää. Erityisesti organisaatioissa joissa on useita rekisterietä ja rekisterinpitäjiä voi tämä olla joskus haastavaa. Rekisteröidylle pitäisi lähtökohtaisesti riittää, että hän ilmaisee toiveensa saada ote kaikista häntä koskevista tiedoista, jotka organisaatiossa on kirjattu hänestä. Tällöin on rekisterinpitäjän, joka saa tietopyynnön varmistettava myös muista rekistereistä, löytyykö niistä pyynnön esittäneen henkilön tietoja. Pyyntöön on vastattava kohtuullisessa ajassa, yleensä kuukauden sisällä.

Tietosuojavaltuutetun toimisto on ohjeistanut asiaa seuraavasti:
”Rekisterinpitäjän täytyy vastata rekisteröidylle ilman aiheetonta viivytystä, joka tapauksessa kuukauden kuluessa pyynnön vastaanottamisesta. Vastauksessa rekisterinpitäjä kertoo toimenpiteistä, joihin se on pyynnön vuoksi ryhtynyt. Jos pyyntöjä on monta tai ne ovat monimutkaisia, rekisterinpitäjä voi ilmoittaa vastauksessaan, että se tarvitsee niiden käsittelyyn enemmän aikaa. Tällöin määräaikaa voidaan jatkaa enintään kahdella kuukaudella. Määräajan jatkaminen on perusteltava.” (https://tietosuoja.fi/oikeus-saada-tutustua-tietoihin)

Jos rekisterinpitäjä kieltäytyy luovuttamasta tietoja pyynnön esittäjälle, on tämä ilmoitettava hänelle kuukauden sisällä. Kieltäytyminen on perusteltava. Tietopyynnön esittämisen tulee lähtökohtaisesti olla rekisteröidylle maksutonta. ainoan poikkeuksen tekee ilmeisen perusteeton tai kohtuuton tietopyyntö.

Tietopyyntöjä on ikävä kyllä käytetty myös väärin. Yleisin tietopyyntöihin liittyvä väärinkäytös on esiintyminen jonain toisena kuin rekisteröitynä ja siten yrittää saada haltuunsa tietoa rekisteröidystä omia tarkoitusperiään varten. On siis ensiarvoisen tärkeää, erityisesti jos tietopyyntö sisältää erityisiä henkilötietoja, että tietopyynnön esittäjä voidaan tunnistaa luotettavasti. Etenkin erityisiä henkilötietoja käsittelevien organisaatioiden on luotava tähän heille sopiva menettely. Tästä syystä myös oikeutta esittää tietopyyntö suullisesti esimerkiksi puhelimessa voidaan rajata.
Toinen tapa käyttää väärin tietopyyntöjä on pyytää niitä niin sanotusti huvikseen tai häiritäkseen organisaation toimintaa. Tietopyyntöjen käsittely on monessa

organisaatiossa suhteellisen hidas ja työläs prosessi. Näissä tapauksessa henkilöä tai henkilöitä, ei itse asiassa kiinnosta heidän oma tietosuojansa vaan heidän motiivinsa on teettää rekisterinpitäjällä turhaa työtä. Tämä ilmiö on suhteellisen harvinainen, mutta ei täysin tuntematon ja valitettavasti sitä on alkanut esiintyä yleisemmin.

7.9 Rekisteriseloste

Rekisteriseloste on asiakirja, jossa rekisterinpitäjä kuvaa henkilötietojen käsittelyä organisaatiossaan. Tietosuojavaltuutetun toimisto on ohjeistanut varsin kattavasti sen sisältöä sivuillaan (**https://tietosuoja.fi/rekisteroidyn-info**rmointi).

Se sisältää tiedot siitä, mitä henkilötietoja kerätään, miksi niitä kerätään, miten niitä käsitellään ja kenelle niitä mahdollisesti jaetaan. Rekisteriseloste on tärkeä väline läpinäkyvyyden ja avoimuuden varmistamisessa, ja sen avulla rekisteröidyt voivat saada tietoa omien henkilötietojensa käsittelystä. Rekisteriseloste on julkinen asiakirja ja sen on oltava saatavilla.

Rekisteriselosteessa tulee olla seuraavat tiedot:

Rekisterinpitäjän tiedot: Rekisteriselosteessa tulee olla rekisterinpitäjän nimi ja yhteystiedot, kuten osoite, sähköpostiosoite ja puhelinnumero.
Henkilötietojen käsittelyn tarkoitus: Rekisteriselosteessa tulee kuvata, miksi henkilötietoja kerätään ja käsitellään, esimerkiksi asiakassuhteen hoitamiseksi tai markkinointitarkoituksiin.
Käsiteltävät henkilötiedot: Rekisteriselosteessa tulee kuvata, mitä henkilötietoja kerätään ja käsitellään, kuten nimi, osoite, puhelinnumero ja sähköpostiosoite.
Henkilötietojen säilytysaika: Rekisteriselosteessa tulee kuvata, kuinka kauan henkilötietoja säilytetään ja milloin ne poistetaan.
Tietojen luovutukset ja siirrot: Rekisteriselosteessa tulee kuvata, kenelle henkilötietoja mahdollisesti jaetaan ja siirretään, esimerkiksi alihankkijoille tai kolmansille osapuolille.Tietosuojaoikeudet: Rekisteriselosteessa tulee kuvata rekisteröityjen oikeudet GDPR:n mukaisesti, kuten oikeus pääsyyn, oikaisuun, poistoon ja siirrettävyyteen.

Yhteystiedot ja lisätiedot: Rekisteriselosteessa tulee olla yhteystiedot, joihin rekisteröidyt voivat ottaa yhteyttä tietosuoja-asioissa, sekä mahdolliset lisätiedot henkilötietojen käsittelystä.

Rekisteriselosteen laatimisesta ja sen saatavuudesta vastaa rekisterinpitäjä. Se tulee laatia selkeällä ja ymmärrettävällä kielellä ja tehdä helposti saataville esimerkiksi organisaation verkkosivuilla. Rekisteriseloste on pidettävä ajan tasalla ja päivitettävä tarvittaessa

8 Tietosuojaa säätelevä lainsäädäntö ja muu regulaatio

Tietosuojaa säädellään Suomessa monella eri tasolla. EU tasolla tietosuojaa sääntelee General Data Protection Regulation eli GDPR. Kansallisella tasolla keskeisin sovellettava säädös on Tietosuojalaki. Muita usein sovellettavaksi tulevia lakeja ovat myös laki viranomaisten toiminnan julkisuudesta (1999/621) ja Laki julkisen hallinnon tiedonhallinnasta (2019/906). Tietosuoja-asioissa valvovana viranomaisena toimii Valtioneuvoston alaisuudessa toimiva Tietosuojavaltuutetun toimisto. EU tasolla tietosuojaa valvoo Euroopan tietosuojaviranomainen (EDPB). Muita tietosuojaa ja henkilötietojen käsittelyä koskevia lakeja ovat:

- Rikosasioiden tietosuoja direktiivi (EU) 2016/680
- Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018)
- Laki sähköisen viestinnän palveluista (2014/917)
- Laki yksityisyyden suojasta työelämässä (2004/759)
- Luottotietolaki (2007/527)

Lisäksi useissa muissa säädöksissä on mainintoja henkilötietojen käsittelystä ja julkisuudesta. Tässä työssä on keskitytty kuitenkin kyseisessä organisaatiossa eniten sovellettaviin lakeihin ja muuhun regulaatioon.

8.1 GDPR

GDPR (General Data Protection Regulation, (EU) 2016/679)) on Euroopan unionin asetus, joka astui voimaan 25. toukokuuta 2018 ja muutti merkittävästi tapaa, jolla henkilötietoja käsitellään ja suojataan EU:ssa. GDPR:n tarkoituksena on vahvistaa yksilöiden oikeuksia heidän henkilötietojensa käsittelyssä sekä parantaa henkilötietojen suojaamista ja hallintaa organisaatioissa.

Yksi GDPR:n keskeisistä tavoitteista on luoda yhtenäiset säännöt henkilötietojen käsittelylle kaikkialla EU:ssa. Organisaatioiden on noudatettava samoja tietosuojasääntöjä riippumatta siitä, missä EU-maassa ne toimivat tai missä henkilötiedot käsitellään. Tarkoituksena on helpottaa sekä kansalaisten että yritysten toimintaa EU:n sisällä, kun tietosuojakäytännöt ovat yhdenmukaiset.

GDPR sisältää useita tärkeitä periaatteita ja vaatimuksia, kuten henkilötietojen käsittelyn lainmukaisuus, oikeudenmukaisuus ja läpinäkyvyys. Organisaatioiden on myös varmistettava, että heillä on lailliset perusteet henkilötietojen käsittelylle ja että he kunnioittavat yksilöiden oikeuksia, kuten oikeutta saada tietoa omista henkilötiedoistaan ja oikeutta tietojen poistamiseen.

GDPR on Euroopan unionin asetus, joka astui voimaan 25. toukokuuta 2018 ja muutti merkittävästi tapaa, jolla henkilötietoja käsitellään ja suojataan EU:ssa. GDPR:n tarkoituksena on vahvistaa yksilöiden oikeuksia heidän henkilötietojensa käsittelyssä sekä parantaa henkilötietojen suojaamista ja hallintaa organisaatioissa.

Yksi GDPR:n keskeisistä tavoitteista on luoda yhtenäiset säännöt henkilötietojen käsittelylle kaikkialla EU:ssa. Tämä tarkoittaa sitä, että organisaatioiden on noudatettava samoja tietosuojasääntöjä riippumatta siitä, missä EU-maassa ne toimivat tai missä henkilötiedot käsitellään. Tämä helpottaa sekä kansalaisten että yritysten toimintaa EU:n sisällä, kun tietosuojakäytännöt ovat yhdenmukaiset.

GDPR sisältää useita tärkeitä periaatteita ja vaatimuksia, kuten henkilötietojen käsittelyn lainmukaisuus, oikeudenmukaisuus ja läpinäkyvyys. Organisaatioiden on myös varmistettava, että heillä on lailliset perusteet henkilötietojen käsittelylle ja että he kunnioittavat yksilöiden oikeuksia, kuten oikeutta saada tietoa omista henkilötiedoistaan ja oikeutta tietojen poistamiseen.

GDPR:ssä määritellään useita keskeisiä periaatteita, jotka ohjaavat henkilötietojen käsittelyä. Tässä muutamia niistä:

Lainmukaisuus, oikeudenmukaisuus ja läpinäkyvyys: Henkilötietoja on käsiteltävä lainmukaisesti, oikeudenmukaisesti ja läpinäkyvästi suhteessa rekisteröityyn eli henkilöön, jonka tietoja käsitellään. Organisaatioiden on ilmoitettava selkeästi, miten ja miksi henkilötietoja käsitellään.
Tarkoitussidonnaisuus: Henkilötietoja saa kerätä ja käsitellä vain määriteltyihin tarkoituksiin, ja niitä saa käyttää vain näiden tarkoitusten mukaisesti.

Datan minimointi: Henkilötietoja kerätä vain se määrä, joka on tarpeen käsittelyn tarkoitusta varten. Organisaatioiden on pyrittävä rajoittamaan kerättävien ja käsiteltävien tietojen määrä mahdollisimman pieneksi.
Tietojen tarkkuus: Henkilötietojen on oltava tarkkoja ja tarvittaessa päivitettyjä. Organisaatioiden on ryhdyttävä asianmukaisiin toimiin varmistaakseen, että virheelliset tai vanhentuneet tiedot poistetaan tai korjataan.
Säilytysrajoitukset. Henkilötietoja saa säilyttää vain niin kauan kuin se on tarpeen käsittelyn tarkoitusten kannalta. Tietojen on oltava poistettava, kun niitä ei enää tarvita.
Eheyden ja luottamuksellisuuden suojaaminen. Henkilötietoja on käsiteltävä siten, että niiden turvallisuus, eheys ja luottamuksellisuus ovat taattuja. Tietojen luvaton tai virheellinen käsittely on estettävä.
Vastuuvelvollisuus: Organisaatioilla on velvollisuus osoittaa, että ne noudattavat GDPR:n vaatimuksia. Tämä voi sisältää tietosuojaperiaatteiden sisällyttämisen organisaation toimintaprosesseihin, asianmukaisten tietosuojatoimenpiteiden toteuttamisen ja dokumentoinnin sekä tarvittaessa yhteistyön tietosuojaviranomaisten kanssa.

8.2 Laki yksityisyyden suojasta työelämässä

Laki yksityisyyden suojasta työelämässä (2004/759) on osa työlainsäädäntöä, ja sen tarkoituksena on suojata työntekijöiden yksityisyyttä ja henkilötietoja työpaikalla.

Yksityisyyden suoja työelämässä on osa työntekijöiden oikeuksia. Laki määrittelee, miten työnantajat voivat kerätä, käsitellä ja säilyttää työntekijöiden henkilötietoja sekä miten heidän yksityisyyttään on kunnioitettava.

Yksi keskeinen osa tätä lakia on työntekijöiden informointi ja suostumus. Työnantajan on kerrottava työntekijöille selvästi, mitä tietoja heistä kerätään, miksi niitä kerätään ja miten niitä käytetään. Lisäksi työntekijöiden suostumus on usein tarpeen ennen kuin henkilötietoja voidaan käsitellä, erityisesti silloin kun kyseessä ovat arkaluonteiset tiedot, kuten terveystiedot.

Toinen osa on tietoturva ja henkilötietojen suoja. Työnantajilla on velvollisuus varmistaa, että työntekijöiden henkilötiedot säilytetään turvallisesti ja suojataan

luvattomalta pääsyltä tai väärinkäytöltä. Tietoturvaan kuuluu myös se, että tarpeettomia tietoja ei säilytetä ja että tiedot poistetaan asianmukaisesti niiden säilytysajan päätyttyä.

Lisäksi laki yksityisyyden suojasta työelämässä käsittelee työntekijöiden oikeuksia tarkastaa omat henkilötietonsa ja mahdollisuutta korjata virheellisiä tietoja. Työntekijöillä on oikeus saada tietoa siitä, mitä tietoja heistä on tallennettu ja miten niitä käsitellään, ja tarvittaessa he voivat pyytää tietojensa korjaamista tai poistamista.

Nykyään teknologian kehitys ja digitalisaatio asettavat uusia haasteita yksityisyyden suojalle työelämässä. Esimerkiksi työntekijöiden sähköpostit, puhelut ja verkkotoiminta voivat sisältää henkilötietoja, jotka on suojattava asianmukaisesti. Lisäksi työntekijöiden valvonta ja seuranta työpaikalla herättävät kysymyksiä yksityisyyden suojasta ja työntekijöiden oikeuksista.

8.3 Tietosuojalaki

Tietosuojalaki (2018/1050) täsmentää GDPR:n soveltamista Suomessa. Siinä säädetään mm. tietosuojan valvontaviranomaisesta ja tämän toimivaltuuksista. Lisäksi sinne on kirjattu sääntelyä ja täsmennyksiä koskien:

- Lapsiin sovellettavasta ikärajasta tietoyhteiskunnan palveluita tarjottaessa
- Erityisten henkilötietoryhmien käsittelystä
- Henkilötietojen käsittelystä journalistisen, akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten
- Henkilötunnuksen käsittelemisestä
- Eräistä tilanteista, joissa yleinen etu on oikeusperuste henkilötietojen käsittelylle rajoituksista rekisteröidyn oikeuksiin.

Tietosuojalakia sovelletaan henkilötietojen käsittelyyn silloin, kun rekisterinpitäjä tai henkilötietojen käsittelijä on sijoittunut Suomeen, tai kun henkilötietoja käsitellään osana EU:ssa sijaitsevan rekisterinpitäjän tai käsittelijän toimintaa. Lisäksi lakia sovelletaan, kun henkilötietoja käsitellään EU:n ulkopuolelta, mutta ne koskevat EU:n kansalaisia.

Tietosuojalain noudattamista valvoo Suomessa tietosuojavaltuutetun toimisto. Tietosuojavaltuutetulla on laajat valtuudet, mukaan lukien oikeus määrätä hallinnollisia sanktioita tietosuojarikkomuksista. Näitä sanktioita voivat olla huomautukset, määräykset ja hallinnolliset sakot.

8.4 Tietosuojavaltuutetun toimisto

Tietosuojavaltuutetun toimisto on Suomessa viranomainen, joka vastaa tietosuojalainsäädännön valvonnasta ja noudattamisen edistämisestä. Sen tehtäviin kuuluu erityisesti henkilötietojen suojaan liittyvien oikeuksien turvaaminen ja tietosuojan toteutumisen valvonta. Toimisto toimii itsenäisesti ja riippumattomasti, ja sen toimintaa ohjaa muun muassa EU:n yleinen tietosuoja-asetus (GDPR) sekä Tietosuojalaki.

Tietosuojavaltuutetun toimiston keskeisimpiä tehtäviä ovat:

- Valvontatehtävät:
- Neuvonta ja ohjaus
- Yhteistyö EU -maiden tietosuojaviranomaisten kanssa
- Edustaminen Euroopan tietosuojaneuvostossa (EDPB)
- Tutkinta- ja tarkastustoiminta
- Tietoisuuden lisääminen:
- Järjestää koulutuksia, seminaareja ja tiedotuskampanjoita.

Tätä kirjoitettaessa Tietosuojavaltuutetun toimistoa johtaa tietosuojavaltuutettu ja hänen apunaan kaksi apulaistietosuojavaltuutettua.

Tietosuojavaltuutetun toimistolla on käytössään myös korjaavia toimivaltuuksia, jotka voi mieltää myös pakkokeinoiksi. Näitä ovat:

- Varoituksen antaminen rekisterinpitäjälle tai henkilötietojen käsittelijälle
- Huomautuksen antaminen rekisterinpitäjälle tai henkilötietojen käsittelijälle
- Määräyksen antaminen rekisterinpitäjälle tai henkilötietojen käsittelijälle

- Rekisterinpitäjä tai henkilötietojen käsittelijä voidaan määrätä oikaisemaan tai poistamaan henkilötietoja tai rajoittamaan niiden käsittelyä
- Henkilötietojen käsittelyn rajoittaminen tai käsittelykiellon asettaminen rekisterinpitäjälle tai henkilötietojen käsittelijälle.
- Sertifioinnin peruuttaminen tai määräyksen antaminen sertifiointielimelle
- Määräyksen antaminen kolmanteen maahan tai kansainväliselle järjestölle tehtävien tiedonsiirtojen keskeyttämisestä.
- Hallinnollisen seuraamusmaksun määrääminen muiden korjaavien toimenpiteiden lisäksi tai niiden asemesta.
- Seuraamusmaksu voi olla enintään 4 % liikevaihdosta tai 20 miljoonaa euroa.

Poikkeuksena seuraamusmaksuun on, että sitä ei voi määrätä julkishallinnon organisaatioille, kuten valtiolle ja valtion liikelaitoksille, kunnille ja seurakunnille. Tietosuojavaltuutetun toimiston ratkaisuista voi valittaa hallinto-oikeuteen ja korkeimpaan hallinto-oikeuteen.

8.5 ISO27001

ISO 27001 on kansainvälinen standardi tietoturvallisuudelle, joka määrittelee ja kuvaa tietoturvallisuuden hallintajärjestelmän (ISMS, Information Security Management System) vaatimukset. Standardi tarjoaa puitteet ja ohjeet organisaatioiden tietoturvallisuuden hallintaan ja auttaa varmistamaan, että tietojärjestelmiä ja -prosesseja suojataan asianmukaisesti.

ISO 27001-standardin tavoitteena on auttaa organisaatioita suunnittelemaan, toteuttamaan, ylläpitämään ja jatkuvasti parantamaan tietoturvallisuuden hallintajärjestelmäänsä. Tämä auttaa organisaatioita suojaamaan arkaluonteisia tietojaan, kuten asiakastietoja, liiketoimintatietoja ja henkilöstötietoja, sekä vähentämään tietoturvallisuusriskejä ja estämään tietoturvaloukkauksia.

ISO 27001-standardi koostuu useista osista, joista tärkeimmät ovat:

Kontekstin määrittely: Organisaation on määriteltävä ja ymmärrettävä toimintaympäristönsä, tietoturvaan vaikuttavat sidosryhmät ja niiden vaatimukset.

Johtamisjärjestelmä: Organisaation johdon on sitouduttava tietoturvallisuuden hallintaan ja varmistettava, että tarvittavat resurssit ja tuki ovat saatavilla.
Riskien arviointi ja hallinta: Organisaation on tunnistettava tietoturvallisuusuhkat ja -haavoittuvuudet sekä toteutettava toimenpiteitä riskien hallitsemiseksi.
Tietoturvasuunnittelu: Organisaation on suunniteltava ja toteutettava tietoturvatoimenpiteitä ja -kontrolleja tietojärjestelmissä ja -prosesseissa.
Tietoturvan valvonta: Organisaation on seurattava ja arvioitava tietoturvatapahtumia, jotta voidaan havaita mahdolliset tietoturvaloukkaukset ja ryhtyä tarvittaviin toimenpiteisiin.
Jatkuvan parantamisen prosessi: Organisaation on jatkuvasti arvioitava ja parannettava tietoturvallisuuden hallintajärjestelmäänsä vastaamaan muuttuvia tarpeita ja uhkia.

ISO 27001-sertifiointi osoittaa, että organisaatio noudattaa kansainvälisiä standardeja tietoturvallisuuden ja -suojan hallinnassa ja että sillä on riittävä tietoturvallisuuden hallintajärjestelmä.
Sertifiointia haetaan hyväksytyltä sertifiointiorganisaatiolta. Sertifiointeja harkittaessa on kuitenkin aina hyvä pitää mielessä, että nämä osoittavat vain organisaation tietoturvallisuuden hallintaa. Tämä ei tee järjestelmästä automaattisesti myös asiakasta parhaalla mahdollisella tavalla suojaavaa, kuten kyberturvallisuuskeskuksen Ohjelmistoturvallisuuden tila 2023 -raportissa (https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjelmistoturvallisuuden%20tila%202023.pdf) mainitaan.

8.6 ISO/IEC 27701

ISO/IEC 27701 on kansainvälinen standardi, joka laajentaa tietoturvan hallintajärjestelmää (ISMS) erityisesti yksityisyyden suojan hallintaan. Se tunnetaan nimellä "Tietosuojan hallintajärjestelmät – Vaateet ja ohjeet", ja se täydentää ISO/IEC 27001- ja ISO/IEC 27002 -standardeja, jotka käsittelevät yleisesti tietoturvan hallintaa. ISO/IEC 27701 julkaistiin elokuussa 2019, ja sen tarkoituksena on auttaa organisaatioita noudattamaan tietosuoja-asetuksia, kuten EU:n yleistä tietosuoja-asetusta (GDPR).

ISO/IEC 27701 antaa perusteet organisaation tietosuojan hallintajärjestelmälle (PIMS, (Privacy Information Management System), Määrittää vaatimukset ja ohjeet osoitusvelvollisuuden täyttämiseen ja määrittelee eri toimijoiden roolit henkilötietojen käsittelyssä organisaation sisällä.

ISO/IEC 27701 sisältää seuraavia asiakokonaisuuksia tietosuojan kehittämiseen:

- Tietosuojapolitiikat ja – ohjeet
- PIMS:n kehittäminen
- Riskienhallinta ja siihen liittyvät menettelyt henkilötietojen käsittelyssä (ml. Vaikutusten arvioinnit (DPIA, Data Protection Impact Assesment))
- Henkilötietojen suojaaminen
- Dokumentointi ja seuranta

Tarkkaa tietoa ISO/IEC 27701 -sertifikaatin yleisyydestä Suomessa ei ole saatavilla. Sertifikaatin käyttö yleistyy hiljalleen erityisesti isoissa organisaatioissa, jotka käsittelevät suuria määriä henkilötietoja ja jotka haluavat varmistaa GDPR:n ja muiden tietosuojalainsäädäntöjen noudattamisen. Sertifiointi itsessään ei kuitenkaan ole vielä osoitus tietosuojaan liittyvän lainsäädännön noudattamisesta. Sertifioinnit kuitenkin mahdollistavat asioinnin monien yhteistyötahojen kanssa, joilla sellainen on vaatimuksena yhteistyölle.

9 Tietosuoja vs. tietoturva

Arkikielessä ja mediassakin termit tietoturva ja tietosuoja menevät usein sekaisin. Tietoturvallisuudella tarkoitetaan kaikkia niitä hallinnollisia ja teknisiä toimenpiteitä, joilla suojataan tiedon käytettävyyttä, eheyttä, luottamuksellisuutta (https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturvasaantely). Tähän luetaan usein mukaan myös kiistämättömyys (todentaminen). Tämä jaottelu on käytössä useilla eri tahoilla Suomessa tätä kirjoitettaessa, mm. valtionhallinnossa, monissa julkisissa palveluissa ja liike-elämässä.
Tietosuoja on yksi tietoturvallisuuden osa-alue. Se keskittyy yksityisyyden suojan turvaamiseen ja sitä puolestaan säätelee sekä EU -tasoinen, että kansallinen normisto.
Tärkeää on kuitenkin huomioida, että tietoturvallisuuden osa-alueet ovat monella tavalla riippuvaisia toisistaan. Yhden osa-alueen pettäessä sillä on vaikutuksia myös muihin osa-alueisiin. Seuraavassa kuvassa kuvattuna tietoturvallisuuden osa-alueet.

Kuvio 3: Tietoturvallisuuden osa-alueet (Miettinen, Juha. E., Tietoturvallisuuden johtaminen, Gummerus, 1999, Jyväskylä)

9.1 Hallinnollinen tietoturvallisuus

Hallinnollinen tietoturvallisuus koostuu tietoturvallisuuden johtamisesta ja erilaisista hallinnollisista prosesseista. Se on osa turvallisuusjohtamista. Juha Leppänen nostaa kirjassaan Yritysturvallisuus käytännössä (Juha Leppänen, Yritysturvallisuus käytännössä, Helsinki, 2007, Talentum) siihen kuuluvaksi mm. tietoturvallisuuspolitiikat ja -ohjeistukset, vastuiden määrittelyt, erilaisten toipumissuunnitelmien ja varautumisen suunnitelmat ja menettelyt sekä luonnollisesti edellä mainittujen toimintojen johtamisen ja resurssoinnin.

Tietoturvallisuuden johtaminen, kuten kaikki muukin turvallisuuden johtaminen, on pohjimmiltaan samanlaista kuin minkä tahansa muunkin toiminnan johtaminen. Tietoturvallisuuden johtamiseen kuuluu myös olennaisena osana tietoturvallisuuden tilannekuvan ylläpito ja sen pohjalta johdon pitäminen tietoisena ajantasaisesta tilanteesta. Tietoturvallisuuden johtaminen keskittyy kokonaisuuden hallintaan, koordinoi toimintaa ja huolehtii riittävistä resursseista toiminnan toteuttamiseksi. Tähän kuuluu myös poikkeamien käsittely ja tarvittavan päätösvallan käyttö ja delegointi.

9.2 Henkilöstöturvallisuus

Tietoturvallisuuden näkökulmasta henkilöstö nähdään usein riskitekijänä. Juha E. Miettinen (1999) määrittelee kirjassaan henkilöstöturvallisuuden toimenpiteiksi joilla työpaikan tietoja suojataan ihmisten aiheuttamilta tahallisilta tai tahattomilta vahingoilta. Tämä kattaa oman henkilöstön lisäksi myös alihankkijat, vierailijat, sidosryhmät jne. Yleisesti voi sanoa, että jos henkilöllä on pääsy työpaikan tiloihin tai tietoihin on myös tietoturvallisuuden näkökohdat huomioitava. Tässä tulee huolehtia ainakin seuraavista:

- Taustatietojen tarkistaminen rekrytoinnissa (mahdollisesti myös vierailijat ja jotkin yhteistyökumppanit sekä sidosryhmät)
- Salassapitosopimukset ja käytänteistä informointi
- Työsuhteen aloitukseen ja päättymiseen liittyvät toimet
- Avainhenkilöiden kartoitus ja siihen liittyvä varautuminen
- Henkilöstön koulutus ja ohjeistus tietoturvallisuusasioissa (ml. matkustaminen)

Uudemmassa riskikäsityksessä esimerkiksi Paul Hopkin (Hopkin P. Fundamentals of risk management 5th edition, 2018, Kogan page limited, USA) riskiin sisältyy myös aina mahdollisuus. Hyvin koulutettu ja osaava henkilöstö on myös merkittävä positiivinen tekijä tietoturvallisuuden ylläpidossa ja kehittämisessä.

9.3 Toimitilaturvallisuus

Elinkeinoelämän keskuslitto (https://ek.fi/hyotytietoa-yrityksille/yritysturvallisuus/) määrittelee toimitilaturvallisuuden työpaikan toimipaikkojen ja -tilojen suojaamiseksi riskienarvioinnissa tunnisteltuilta uhilta. Toimitilaturvallisuus jaetaan neljään osa-alueeseen. Näitä ovat:

1. Toimitilojen turvallisuusluokittelu
2. Rakenteellinen ja tekninen suojaaminen
3. Valvonta
4. Sopimusten hallinta

Tietoturvallisuuden kannalta tilojen turvallisuusluokittelussa on keskeistä, että tiloissa, joissa käsitellään arkaluonteista tietoa ei liiku asiattomia henkilöitä. Nämä tilat tulee tunnistaa ja rajata henkilöiden liikkumista näissä tiloissa. Tulee myös pyrkiä siihen, että henkilöiden liikkuminen tiloissa on myös jälkeenpäin todennettavissa tavalla tai toisella. Tähän on olemassa useita erilaisia teknisiä toteutustapoja, joista työpaikka valitsee riskiperusteisesti itselleen sopivimman vaihtoehdon.

Harri Koskenranta käytti esityksessään (http://www.cse.hut.fi/fi/opinnot/T-110/T-110.5610/2007/kalvot/kuorisuojaus-6.pdf) yleisesti käytössä olevaa kehäsuojauksen periaatetta. Siinä tietoja suojataan neljällä eri kehällä. Näitä kehiä ovat:

1. Kehäsuojaus
2. Aluesuojaus
3. Kuorisuojaus
4. Kohdesuojaus

Päästäkseen käsiksi suojattavaan tietoon on tekijän käytännössä läpäistävä kaikki suojauksen kehät jotka voivat estää pääsyn ja/tai tunnistaa tekijän. Toimitilojen suojausta suunniteltaessa on hyvä käyttää ”Path of least resistance” -ajattelua eli suojaukseen ei saisi jäädä heikkoja lenkkejä. Hyvä lukitus, kulunvalvonta, hälytyslaitteisto ja tukeva ovi eivät muodosta hyvää suojausta, jos tilaan pääsee myös kevyen väliseinän läpi. Organisaatiosta ja käsiteltävän tiedon arkaluontoisuudesta riippuen voi joskus olla myös rajoituksia tiedon viemiseen turvallisen käsittelytilan ulkopuolelle.

9.4 Tietojenkäsittely

Juha E. Miettisen mukaan (Miettinen, Juha. E.1999) henkilötietojen käsittelyssä on huomioitava henkilöt, jotka tietoja käsittelevät sekä tiedon koko elinkaari sen syntymisestä sen poistamiseen.
Henkilötietojen käsittelijällä on oltava tietoinen siitä, milloin hän käsittelee henkilötietoja ja siitä millaisia vaikutuksia käsittelytoimilla voi olla niiden kohteelle. Lisäksi henkilötietojakäsittelevien kanssa on oltava olemassa salassapitosopimukset.

9.5 Tiedon elinkaari

Tiedon elinkaariajattelu on keskeinen osa henkilötietojen käsittelyä. Valtionvarainministeriön tiedonhallinnan lautakunnan esityksessä (https://vm.fi/documents/10623/123922064/Torro+Heidi+-Tiedon+elikaari+20220608.pdf/52fa46e5-5d52-b28a-affc-34437171d622/Torro+Heidi+-Tiedon+elikaari+20220608.pdf?t=1655200575795) Heidi Torro jakaa tiedon elinkaaren vaiheet seuraavasti:

1. tiedon tuottaminen tai vastaanotto
2. säilytys
3. käyttö
4. jakaminen
5. siirto
6. arkistointi tai tuhoaminen

On tärkeää, että henkilötietoja käsitellään asianmukaisesti niiden koko elinkaaren ajan. Tehdyn vaikutusten arvioinnin perusteella suurimmat ongelmat liittyivät tiedon tuottamiseen ja vastaanottoon sekä tiedon arkistointiin ja poistamiseen.

Tiedon tuottamiseen liittyvät ongelmat keskittyivät organisaation tarjoamiin verkkotyökaluihin ja erityisesti niiden ”vapaakenttiin”. Näissä käyttäjät tuottavat itse tiedon järjestelmään ja organisaatiolla ei ole mahdollisuutta tähän vaikuttaa eikä myöskään valvoa sitä.

Tiedon poistamiseen ja arkistointiin liittyvät haasteet taas koskivat pääosin puutteellista ohjeistusta poistamisen määräajoista ja tämän automatisointia. Viimeisimmän tiedon mukaan tätä valmisteltiin organisaatiossa. Arkistointiin liittyi samankaltaisia ongelmia ja vaikutusten arviointi paljasti puutteita myös tämän ohjeistuksessa. ja käytänteissä.

9.6 Laitteistot

Laitteistoturvallisuuden perustan muodostaa niiden tekninen rakenne (Miettinen, Juha. E. 1999.). Laitteistoturvallisuus lähtee siis liikkeelle jo päätöksestä hankkia jokin henkilötietojen käsittelyssä käytettävä laite. Laitteiden hankintaan suunniteltaessa on arvioitava, millaisia ominaisuuksia laitteessa tulee olla ja onko joissakin komponenteissa esimerkiksi asetettava rajoituksia vaikkapa komponentin materiaaleille, valmistusmaalle, ohjelmistolle, jne. Nämä tulee huolehtia kuntoon jo ennen kilpailutusta sillä jälkikäteen syystä tai toisesta soveltumattoman komponentin tai ominaisuuden lisääminen voi olla hyvin kallista ja/tai hankalaa. Tässä hyvä perusajatus on tunnistaa tarvittavan laitteiston vaatimukset ja hankkia vain vaatimukset täyttäviä laitteita. Laitteistoturvallisuudessa huomioitavia osa-alueita ovat (Miettinen. Juha. E.1999):

1. Pääsynvalvonta (tekninen/ohjelmistollinen)
2. Tapahtumatietojen kerääminen
3. Varaosien saatavuus
4. Varmentaminen ja varmuuskopiointi
5. Laitteiden energian saannin varmistaminen
6. Laitteistodokumentaatio
7. Ylläpito- ja huoltosopimukset

Tietosuojan kannalta näistä keskeisimpiä ovat pääsynvalvonta (käyttäjien oikeudet) ja tapahtumatietojen kerääminen. Pääsynvalvonta voidaan toteuttaa teknisellä laitteella, esimerkiksi asiointikortin tms. lukijan avulla tai ohjelmistollisesti. Joissain organisaatioissa on käytössä näiden molempien yhdistelmä. Monissa organisaatioissa on käytössä vain ohjelmistollinen, käyttäjätunnuksiin ja salasanoihin perustuva järjestelmä.

9.7 Ohjelmistot

Ohjelmistoturvallisuuden osa-alueeseen kuuluvat kaikki henkilötietojen käsittelyssä käytettävät ohjelmistot, sovellukset sekä niitä suojaavat ohjelmistot. Ohjelmistoturvallisuudessa keskitytään ohjelmistojen suojaamiseen ja niiden haavoittuvuuksien minimointiin. Kyberturvallisuuskeskus määrittelee ohjelmistoturvallisuuden seuraavasti: ” Kyberturvallisuuden osa-alue, joka kattaa ohjelmistojen suunnittelun, toteutuksen ja käytön turvallisuuden” (https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjelmistoturvallisuuden%20tila%202023.pdf).

Ohjelmistoturvallisuuden keskeisimmät osa-alueet ovat:

- Haavoittuvuuksien tunnistaminen ja hallinta (Staattinen ja dynaaminen analyysi, penetraatiotestaukset)
- Koodin tarkastukset ja turvallinen koodaus
- Salaus ja avainten hallinta
- Käyttöoikeuksien hallinta
- Logitus ja seuranta
- Turvallisuusstandardit ja -sertifikaatit
- Haavoittuvuuksien hallinta ja päivitykset

Erityisesti ohjelmistojen hankinta ja ylläpito vaativat asiantuntemusta. Ohjelmistojen hankintaa suunniteltaessa on tärkeää pitää mielessä mitä ohjelmalla tullaan tekemään ja millaisia tietoja sillä tullaan käsittelemään. Kaikki ohjelmat, jotka toimintojensa puolesta sopisivat henkilötietojen käsittelyyn eivät välttämättä sovi siihen ominaisuuksiensa puolesta. Monet pilvi-pohjaiset ohjelmat ja

sovellukset esimerkiksi siirtävät tietoja EU/ETA alueen ulkopuolelle. Samoin ohjelmiston turvallisuusominaisuuksissa voi olla puutteita. Ohjelmistoa valittaessa on otettava huomioon myös päivitettävyys, tietoturvallisuus ja käytön helppous. Mikäli organisaatio katsoo, ettei sillä itsellään ole riittävää asiantuntemusta ohjelmistojen turvallisuudesta, on erittäin suositeltavaa hankkia sitä ennen hankintapäätöstä.

9.8 Käyttötoiminnot

Kirjassa Tietoturvallisuuden johtaminen (Miettinen, 1999) käyttötoimintojen turvallisuus mainitaan käyttötoimintojen turvallisuuden liittyvän läheisesti laitteisto- ja ohjelmistoturvallisuuteen. Se sisältää seuraavat osa-alueet:

- Käyttöoikeuksien hallinta
- Laitteisiin ja järjestelmiin kytkeytyminen
- Salasanojen hallinnointi
- Laitteiden ja järjestelmien käytön valvonta
- Kriittisten tehtävien hajauttaminen
- Varmuuskopiointi

Käyttöoikeuksien hallinnassa, perusmäärittelyjen jälkeen, usein haastavimmat tilanteet syntyvät henkilövaihdosten yhteydessä. Etenkin jos uusi henkilö tulee uuteen tehtävään, on helppoa vain antaa hänelle laajat käyttöoikeudet. Käyttöoikeuksien tulee kuitenkin perustua todelliseen tarpeeseen, ei käytännöllisyyteen. Toinen huomionarvoinen tilanne on, kun henkilö vaihtaa tehtävää talon sisällä. Sama pätee myös kytkeytymiseen erilaisiin järjestelmiin ja laitteisiin. Monessa organisaatiossa on rajoitettu oikeutta kytkeä puhelin, jokin ulkoinen muisti tai muu laite organisaation tietokoneeseen. Tämä kytkeminen tarkoittaa sekä langallista, että langatonta liittämistä. Organisaatio ei voi hallita työtekijöiden omia laitteita, joten nämä voivat muodostaa tietoturvariskin.

Organisaation omistamien laitteiden käyttöä ja järjestelmiä tulee valvoa tietoturvariskien varalta. Tämä valvonta ei saa kuitenkaan loukata työntekijän yksityi-

syyttä. Työntekijöiden tekniseen valvontaan liittyvät asiat tulee käsitellä yhteistoimintamenettelyssä ja niistä tulee tiedottaa henkilöstölle. Laki yksityisyyden suojasta työelämässä 21§ (2021/1337) säätelee tätä toimintaa.

Mikko Nyyssölän (Nyyssölä M. Yksityisyyden suoja työsuhteessa, Talentum. 2014. Viro. Print Best) mukaan väärinkäytöksiä epäiltäessä voidaan kuitenkin asian tutkintaan ja käsittelyyn käyttää myös sellaisia tietoja joiden valvonnasta ei ole yhteistoiminnassa sovittu ja tiedotettu. Näistä esimerkkinä välitystietojen käyttö tutkinnassa joiden käyttöön Tietoyhteiskuntakaaren 146§ (917/2014) antaa mahdollisuuden.

Kriittisten toimintojen hajauttaminen on varautumista monenlaisiin ongelmatilanteisiin. Perusajatuksena on, että yhden toiminnon tai laitteen ollessa poissa käytöstä tätä voidaan ainakin osittain korvata esimerkiksi muualle sijoitetulla vastaavalla toiminnolla tai laitteella. Tämä on myös osa laajempaa varautumisen kokonaisuutta.

Varmuuskopiointiin on pääsääntöisesti paras ratkaisu automatisoida se. Varmuuskopiot tosin muodostavat oman riskinsä itsessään sillä myös ne voivat vaarantaa tietoturvan. Varmuuskopiot tulee salata ja niiden siirto on myös suunniteltava turvalliseksi. Varmuuskopiointiin käytetään paljon pilvipalveluja, näiden tulee sijaita EU/ETA alueella mikäli ne sisältävät henkilötietoja.

10 Pseudonymisoidut ja anonymisoidut tiedot

Pseudonymisointi on tietosuojamenetelmä, jossa henkilötietoja muokataan siten, että niiden suora yhdistäminen tiettyyn henkilöön ilman lisätietoja muuttuu mahdottomaksi. Tämä tehdään useimmiten korvaamalla tunnistettavat tiedot, kuten nimi tai sähköpostiosoite, yhdellä tai useammalla keinotekoisella tunnisteella. Pseudonymisoinnin tavoitteena on suojata yksilöiden yksityisyys erityisesti datan käsittelyn ja analysoinnin yhteydessä.

Pseudonymisoinnissa ensimmäinen askel on tunnistaa ne henkilötiedot, jotka ovat pseudonymisoitavia, esimerkiksi nimet, osoitteet tai muut yksilölliset tunnisteet ja nämä korvataan pseudonyymeillä, eli jollain tunnisteella. Pseudonymisointiin liittyvät säännöt ja menetelmät on suunniteltava huolellisesti, jotta alkuperäisiä tietoja ei voida palauttaa tai yhdistää henkilöön ilman lisätietoja. Kun data on pseudonymisoitu, sitä voidaan käyttää esimerkiksi tutkimuksessa tai analytiikassa ilman, että yksittäisten henkilöiden yksityisyys vaarantuu. Tämä on erityisen tärkeää suurten datamäärien analysoinnissa, missä yksityisyyden suojan riskit ovat merkittäviä.

Anonymisoinnissa tiedot käsitellään siten, että henkilöiden tunnistaminen ei ole enää mahdollista millään lisätiedoilla. Anonymisointi poistaa mahdollisuudet yhdistää data takaisin alkuperäiseen henkilöön.

Pseudonymisointi on tehokas tapa suojata henkilötietoja silloin, kun anonymisointia ei voida tehdä tai kun datan on säilytettävä tietty yhteys alkuperäiseen kontekstiinsa tutkimuksellisista tai operatiivisista syistä.

11 Tekoälyn käyttö tietosuojan hallinnassa

Tekoälyllä voisi olla merkittävä rooli tietosuojan hallinnassa useilla eri tavoilla. Yksi keskeisimmistä on sen kyky hallita monimutkaisia prosesseja ja analysoida niitä, mikä voi parantaa tietosuojan valvontaa ja varmistaa sääntöjen noudattamisen. Tekoälyä voidaan käyttää henkilötietojen tunnistamiseen ja luokitteluun suurissa tietokannoissa, mikä helpottaa tietosuojan riskienhallintaa ja tietojen suojaamista. Tekoälyn käyttö on lisääntymässä myös tietopyyntöjen käsittelyssä ja se parantaa samalla rekisteröityjen yksityisyyden suojaa. Varsinaisia käsittelytoimia ei tarvitse tehdä niin paljon. Lisäksi tekoäly voi auttaa havaitsemaan poikkeavaa toimintaa ja havaita tietoturvaloukkauksia tehokkaammin kuin perinteiset manuaaliset menetelmät.

11.1 Tekoälyn tarjoamat hyödyt ja mahdollisuudet

Tekoälyn käyttö tietosuojan hallinnassa tarjoaa useita hyötyjä ja mahdollisuuksia. Tekoäly voi analysoida suuria tietomääriä nopeasti ja tarkasti, mikä mahdollistaa tehokkaamman tietosuojan hallinnan ja riskien tunnistamisen. Tämä luonnollisesti vaatii sen, että tekoäly on kyetty ohjaamaan tarkastelemaan oikeita asioita oikeista paikoista.

Automaatio mahdollistaa sen, että tekoäly voi suorittaa monimutkaisia tehtäviä, kuten tietojen luokittelua ja suojausta, ilman ihmisen jatkuvaa valvontaa. Tämä paitsi tehostaa valvontaa usein myös vähentää virheitä ja vääriä ”hälytyksiä”. Tekoäly voi tarjota reaaliaikaista valvontaa ja hälytyksiä mahdollisista tietoturvaloukkauksista, mikä nopeuttaa ja tehostaa niihin reagointia. Hyvin suunniteltu tekoäly voi auttaa varmistamaan, että henkilötietoja käsitellään lainmukaisesti ja yksilöiden oikeudet säilyvät. Rekisteröityjen yksityisyys paranee antamalla tekoälyn hoitaa monia käsittelytoimia ja valvontaa. Tekoälyn konfiguroinnissa on kuitenkin aiheellista olla tarkkana, ettei sen käytöllä synny myös rekisteröityihin kohdistuvaa automaattista päätöksentekoa. Silloin tekoälyn käyttö täytyy informoida rekisteröidyille asianmukaisesti ja siitä on kerrottava rekisteriselosteessa.

11.2 Tekoälyn käytön haasteet

Vaikka tekoälyn käytöllä on monia etuja tietosuojan hallinnassa, siihen liittyy myös merkittäviä riskejä ja haasteita. Tekoälyalgoritmit voivat sisältää piilotettuja ennakkoluuloja ja vinoumia, jotka voivat johtaa epäoikeudenmukaisiin päätöksiin ja tietosuojan loukkauksiin. Tekoälyn käytössä ja konfiguroinnissa on voitu tehdä virheitä, jotka voivat johtaa mahdollisiin tietoturvaloukkauksiin. Tämä on huomioitava erityisesti silloin, kun käsitellään erityisiä henkilötietoja.

Tekoälyalgoritmit voivat olla vaikeita selittää, mikä vaikeuttaa niiden toiminnan ymmärtämistä ja arviointia. Tekoälyn tekemät havainnot, johtopäätökset ja ratkaisut eivät välttämättä ole helposti arvioitavissa. Tämä heikentää toiminnan läpinäkyvyyttä ja on joissain tapauksissa selitteetöntä. Ei yksinkertaisesti ole käytössä tapaa tarkastella tekoälyn ratkaisun perusteita. Tämä saattaa joskus olla haastavaa myös vastuukysymysten tarkastelussa. Oikeudellinen vastuu tekemisistä ja tekemättä jättämisistä on aina rekisterinpitäjällä. On siis varsin mahdollista, että rekisterinpitäjä joutuu oikeudelliseen vastuuseen tekoälyn tekemästä toimesta tai ratkaisusta.

Tekoälyä tulee käyttää eettisesti ja vastuullisesti. Sen käytössä on oltava selkeät eettisiä periaatteet ja säännöt, joita noudatetaan tekoälyalgoritmien suunnittelussa ja käytössä. Tekoäly ei saa syrjiä ketään ja sen oltava tasapuolinen eri käyttäjäryhmien ja rekisteröityjen suhteen. Tekoälyn päätöksentekoprosessin tulee olla mahdollisimman läpinäkyvä ja selitettävissä.

12 Tietosuojan hallintamalli

Kuva 3: Tietosuojan hallintamalli

Tietosuojan hallintamalli on kuvaus (Kuva 3) prosessista, jolla organisaatio toteuttaa tietosuojaa toiminnassaan. Siinä kuvataan vaatimukset, jotka sille asetetaan ja mahdolliset uhat rekisteröidyille ja organisaatiolle, jotka tulee ottaa huomioon. Hallintamallin osa-alueet ovat osia, joista hallintamalli rakentuu.
Tässä, kuten muussakin turvallisuudessa on tärkeää huomioida, että osa-alueet ovat usein riippuvaisia toisistaan. Kun yksi osa pettää, se vaikuttaa heikentävästi myös muihin osa-alueisiin. Jos esimerkiksi henkilöstöstä joku ei tunnista mahdollista tietosuoja ongelmaa eivät tietosuoja-asiantuntijat voi toimia koska heille ei kulkeudu tieto ongelmasta. Tämä taas johtaa siihen, että riskien arviointi on puutteellinen ja siten ongelmaa ei pystytä huomioimaan tietoturvallisuudessa. Syntyy negatiivinen ”domino- efekti”. Kun yksi palikka kaatuu, se kaatuessaan kaataa muutkin. Tästä syystä on kokonaisuuden hallinta erityisen tärkeää, tietosuojan ketju on juuri niin vahva kuin sen heikoin lenkki.

12.1 Tietosuojan hallintamalli ja suojattavat edut

Tietosuojan hallintamallilla suojattavat edut voidaan jakaa kahteen eri tyyppiin, vaatimusten mukaisuuden varmistamiseen ja riskiperusteisiin.
Vaatimusten mukaisuuden varmistamiseen liittyvät seikat perustuvat kansalliseen ja EU -tason sääntelyyn, kun taas riskiperusteiset perustuvat tunnistettuihin riskeihin joko organisaatiolle tai rekisteröidyille.

Vaatimusten mukaisuuteen liittyvät riskit voivat toteutuessaan aiheuttaa merkittäviä oikeudellisia ja välillisiä seurauksia. Näitä seurauksia voivat olla:

1. Oikeudenkäyntikulut
2. Sakot ja yhteisösakot
3. Mahdolliset vahingonkorvaukset
4. Mainehaitat ja negatiivinen julkisuus
5. Menetetyt asiakkaat ja yhteistyökumppanit

12.2 Henkilöstö

Henkilöstö, ja ennen kaikkea henkilöstön osaaminen on monessa mielessä tärkein yksittäinen tekijä tietosuojan toteutumisessa. Se, että henkilöstöllä on kyky tunnistaa, milloin käsiteltävä tieto on tai muuttuu tietosuojan käsittämäksi henkilötiedoksi, on avain asianmukaiseen käsittelyyn. Toinen määrittävä tekijä on osaaminen, eli henkilöstö on perehdytetty oikeisiin toimintamalleihin.

Lähtökohta kaikelle toiminnalle henkilötietojen käsittelyssä on, että henkilöt, jotka sitä tekevät ovat tehtävään soveltuvia. Tämä tarkoittaa käytännössä sitä, että henkilöllä on riittävät tiedot ja taidot tehtävän suorittamiseksi ja hän on henkilökohtaisilta ominaisuuksiltaan tehtävään sopiva. Henkilötietojen käsittelyä työssään tekevän henkilön valinta lähtee jo rekrytoinnista. Organisaation tulee määrittää jo rekrytointia suunnitellessaan millaisia ominaisuuksia, tietoja ja taitoja henkilön tulevat työtehtävät edellyttävät. Tämän pohjalta määritetään vaatimukset mahdollisesti palkattavalle henkilölle. Mikäli henkilö on siirtymässä hen-

kilötietojen käsittelyä sisältäviin tehtäviin työpaikan sisältä, tulee henkilön soveltuvuutta arvioida paitsi henkilön ominaisuuksien, myös lisäperehdytyksen näkökulmasta. Millaista jatkokoulutusta henkilö mahdollisesti tarvitsee?

Valittavan henkilön luotettavuuteen ja henkilökohtaisiin ominaisuuksiin on syytä kiinnittää erityistä huomiota. Joillain organisaatioilla on mahdollisuus käyttää turvallisuusselvitysmenettelyä (Turvallisuusselvityslaki 2014/726) mutta isolla osalla organisaatioita tätä mahdollisuutta ei ole käytettävissään. Silloin on perusteltua käyttää erilaisia soveltuvuustestejä ja kiinnittää erityistä huomiota henkilön työhistoriaan.

Henkilötietoja käsittelevä henkilö tulee perehdyttää tehtäväänsä huolellisesti. Hänellä täytyy olla hyvä käytännön ymmärrys tietosuojaa säätelevästä lainsäädännöstä ja muusta sääntelystä. Henkilön on osattava käyttää hänen käytössään olevia ohjelmistoja ja laitteita.
Tärkeintä on kuitenkin perehdytys tehtävään. Henkilötietoja käsittelevän henkilön on tunnettava organisaation käytänteet ja ohjeet. Tämä osaaminen on tavalla tai toisella myös varmistettava ja myös dokumentoitava. Se on tärkeä osa rekisterinpitäjän lakisääteistä osoitusvelvollisuutta huolehtia rekisteröidyn tietojen asianmukaisesta käsittelystä. Tämä perehdytys mielletään usein projektiksi, jolla on alku- ja päätepiste. Tämä on kuitenkin miellettävä enemmänkin prosessina, eli se on jatkuvaa toimintaa organisaatiossa.

12.3 Tietosuoja-asiantuntijat

Organisaation on hankittava tietosuoja-asioihin erikoistunutta osaamista. Tätä voi hankkia käytännössä kolmella eri tavalla:

- Kouluttamalla ja perehdyttämällä henkilöä
- Ostamalla asiantuntijuutta ulkopuolelta
- Rekrytoinneilla

Etenkin organisaatioissa, joissa henkilötietoja käsitellään laajamittaisesti, on usein järkevintä hankkia tämä osaaminen omaan henkilöstöön. Satunnaisem-

massa tarpeessa paras vaihtoehto on usein hankkia asiantuntijapalveluita ulkopuolelta. Tietosuoja-asiantuntijat voidaan siis karkeasti jakaa sisäisiin ja ulkoistettuihin tahoihin.

Tietosuojan sisäisiä asiantuntijoita voi olla organisaation koosta ja toiminnasta riippuen monenlaisia. Tietosuojavastaava on GDPR:n tuntema sisäinen asiantuntija joka usein mainitaan ensimmäisenä. Hänen tulee olla perehtynyt tietosuojaan varsin syvällisesti. On kuitenkin hyvä huomata, että etenkin isommissa organisaatioissa henkilötietojen käsittelyä tehdään monissa eri järjestelmissä ja ohjelmistoissa. Tietosuojavastaavan ei ole mielekästä (eikä käytännössä usein edes mahdollista) perehtyä näihin kaikkiin riittävästi, siksi hän tarvitsee avukseen henkilöitä, jotka tuntevat järjestelmät ja ohjelmistot. Keskeinen osa tietosuojavastaavan ammattitaitoa on osata hyödyntää näiden henkilöiden asiantuntemusta työssään. Tietosuojavastaavan tehtävä ei ole tietää kaikesta tietosuojaan liittyvästä kaikkea, vaan pikemminkin osata kysyä oikeat kysymykset oikeilta ihmisiltä. Tämä toiminta on osaltaan myös osaamisen varmistamista ja ”piiloperehdyttämistä” henkilötietoja käsittelevälle henkilölle. Hyvässä vuorovaikutuksessa molemmat osapuolet oppivat keskustelusta.

Ulkopuolisia asiantuntijoita käytettäessä on varmistuttava siitä, että valittavalla yhteistyökumppanilla on riittävä ajantasainen asiantuntemus. Sopivan kumppanin löydyttyä on suositeltavaa pyrkiä luomaan pidempiaikainen kumppanuussuhde. Tämä vähentää merkittävästi tarvetta esitellä asioita ja perehdyttää kumppania käytänteisiin. Kilpailutukseen liittyvä ohjeistus ja sääntely voi tosin tätä joskus vaikeuttaa.

Tietosuojavaltuutetun toimisto vastaa myös kysymyksiin ja tiedusteluihin yksittäisissä asioissa. Yhdeksi heidän tehtävistään on kirjattu ” edistää tietoisuutta henkilötietojen käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista, velvollisuuksista ja oikeuksista” (https://tietosuoja.fi/tehtavat). Heitä viranomaisena velvoittaa hyvän hallinon oikeusperiaatteet joihin mm. neuvonta ja yhteistyö kuuluvat.

12.4 Suojattavien tietojen tunnistaminen ja käsittely

Suojattavien tietojen tunnistaminen ja niiden käsittelyyn liittyvät mahdolliset ongelmatilanteet tehdään pääsääntöisesti jo rekisterin luomisvaiheessa. Tässä vaiheessa tehtyjä päätöksiä ja niiden toteutumista vielä arvioidaan uudelleen järjestelmällisemmin vaikutusten arvioinnissa (DPIA).

Nämä menettelyt eivät kuitenkaan ole vastaus kaikkiin mahdollisiin ongelmatilanteisiin. Organisaatiolla voi olla henkilörekistereitä, joissa on monen tasoista tietoa rekisteröidyistä ja jokin yksittäinenkin tieto voi muuttaa tietosuojan kannalta koko rekisterin luonteen. Käytännön esimerkki:

Työpaikka X järjestää koulutustilaisuuden. Mukaan on tulossa noin 30 henkilöä ja heille järjestetään kahvitus. Työpaikka X kyselee osallistujilta mahdollisia ruoka-aineallergioita tarjoilujen järjestämiseen. Osallistujat vastaavat ja toimittavat tiedot ruoka-aineallergioistaan.

Koulutuksen osallistujaluettelo on monessa mielessä henkilörekisteri. Se sisältää tässä esimerkkitapauksessa henkilön nimen, työpaikan, työtehtävän ja yhteystiedot. Ei kuitenkaan mitään erityisiä henkilötietoja. Tämän luonne muuttuu, kun sinne kirjataan tietoa osallistujien ruoka-aine allergioista. Ne ovat terveyteen liittyvää tietoa ja siten erityisiä henkilötietoja. Tällaisia listoja on käsiteltävä rajatusti ja niiden tuhoamisesta on huolehdittava asianmukaisesti.

Organisaatiossa on tärkeää tunnistaa suojattavat, henkilötietoina käsiteltävät tiedot. Samoin on tärkeää havaita, milloin käsitellään erityisiä henkilötietoja. On perusteltua luokitella ”tavanomaisille” henkilötiedoille omat menettelytavat ja erityisille henkilötiedoille näitä tarkentavat menettelytavat. Henkilöstöllä on oltava valmiudet tunnistaa henkilötiedot ja luokitella nämä käsittelytoimissaan. Samoin automaattisen käsittelyn protokollat on suunniteltava siten, että rekisteröityjen yksityisyys ei vaarannu.

12.5 Sidosryhmät ja sopimukset

Henkilörekisterien käsittelyssä, ylläpidossa ja teknisessä toteutuksessa on usein mukana useita eri toimijoita. Samoin organisaatio saattaa käsitellä henkilötietoja jonkun toisen toimeksiannosta. Ohjelmistojen, verkkoalustojen, pilvipalveluiden jne. toteutuksesta ja ylläpidosta vastaa usein jokin toinen taho.

Kun organisaatio toimii toimeksiantajana jollekin toiselle organisaatiolle henkilötietojen käsittelyssä, tulee tästä organisaatiosta henkilötietojen käsittelijä. Tästä on tehtävä heidän kanssaan käsittelysopimus, jossa rekisterinpitäjänä toimiva organisaatio määrittelee käsittelyn ehdot ja rajoitukset.
Sama toimii myös toisinpäin, jos organisaatio saa joltain toiselta organisaatiolta toimeksiannon, joka sisältää tavalla tai toisella henkilötietojen käsittelyä on tästä tehtävä käsittelysopimus rekisterinpitäjänä toimivan organisaation kanssa.

Mikäli organisaatio toimii rekisterinpitäjänä, on tällä aina vastuu henkilötietojen turvallisesta käsittelystä. Tätä vastuuta ei voi yleensä sopimuksin siirtää henkilötietojen käsittelijälle. Rekisterinpitäjänä toimivan organisaation on varmistuttava siitä, että henkilötietoja käsittelevälle organisaatiolla on riittävät valmiudet ja kyvykkyydet hoitaa toimeksianto sovitulla tavalla. Tästä on laadittava kirjallinen henkilötietojen käsittelysopimus heidän kanssaan. Tämä on myös yksi tapa huolehtia rekisterinpitäjän osoitusvelvollisuudesta.

Sopimuksessa tulee sopia ainakin seuraavista seikoista:

- Yleiset oikeudet ja velvollisuudet
- Tietoturvallisuuden vaatimukset
- Alihankkijoiden käyttö
- Henkilötietojen siirrot ja niihin liittyvät menettelyt
- Tietoturvaloukkauksista ilmoittaminen
- Auditoinnit
- Salassapito
- Vastuunrajaukset
- Voimassaolo ja sen rajaukset

Tämän liitteeksi tulee tehdä yksityiskohtainen listaus siitä, mitä käsittelytoimia sopimus oikeuttaa tekemään. Mikäli mahdollista, on perusteltua myös käydä sopimuskumppanin tiloissa ja todeta itse tietoturvallisuuden näkökulmasta mahdollisen sopimuskumppanin toiminnan taso.

12.6 Riskienhallinta

Tietosuojan kaksi kulmakiveä erityisesti rekisterinpitäjän näkökulmasta ovat riskiperusteisuus ja osoitusvelvollisuus. Hyvin toteutettu riskienhallinta kattaa laajalti myös osoitusvelvollisuuden vaatimusta. Riskienhallinnan menettelyt tunnistavat, arvioivat ja toteuttavat toimenpiteet tunnistettujen riskien hallitsemiseksi. Tämä kaikki dokumentoidaan ja saadaan jatkuvasti päivittyvää tietoa siitä mitä on tehty, mitä on tekeillä ja mitä ollaan tulevaisuudessa tekemässä. Tietosuojassa riskienarviointi keskittyy riskeihin rekisteröinnin rekisteröidylle aiheuttamiin riskeihin, mutta tässä samassa yhteydessä on järkevää arvioida myös riskit organisaation ja rekisterinpitäjän näkökulmasta. Näin käytännössä samalla työllä saadaan hoidettua kaksi asiaa samalla kertaa.

Riskienarvioinnin ensimmäinen vaihe on suunnittelu. Tässä valitaan tarkastelun kohde ja tehdään tarvittavat rajaukset. Suunnitelmassa tulee olla myös ainakin suuntaa antava aikataulu ja kuvaus riskienarvioinnin menetelmistä ja laajuudesta, jolla se toteutetaan. Riskienarvioinnille on hyvä nimetä myös vastuuhenkilö, joka huolehtii läpiviennistä ja raportoinnista.

Seuraavaksi riskit tunnistetaan sovitulla tavalla. Riskien tunnistaminen on hyvä erottaa aluksi riskien arvioinnista. Tunnistamisvaiheessa käytännössä ”sana on vapaa”. Jos jokin työryhmän jäsen näkee mahdollisen ongelman jossain asiassa, se kirjataan ylös myöhempää tarkastelua varten. Riskien tunnistamisessa on hyvä käyttää apuna erilaisia pohjia ja avainsanaluetteloita (”tsekkilistoja”). nämä auttavat merkittävästi käymään läpi tietosuojan kannalta olennaiset asiat ja toisaalta toimivat itsessään usein myös rajauksina joilla merkitykseltään vähäisemmät seikat voidaan jättää huomioimatta.

Tunnistettujen riskien arvioinnissa tarkastelu tapahtuu kahden ulottuvuuden kautta. Nämä ovat riskin toteutumisen todennäköisyys ja riskin toteutuessaan

aiheuttamat seuraukset. On hyvä huomata, että nämä ovat aina perusluonteeltaan ennusteita tai työryhmän näkemyksiä. Riskienarviointi ei ole koskaan absoluuttisen tarkkaa. Todennäköisyyden ja seurausten yhdistelmästä saadaan usein jonkin taulukon tai kaavan mukaan riskille arvo, joka kuvaa sen suuruutta. Näin riskit saadaan suuruusjärjestykseen. Joskus on perusteltua myös arvioida riskin merkittävyyttä hieman laajemmin. Tällainen tarkastelu on usein organisaatiotason tarkastelua riskin merkityksestä rekisteröidylle tai organisaatiolle.

Toimenpiteitä tarkasteltaessa ja suunniteltaessa on hyvä painottaa ratkaisuja sellaisiin toimenpiteisiin, jotka vaikuttavat mahdollisimman laajasti. Näillä valinnoilla saadaan usein paitsi tehokas keino riskin hallitsemiseksi ja hallittua mahdollisesti useita eri riskejä, myös kasvatettua organisaation resilienssiä mahdollisesti jo tunnistamattomia riskejä vastaan. Toimenpiteiden toteutukselle on aina nimettävä vastuuhenkilö.

Riskienarvioinnit, niiden tulokset ja seuranta on tärkeää dokumentoida hyvin. Tämä dokumentaatio mahdollistaa paitsi toiminnan seurannan ja kehittämisen, on myös tärkeä osa osoitusvelvollisuuden toteuttamista. Organisaatio kykenee osoittamaan, että se on järjestelmällisesti pyrkinyt tunnistamaan ja arvioimaan rekisteröidyille rekisteröinnistä aiheutuvia riskejä ja haittoja.

12.7 Tietoturva

Tietoturvallisuuden piiriin voidaan katsoa kuuluvaksi kaikki ne menettelyt, jotka tavalla tai toisella pyrkivät suojaamaan tiedon käytettävyyttä, eheyttä ja luottamuksellisuutta.

Tiedon käytettävyys on yksi tietoturvan keskeisistä osa-alueista, ja se tarkoittaa, että tiedot ovat saatavilla ja käytettävissä silloin, kun niitä tarvitaan. Käytettävyys tarkoittaa, että tiedot ja järjestelmät ovat saatavilla valtuutetuille käyttäjille aina, kun niitä tarvitaan.

Käytettävyyden voivat vaarantaa esimerkiksi:

- Tekniset ongelmat
- Kyberhyökkäykset:
- Luonnonkatastrofit, onnettomuudet ja muut kriisit:
- Inhimilliset virheet

Tiedon käytettävyyden varmistamiseksi organisaatioiden tulee toteuttaa useita toimenpiteitä. Näitä ovat Whitman & Bratfordin (Whitman, M. E., & Mattord, H. J. (2018). Principles of Information Security. Cengage Learning.) mukaan

- Varmuuskopiointi
- Redundanssi
- Häiriönsietokyky
- Palautussuunnitelmat
- Kyberturvallisuus
- Käyttäjäkoulutus

Käytettävyys liittyy läheisesti tietosuojaan. Mikäli kerätty tieto ei ole käytettävissä sellaisessa muodossa, joka soveltuu käyttötarkoitukseen, on koko henkilörekisterin merkitys kyseenalainen. Miksi rekisteröidä, jos tiedolle ei ole käyttöä?

Tiedon eheys on yksi tietoturvan keskeisistä periaatteista, joka tarkoittaa tiedon tarkkuuden, täydellisyyden ja johdonmukaisuuden säilyttämistä koko sen elinkaaren ajan. Eheys varmistaa, että tieto ei muutu luvattomasti tai tahattomasti ja että se pysyy luotettavana ja käyttökelpoisena päätöksenteossa.
Tieto voi korruptoitua mm. inhimillisten virheiden, kyberhyökkäysten, teknisten vikojen tai onnettomuuksien seurauksena.
Tiedon eheyttä on ylläpidettävä koko tietojen elinkaaren ajan, alkaen tiedon luomisesta sen arkistointiin ja hävittämiseen saakka. Yleisesti käytössä olevia menettelyjä tiedon eheyden varmistamisessa ovat:

- Tarkistussummat ja hajautusfunktiot:
- Digitaaliset allekirjoitukset

- Versiohallinta
- Pääsynhallinta
- Auditointilokit

Monissa tietokantaohjelmistoissa on tiedon eheyttä varmistavia ja seuraavia toimintoja. Sekä tiedon, että tietojen siirron salaus turvaa myös osaltaan tiedon eheyttä. Asianmukainen automatisoitu varmuuskopiointi mahdollistaa monissa tapauksissa korruptoituneen tiedon palauttamisen.

Tiedon luottamuksellisuus tarkoittaa sitä, että tieto on suojattu luvattomalta käytöltä ja paljastamiselta. Luottamuksellisuuden turvaaminen varmistaa, että ainoastaan valtuutetut henkilöt voivat päästä käsiksi tietoon ja käyttää sitä.

Tiedon luottamuksellisuuden suojaamisen osa-alueet ovat:

- Tietojen salaaminen
- Käyttöoikeuksien hallinta
- Tietojen käsittelykäytännöt
- Henkilötietojen suoja
- Sopimukset ja lainsäädäntö

Henkilötietojen luottamuksellisuuden varmistamiseksi on perusteltua salata säilytettävät tiedot ja tietoliikenne niiden siirron aikana. Pääsy tietoihin tulee olla vain tunnistetuilla ja niihin valtuutetuilla henkilöillä. Tarvittaessa tiloja sekä laitteita, joilla tietoja käsitellään, voidaan rajata. Tämä tapahtuu erilaisin kulun- ja pääsynvalvonnan keinoin.
Edelleen kuitenkin yksi yleisimmistä tiedon luottamuksellisuuden vaarantavista tekijöistä on ihminen. Henkilöstöä tulee kouluttaa ja perehdyttää säännöllisesti tietoturvan ja -suojan menettelytavoissa. Luottamuksellisuuden ylläpito vaatii jatkuvaa valvontaa, teknisten ratkaisujen käyttöä sekä henkilöstön sitoutumista tietoturvakäytäntöihin.

12.8 Tietopyynnöt

Tietopyyntöjen käsittely on prosessi, jossa organisaatiot vastaavat saamiinsa tietopyyntöihin esimerkiksi asiakkaiden, työntekijöiden tai viranomaisten taholta. Tämä prosessi on tärkeä lainsäädännön ja tietosuoja-asetuksen (GDPR), mukaisen läpinäkyvyyden ja tietosuojan varmistamiseksi.

Tietopyynnön käsittely voidaan jakaa seuraaviin vaiheisiin (Krakau, T., & Haapalehto, S., Tietopyynnöt ja henkilötietojen luovuttaminen. Alma Talent. 2020. Helsinki):

- Pyynnön vastaanottaminen ja kirjaaminen
- Pyynnön vahvistaminen
- Identiteetin varmistaminen
- Pyynnön täsmentäminen
- Tietojen kerääminen
- Tietojen suodattaminen
- Tietojen toimittaminen

Tiedot tulee luovuttaa tietopyynnön esittäjälle sovitussa muodossa kuukauden kuluessa. Tavalla tai toisella on varmistettava, että tietopyynnön esittäjä on saanut tiedot.
Lähetetyt tiedot tulee dokumentoida, (mitä tietoja luovutettiin, kenelle, ajankohta, käsittelijä ja käsittelytapa) jotta voidaan myöhemmin osoittaa oman toiminnan oikeellisuus. Tätä dokumentaatiota tulee säilyttää lainsäädännön mahdollisesti edellyttämän ajan.

Tietopyynnön esittäjällä on oikeus esittää saamaansa vastaukseen korjauksia ja lisäselvityspyyntöjä. Tietopyynnöt perustuvat usein lainsäädäntöön ja organisaation tulee sitoutua lain noudattamiseen. Avoimuuden ja läpinäkyvyyden periaate on tietopyyntöjen käsittelyssä isossa roolissa. Tämä prosessi muokkaa osaltaan myös organisaation julkisuuskuvaa.
Organisaation on aiheellista kehittää tietopyyntöjen käsittelyyn hyvät käytänteet ja nimetä erikseen henkilöt, jotka näitä tekevät. Tekoälyn käytöllä tietopyyntöjen käsittelyä voidaan merkittävästi tehostaa ja tämä tarjoaa myös mahdollisuuksia

vähentää käsittelyä ihmisten toimesta. Tämä osaltaan parantaa sekä selvitysten luotettavuutta että rekisteröityjen yksityisyyden suojaa.

12.9 Poikkeamien ja tietoturvaloukkausten käsittely

Tietoturvaloukkausten käsittely on kriittinen prosessi, jonka avulla organisaatiot voivat minimoida vahingot, suojata tietoja ja noudattaa lakisääteisiä vaatimuksia tietoturvaloukkausten tapahtuessa. Tietoturvaloukkaus voi olla luvaton pääsy tietoihin, tietojen menettäminen/korruptoituminen tai tahallinen tietojen manipulointi. Tietoturvaloukkauksen käsittely voidaan jakaa seuraaviin vaiheisiin:

- Havaitseminen
- Kirjaaminen
- Loukkausten arviointi
- Tietojen kerääminen
- Korjaavat toimenpiteet
- Eristäminen
- Korjaaminen
- Ilmoitukset (sisäiset/ulkoiset)
- Viestintä
- Jälkikäsittely ja analyysi
- Opitun hyödyntäminen

Asianmukaisesti käsitelty tietoturvaloukkaus vähentää riskejä ja vahinkoja sekä parantaa organisaation kykyä reagoida tulevaisuudessa tapahtuviin tietoturvahyökkäyksiin.
Mikäli riski rekisteröidyille arvioidaan suureksi, on rekisteröityjä informoitava tietoturvaloukkauksesta ja ilmoitettava asiasta Tietosuojavaltuutetun toimistolle 72h kuluessa. Tietoturvaloukkaus on aina itsetarkastelun ja kehittymisen paikka eli niissä voidaan nähdä myös positiivinen puoli.

12.10 Tietosuojapolitiikka ja -strategia

Tietosuojapolitiikka on dokumentti, joka määrittelee organisaation sitoumukset ja käytännöt henkilötietojen suojaamiseksi. Se on myös organisaation ylimmän johdon linjaus ja tahdonilmaus. Se tarjoaa yleiset periaatteet henkilötietojen käsittelystä henkilöstölle ja tiedottaa ulkopuolisille tahoille, kuten asiakkaille ja sidosryhmille, siitä, miten organisaatio käsittelee ja suojaa henkilötietoja.

Tietosuojapolitiikan yksi keskeinen tarkoitus on luottamuksen rakentaminen, niin sisäisesti kuin ulkoisesti. Tällä organisaatio sitoutuu noudattamaan vallitsevaa lainsäädäntöä ja hyviä käytänteitä. Osaltaan tämä myös luo positiivista julkisuuskuvaa organisaatiosta luotettavana toimijana, joka arvostaa rekisteröityjen oikeuksia.

Tietosuojastrategia kuvaa yleisellä tasolla, miten organisaatio tietosuojapolitiikkaa toteuttaa. Siinä kuvataan, miten henkilötietoja kerätään, käytetään, säilytetään ja luovutetaan. Strategia varmistaa, että tietojen käsittely on lainmukaista, tarkoituksenmukaista ja läpinäkyvää. Siinä voi olla myös kuvaus siitä, millaisia teknisiä ja organisatorisia toimenpiteitä organisaatio tekee suojatakseen henkilötietoja luvattomalta käytöltä ja paljastamiselta.
Tietosuojastrategiassa usein myös kuvataan myös toimintaa tietoturvaloukkaustilanteissa, kuten informointikäytänteitä rekisteröidyille ja viranomaisille.

Tietosuojastrategia on laajempi suunnitelma, joka määrittelee organisaation pitkän aikavälin tavoitteet ja lähestymistavat henkilötietojen suojaamiseksi. Se auttaa varmistamaan, että tietosuojakäytännöt ovat johdonmukaisia ja integroituja organisaation liiketoimintatavoitteisiin.

Tietosuojastrategiassa voi olla myös määriteltynä pitkän aikavälin visio ja keskeiset tavoitteet ja kuvaus tietosuojan hallinnoinnista sekä valvonnasta organisaatiossa.

Osana tietosuojastrategiaa voi olla myös kriisiviestintäsuunnitelma tietoturvaloukkausten varalta.

Tietosuojapolitiikka ja -strategia ovat keskeisiä työkaluja organisaation tietosuojan hallinnassa ja kehittämisessä, ja ne auttavat varmistamaan, että henkilötietojen käsittely on turvallista ja läpinäkyvää.

12.11 Omavalvonta

Tietosuoja omavalvonta tarkoittaa organisaation sisäisiä menettelyjä ja käytäntöjä, joilla varmistetaan, että henkilötietojen käsittely noudattaa tietosuojalainsäädäntöä ja organisaation omia tietosuojapolitiikkoja. Omavalvonta on jatkuva prosessi, joka auttaa tunnistamaan, arvioimaan ja hallitsemaan tietosuojariskejä sekä parantamaan tietosuojakäytäntöjä.

Nimitetään tietosuojavastaava, joka valvoo tietosuojaan liittyviä käytäntöjä ja menettelyjä. Tietosuojavastaavan tehtäviin kuuluu muun muassa henkilöstön koulutus, tietosuojakäytäntöjen seuranta ja tietosuojaloukkausten käsittely. Tietosuojavastaava on usein keskeisin yksittäinen toimija omavalvonnassa ja hän koordinoi sitä.
Tietosuojavastaava huolehtii osaltaan myös siitä, että tietosuojaan kohdistuvia riskejä seurataan ja arvioidaan säännöllisesti. Arviointien perusteella tunnistetaan ja priorisoidaan riskit sekä määritellään toimenpiteet niiden hallitsemiseksi. Nämä riskienarvioinnit ovat keskeinen osa omavalvontaa.

Erilaisia henkilötietojen käsittelyyn liittyviä prosesseja seurataan ja auditoidaan säännöllisesti. sisäisten auditointien lisäksi on usein perusteltua käyttää myös määrävälein ulkoisia auditoijia. Näin varmistetaan käytänteiden ja menettelyjen ajantasaisuus.

Dokumentoidaan kaikki tietosuojatoimet ja -prosessit sekä niiden tulokset. Laaditaan säännöllisiä raportteja johdolle ja muille sidosryhmille tietosuojan tilasta ja kehityksestä. Omavalvonta auttaa varmistamaan, että organisaatio noudattaa soveltuvaa tietosuojalainsäädäntöä
Tietoturvaloukkauksien simuloinnilla harjoitellaan tietoturvaloukkauksien käsittelyä simuloimalla mahdollisia tilanteita. Nämä harjoitukset paljastavat usein heikkoja kohtia käytänteissä. Tietosuojan omavalvonta on keskeinen osa organisaation tietosuojan hallintaa ja kehittämistä.

13 JOHTOPÄÄTÖKSET JA POHDINTA

Työn tavoitteena oli luoda malli, joka yhdenmukaistaa tietosuojaan liittyviä menettelyjä ja käytänteitä mutta kuitenkin skaalautuu tarpeen mukaan. Keskeisimpänä tutkimuskysymyksenä olikin mitä tällaisen mallin sitten pitäisi sisältää ja mitä sen pitäisi ottaa huomioon?
Työstä rajattiin pois viranomaisrekisterit ja muut rekisteröidyn tahdosta riippumattomat henkilörekisterit. Näiden käsittely olisi laajentanut työtä tarpeettoman paljon.

Olen lyhyesti sanottuna malliin tyytyväinen. Se kuvaa mihin haasteisiin tietosuojatoiminnan on organisaatiossa kyettävä vastaamaan ja keinot, joilla organisaatio niihin vastaa.
Jokainen mallin osa-alue on itsessään kuitenkin laaja asiakokonaisuus, monista niistä, tai jopa niiden yksittäisistä osa-alueista, voisi tehdä hyvinkin laajan selvityksen. Tämän työn tarkoitus oli kuitenkin olla geneerinen malli, joka soveltuu mahdollisimman monenlaisten henkilörekisterien hallintaan erilaisissa organisaatioissa. Yksityiskohtaisia neuvoja kysymyksiin työstä ei kuitenkaan välttämättä löydä. Työn anti lukijalle on auttaa oikeiden kysymysten äärelle ja toimia ”tee ainakin nämä” -listana. Se ei mene kovinkaan syvälle yksittäisiin asioihin ja tämä on myös työn heikkous.

Tietosuoja on varsin laaja asiakokokonaisuus, joka sisältää monimutkaisia kokonaisuuksia niin tekniseltä, juridiselta kuin hallinnolliseltakin puolelta. Tässä työssä keskityin lähinnä tietosuojan hallintoon. Tietosuojassa on tärkeää kuitenkin huomata, että osa-alueita ei voi erottaa toisistaan. Kun yhtä osa-aluetta muutetaan, lähes poikkeuksetta muutoksia joudutaan tekemään myös muissa osa-alueissa. Tämän hahmottamisessa tästä tietosuojan hallintamallista on varmasti apua. Hallinnon täytyy tuntea tietosuojan osa-alueet ja niiden keskinäiset riippuvuussuhteet jotta osataan ohjata oikeat ihmiset tekemään oikeita asioita sekä laittaa asioita tärkeysjärjestykseen. Tässä kysymys on siis kokonaisuuden hallinnasta.

Työn luotettavuus on kirjoitushetkellä hyvä, mutta tietosuojan sääntelyyn liittyvissä asioissa on normit aina syytä varmistaa ajantasaisesta lähteestä. Tietosuojan sääntely muuttuu suhteellisen nopeasti ja se on monelta osin velvoittavaa sääntelyä.

Vaikka käyttämäni tietoturvallisuuden osa-alueiden jaottelu on suhteellisen vanha (vuodelta 1999) on se edelleen monessa organisaatiossa käytössä lähes sellaisenaan. Osa-alueiden sisällön olen pyrkinyt päivittämään tämän päivän normien mukaiseksi. Valitsemani lähteet ovat enimmäkseen kirjoitushetkellä voimassaolevaa lainsäädäntöä tai muuten peräisin viranomaisilta tai muilta luotetuilta tahoilta. Näissä olen pyrkinyt välttämään tulkintaa mahdollisimman paljon ja kertomaan tiedon sellaisena kuin se on kyseisen tahon toimesta esitetty.

Työn eettisyydessä ja puolueettomuudessa en näe ongelmaa. Tietosuojaan liittyvä työ on lähtökohtaisesti eettisyyttä edistävää, ei vaarantavaa. Koko tietosuoja toiminnan idea on pohjimmiltaan ohjata rekisterinpitäjiä toimimaan eettisesti keräämiensä tietojen kanssa ja suojata ihmisten yksityisyyttä ja oikeuksia. Nykyään olen vaihtanut työtehtäviä toisiin ja en työskentele tällä hetkellä tietosuojan parissa missään roolissa. Tietosuojavastaavan tehtävä ei myöskään ole olla kenenkään puolella tai jotakin toista vastaan. Vaikka hän valvoo rekisteröityjen oikeuksien toteutumista, hän myös auttaa rekisterinpitäjää hoitamaan velvoitteensa parhaalla mahdollisella tavalla.

13.1 Opinnäytetyön prosessi

Opinnäytetyön tekeminen aloitettiin jo vuonna 2021. Pidin kuitenkin opiskelussa taukoa ja varsinainen työ tehtiin syksyn 2023 ja kevään 2024 välillä. Työn viimeistelyä vaikeutti, että syksyllä 2023 vaihdoin toisen työnantajan palvelukseen ja lähestymistapaa työhön piti hieman muuttaa. Työ muutettiin täysin geneeriseksi tietosuojan hallintamalliksi ohjaajani Jussi Yläsen ajatuksesta toukokuussa 2024. Työstä siis poistettiin viittaukset organisaatioihin tai henkilöihin.

Työn eteneminen oli seuraava:

1. Työn ideaperi esitettiin 25.11.2021
2. Väliesitys oli 14.3.2024
3. Viimeistelemättömän työn esitys 23.5.2024
4. Työn palautus tarkastukseen 2.6.2024

Työskentelimme varsin tiiviissä yhteistyössä opponoitavani/opponenttini kanssa. Hän on myös tämän työn opponentti. Meillä oli kerran säännöllisesti kerran viikossa teams -palaveri. Lisäksi meillä oli lukuisia muita palavereja ja keskusteluja opinnäytetöistämme. Haluan tässä myös kiittää häntä merkittävästä tuesta ja avusta tämän työn valmistumiselle.

Huhtikuulle 2024 oli alun perin suunniteltu haastatteluja tähän työhön liittyen mutta nämä peruuntuivat aikataulu haasteiden takia. Nämä olisivat varmasti tuoneet lisäarvoa työlle.

13.2 Aiheita jatkotutkimukselle

Itselleni, näin riskienhallinta taustaisena, on isoimpana kehittämiskohteena tietosuojassa tällä hetkellä noussut esiin vaikutusten arvioinnit eli DPIA -menettelyt ja niiden toteutus. Näissä käytetään usein menetelmänä monessa mielessä vanhentunutta avainsana listaa riskien tunnistamiseen. Avainsanalistat ovat sinällään, olettaen että niitä päivitetään, menetelmänä hyvä mutta käytössä ei ole mitään tukevaa tai rinnakkaista menettelyä, joka huomioisi asioita, joita listassa ei ole. Tämä aiheuttaa joskus sen, että riskejä avainsanalistan ulkopuolelta jää tunnistamatta vaikka nämä olisivat joskus ilmeisiäkin. Tunnistamatonta riskiä ei useimmiten voi hallita. Hyvä resilienssi voi osaltaan auttaa tässä, mutta tämä hallinta on tiedostamatonta, ei tietoista toimintaa.
Tähän samaan aiheeseen liittyvä on myös tunnistettujen riskien arviointi menettelyt. DPIA:ssa käytetään edelleen usein vanhentuneita riskimatriiseja, vaikka parempia menetelmiä olisi käytettävissä riskin suuruuden määrittämiseen. Riskimatriisit usein korostavat ”katastrofaalisten” riskien merkitystä riippumatta siitä miten epätodennäköisiä ne ovat. Tämä taas ohjaa päätöksentekoa ja resurssit

ohjautuvat joskus vääriin kohteisiin. Tämä ei ole tehokasta eikä taloudellista toimintaa. Vaikutusten arviointien rooli on kuitenkin pohjimmiltaan hankkia tietoa päätöksenteon tueksi ja sitä kautta toteuttaa toimenpiteitä riskien hallitsemiseksi. Yleisesti voisi siis todeta, että tietosuojan vaikutusten arvioinneissa olisi paljon kehitettävää.

Toinen tieto, joka minut yllätti aikoinaan tietosuojavastaavana toimiessani, oli henkilörekistereitä ylläpitävän tai muodostavan verkkopalvelujen tarjoajien heikko osaaminen tietosuoja-asioissa. Olisi ollut erittäin hyödyllistä, jos heillä olisi jonkinlainen sertifiointi järjestelmä tai peruskoulutus tietosuoja- asioihin. Tällaisen koulutuksen tarvetta ja mahdollista sisältöä olisi hyvä selvittää tarkemmin.

Kolmantena tulee mieleen tietosuojavastaavien osaaminen. Heille ei ole määritelty mitään pakollista tai edes suositeltua koulutusta. Tällä hetkellä tilanne on edelleen se, että tämä on pitkälti tietosuojavastaavien oman mielenkiinnon ja kouluttautumisen varassa ja työpaikat tukevat heitä tässä enemmän tai vähemmän. Tietosuojavastaavien osaamisessa on valtavia eroja. Olisi erittäin perusteltua selvittää vaihtoehtoja tämän ongelman ratkaisemiseksi ja löytää jokin ratkaisu tähän.

14 LÄHTEET

Verkko

Erityisten henkilötietoryhmien käsittely. n.d. Tietosuojavaltuutetun toimisto. Viitattu 9.3.2024
https://tietosuoja.fi/erityisten-henkilotietoryhmien-kasittely

Hallinto-oikeus piti voimassa tietosuojavaltuutetun päätökset vakuutusyhtiöiden terveystietojen käsittelystä. 25.1.2024 Viitattu 1.3.2024
https://tietosuoja.fi/-/hallinto-oikeus-piti-voimassa-tietosuojavaltuutetun-paatokset-vakuutusyhtioiden-terveystietojen-kasittelysta

Henkilötietojen käsittelyn roolit ja vastuut tieteellisessä tutkimuksessa. n.d. Tietosuojavaltuutetun toimisto. Viitattu 20.5.2024
https://tietosuoja.fi/henkilotietojen-kasittelyn-roolit-ja-vastuut

Henkilöstö- ja toimitilaturvallisuus. 19.3.2007. Aalto, teknillinen korkeakoulu
http://www.cse.hut.fi/fi/opinnot/T-110/T-110.5610/2007/kalvot/kuorisuojaus-6.pdf

Kasvatuksen ja koulutuksen tietomurto. 22.5.2024. Helsingin kaupunki. Viitattu 2.6.2024
https://www.hel.fi/fi/paatoksenteko-ja-hallinto/tietomurto
Kerro käsittelystä rekisteröidylle. n.d. Tietosuojavaltuutetun toimisto. Viitattu 10.5.2024
https://tietosuoja.fi/rekisteroidyn-informointi

Luottokelpoisuuden arviointimenettely. n.d. Yhdenvertaisuus- ja tasa-arvolautakunta. Viitattu 3.1.2024
https://www.yvtltk.fi/material/collections/20230609132927/Hs0XG8IKF/Tapausseloste_YVTltk_2xx_2017_luottokelpoisuuden_arviointimenettely.pdf

Marinin hallituksen ministerin terveystietoja urkittu Husissa – epäilty on Suomen ja Venäjän kaksoiskansalainen. 4.5.2024. MTV uutiset. Viitattu 6.5.2024
https://www.mtvuutiset.fi/artikkeli/sk-marinin-hallituksen-ministerin-terveystietoja-urkittu-husissa-epailty-on-suomen-ja-venajan-kaksoiskansalainen/8689902

Mikä on tietoturvaloukkaus ja miten sellaisen sattuessa pitää toimia? 1.6.2024. Euroopan komissio
https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_fi

Ohjelmistoturvallisuuden tila 2023 Nykytilaraportti. 12.10.2023 Viitattu 13.3.2024
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Ohjelmistoturvallisuuden%20tila%202023.pdfhttps://tietosuoja.fi/rekisteroidyn-oikeudet

Tietoturvapoikkeamatilanteiden hallinta. n.d. Valtiovarainministeriön julkaisuja 8/2017. Viitattu 1.4.2024
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79258/VM_8_2017.pdf?sequence=6&isAllowed=y

Tiedon elinkaari julkisessa hallinnossa. 8.6.2022. Tiedonhallintalautakunta. Viitattu 4.5.2024
https://vm.fi/documents/10623/123922064/Torro+Heidi+-Tiedon+elikaari+20220608.pdf/52fa46e5-5d52-b28a-affc-34437171d622/Torro+Heidi+-Tiedon+elikaari+20220608.pdf?t=1655200575795

Tietoturvasääntely. 26.2.2024 Traficom. Viitattu 3.3.2024
https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturvasaantely

Rekisteröidyn suostumus. n.d. Tietosuojavaltuutetun toimisto. Viitattu 20.5.2024
https://tietosuoja.fi/rekisteroidyn-suostumus

Vaikutustenarviointi. n.d. Tietosuojavaltuutetun toimisto. Viitattu 20.4.2024
https://tietosuoja.fi/vaikutustenarviointi

Tietosuojavaltuutetun päätös luetteloksi käsittelytoimista, joiden yhteydessä on tehtävä vaikutustenarviointi. n.d. Tietosuojavaltuutetun toimisto. Viitattu 13.2.2024
https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista

Tietosuojavastaavat. n.d. Tietosuojavaltuutetun toimisto. Viitattu 19.4.2024
https://tietosuoja.fi/tietosuojavastaavat

Opinnäytteet

Mikael Nuotio, Profilointi ja vakuutusriskin arviointi, Aalto-yliopisto, 2023

Heinonen H. Strategian merkitys tietoturvan johtamisessa. Jyväskylän ammattikorkeakoulu. 2020

Heiskanen Ari, Maine ja maineenhallinta: Miten lahtelaiset ovat ottaneet Mediakulman vastaan? Lahden ammattikorkeakoulu. 2009.

Kirjat:

Aula, P. & Mantere, S. 2005. Hyvä yritys: Strateginen maineenhallinta. Helsinki: WSOY

Hirsjärvi, S., Remes, P., & Sajavaara, P. 2016. Tutki ja kirjoita. Porvoo: Bookwell Oy.

Hopkin P. Fundamentals of risk management 5th edition, 2018, Kogan page limited, USA

Krakau, T., & Haapalehto, S., Tietopyynnöt ja henkilötietojen luovuttaminen. Alma Talent. 2020. Helsinki

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Jyväskylä. Gummerus kirjapaino Oy

Miettinen, Juha. E., Tietoturvallisuuden johtaminen, Gummerus. 1999. Jyväskylä

Miettinen Juha. E., Yritysturvallisuuden käsikirja, Kauppakaari. 2002. Helsinki

Nyyssölä, M., Yksityisyyden suoja työsuhteessa, Talentum. 2014. Viro. Print Best

Whitman, M. E., & Mattord, H. J. Principles of Information Security. 2018. U.S.A., Cengage Learning.

Luennot:

Johdatus tiedusteluun. 2024. Verkkokoulutus. Jyväskylän yliopisto. 5.1.2024.

Pönkä, H. Innowise. 2020. Tietosuojavastaavan tehtävä ja henkilötietojen käsittelyn perusteita. Luento. Tietosuojavastaavien peruskoulutus. Snellman -kesäyliopisto. 3.12.2020.