Opinnäytetyö (AMK)

Liiketalouden koulutusohjelma

2020

Jari Virta

TIETOSUOJA TURVALLISUUSPALVELUISSA

- Keskeiset säädökset ja käsittelytoimet

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Liiketalouden koulutusohjelma

2020 | 65 sivua

Jari Virta

TIETOSUOJA TURVALLISUUSPALVELUISSA

- Keskeiset säädökset ja käsittelytoimet

Opinnäytetyön aiheena oli tietosuoja turvallisuuspalveluissa. Tutkimuksessa turvallisuuspalvelut oli rajattu Suomessa toimiviin, lain yksityisistä turvallisuuspalveluista sisältämiin ja ohjaamiin turvallisuuspalveluihin. Tutkimuksen tietoperusta oli EU:n yleinen tietosuoja-asetus ja tätä täydentävä kansallinen lainsäädäntö. Opinnäytetyön toimeksiantaja oli Suomen Turvapalvelu.

Tutkimuksen yleisenä tavoitteena oli konkretisoida kirjallisesti EU:n tietosuoja-asetuksen ja tietosuojalain keskeiset säädökset turvallisuuspalveluyrityksen näkökulmasta. Toimeksiantajan asettama opinnäytetyötavoite oli selvittää ja dokumentoida EU:n tietosuoja-asetuksen ja tietosuojalain keskeiset säädökset ja käsittelytoimet selkeäksi ja hyödynnettäväksi käsikirjaksi.

Teoriatiedon hankkiminen perustui pääasiassa EU:n tietosuoja-asetuksen, tietosuojalain ja EU:n tietosuojatyöryhmän lausuntojen lukemiseen ja tutkimiseen, sekä joidenkin tietosuojasta kirjoitettujen kirjallisten tuotosten lukemiseen. Tutkimuksessa hyödynnettiin empiiristä tietoa ja osaamista. Tietosuojasäädöksiä ja käsittelytoimia arvioitiin ja pohdittiin työ- ja yrityselämässä.

Tuloksena syntyi tavoitteen mukainen tietosuoja-asetuksen ja tietosuojalain keskeiset säädökset ja käsittelytoimet sisältävä ja avaava käsikirjamainen opinnäytetyö. Opinnäytetyötä voi hyödyntää henkilötietoja käsittelevien henkilöiden koulutuksessa ja tietosuojaoppaana toimialan yrittäjille. Tätä tutkimistyötä voisi jatkaa keskittymällä yksityiskohtaisemmin riskien ja vaikutusten arviointiin.

ASIASANAT:

Tietosuoja, henkilötietojen käsittely, EU:n yleinen tietosuoja-asetus, GDPR, turvallisuuspalvelut.

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Administration

2020 | 65 pages

Jari Virta

DATA PROTECTION IN SECURITY SERVICES

- Key regulations and processing activities

The topic of the thesis was data protection in security services. In the study security services were limited to security services operating in Finland and included in and directed by the Private Security Services Act. The database for the study was the EU General Data Protection Regulation and complementary national legislation. The thesis was commissioned by Suomen Turvapalvelu.

The general objective of the study was to concretize in writing the key provisions of the EU Data Protection Regulation and the Data Protection Act from the perspective of a security service company. The aim of the thesis set by the client was to find out and document the key legal decrees and processing activities of the EU Data Protection Regulation and the Data Protection Act's decrees into a clear and beneficial manual.

The acquisition of theoretical knowledge was mainly based on reading and researching the EU Data Protection Regulation, the Data Protection Act and the opinions of the EU Data Protection task force, as well as reading some written works on data protection. The study utilized empirical knowledge and expertise. Data protection regulations and processing activities were assessed and discussed in working and business life.

The result was a handbook-like thesis containing and opening the key regulations and processing activities of the EU Data Protection Regulation and the Data Protection Act in accordance with the objective. The thesis can be utilized in the training of persons handling personal data and as a data protection guide for entrepreneurs in the field. This research could be continued by focusing more closely on risk and impact assessment.

KEYWORDS:

Data protection, Processing of personal data, EU General Data Protection Regulation, GDPR, Security services.

SISÄLTÖ

KUVAT

SANASTO

Lähde:	**EU:n yleinen tietosuoja-asetus, artikla 4**
Biometrinen tieto	”Tarkoitetaan kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa”.
Henkilötieto	”Tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, jäljempänä ’rekisteröity’, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella”.
Henkilötietojen käsittelijä	”Tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun”.
Kolmas osapuoli	”Tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta toimielintä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää ja henkilöä, joilla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena”.
Käsittely	”Tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista”.
Käsittelyn rajoittaminen	”Tarkoitetaan tallennettujen henkilötietojen merkitsemistä tarkoituksena rajoittaa niiden myöhempää käsittelyä”.
Profilointi	”Tarkoitetaan mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia, erityisesti analysoidaan tai ennakoidaan piirteitä, jotka liittyvät kyseisen luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin”.

Pseudonymisointi	”Tarkoitetaan henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu”.
Rekisteri	”Tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu”.
Rekisterinpitäjä	”Tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti”.
Rekisteröidyn suostumus	”Tarkoitetaan mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen”.
Terveystiedot	”Tarkoitetaan luonnollisen henkilön fyysiseen tai psyykkiseen terveyteen liittyviä henkilötietoja, mukaan lukien tiedot terveyspalvelujen tarjoamisesta, jotka ilmaisevat hänen terveydentilansa”.
Tietoturvaloukkaus	”Tarkoitetaan tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin”.
Vastaanottaja	”Tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, jolle luovutetaan henkilötietoja, oli kyseessä kolmas osapuoli tai ei. Viranomaisia, jotka mahdollisesti saavat henkilötietoja tietyn tutkimuksen puitteissa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti ei kuitenkaan pidetä vastaanottajina; näiden viranomaisten on käsiteltävä kyseisiä tietoja sovellettavia tietosuojasääntöjä noudattaen käsittelyn tarkoitusten mukaisesti”.
Yritys	”Tarkoitetaan taloudellista toimintaa harjoittavaa luonnollista henkilöä tai oikeushenkilöä sen oikeudellisesta muodosta riippumatta, mukaan lukien kumppanuudet tai yhdistykset, jotka säännöllisesti harjoittavat taloudellista toimintaa”.

1 JOHDANTO

Tämän opinnäytetyön aiheena on tietosuoja turvallisuuspalveluissa. Opinnäytetyössä tutkitaan henkilötietojen käsittelyä tietosuojalakien ja asetusten asettamien vaatimusten mukaisuuden näkökulmasta turvallisuuspalveluissa. Tutkimuksessa turvallisuuspalvelut on rajattu Suomessa toimiviin, lain yksityisistä turvallisuuspalveluista sisältämiin ja ohjaamiin turvallisuuspalveluihin, eli vartiointi-, järjestyksenvalvonta- ja turvasuojaustoimintaan. Tarkasti toimialaan rajattuna tutkimus voi olla hyödyksi alalla toimiville yrityksille niiden tarkastellessa tietosuojaan liittyviä käytäntöjään tai uusille aloitteleville yrityksille.

Tutkimuksen pääasiallinen tietoperusta on EU:n tietosuoja-asetus ja tätä täydentävä kansallinen lainsäädäntö. EU:n tietosuoja-asetus on osin vaikeaselkoinen ja monitulkintainen. Asetuksen voimaantulon jälkeinen käytäntö, voimaan astuneet tai päivitetyt kansalliset lait, esiin nousseet ja nousevat oikeustapaukset tulevat osaltaan ohjaamaan ja tarkentamaan EU:n tietosuoja-asetuksen edellyttämiä henkilötietojen käsittelyyn liittyviä toimia ja toimintamalleja. Yrityksiä palvelevia käytännönläheisiä, yksinkertaistettuja, mutta riittävän tietoperustan kattavia teoria- ja toimintaohjeita on edelleen liian suppeasti.

Opinnäytetyön toimeksiantaja on turvallisuuspalveluja tarjoava Suomen Turvapalvelu. Tutkimuksen tavoitteena on konkretisoida kirjallisesti EU:n tietosuoja-asetuksen ja tietosuojalain keskeiset vaatimukset, sekä niiden edellyttämät velvoitteet turvallisuuspalveluja tuottavien yritysten näkökulmasta. Tutkimuksen tavoite on vastata kysymykseen, miten huomioida tietosuojaan liittyvät oikeudet ja velvollisuudet tietosuoja-asetuksen ja tietosuojalain säädösten mukaisesti. Toimeksiantajan antama opinnäytetyötavoite on selvittää ja dokumentoida EU:n tietosuoja-asetuksen ja tietosuojalain keskeiset säädökset ja käsittelytoimet selkeäksi käsikirjaksi turvallisuuspalveluyrityksen käyttötarpeisiin. Käsikirjamaisuutensa vuoksi opinnäytetyön sisällysluettelo laaditaan yksityiskohtaiseksi.

Teoriatiedon hankkiminen ja omaksuminen perustuu tietosuojaa säätelevien lakien ja asetusten, sekä lausuntojen ja myös näitä käsittelevien kirjallisten tuotosten lukemiseen. Teoriatietoa sovelletaan käytäntöön työ- ja yrityselämässä ja tietosuojateoriaa ja käytäntöjä arvioidaan ja analysoidaan. Tutkimus on kvalitatiivinen työ, jossa sovelletaan konstruktiivista tutkimusmallia. Tutkimuksessa hyödynnetään empiiristä tietoa ja osaamista. Opinnäytetyössä tutkimusmenetelmistä on käytössä muun muassa dokumenttianalyysi, haastattelu, havainnointi kuten esimerkiksi prosessien tarkastelu ja vertailukehittäminen.

2 TIETOSUOJAN JA TOIMIALAN TAUSTA

Tämä luku käsittää opinnäytetyössä käsiteltävän aiheen ja toimialan yleisesittelyn sekä havainnollisen yleiskuvauksen toimialalla käsiteltävistä henkilötiedoista eri osapuolten välillä. Tämä luku on samalla alustus seuraaviin lukuihin, koska luku kuvaa henkilötietojen käyttötarkoituksien nykytilan arviointia edeltävän kartoituksen tunnistamalla muun muassa mistä ja mihin henkilötietoja kerätään, ketkä niitä käsittelevät ja mihin niitä mahdollisesti luovutetaan. Tämä luku on henkilötietojen käsittelyprosessin näkökulmasta aloitus, jonka keskeisin asia on henkilötietojen ja käsittelyn osapuolten tunnistaminen.

2.1 Yksityiset turvallisuuspalvelut

2.1.1 Yksityiset turvallisuuspalvelut yleisesti

Yksityisillä turvallisuuspalveluilla tarkoitetaan vartioimisliiketoiminnan, järjestyksenvalvojatoiminnan ja turvasuojaustoiminnan muodostamaa kokonaisuutta. Toimiala on pääasiallisesti elinkeinoluvanalaista toimintaa. Turvallisuusalan elinkeinolupia oli poliisin 9.4.2020 päivätyn rekisterin mukaan 842 kpl. Yksityiset turvallisuuspalvelut työllistävät Suomessa Finnsecurity Ry:n tekemien toimialatutkimusten ja selvityksien mukaan yli 15 tuhatta henkilöä alan kokonaisliikevaihdon ollessa toimijoiden Kilpailu- ja kuluttajavirastolle (myöhemmin KKV) 2018 antamana itsearviointina 1900 - 2000 miljoonaa euroa.

Yksityisten turvallisuuspalveluiden elinkeinolupa asioista, yleisestä ohjauksesta ja valvonnasta vastaa poliisihallitus. Suomessa toimivat 11 poliisilaitosta vastaavat yksityisten turvallisuuspalveluiden sekä vartijoiden, voimankäyttökouluttajien, asekouluttajien, järjestyksenvalvojien, järjestyksenvalvojakoulutuksen järjestäjien, järjestyksenvalvojakouluttajien, turvasuojaajien ja vastaavien hoitajien toiminnan valvonnasta toimialueellaan.

Valvontaa tehdäkseen poliisi pitää tietoja vartijoista, voimankäyttökouluttajista, asekouluttajista, järjestyksenvalvojista, turvasuojaajista, järjestyksenvalvojakouluttajista, turvallisuusalan elinkeinoluvan haltijoista sekä niiden vastaavista hoitajista ja lain yksityisistä turvallisuuspalveluista (myöhemmin LYTP) 71 §:n 2 momentin 2 kohdassa tarkoitetuista vastuuhenkilöistä (turvallisuusalan valvontatiedot). Turvallisuusalan valvontatiedoista säädetään tarkemmin henkilötietojen käsittelystä poliisitoimessa annetussa laissa (761/2003). Turvallisuusalan elinkeinoluvan haltijan on annettava kalenterivuosittain

poliisihallitukselle vuosi-ilmoitus. Turvallisuusalan elinkeinoluvan haltijan on tehtävä LYTP:n vaatiman muutosilmoituksen siinä määritetyistä muuttujista. Poliisin suorittaman viranomaisvalvonnan, toimenpiteiden kohteena olevien henkilöiden oikeusturvan sekä toimeksiantajien tietojensaantioikeuden turvaamiseksi vartijan ja järjestyksenvalvojan tulee laatia vartiointi- ja järjestyksenvalvojatehtävissä laissa säädetty tapahtumailmoitus.

2.1.2 Vartioimisliiketoiminta

Ansiotarkoituksessa tapahtuva ja toimeksiantosopimukseen perustuva vartioimisliiketoiminta on kokonaan turvallisuusalan elinkeinoluvan alaista toimintaa. Vartija vartioi omaisuutta, suojaa henkilön koskemattomuutta, paljastaa vartioimiskohteeseen ja/tai toimeksiantajaan kohdistuneita rikoksia, suorittaa arvokuljetustehtäviä, toimii turvatarkastajana, reseptionistinä tai hälytyskeskuspäivystäjänä.

Vartijan työssä toimi vuonna 2018 tilastokeskuksen mukaan 8500 henkilöä. Toimiala on vahvasti miesvaltainen, naisia alalla oli edellä mainitun lähteen ja vuoden mukaan 21 prosenttia vartijoista. Vartiointityötä tehdään läsnäolopalvelujen muodossa vartioitavissa kohteissa tai vartioitavilla alueilla paikallisesti ja liikkuvien palvelujen muodossa vartiokierrostyyppisesti tai turvahälytyksestä.

2.1.3 Järjestyksenvalvojatoiminta

Ansiotarkoituksessa tapahtuva ja toimeksiantosopimukseen perustuva järjestyksenvalvojatoiminta on yleisessä kokouksessa tai yleisötilaisuudessa toimivaa järjestyksenvalvojatoimintaa lukuun ottamatta kokonaan turvallisuusalan elinkeinoluvan alaista toimintaa.

Järjestyksenvalvoja ylläpitää järjestystä ja turvallisuutta, sekä estää ja ennaltaehkäisee rikoksia ja onnettomuuksia toimialueellaan, johon hänet on poliisin toimesta luvallisesti asetettu. Järjestyksenvalvoja voidaan Suomessa asettaa vain laissa säädettyihin kohteisiin. Näitä kohteita ovat:

- yleinen kokous
- yleisötilaisuus
- yksityistilaisuus

- leirintäalue
- matkustajien kuljettamista suorittava alus
- majoitus- ja ravitsemisliike
- yliopisto ja ammattikorkeakoulu

Lisäksi poliisilaitos voi antaa luvan asettaa järjestyksenvalvojia poliisin tai rajavartiolaitoksen avuksi seuraaviin kohteisiin:

- terveyden- tai sosiaalihuollon toimipisteeseen koulukoteja tai lastensuojelulaitoksia lukuun ottamatta
- Kansaneläkelaitoksen toimipisteeseen ja työ- ja elinkeinotoimistoon
- kauppakeskukseen
- liikenneasemalle ja satamaan
- lentopaikkaan
- joukkoliikenteen kulkuneuvoon

Poliisin tai rajavartiolaitoksen avuksi asetetulla järjestyksenvalvojalla tulee olla järjestyksenvalvojakortti sekä vartijakortti, eli laajempi koulutus. Toimeksisaajalla tulee olla turvallisuusalan elinkeinolupa sekä vartiointitoiminnassa että järjestyksenvalvojatoiminnassa.

2.1.4 Turvasuojaustoiminta

Ansiotarkoituksessa tapahtuva ja toimeksiantosopimukseen perustuva hyväksymistä edellyttävä turvasuojaustoiminta on kokonaan turvallisuusalan elinkeinoluvan alaista toimintaa. Hyväksymistä edellyttävällä turvasuojaustoiminnan turvasuojaustehtävällä tarkoitetaan sähköisten ja mekaanisten lukitusjärjestelmien, murtohälytysjärjestelmien ja kulunvalvontajärjestelmien asentamista, korjaamista tai muuttamista.

Turvallisuusalan elinkeinolupaa ja turvasuojaajakorttia ei edellytetä edellä mainittujen turvasuojaustehtävien kaapelointityöhön. Kameravalvontajärjestelmien asentaminen, korjaaminen ja muuttaminen ei ole turvallisuusalan elinkeinoluvan alaista toimintaa, eikä siten vaadi tehtävien suorittajalta turvasuojaajakorttia, vaikka tekemisenä turvasuojaustoimintaa onkin. Mikäli kameravalvontajärjestelmä on integroitu murtohälytysjärjestelmään tai toisin päin, on tällainen turvasuojaustoiminta silloin elinkeinoluvan alaista turvasuojaustoimintaa.

2.2 Tietosuoja eli henkilötietojen käsittely

2.2.1 Henkilötietojen käsittelystä yleisesti

Tietosuoja on perusoikeus, joka mahdollistaa rekisteröidyn oikeuksien toteutumisen ja turvaamisen henkilötietojen käsittelyssä. Henkilötietojen käsittelyn on aina perustuttava lakiin. Henkilötietoja ovat kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, eli ihmiseen. Henkilötietoja voi olla sähköisissä tiedostoissa ja tietokannoissa, paperilla eri käsittelytapamuodoissa ja kuva- tai äänitallenteina.

Tietosuojan eli henkilötietojen käsittelyn yleissääntely perustuu tällä hetkellä EU:n yleiseen tietosuoja-asetukseen, joka tuli voimaan koko EU:n alueella 25.5.2018. Asetus on sellaisenaan suoraan sovellettavaa lainsäädäntöä Suomessa ja sitä täydentää 1.1.2019 voimaan tullut kansallinen tietosuojalaki. Yleislakeja tulee tulkita ja soveltaa rinnakkain. Henkilötietojen käsittelyä säännellään Suomessa yleislakien lisäksi lukuisissa erityislaeissa, joista ehkä vaikuttavin yrityselämässä on laki yksityisyyden suojasta työelämässä. Voimassa oleva lainsäädäntö edellyttää, että henkilötietoja käsittelevä yritys pystyy osoittamaan noudattavansa tietosuoja-asetuksen ja kansallisen tietosuojalain sääntelyä. Yritysten on toiminnassaan tärkeätä varmistua muun muassa siitä, että henkilötietojen käsittelyä koskeva dokumentointi, sisäinen ohjeistus ja varautumistoimet ovat kunnossa.

2.2.2 Viranomaisvalvonta ja sanktiot tietosuojarikkomuksissa

Tietosuoja-asetuksessa säädetään riippumattomista valvontaviranomaisista. Säädöksen mukaisesti jokaisen jäsenvaltion tulee varmistua siitä, että riippumaton valvontaviranomainen on vastuussa tietosuoja-asetuksen soveltamisen valvonnasta maassa. Jotta tietosuoja-asetuksen soveltaminen olisi jäsenvaltioissa mahdollisimman yhdenmukaista kaikkialla unionissa, valvontaviranomaisten tulee tehdä tiivistä yhteistyötä keskenään.

Suomessa asia on ratkaistu siten, että tietosuojavaltuutetun toimisto on kansallinen valvontaviranomainen, joka valvoo tietosuojalainsäädännön noudattamista maassamme. Tietosuojavaltuutetun toimistossa toimii tietosuojavaltuutettu sekä hänen kaksi apulaistietosuojavaltuutettua. Tietosuojavaltuutettu ja apulaistietosuojavaltuutetut ovat tehtävässään itsenäisiä ja riippumattomia. Suomen valtioneuvosto nimittää heidät viiden

vuoden toimikaudeksi kerrallaan. Lisäksi tietosuojavaltuutetun toimistossa työskentelee noin 40 tietosuoja-asiantuntijaa toteuttamassa tietosuojavaltuutetun valvontavelvoitetta.

Valvontaviranomaisen tehtävänä on muun muassa tietosuoja-asetuksen soveltamisen valvominen Suomessa, tietosuoja-asioita koskevan tietoisuuden edistäminen, henkilötietojen käsittelyn osapuolten ohjauksesta huolehtiminen, antaa lausuntoja ja vastaanottaa ilmoituksia, arvioida ennakkokuulemisia korkean riskin tietojenkäsittelystä, hyväksyä käytännesääntöjä ja vakiosopimuslausekkeita, kannustaa ottamaan käyttöön sertifiointeja, akkreditoida sertifiointielin ja peruuttaa myönnettyjä sertifikaatteja ja paljon muuta.

Valvontaviranomaisella on erittäin laajat tutkintavaltuudet tietosuoja-asioihin liittyen. Näihin kuuluvat muun muassa oikeus määrätä tarvittaessa rekisterinpitäjä tai henkilötietojen käsittelijä tai molemmat näistä antamaan tarvittavat tiedot, oikeus toteuttaa tarkastus tai tarkastuksia sekä oikeus saada pääsy henkilötietoihin ja oikeus päästä rekisterinpitäjän sekä henkilötietojen käsittelijän käyttämiin toimitiloihin tai tarvittaessa molempiin näistä.

Tietosuojavaltuutetun toimiston mukaisesti se voi käyttää seuraavia korjaavia toimivaltuuksia tietosuojarikkomuksissa sen varmistamiseksi, että yritys noudattaisi säädöksiä:

- huomautuksen antaminen
- varoituksen antaminen
- määräyksen antaminen ja mahdollinen uhkasakko
- henkilötietojen käsittelyn rajoittaminen tai käsittelykiellon asettaminen rekisterinpitäjälle tai henkilötietojen käsittelijälle väliaikaisesti tai pysyvästi

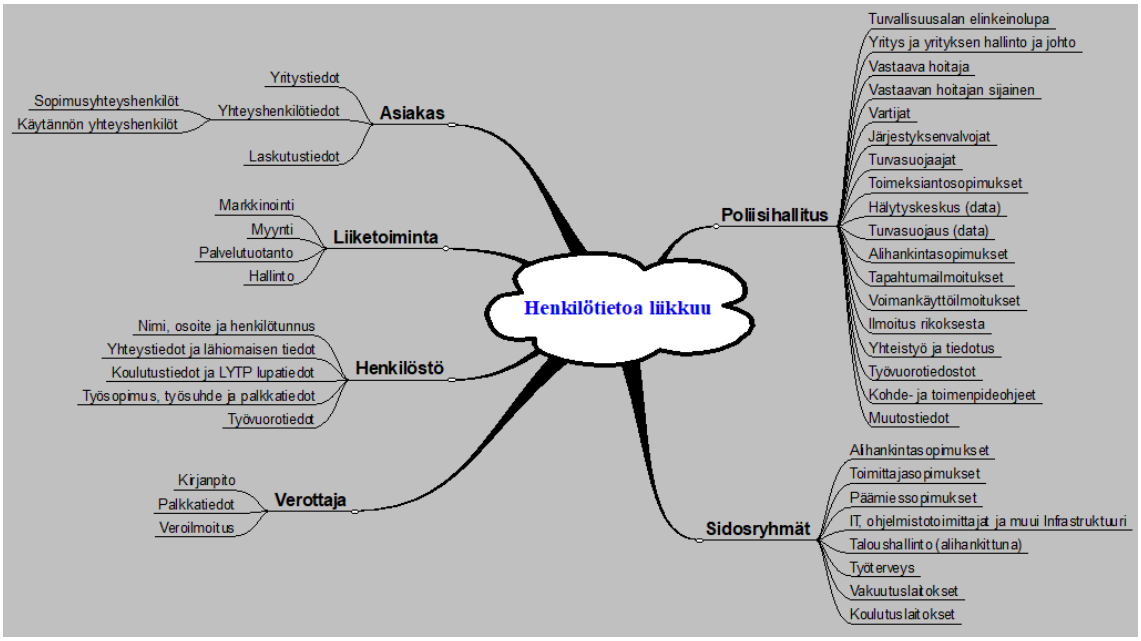
Tietosuojavaltuutettu ja apulaistietosuojavaltuutetut muodostavat Suomessa seuraamuskollegion. Kollegion tehtävänä on tietosuoja-asetuksen mukaisten hallinnollisten seuraamusmaksujen, eli hallinnollisten sakkojen määrääminen, kun edellä mainittu huomautus, varoitus tai määräys eivät ole tuottaneet tulosta. Kollegion puheenjohtajana toimii tietosuojavaltuutettu. Hallinnollisen seuraamusmaksun määrääminen edelleen korjaavien toimenpiteiden lisäksi tai niiden asemasta voi olla yritykselle seuraavanlainen:

- perustavanlaatuisten velvoitteiden rikkomisesta enintään 4 % yrityksen kokonaisliikevaihdosta tai 20 miljoonaa euroa, sen mukaan kumpi näistä on suurempi
- muiden asetettujen velvoitteiden rikkomisesta enintään 2 % yrityksen kokonaisliikevaihdosta tai 10 miljoonaa euroa, sen mukaan kumpi näistä on suurempi

Nämä tehtävät, oikeudet ja valtuudet edesauttavat yhteistoimintaa yritysten kanssa.

2.2.3 Millaisia henkilötietoja ja kenen välillä turvallisuuspalveluissa liikkuu

Yksityiset turvallisuuspalvelut eivät rekisterinpitäjän roolissa juurikaan poikkea muista toimialoista henkilötietojen käsittelyn vaatimuksissa tai toteuttamisessa. Eroavaisuus muihin toimialoihin tulee palvelutuotannossa, jossa ala toimii henkilötietojen käsittelijänä ja turvallisuusalan elinkeinoluvan alla. Toimialaa ohjaa ja valvoo poliisihallitus. Turvallisuuspalvelut käsittelee palvelutuotannossa laaja-alaisesti rekisteröityjen henkilötietoja.



Kuva 1. Henkilötietojen liikkuminen turvallisuuspalveluissa.

Kuva 1 havainnollistaa kenen välillä henkilötietoja turvallisuuspalveluissa liikkuu. Havainnollisesta miellekarttakuvasta on helppoa alkaa kartoittamaan henkilötietojen käyttötarkoituksia, rekisteröityjen ryhmiä ja käsiteltäviä henkilötietoryhmiä rekisterinpitäjän näkökulmasta, henkilötietojen käsittelijän näkökulmasta sekä rekisteröidyn näkökulmasta. Miellekarttakuvasta voidaan myös hahmottaa, kenelle toimijalle yrityksessä henkilötietoja siirretään käsiteltäväksi ja kenelle henkilötietoja luovutetaan. Miellekarttakuva toimii myös hyvänä aputyökaluna, kun hahmotetaan mitä järjestelmiä yrityksessä käytetään missäkin henkilötietojen käsittelyä koskevassa toiminnossa tai yhteydenpidossa.

Henkilötietojen käyttötarkoituksia ovat esimerkiksi seuraavat:

- suoramarkkinointi
- viestintä
- asiakassuhteiden hallinta
- omistajatietojen hallinta
- rekrytointi
- työsuhteiden hallinta
- toimittajasuhteiden hallinta
- viranomaisvelvoitteiden hoito
- yritysturvallisuuden hallinta
- turvallisuuspalvelujen tuotanto

Rekisteröityjen ryhmiä ovat esimerkiksi seuraavat:

- potentiaaliset asiakkaat
- asiakkaat
- osakkeen omistajat / yrittäjät
- työnhakijat
- työntekijät
- tavaran- ja palveluntoimittajat
- muut sidosryhmät
- toimenpiteiden kohteet

Henkilötietoryhmiä ovat esimerkiksi seuraavat:

- nimitiedot
- yhteystiedot
- henkilötunnus
- henkilönumero
- veronumero
- korttien lupanumerot
- aselupanumerot
- IP osoite ja lokitiedot
- kulunvalvontatunniste + lokitiedot
- käyttökoodi + lokitiedot
- avaintunniste
- video-/kuvatallenne + lokitiedot
- erityiset henkilötietoryhmät
- rikostuomiot ja rikkomukset

Toimijoita, joille henkilötietoja siirretään käsiteltäviksi voivat olla esimerkiksi:

- turvallisuuspalvelut
- SaaS ohjelmistot ja IT-palvelut
- taloushallintopalvelut
- työterveyspalvelut

Toimijoita, joille henkilötietoja luovutetaan voivat olla esimerkiksi:

- tulorekisteri
- veroviranomainen
- työeläkeyhtiö
- vakuutusyhtiö
- työttömyysrahasto
- pankki- ja rahoituslaitokset
- poliisihallitus
- ammattiyhdistysliike
- koululaitokset
- muut viranomaiset

Näin henkilötiedot jaotellaan käyttötarkoituksiensa alle aivan kuin aiemmin rekistereihin.

3 KÄSITTELYN PERIAATTEET JA LAINMUKAISUUS

Luvussa käsitellään käsittelyn periaatteet ja osoitusvelvollisuus sekä käsittelyperusteet. Tietosuoja-asetus edellyttää, että rekisterinpitäjä noudattaa henkilötietojen käsittelyä koskevia periaatteita ja laillisia käsittelyperusteita henkilötietoja käsitellessään. Henkilötietojen käsittelyssä yrityksen tulee huomioida, että rekisterinpitäjän on tietosuoja-asetuksen osoitusvelvollisuuden mukaisesti voitava osoittaa, että se noudattaa henkilötietojen käsittelyä koskevia periaatteita ja asetuksen muuta sääntelyä käsitellessään henkilötietoja. Pelkkä lainsäädännön noudattaminen ei riitä vaan dokumentointivaatimus korostuu. Tietosuoja perustuu lakiin ja asetuksiin, hallittuun ja hyvin johdettuun toimintaan.

3.1 Henkilötietojen käsittelyä koskevat periaatteet

3.1.1 Käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Henkilötietoja on käsiteltävä lainmukaisesti ja asianmukaisesti sekä rekisteröidyn kannalta tarkasteltuna läpinäkyvästi. Henkilötietojen käsittelyn tulee aina perustua johonkin lailliseen käsittelyperusteeseen, kuten esimerkiksi asiakas- tai työsuhteeseen perustuvaan sopimukseen tai oikeutettuun etuun. Mikäli laillista käsittelyperustetta henkilötietojen käsittelylle ei ole henkilötietoja ei voi eikä tule käsitellä.

Kohtuullisuus tarkoittaa yhtä lailla reiluutta ja suojaa salassa tapahtuvalta tietojen keräämiseltä ja tietojen väärin käsittelyltä sekä varmistaa, että rekisteröity tietää henkilötietojensa käsittelyn luonteesta ja tarkoituksesta.

Läpinäkyvyyden periaate taasen tarkoittaa sitä, että rekisteröityjen kannalta katsottuna heille tulisi olla läpinäkyvää ja selkeää se miten ja kuinka laajasti heidän henkilötietojansa kerätään ja käsitellään tai niitä on tarkoitus käsitellä. Yksi läpinäkyvyyden elementti on rekisteröityjen informointi selkeästi ja ymmärrettävästi sekä tieto siitä, kuka on rekisterinpitäjä ja mikä on henkilötietojen käsittelyn tarkoitus ja sen peruste. Rekisteröityjä tulee informoida selkeästi myös heidän oikeuksistaan, käsittelyyn liittyvistä riskeistä ja niitä varten tehdyistä suojaustoimista.

3.1.2 Käyttötarkoitussidonnaisuus

Henkilötietoja voi kerätä vain tiettyä nimenomaista ja laillista käsittelytarkoitusta varten. Henkilötietoja voi ja tulee käsitellä siten vain jonkun tietyn tehtävän hoitamiseksi. Käsittelyn tarkoituksia voi olla esimerkiksi toimeksiantosopimusten (asiakas) hoitaminen, suoramarkkinointi, työsuhteen osapuolten oikeuksien ja velvollisuuksien hoitaminen, työntekijöiden rekrytointi ja valinta, sekä toimittaja- ja alihankintasopimussuhteiden hoitaminen.

Henkilötietojen keräämisen tulee olla rekisterinpitäjän toiminnan kannalta tarpeellista ja asiallisesti perusteltavissa. Henkilötietoja ei saa myöhemmin käsitellä sen käyttötarkoituksen kannalta yhteensopimattomasti. Yrityksen on aina varmistettava se, ettei jo kerättyjä henkilötietoja käytetä muuhun kuin niiden ennalta määrittelemään tarkoitukseen.

Lisäksi todettakoon ilmeinen eli se, että jos jokin yritykselle tarvittava toimenpide voidaan tehdä ilman henkilötietojen keräämistä ja niiden käsittelyä, ei henkilötietoja tulisi silloin kerätä ja käsitellä lainkaan.

3.1.3 Tietojen minimointi

Käsiteltävien henkilötietojen on oltava asiallisia, olennaisia ja tarpeellisia niille määriteltyjen käyttötarkoituksien kannalta tarkasteltuna. Toisin sanottuna käsiteltävien henkilötietojen tulee olla riittäviä mutta rajoituttua siihen mikä on välttämätöntä henkilötietojen käsittelyn tarkoituksen kannalta.

Todettakoon se, että henkilötietoja voidaan kerätä ja käsitellä henkilön suostumuksella, mutta suostumuskaan ei oikeuta rekisterinpitäjää käsittelemään henkilötietoja tarpeettomasti. Henkilötietojen tulee siis aina olla tarpeellisia ja perusteltuja niille tarkoitettuun käyttötarkoitukseensa eikä muita tietoja tule käsitellä.

3.1.4 Tietojen täsmällisyys

Henkilötietojen tulee olla täsmällisiä. Jotta henkilötiedot pysyisivät täsmällisinä niitä tulee päivittää säännöllisesti ja tarpeen mukaan. Yrityksen on tehtävä kaikki tarpeellinen varmistustoiminta ja kohtuulliset toimenpiteet sen varmistamiseksi, että henkilötiedot pysyisivät täsmällisinä ja että virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.

Rekisterinpitäjän on periaatteen myötä syytä varmistaa keräämiensä henkilötietojen laatu ja tarkistaa aika ajoin, että henkilötiedot ovat virheettömät. Rekisterinpitäjän on syytä luoda toimiva prosessi sille, että ilmoitetut tai tietoon muutoin saadut henkilötietomuutokset tulevat vietyä päivitystietoina järjestelmiin siten, että niissä olisi ajan tasalla olevat tiedot.

3.1.5 Tietojen säilytyksen rajoittaminen

Henkilötietoja tulee säilyttää ainoastaan ja vain niin kauan kuin on tarpeen niiden käsittelytarkoituksen toteuttamiseksi tietoja säilyttää. Mikäli laki ei edellytä tiettyä säilytysaikaa käsittelyperusteen päätyttyä henkilötiedot tulee poistaa heti, kun käsittelytarkoitus on päättynyt. Henkilötietojen säilytysajan tulee lähtökohtaisesti olla mahdollisimman lyhyt.

Mikäli laki vaatii henkilötietojen säilyttämistä tietyn ajan varsinaisen käsittelyperusteen päätyttyä, tulee tiedot säilyttää laissa määritetyn ajan. Näitä tietyn aikaa säilytettäviä, henkilötietoja sisältäviä toimenpiteitä ovat esimerkiksi toimeksiantosopimus, toimeksiantosopimus alihankinnasta, kirjanpitotiedot, tapahtumailmoitus, työsopimuksiin liittyvät velvoitteet ja työsopimustiedot sekä muut vastaavat laissa määritellyt tiedot.

3.1.6 Tietojen eheys ja luottamuksellisuus

Henkilötietoja yrityksen tulee käsitellä aina niin, että varmistetaan henkilötietojen asianmukainen turvallisuus ja luottamuksellisuus. Tiedot tulee suojata luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Rekisterinpitäjän tulee ennaltaehkäistä luvaton pääsy henkilötietoihin tai henkilötietojen käsittelyyn käytettyihin laitteistoihin ja ohjelmiin sekä estää henkilötietojen, laitteistojen ja ohjelmien luvaton käyttö.

Tietoturvaan ja siten myös tietosuojaan liittyvistä teknisistä suojaustoimenpiteistä ja organisatorisista toimenpiteistä, kuten henkilökunnan tietoturvaan- ja tietosuojaan liittyvistä toimintaohjeista sekä koulutuksista on kerrottu tarkemmin erityisesti niitä asioita käsiteltävien aiheiden ja aihekokonaisuuksien yhteydessä.

3.2 Rekisterinpitäjän osoitusvelvollisuus

Kaikkia edellä mainittuja tietosuojaperiaatteita on noudatettava kaikissa henkilötietojen käsittelyn vaiheissa. Noudattamisen lisäksi rekisterinpitäjän on pystyttävä myös osoittamaan todeksi, että näin on myös toimittu. Osoitusvelvollisuus on melko kattava ja yhtä lailla käsittelyn yksityiskohtiin menevä, kuin tietosuojaa kokonaiskuvana tarkasteleva.

Osoitusvelvollisuuden täyttämiseksi rekisterinpitäjän on arvioitava mitä tietosuoja ja tietosuojaperiaatteet käytännön toiminnassa tarkoittavat ja miten ne toteutuvat tai tulevat toteutumaan rekisterinpitäjän omassa yritystoiminnassa. Tämä vaatii suunnitelmallisuutta ja suunniteltujen toimenpiteiden sekä tehtyjen toimenpiteiden dokumentointia.

Yritysten tulee kuvata henkilötietojen käsittelyyn liittyvät prosessinsa sekä dokumentoida miten tietosuojaperiaatteita käytännössä noudatetaan. Osoitusvelvollisuuden toteuttaminen edellyttää käytännössä suunnittelua, varautumista ja kykyä osoittaa toteutetut toimenpiteet dokumentaation avulla toteutetuiksi.

Suositeltavaa olisi, että jokainen yritys laatisi omat sisäiset ohjeensa tietosuojaperiaatteistaan ja tietosuojakäytännöistään sekä kokoaisi tietosuojaan liittyvät dokumentit, sopimukset ja selosteet siten, että ne olisivat kaikkien niitä tarvitsevien helposti löydettävissä ja että niiden avulla olisi helposti sekä nopeasti muodostettavissa kokonaiskuva yrityksen suorittamasta henkilötietojen käsittelystä ja sen noudattamasta tietosuojasta.

Tietosuoja-asetuksen mukaan yrityksen osoitusvelvollisuuden toteuttamiseksi tehtävät toimenpiteet ja dokumentit ovat ainakin seuraavat;

- Henkilötietojen käsittelyn yleinen kuvaus, eli rekisterinpitäjän roolissa laadittu seloste käsittelytoimista (artikla 30)
    - rekisterinpitäjä ja tietosuojavastaava
    - käsittelyn tarkoitukset
    - kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä
    - ryhmät, joille henkilötietoja luovutetaan
    - tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle
    - henkilötietojen säilytysajat
    - kuvaus teknisistä ja organisatorisista suojaamistoimista
- Henkilötietojen käsittelijän roolissa laadittu seloste käsittelytoimista (artikla 30)

    - henkilötietojen käsittelijä ja tietosuojavastaava
    - rekisterinpitäjät, joiden lukuun henkilötietojen käsittelijä toimii
    - kunkin rekisterinpitäjän lukuun suoritettujen käsittelyiden ryhmät
    - tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainväliselle järjestölle
    - kuvaus teknisistä ja organisatorisista suojaamistoimista
- Kuvaus yrityksen sisäänrakennetusta ja oletusarvoisesta tietosuojasta, eli tietosuojaperiaatteiden toteutuminen omassa yritystoiminnassa (artikla 5 ja 25)
- Rekisteröityjen informointikäytännöt ja dokumentit (artikla 12, 13 ja 14)
- Käsittelyn oikeusperustetta koskevat menettelyarvioinnit (artiklat 6-10)
    - jos käytetään suostumusta – suostumukseen liittyvä dokumentaatio
    - jos käytetään oikeutettua etua – tehty tasapainotesti
- Muut sisäiset ja ulkoiset ohjeistukset (artikla 12, 13, 14, 24, 25, 28, 29, 32)
    - riskienarviointia ja suojaamistoimia koskeva dokumentaatio
    - ohjeet (sisäiset ja ulkoiset) rekisteröidyn oikeuksien toteuttamiseksi
    - käsittelyohjeet henkilötietoja käsitteleville työntekijöille
    - käsittelyohjeet henkilötietojen käsittelijöille
    - yrityksen sisäiset tarkastukset ja ulkopuolisten auditoinnit
    - muut mahdolliset ohjeistukset
- Yrityksen tekemiä vaikutustenarviointeja (artikla 35) ja ennakkokuulemista (artikla 36) käsittelevä dokumentaatio
- Henkilötietoihin kohdistuvien tietoturvaloukkausten dokumentointi (artikla 33 ja 34) ja tämän menettelyprosessin kuvaus ja dokumentaatio
- Tietosuojavastaavan (jos on) tehtäviin liittyvä dokumentaatio (artikla 37-39)
    - tehtävä- ja asemakuvauksen lisäksi on suositeltavaa aina dokumentoida suositukset ja niistä tehdyt poikkeukset perusteluineen
- Tehdyt tietojenkäsittelysopimukset henkilötietojen käsittelijöiden kanssa (artikla 28)
- Kuvaus yhteisrekisterinpitäjien vastuualueista (artikla 29)
- Henkilötietojen siirtoa EU:n ulkopuolelle koskeva dokumentaatio (tietosuoja-asetuksen 5:s luku)

Jokaisen rekisterinpitäjän ja henkilötietojen käsittelijän, niin pienen kuin ison yrityksen tulee huomioida ja toteuttaa edellä luetellut asiat osoitusvelvollisuuden todentamiseksi.

3.3 Henkilötietojen käsittelyn lainmukaiset käsittelyperusteet

3.3.1 Suostumus

Henkilötietojen käsittely voi perustua rekisteröidyn antamaan suostumukseen. Suostumuksen tulee EU:n tietosuoja-asetuksen mukaan olla ”rekisteröidyn vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla hän hyväksyy henkilötietojensa käsittelyn”. Suostumus edellyttää rekisteröidyltä aina aktiivista toimintaa, kuten esimerkiksi ruudun rastittaminen verkkosivuilla tai suostumuslomakkeen täyttäminen ja allekirjoittaminen. Suostumusta ei siten voi antaa vaikenemalla tai jättämällä suostumuksen edellyttämä toimenpide toteuttamatta. Esimerkiksi rekisteröidyn suostumusta ei tästä syystä voida katsoa annetuksi verkkosivuilla jo valmiiksi rastitetulla ruudulla. Jotta suostumus olisi tietoinen tahdonilmaisu, rekisteröidyn pitää tietää ainakin se, kuka hänen henkilötietojaan käsittelee ja mihin tarkoitukseen, sekä missä laajuudessa.

Suostumuksen vapaaehtoisuus edellyttää, että rekisteröidyllä on todellinen vapaus valita haluaako hän henkilötietojansa käsiteltävän vai ei, ja että hänellä on mahdollisuus kieltäytyä suostumuksesta tai myöhemmin peruuttaa jo antamansa suostumus. Suostumusta ei myöskään katsota vapaaehtoisesti annetuksi jos esimerkiksi palvelun tarjoamisen edellytyksenä on suostumuksen antaminen, vaikka henkilötietojen käsittely ei olisi ollut tarpeellista kyseisen palvelun toteuttamiseksi tai tarjoamiseksi. Suostumuksen on myös katettava kaikki käsittelytoimet, eli suostumus on pyydettävä ja annettava kaikkia käsittelytoimia varten erikseen tai yhdellä kertaa kuitenkin aina erikseen yksilöidysti. Mikäli henkilöllä ei ole mahdollisuutta antaa erillistä suostumusta eri henkilötietojen käsittelytoimille, suostumusta ei voida katsoa annetuksi vapaaehtoisesti. Suostumuksen hyväksymisen keskeisenä vaatimuksena voidaan pitää suostumuspyynnön selkeyttä, eli rekisteröityvän henkilön tulee tietää selkeästi se, mihin käsittelytoimiin hän suostumuksen pyynnössä suostumuksensa antaa.

Rekisterinpitäjän on pystyttävä osoittamaan, että rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn. Suostumus voidaan antaa kirjallisesti, sähköisesti tai suullisesti. Koska todentamisvelvoite on olemassa, suullista suostumusta ei yksinään voida suositella toteen näyttämisen vuoksi, vaan suostumus tulisi osoittaa myös kirjallisesti tai sähköisesti, jotta se voitaisiin todentaa aukottomasti. Suostumuksen peruuntuminen ei vaikuta takautuvasti henkilötietojen käsittelyn lainmukaisuuteen. Rekisteröidyllä

on oikeus peruuttaa suostumuksensa milloin tahansa ja sen on oltava yhtä helppoa, kuin oli suostumuksen antaminenkin.

Arkaluontoisten tietojen käsittelyssä suostumuksessa tulisi kiinnittää erityistä huomiota täsmentämällä tarkalleen, mitä tiettyä arkaluonteista tietoa suostumus koskee ja pyytää tarkennettu suostumus asian käsittelyyn aina kirjallisesti ja käsiteltävä tieto yksilöidysti.

Rekisterinpitäjän on aina pystyttävä osoittamaan, että rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn. Tämän velvollisuuden osoittamiseksi todeksi korostuu rekisterinpitäjän dokumentointi. Suostumus on todennettava dokumentoidusti aina, oli se annettu missä muodossa tahansa rekisterinpitäjälle.

3.3.2 Sopimus

Henkilötietojen käsittely voi perustua sopimuksen täytäntöönpanemiseksi, jossa rekisteröity on osapuolena tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä. Kerättävien ja käsiteltävien henkilötietojen tulee liittyä ja olla tarpeellisia sekä perusteltavissa olevia sopimuksen täytäntöön panemisen ja myöhemmin osapuolten välisen sopimuksen mukaisten velvoitteiden hoitamisen kannalta.

Sopimussuhde voi olla kysymyksessä esimerkiksi asiakkaan, tavaran- tai palveluntoimittajan, alihankkijan, rahoituslaitoksen, vakuutuslaitoksen ja työntekijän kanssa. Sopimukseksi tässä asiassa lasketaan myös toimitus- ja maksutietojen kerääminen esimerkiksi verkossa, jotta verkossa ostetut tavarat voidaan toimittaa rekisteröidylle, sekä ostotapahtuma veloittaa tai laskuttaa oston suorittajalta. Sopimuksen tekemistä edeltäviin toimenpiteisiin taas lasketaan esimerkiksi tarjouksen tekeminen palveluista tai tuotteista.

3.3.3 Lakisääteiset velvoitteet

Henkilötietojen käsittely on mahdollista rekisterinpitäjän lakisääteisen velvoitteen täyttämiseksi. Tällainen on esimerkiksi tilanne, jossa osakeyhtiön on osakeyhtiölain perusteella pidettävä osakasluetteloa, jolloin osakkaiden henkilötietojen käsittely on tarpeen osakeyhtiölain asettamien velvoitteiden perusteella. Lakisääteinen velvoite on kysymyksessä myös silloin, kun työnantajien on ilmoitettava työntekijöidensä palkkatiedot tulorekisteriin muun muassa sosiaaliturva- ja veroviranomaisten palkkatietojensaantia varten.

Käsittelyperuste edellyttää siis aina sitä, että henkilötietojen käsittelylle lakisääteisellä velvoitteella on oltava peruste unionin oikeudessa tai Suomen kansallisessa lainsäädännössä. Suomessa henkilötietojen käsittelystä säädetään laajasti esimerkiksi sektorikohtaisessa lainsäädännössä. Myös LYTP säätää henkilötietojen käsittelystä mm. tapahtumailmoituksessa ja viranomaisraportoinnissa, kuten vuosi-ilmoituksen antamistiedoissa.

3.3.4 Elintärkeä etu

Henkilötietojen käsittelyn edellytykseksi voi tulla tarve rekisteröidyn ja toisen luonnollisen henkilön elintärkeiden (esimerkiksi hengen) etujen suojelemiseksi. Tämä käsittelyperuste tulee sovelletuksi käytännössä vain silloin, kun käsittelyllä ei ole muuta oikeusperustetta. Säännös voi tulla sovelletuksi esimerkiksi silloin, kun rekisteröity ei kykene antamaan suostumustaan tai kyseessä on laajan ihmisjoukon käsittävä hätätilanne, jossa suostumusta ei pystytä saamaan henkilöiltä yksilöllisesti.

Vastaavanlainen poikkeustilanneperusteinen tämän kohdan käsittelyperusteen käyttöä perustellusti puoltava syy voi tulla kyseeseen myös niin, että käsittelylle on tarve muiden ihmisten elintärkeiden etujen suojaamiseksi ja suostumusta ei voida katsoa pystyvän tätä varten saamaan henkilöltä itseltään tai sen saaminen ei ole tarkoituksenmukaista.

3.3.5 Yleinen etu tai julkisen vallan käyttö

Henkilötietojen käsittely on sallittua, kun se on tarpeellista yleisen edun mukaisen tehtävän tai toimenpiteen suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Käsittelyperusteet koskettavat pääasiassa suoraan soveltaen vain viranomaisia ja viranomaistoimintaa. Epäsuorasti esimerkiksi julkisen vallan käyttö koskettaa yksityisiä turvallisuuspalveluita toimialan lainsäädännön ja poliisin asettamistoimien kautta, mutta se ei ole toimialalle henkilötietojen käsittelyperuste.

Nämä käsittelyperusteet ovat kuitenkin tietyllä lailla mukana myös turvallisuuspalveluiden arjessa, koska osa toimeksiantajista soveltaa näitä käsittelyperusteinaan ja ne on siksi hyvä tiedostaa. Kohdan sääntelyä on tarkennettu kansallisessa tietosuojalaissa.

3.3.6 Oikeutettu etu

Henkilötietojen käsittely voi olla perusteltua tietosuoja-asetuksen mukaan oikeutetun edun perusteella, kun ”käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi”. Oikeutetun edun ja rekisteröityjen oikeuksien välinen vertailu jää rekisterinpitäjän omakohtaisesti punnittavaksi, tehtäväksi ja vastuulle.

Tietosuoja-asetuksen mukaan oikeutettu etu voi olla olemassa esimerkiksi tapauksessa, jossa rekisterinpitäjän ja rekisteröidyn välillä on merkityksellinen ja asianmukainen suhde. Tällainen suhde olisi muun muassa asiakassuhde ja työsuhde. Näissä edellä mainituissa suhteissa voi rekisterinpitäjälle tulla perusteltavissa oleva syy henkilötietojen lisäkeräämiseen ja niiden käsittelyyn, jotka eivät ole perusteltavissa sopimuskäsittelyperusteella. Lisäksi oikeutetun edun käytön piiriin kuuluu yrityksen suorittama suoramarkkinointi potentiaalisille asiakkaille ja asiakkaille, kunhan huomioidaan vastaanottajan mahdollisuus kieltää suoramarkkinointi. Oikeutetun edun piiriin kuuluu myös esimerkiksi oman toimipisteen suojaaminen esimerkiksi kameravalvonnalla, rikosilmoitinjärjestelmällä ja kulunvalvonnalla ja tästä johtuvat henkilötiedot ja niiden käsitteleminen.

Tietosuojatyöryhmä (WP217) on todennut lausunnoissaan, että oikeutettua etua ei tulisi pitää kaiken sellaisen henkilötietojenkäsittelyn käsittelyperusteena, johon ei voida soveltaa mitään muista käsittelyperusteista. Lisäksi ryhmä on todennut, että käsittelyn tulee olla melko konkreettinen, jotta sitä voidaan punnita rekisteröidyn etuja, perusoikeuksia ja -vapauksia vasten. Heikko tai spekulatiivinen etu ei tule hyväksyttävänä kysymykseen. Oikeutetun edun perusteella käsittely edellyttää, että se on lainmukaista ja asianmukaista. Lainmukaisuus edellyttää käsittelyn tapahtuvan lainmukaisen rekisterinpitäjän intressin suojaamiseksi. Asianmukaisuuteen kuuluvat vaatimukset edellyttävät oikeutetun edun riittävän tarkkaa määrittämistä sekä sen tosiasiallisuutta ja ajankohtaisuutta. Asianmukaisuuteen kuuluu luonnollisesti kaikkien tietosuojaperiaatteiden noudattaminen.

Oikeutettua etua ei käytetä viranomaisten henkilötietojen käsittelyn käsittelyperusteena.

3.4 Käsittely muuta kuin alkuperäistä tarkoitusta varten

Tietyin ehdoin käsittely on mahdollista muuta kuin alkuperäistä tarkoitusta varten. Jos käsittely tapahtuu muuta kuin sitä alkuperäistä tarkoitusta varten, jonka vuoksi tiedot oli kerätty, eikä henkilötietojen käsittely perustu rekisteröidyn suostumukseen, eikä unionin tai Suomen lainsäädäntöön, yrityksen tulee ottaa huomioon seuraavat asiat varmistaakseen käsittelyssä sen, että muuhun tarkoitukseen tapahtuva käsittely on yhteensopivaa alkuperäisen käsittelytarkoituksen kanssa. Näitä ovat tietosuoja-asetuksen mukaan:

(I) henkilötietojen keruun tarkoitusten ja aiotun myöhemmän käsittelyn tarkoitusten väliset yhteydet
(II) henkilötietojen keruun asiayhteys erityisesti rekisteröityjen ja rekisterinpitäjän välisen suhteen osalta
(III) henkilötietojen luonne, erityisesti se, käsitelläänkö erityisiä henkilötietojen ryhmiä tai rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja
(IV) aiotun myöhemmän käsittelyn mahdolliset seuraukset rekisteröidyille
(V) asianmukaisten suojatoimien, kuten salaamisen tai pseudonymisoinnin, olemassaolo

Käytännössä säännöksen nojalla on mahdollista käsitellä henkilötietoja toissijaiseen käyttötarkoitukseen esimerkiksi silloin, kun henkilötietojen käsittelyperusteena on oikeutettu etu, kunhan säännöksessä kirjatut reunaehdot otetaan tarkasteluun ja huomioon.

3.5 Tiedot, joiden käsittely vaatii erityisiä käsittelyperusteita

Erityisiä henkilötietoryhmiä / arkaluonteisia henkilötietoja ovat tiedot, joista ilmenee:

- rotu tai etninen alkuperä
- poliittiset mielipiteet
- uskonnollinen tai filosofinen vakaumus
- ammattiliiton jäsenyys
- geneettiset ja biometriset tiedot, joita käsitellään henkilön yksiselitteistä tunnistamista varten
- terveyttä koskevat tiedot
- seksuaalinen käyttäytyminen ja suuntautuminen

Pääsääntöisesti erityisiä henkilötietoryhmiä koskevia tietoja ei saa käsitellä. Tietosuoja-asetuksessa on kuitenkin säädetty erityisiä perusteita, joiden täyttyessä yritys saa käsitellä arkaluonteisia tietoja. Yksityisten turvallisuuspalveluiden näkökulmasta tarkasteltuna kyseisiä perusteita olisivat seuraavat:

- rekisteröidyn antama suostumus nimenomaisen erityisiä henkilötietoryhmiä koskevan henkilötiedon käsittelyyn yhtä tai yksilöidysti useampaa tarkoitusta varten, mikäli se ei ole ristiriidassa sovellettavan yleis- ja erityislainsäädännön kanssa
- käsittely on tarpeen rekisterinpitäjän ja rekisteröidyn välisten velvoitteiden ja oikeuksien noudattamiseksi lähinnä työoikeuden, joissakin yksittäistapauksissa muun erityislainsäädännön perusteella
- käsittely koskee henkilötietoja, jotka rekisteröity on nimenomaisesti saattanut julkiseksi
- käsittely on tarpeen rekisteröidyn ja toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi, henkilön ollessa esimerkiksi estynyt antamasta omaa suostumustaan, tilanne liittyy luonnonkatastrofiin tai ihmisen aiheuttamaan vaaratilanteeseen
- käsittely on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi

Tietosuoja-asetuksen yleisistä periaatteista, sekä riskiperusteisen lähestymistavan takia, erityisten henkilötietoryhmien käsittely edellyttää asianmukaisia ja erityisiä suojatoimia. Nämä koskevat yksityisiä turvallisuuspalveluja ja myös näiden toimeksiantajia.

3.6 Asiakkaiden arkaluontoisten henkilötietojen käsittely

Yksityiset turvallisuuspalvelut toimivat ansaintatarkoituksessa ja toimeksiannosta eli toimeksiantosopimusperusteisesti ulkoistettuna palveluna. Tietosuojalainsäädännön näkökulmasta yksityiset turvallisuuspalvelut toimivat henkilötietojen käsittelijän roolissa. Ala siis käsittelee henkilötietoja rekisterinpitäjän ohjeiden mukaisesti, puolesta ja lukuun, sekä toimialan sovellettava lainsäädäntö huomioiden, joka ei ole ristiriidassa edelliseen.

Yksityisillä turvallisuuspalveluilla ei ole tarvetta eikä perustetta käsitellä asiakkaan, asiakkaan henkilökunnan tai kolmannen osapuolen arkaluontoisia henkilötietoja muuta kuin toimeksiannon tehtävän, tilanteen ja toimenpiteen niin vaatiessa tai edellyttäessä ja

mikäli tällaisen arkaluonteisen henkilötiedon käsittely on vartiointi-, järjestyksenvalvoja- ja turvasuojaustoiminnan kannalta perusteltavissa. Toimeksiantaja on aina rekisterinpitäjä.

Käytännössä arkaluontoinen henkilötieto voi tulla tietoon myös välillisesti niin vartiointi-, järjestyksenvalvoja- kuin turvasuojaustehtävissä. Tehtävän yhteydessä välillisesti saatu tieto tai havainto arkaluontoisista henkilötiedoista ei vaadi käsittelyperustetta, koska tieto on joko oma havainto, kuultu, nähty tai kohdehenkilöltä vapaaehtoisesti saatu tieto, eikä saatu tieto edellyttänyt tehtäväksi toimenpiteitä, kirjaamista tai tallentamista, eikä se siten johtanut arkaluontoisten henkilötietojen käsittelyyn lain tarkoittamassa muodossa.

3.7 Työntekijöiden arkaluontoisten henkilötietojen käsittely

Työntekijöiden arkaluontoisten henkilötietojen käsittely on sallittua, jos niiden käsittely on tarpeen yrityksen tai rekisteröidyn velvoitteiden tai erityisten oikeuksien noudattamiseksi työoikeuden alalla ja siinä laajuudessa kuin se sallitaan lainsäädännössä tai työehtosopimuksissa. Näin yritys on oikeutettu käsittelemään esimerkiksi tietoja, joilla määrittää soveltuva työsopimus tai tilittää työntekijöidensä ammattiliiton jäsenmaksut.

Työntekijöiden terveydentilatietojen käsittelystä säädetään tarkemmin laissa yksityisyyden suojasta työelämässä, siinä todetaan, että työnantajalla on oikeus käsitellä työntekijän terveydentilaa koskevia tietoja, kun tiedot on saatu työntekijältä itseltään tai kirjallisella suostumuksella muualta ja tietojen käsittely on tarpeellista sairausajan palkan suorittamiseksi tai poissaolon selvittämiseksi, taikka jos työntekijä haluaa selvitettävän työkykyisyyttään.

Yrityksessä työntekijöiden terveydentilatietoja saavat käsitellä henkilöt, jotka valmistelevat tai tekevät työsuhteita koskevia päätöksiä tai laittavat niitä toimeen. Näitä ovat käytännössä henkilöstöhallinnosta vastaavat ja esimiehet. Yrityksen on työnantajana nimettävä nämä henkilöt ja määriteltävä tehtävät, joille näitä tehtäviä kuuluu.

Työntekijöiden terveydentilaa koskevat tiedot tulee pitää erillään muista henkilötiedoista.

3.8 Rikostuomiot ja rikkomukset

Rikostuomioihin ja rikkomuksiin tai niihin liittyviin turvaamistoimiin liittyviä henkilötietoja saa tietosuoja-asetuksen mukaan käsitellä vain jos:

- käsittely tapahtuu viranomaisen valvonnassa
- käsittely sallitaan lainsäädännössä

Yritys yleisesti ei voi käsitellä näitä tietoja ilman erityistä perustetta, vaikka rekisteröidyn tietojen käsittely olisi muuten oikeutettua. Esimerkiksi henkilön itse antama suostumus ei oikeuta käsittelyyn.

Tietosuojalaissa on lisäksi säädetty tarkennuksena seuraavaa; rikostuomioihin ja rikkomuksiin tai niihin liittyviin turvaamistoimiin koskevia henkilötietoja saa käsitellä jos:

- ”käsittely on tarpeen oikeusvaateen selvittämiseksi, laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi”
- ”vakuutuslaitoksen käsitellessä vakuutustoiminnassa saatuja tietoja vakuutetun ja korvauksenhakijan terveydentilasta, sairaudesta tai vammaisuudesta taikka sellaista häneen kohdistetuista hoitotoimenpiteistä tai niihin verrattavista toimista, jotka ovat tarpeen vakuutuslaitoksen vastuun selvittämiseksi”
- ”tietojen käsittelyyn, josta säädetään laissa tai joka johtuu välittömästi rekisterinpitäjälle laissa säädetystä tehtävästä”
- ”tieteellistä tai historiallista tutkimusta taikka tilastointia varten tehtävään tietojen käsittelyyn”

Yksityisissä turvallisuuspalveluissa voidaan näitä tietoja käsitellä laissa perusteltavissa olevin osin ja mitä vartioimis- tai järjestyksenvalvojatehtävä ja toimeksianto edellyttää.

Tietosuoja-asetuksen yleisistä periaatteista, sekä riskiperusteisen lähestymistavan takia, erityisten henkilötietoryhmien käsittely edellyttää asianmukaisia ja erityisiä suojatoimia. Nämä koskevat yksityisiä turvallisuuspalveluja ja myös näiden toimeksiantajia.

3.9 Henkilötunnus

Yritys saa käsitellä henkilötunnusta yksiselitteisellä suostumuksella tai mikäli yksiselitteinen yksilöiminen on tärkeää rekisterinpitäjän ja rekisteröidyn oikeuksien ja velvollisuuksien toteuttamiseksi. Avainasia on se, että rekisteröidyn yksiselitteinen yksilöiminen on tärkeää; riittävää ei ole se, että käsittely esimerkiksi helpottaisi tai nopeuttaisi käsittelyä.

Henkilötietoja voidaan lisäksi käsitellä:

- luotonannossa
- saatavan perimisessä
- vakuutustoiminnassa
- luottolaitostoiminnassa
- vuokraus- ja lainaustoiminnassa
- luottotietotoiminnassa
- terveydenhuollossa
- sosiaalihuollossa ja muun sosiaaliturvan toteuttamisessa
- virka-, työ- ja muita palvelusuhteita ja niihin liittyviä etuja koskevissa asioissa

Kun yrityksessä käsitellään henkilötunnuksia, on huolehdittava käsittelystä ja toiminnoista, jotka estävät ja varmistavat henkilötunnuksen tarpeettoman tulostumisen tulostettuihin tai lähetettäviin lomakkeisiin, kirjeisiin, laskuihin, sähköpostiviesteihin, henkilökortteihin, työvuorolistoihin ja luetteloihin sekä muihin vastaaviin perusteettomasti.

Henkilötunnusta ei ole tarkoitettu henkilöiden tunnistamiseen vaan yksilöimiseen muista. Henkilöllisyys pitää todentaa esimerkiksi passilla, henkilökortilla tai sähköisin tunnistusmenetelmin. Vartijalla ja järjestyksenvalvojalla on LYTP:n mukaan oikeus kirjata henkilötunnus tapahtumailmoituksessa. Kirjauksessa korostuu todentaminen ja yksilöinti.

4 KÄSITTELYN OSAPUOLET

Luvussa käsitellään käsittelyn osapuolien välillä olevia lainmäärityksiä. Henkilötietojen käsittelyssä voi olla yhtä aikaa mukana useita tai jopa lukuisia osapuolia. Keskeinen osapuoli on se luonnollinen henkilö, ihminen eli rekisteröity, jonka henkilötietoja käsitellään. Tietosuojalainsäädäntö suojelee luonnollisen henkilön oikeuksia omiin henkilötietoihinsa ja määrittää käsittelyn osapuolien keskinäiset roolit, oikeudet, velvollisuudet ja vastuut.

4.1 Rekisterinpitäjä

4.1.1 Rekisterinpitäjän rooli ja sen määräytyminen

Yrityksen on olennaista ja tärkeää määrittää, missä roolissa yritys milloinkin toimii. Yksityisten turvallisuuspalveluiden tuottaja toimii usein kaikissa näissä rooleissa. Roolit määräytyvät tosiasiallisen aseman perusteella eikä keskinäisistä rooleista voi sopia osapuolten välillä toisin. Rekisterinpitäjä on luonnollinen henkilö eli ihminen, yritys, viranomainen tai vastaava taho, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.

Turvallisuuspalvelujen näkökulmasta kunkin käsittelytilanteen rooli määräytyy sen mukaan, mikä taho tai toimija tosiasiassa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Kun turvallisuusalan yritys lähestyy potentiaalisia asiakkaita tai asiakkaidensa edustajia kaupallisesti tai työntekijöitään yritys toimii rekisterinpitäjän roolissa. Kun turvallisuusalan yritys suorittaa toimeksiantosopimuksensa mukaista tehtävää vartiointi-, järjestyksenvalvoja- ja/tai turvasuojaustoiminnassa yritys toimii henkilötietojen käsittelijän roolissa, koska se tosiasiassa toimii asiakkaansa antamien ohjeiden mukaan ja heidän lukuunsa. Yrityksen toimittamissa turvallisuuspalveluissa käyttämänsä alihankkijat ovat myös henkilötietojen käsittelijöitä yrityksen solmimassa palvelujen toimitusketjussa.

4.1.2 Rekisterinpitäjän vastuut ja erityiset velvoitteet

Yrityksellä on rekisterinpitäjänä toimiessaan aina viimesijainen vastuu henkilötietojen käsittelyn lainmukaisuudesta. Rekisterinpitäjä vastaa tietosuoja-asetuksen mukaan myös siitä, että rekisterinpitäjän liike- ja muussa toiminnassaan käyttämät henkilötietojen

käsittelijät noudattavat henkilötietojen käsittelyssä unionissa sovellettavaa lainsäädäntöä. Yritys on velvoitettu huomioimaan asia alihankinta- ja yhteistyökumppaneita valittaessa.

Rekisterinpitäjän on tietosuoja-asetuksen mukaisesti toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joiden avulla voidaan varmistaa ja myös osoittaa se, että tietosuoja-asetusta noudatetaan. Suojaustoimia suunnitellessaan ja toteuttaessaan on yrityksen otettava huomioon henkilötietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä näiden henkilötietojen käsittelyyn liittyvät riskit. Riskiperusteinen lähestymistapa edellyttää ja tarkoittaa sitä, että suojaustoimenpiteet on suhteutettava henkilötietojen käsittelystä rekisteröidyn oikeuksille ja vapauksille mahdollisesti aiheutuvaan riskiin. Yritysten siis pitää arvioida millaisia tietosuojariskejä käsittely sisältää ja millaisia vahinkoja käsiteltävien henkilötietojen paljastuminen ulkopuolisille tai rekisteröidylle aiheuttaa. Koska yksityisten turvallisuuspalveluiden henkilötietojen käsittelyyn sisältyy myös erityisten henkilötietoryhmien sekä rikostuomioiden ja rikkomusten käsittelyä, pitää henkilötietojen turvalliseen ja riskiperusteiseen käsittelyyn kiinnittää erityistä huomiota.

4.1.3 Yhteisrekisterinpitäjät

Vähintään kaksi rekisterinpitäjänä toimivaa yritystä voi toimia yhteisrekisterinpitäjänä, jos yritykset määrittävät yhdessä henkilötietojen käsittelyn käyttötarkoitukset. Yhteisrekisterinpitäjäyritysten on määriteltävä keskenään kunkin yhteisrekisterinpitäjän vastuualueet tietosuoja-asetuksen noudattamiseksi. Yhteisrekisterinpitäjät voivat niin päättäessään määritellä kuka rekisterinpitäjistä toimisi osapuolten yhteyspistetahona rekisteröidyille.

Vastuualueet tulee määritellä osapuolten osalta läpinäkyvästi. Erityisesti osapuolten vastuut rekisteröityjen oikeuksien toteuttamisesta ja rekisteröityjen informoimisesta on jaettava ja määritettävä. Yhteisrekisterinpitäjät voivat toteuttaa vastuualueiden läpinäkyvän määrittelyn ja informoimisen esimerkiksi tietosuojaselosteella. Huomioida tulee kuitenkin se, että rekisteröidyillä on aina oikeus käyttää tietosuoja-asetuksen mukaisia oikeuksia suhteessa kuhunkin rekisterinpitäjään ja jokaista rekisterinpitäjää vastaan. Tästä syystä jokaisen pitää varmistaa omat valmiutensa suhteessa rekisteröityihin, vaikka yhteisrekisterinpitäjien keskinäisissä sopimuksissa ja sopimussuhteissa vastuut olisivatkin jaettu. Käytännössä siis yhteisrekisterin pitäminen johtaa yhteiseen vastuuseen, jossa jokainen rekisterinpitäjä on täydessä korvausvelvollisuudessa yhteisen rekisterinpidon

aiheuttamasta vahingosta. Näin on turvattu rekisteröidyille tehokas korvauksensaantioikeus. Yhteisvastuun vuoksi kannattaa tarkasti harkita kenen kanssa tällaista harjoittaisi.

4.2 Henkilötietojen käsittelijä

4.2.1 Henkilötietojen käsittelijän rooli ja sen määräytyminen

Henkilötietojen käsittelijä on tietosuoja-asetuksen mukaan luonnollinen henkilö, oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietojen käsittelijä voi siten käsitellä henkilötietoja vain ja ainoastaan rekisterinpitäjän antamien ohjeiden mukaisesti; ohjeet tulee antaa dokumentoidusti. Rekisterinpitäjän ja henkilötietojen käsittelijän on tehtävä kirjallinen tietojenkäsittelysopimus.

Yksityisten turvallisuuspalveluiden tuottaja on siis edellä rekisterinpitäjäkohdassa 4.1.1 kuvatusti palvelutuotantonsa osalta henkilötietojen käsittelijä. Tietosuoja-asetuksen mukaan henkilötietojen käsittelijä saa käsitellä henkilötietoja vain ja ainoastaan rekisterinpitäjän antamien ohjeiden mukaisesti. Henkilötietojen käsittelijän on tarkasti huomioitava roolinsa rajat. Mikäli henkilötietojen käsittelijänä toimiva yritys käsittelytoiminnoissaan määrittelee itsenäisesti henkilötietojen käsittelyn tarkoituksia ja keinoja, tulkitaan henkilötietojen käsittelijä rekisterinpitäjäksi. Tällöin kyseistä yritystä velvoittavat kaikki tietosuoja-asetuksen rekisterinpitäjälle asettamat velvoitteet, mukaan lukien osoitusvelvollisuus ja suora velvollisuus vastata rekisteröityjen pyyntöihin. Yksityisten turvallisuuspalveluiden tuottaja on velvoitettu toimialansa lainsäädännössä määritetysti luovuttamaan henkilötietoja erilaisten raporttien ja ilmoitusten sisältämässä muodossa poliisihallitukselle ja paikallispoliisille. Kyseessä ei ole käsittelysääntöä rikkova ”itsenäinen henkilötietojen käsittelyn tarkoitus” vaan lakisääteinen velvoite, joka on osa tehtyä toimeksiantoa.

Henkilötietojen käsittelijän roolissa toimivat esimerkinomaisesti myös yrityksen mahdollisesti ulkoistamat kirjanpitoa-, palkanlaskentaa, tietojenkäsittelyä-, ohjelmistoalustoja- ja turvallisuuspalveluja alihankintasopimuksella tuottavat palveluntoimittajat. Viranomaiset, eläkevakuutusyhtiöt, vahinkovakuutusyhtiöt, työllisyysrahasto, pankkipalvelut ja rahoituslaitokset ovat itsenäisiä rekisterinpitäjiä, joille yritys luovuttaa henkilötietoja.

4.2.2 Henkilötietojen käsittelijän vastuut ja erityiset velvoitteet

Henkilötietojen käsittelijä voi käsitellä henkilötietoja vain ja ainoastaan rekisterinpitäjän dokumentoitujen ohjeiden mukaisesti ja lukuun. Henkilötietojen käsittelijät noudattavat henkilötietojen käsittelyssä unionissa sovellettavaa lainsäädäntöä ja heidän tulee huolehtia yrityksessään tarvittavista teknisistä ja organisatorisista suojaustoimista. Rekisterinpitäjän ja henkilötietojen käsittelijän tulee tehdä kirjallinen tietojenkäsittelysopimus.

Henkilötietojen käsittelijän palveluksessa olevat henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta ja tekemään siitä sopimuksen tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus. Yksityisissä turvallisuuspalveluissa (LYTP:ssa) on salassapitovelvollisuutta koskeva maininta ja toimialan työsopimuksissa pääasiassa on salassapitovelvollisuutta koskeva maininta. Lisäksi näitä tehdään erikseen pyydettäessä ja turvallisuusselvityksien yhteydessä. Henkilötietojen käsittelijä saa käyttää alihankintakumppania vain rekisterinpitäjän luvalla.

4.3 Rekisteröity

4.3.1 Rekisteröidyn rooli ja sen määräytyminen

Rekisteröity on luonnollinen henkilö eli ihminen, jonka henkilötietoja käsitellään. Meistä jokainen on rekisteröity. Olemme rekisteröity erilaisten viranomaisten rekistereissä ja tietokannoissa, työnantajalla tai omassa yritystoiminnassa, oppilaitoksessa tai harrastustoiminnassa ja monessa muussa toiminnassa, jossa olemme mukana henkilötiedoillamme. Tietosuojalait suojaavat kaikkien meidän rekisteröityjen oikeuksia ja vapauksia.

Tietosuoja-asetuksessa henkilötiedolla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön eli ihmiseen liittyviä tietoja. Tunnistettavana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti hänen tunnistetietojensa perusteella. Määritelmä on varsin laaja. Kyse on henkilötiedoista, kun tietojen perusteella voidaan tietää tai saada selville kenestä on kyse. Kun asetuksessa kyse on tunnistettavan tai tunnistettavissa olevan henkilön tietojen käsittelystä tulee tietosuoja-asetus sellaisenaan heti sovellettavaksi. Varsinaista rekisteriä ei tarvitse olla. Rekisteröidyn ei siis tarvitse olla kirjattuna varsinaisesti rekisteriin ollessaan rekisteröity.

4.3.2 Oikeus saada läpinäkyvää informaatiota henkilötietojen käsittelystä

Yrityksellä on rekisterinpitäjän roolissa toimiessaan velvollisuus informoida avoimesti henkilötietojen käsittelystä jo ennen käsittelytoimien aloittamista. Tietosuoja-asetuksen mukaan käsittelyn tulisi olla läpinäkyvää. Rekisteröityjen tulisi saada tieto siitä, miten heitä koskevia henkilötietoja kerätään, mihin niitä käytetään, missä määrin niitä käsitellään tai tullaan käsittelemään. Informaation on oltava helposti ja nopeasti saatavilla ja kaikki tieto on annettava selkeällä kielellä.

Tietosuoja-asetuksen rekisteröityjen informoimisesta määräämiä tietoja on toimitettava:

- tiiviisti esitetysti
- läpinäkyvästi
- helposti ymmärrettävässä muodossa
- helposti saatavissa olevassa muodossa
- selkeällä ja yksinkertaisella kielellä

Käytännössä yrityksen tulisi pitää kuvaus henkilötietojen käsittelystä rekisteröityjen saatavissa. Tiedot on toimitettava kirjallisesti tai muulla tavoin ja tapauksen mukaan sähköisessä esitysmuodossa. Tietosuoja-asetuksessa ei ole säädetty rekisteriselosteesta tai tietosuojaselosteesta vaan rekisteröityjen informoimisesta. Käytännössä tietosuojaselosteita käytetään. Läpinäkyvyyden vaatimus vaatii myös tietojärjestelmiltä kykyä tähän. Rekisteröityjen informointia kuvataan yksityiskohtaisemmin seuraavassa luvussa.

4.3.3 Oikeus saada pääsy tietoihin

Rekisteröidyllä on oikeus saada vahvistus siitä, käsitteleekö yritys häntä koskevia henkilötietoja. Mikäli yritys käsittelee rekisteröidyn henkilötietoja, rekisteröidyllä on tietosuoja-asetuksen mukaan oikeus saada pääsy henkilötietoihin, sekä lisäksi saada seuraavat tiedot:

- käsittelyn tarkoitukset
- käsiteltävät henkilötietoryhmät
- vastaanottajat tai vastaanottajaryhmät, joille yritys on luovuttanut henkilötietoja tai joille yrityksellä on tarkoitus niitä luovuttaa

- henkilötietojen suunniteltu säilytysaika tai jos sellaista ei voida ilmoittaa on ilmoitettava säilytysajan määrittämiskriteerit
- rekisteröidyn oikeus pyytää yritystä oikaisemaan tai poistamaan häntä koskevia tietoja ja oikeus rajoittaa tai vastustaa yrityksen henkilötietojen käsittelyä näissä
- rekisteröidyn oikeus tehdä valitus valvontaviranomaiselle
- kaikki henkilötietojen alkuperästä käytettävissä olevat tiedot, jos henkilötietoja ei kerätä rekisteröidyltä itseltään
- automaattisen päätöksenteon (profilointi) mukanaolo ja jos sitä tehdään, keskeiset tiedot käsittelyyn liittyvästä logiikasta, merkittävyydestä ja mahdollisista seurauksista rekisteröidylle

Pääsy tietoihin toteutetaan käytännössä siten, että rekisteröidylle toimitetaan hänestä käsiteltävistä henkilötiedoista jäljennös sekä yrityksen tietosuojaseloste tai erillinen tätä varten tehty seloste. Huomioitavaa on se, että jäljennöksen toimittaminen rekisteröidyn henkilötiedoista ei saa vaikuttaa haitallisesti muiden rekisteröityjen oikeuksiin ja vapauksiin. Siten rekisteröidylle itselleen ei tarvitse antaa esimerkiksi tietoja, jotka sisältävät myös muiden henkilöiden henkilötietoja tai ovat luonteeltaan yrityksen liikesalaisuuksia.

4.3.4 Oikeus tietojen oikaisemiseen

Henkilötietojen virheettömyys on osa rekisteröityjen oikeusturvaa tietosuoja-asioissa. Oikaisuoikeus täydentää henkilötietojen käsittelyn periaatteiden mukaista tietojen täsmällisyysperiaatetta. Oikaisuoikeus myös ehkäisee osaltaan mahdollisia myöhempiä oikeudenloukkauksia. Oikaiseminen tarkoittaa, että rekisteröity voi:

- korjata virheellisiä tietoja
- korjata ja poistaa vanhentuneita ja siksi nykyisin vääriä tietoja
- täydentää puutteellisia tietoja

Jos rekisteröidyn oikaistavaksi ilmoitetulla tiedolla on oikeudellisia vaikutuksia tai sillä voi olla oikeudellisia vaikutuksia, tiedon oikeellisuus tulee varmistaa ja todentaa tarkemmin. Rekisteröidyn henkilötietojen oikaisuoikeus koskee vain häntä itseään koskevia tietoja. Oikaisu, joka on todettu perustellusti oikeaksi, on tehtävä ilman aiheetonta viivytystä.

4.3.5 Oikeus tietojen poistamiseen, eli oikeus tulla unohdetuksi

Rekisteröidyllä on oikeus saada yritys poistamaan häntä koskevat tiedot eli oikeus tulla unohdetuksi seuraavissa tilanteissa:

- rekisteröidyn henkilötietoja ei enää tarvita niihin käyttötarkoituksiin, joita varten ne kerättiin tai joita varten niitä käsiteltiin
- rekisteröity peruuttaa suostumuksensa henkilötietojensa käsittelyyn siihen tarkoitukseen, johon käsittely on suostumuksella perustunut, eikä yrityksellä ole käsittelyn jatkamiselle muuta laillista perustetta
- rekisteröity vastustaa käsittelyä vastustamisoikeutensa perusteella, eikä käsittelylle ole muuta perustetta tai kun rekisteröity vastustaa käsittelyä suoramarkkinointitarkoituksiin
- henkilötietoja on käsitelty lainvastaisesti
- henkilötiedot on poistettava unionin tai kansalliseen lainsäädäntöön perustuvan yritystä velvoittavan säädöksen noudattamiseksi
- henkilötiedot on kerätty tarjottaessa tietoyhteiskunnan palveluja suoraan lapselle

Rekisteröidyn oikeus tulla unohdetuksi on rajoitettu. Lisäksi edellä listattuja ei sovelleta, jos käsittely on tarpeen:

- sananvapautta ja tiedonvälityksen vapautta koskevan oikeuden käyttämiseksi,
- rekisterinpitäjään sovellettavan lainsäädäntöön perustuvan ja käsittelyä edellyttävän lakisääteisen velvoitteen noudattamiseksi
- ennaltaehkäisevää tai työterveydenhuoltoa koskevia tarkoituksia varten ja kansanterveyteen liittyvän yleisen edun vuoksi
- yleisen edun mukaisia arkistointitarkoituksia tai tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten, mikäli oikeus todennäköisesti estäisi kyseisen käsittelyn tai vaikeuttaisi sitä suuresti
- oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi

Mikäli käsitellyt tiedot tulee poistaa, tulee niiden poisto tehdä ilman aiheetonta viivytystä.

4.3.6 Oikeus käsittelyn rajoittamiseen

Rekisteröidyllä on oikeus seuraavissa tilanteissa siihen, että yritys rajoittaa hänen henkilötietojensa käsittelyä:

- rekisteröity on kiistänyt henkilötietojensa paikkansa pitävyyden
- käsittely on lainvastaista ja rekisteröity vastustaa henkilötietojen poistamista ja vaatii sen sijaan niiden käytön rajaamista
- rekisterinpitäjä ei enää kyseessä olevia henkilötietoja tarvitse käsittelyn tarkoituksiin, mutta rekisteröity tarvitsee niitä oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi
- rekisteröity on vastustamisoikeutensa perusteella vastustanut henkilötietojen käsittelyä odottaessa todentamista kysymyksessä syrjäyttävätkö rekisterinpitäjän oikeutetut perusteet rekisteröidyn perusteet

Käytännössä kysymys on aktiivisen käsittelyn rajoittamisesta. Yritys saa säilyttää tiedot, mutta se saa käsitellä niitä ainoastaan:

- rekisteröidyn suostumuksella
- oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi
- toisen henkilön tai yrityksen oikeuksien suojaamiseksi

Käytännössä rekisterinpitäjä voi toteuttaa käsittelyn rajoittamisen esimerkiksi siirtämällä tiedot toiseen käsittelyjärjestelmään tai estämällä käyttäjien pääsyn tietoihin. Tietosuojavaltuutetun antaman ohjeistuksen perusteella käsittelyn rajoittaminen on ilmaistava järjestelmässä selkeästi ja varmistettava teknisesti niin, etteivät tiedot myöhemmin joudu käsittelytoimien kohteiksi. Mikäli tietojen käsittelyn rajoitus poistetaan, yrityksen on ilmoitettava rekisteröidylle siitä etukäteen.

4.3.7 Tietojen oikaisun, poiston tai käsittelyn rajoittamisen ilmoitusvelvollisuus

Tietosuoja-asetuksessa säädetään henkilötietojen oikaisua, poistamista tai käsittelyn rajoitusta koskevasta ilmoitusvelvollisuudesta. Säädöksen mukaan rekisterinpitäjän on ilmoitettava käsittelyssä tehdyistä henkilötietojen oikaisuista, poistamisista tai käsittelyn rajoituksista kaikille vastaanottajille jolle rekisterinpitäjä on henkilötietoja luovuttanut.

Ilmoitusvelvollisuutta ei ole, jos toimenpide osoittautuu rekisterinpitäjälle mahdottomaksi tai toimenpide vaatisi kohtuutonta vaivaa. Jos rekisterinpitäjä jättää ilmoitusvelvollisuuden tekemättä, hänen tulee osoittaa jommankumman perusteen olemassaolo todeksi osoitusvelvollisuuden täyttymisen vuoksi. Lisäksi jos ja vain kun rekisteröity itse sitä pyytää, tulee rekisterinpitäjän ilmoittaa rekisteröidylle näistä henkilötietojen vastaanottajista.

4.3.8 Oikeus siirtää tiedot järjestelmistä toiseen

Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on itse toimittanut yritykselle jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, sekä oikeus siirtää kyseessä olevat tiedot toiselle yritystoimijalle tai muulle rekisterinpitäjälle jos:

- rekisteröidyn tietojen käsittelyperuste perustuu suostumukseen tai sopimukseen ja
- henkilötietojen käsittely suoritetaan automaattisesti

Mikäli henkilötietojen käsittelyperuste ei perustu suostumukseen tai sopimukseen ei rekisteröidyllä ole oikeutta siirtää tai pyytää siirtämään henkilötietoja järjestelmästä toiseen. Siirto-oikeus koskee ainoastaan tietoja jotka rekisteröity on itse toimittanut yritykselle. Itse toimitetuksi luetaan kaikki rekisteröidyn toimesta tapahtunut aktiivinen toiminta. Jos henkilöllä on tietojen siirto-oikeus, hänellä on oikeus saada siirto suoraan yritykseltä toiselle, jos se on teknisesti mahdollista. Rekisterinpitäjien tulisi tätä oikeutta mahdollistaa. Siirto-oikeus ei saa vaikuttaa haitallisesti muiden oikeuksiin tai vapauksiin.

4.3.9 Käsittelyn vastustamisoikeus

Rekisteröidyllä on oikeus henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella vastustaa häntä koskevien tietojen käsittelyä kun käsittely perustuu yrityksen oikeutettuihin etuihin. Tässä tapauksessa yritys ei saa käsitellä henkilötietoja ellei se voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy, joka syrjäyttää rekisteröidyn edut, oikeudet ja vapaudet. Vastustamisesta huolimatta käsittelyä voidaan jatkaa jos se on tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi.

Mikäli rekisteröidyn henkilötietoja käsitellään suoramarkkinointia varten, rekisteröidyllä on oikeus milloin tahansa vastustaa häntä koskevien henkilötietojen käsittelyä suoramarkkinointitarkoitukseen. Kielto kattaa myös suoramarkkinointiin liittyvän profiloinnin. Rekisteröidyn käyttäessä vastustamisoikeuttaan suoramarkkinointiin hänen henkilötietojaan ei saa enää käsitellä. Mikäli henkilötietojen käyttämiselle on muutoin perusteet, voidaan henkilötietojen käyttöä muihin käsittelytarkoituksiin jatkaa normaaliin tapaan.

4.3.10 Automatisoituihin päätöksiin ja profilointiin liittyvät oikeudet

Tietosuoja-asetuksen mukaan ”rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi”. Oikeus olla joutumatta automatisoidun päätöksen kohteeksi ei koske pitkälle automatisoitua päätöksentekoprosessia, joka on osin manuaalinen, eli prosessiin osallistuu jossain vaiheessa ihminen.

Yritys saa käyttää automatisoitua päätöksentekojärjestelmää seuraavissa tapauksissa:

- päätös on välttämätön rekisteröidyn ja yrityksen välisen sopimuksen tekemistä tai täytäntöönpanoa varten
- päätös on hyväksytty lainsäädännössä
- päätös perustuu rekisteröidyn nimenomaiseen suostumukseen

Mikäli yrityksessä käytetään automatisoitua päätöksentekojärjestelmää, yrityksen on toteutettava asianmukaiset toimenpiteet rekisteröityjen oikeuksien ja vapauksien, sekä myös oikeutettujen etujen suojaamiseksi. Käytännössä se tarkoittaa sitä, että rekisteröidyllä tulee olla vähintään:

- oikeus vaatia, että tiedot käsittelee yrityksen puolesta ihminen
- oikeus esittää kantansa ja riitauttaa päätös

Automatisoitu päätöksenteko ei saa perustua arkaluontoisiin tietoihin muutoin kuin siinä tapauksessa, että niiden käsittelyyn on saatu suostumus tai niiden käsittely on tarpeen tärkeää yleistä etua koskevasta syystä ja lainsäädännön nojalla. Automaattinen henkilötietojen käsittely lisää käsittelyyn liittyviä riskejä ja vaikuttaa siten velvollisuuteen tehdä tietosuojaa koskeva vaikutusten arviointi.

5 KÄSITTELYN HALLINTATOIMET KÄYTÄNNÖSSÄ

Luvussa käsitellään henkilötietojen käytännön hallintatoimet eri osapuolten välillä ja mitä ne käytännössä vaativat yrityksiltä tehtäväksi. Käsittelyssä on rekisteröityjen oikeudet ja informointivaatimukset, käsittelyn osapuolten väliset tietojenkäsittely- ja luovutussopimukset sekä valvontaviranomaista varten tehtävät selosteet käsittelytoimista. Luvun keskeinen osa on henkilötietojen käsittelyn turvallisuus ja mitä se edellyttää yrityksiltä.

5.1 Rekisteröityjen informointi

5.1.1 Rekisteröidylle informoitavat henkilötietojen käsittelyyn liittyvät tiedot

Tietosuoja-asetuksessa on eroteltu henkilötietojen keräämistilanteet kahteen, ensimmäiseksi tilanteeseen, jossa henkilötiedot kerätään rekisteröidyltä itseltään ja toiseksi tilanteeseen, jossa ne kerätään jostain muualta. Useimmissa tapauksissa ja useimmille yrityksille voisi kuitenkin olla järkevää esittää tiedot näiden yhteisellä tietosuojaselosteella tai muulla tavalla. Rekisteröidylle informoitavat tiedot on kuitenkin alla eriytetty.

Kun rekisteröidyltä itseltään kerätään häntä koskevia henkilötietoja, on yrityksen rekisterinpitäjänä toimitettava rekisteröidylle kaikki seuraavat tiedot samassa yhteydessä, kun henkilötiedot saadaan:

- yrityksen identiteettitiedot ja tapauksen mukaan rekisterinpitäjän edustajan nimi, sekä yhteystiedot
- yrityksen tietosuojavastaavan yhteystiedot, jos yrityksellä on nimetty tietosuojavastaava
- henkilötietojen käsittelyn tarkoitukset (esimerkiksi suoramarkkinointi- ja viestintä, asiakassuhteiden hallinta, työntekijöiden rekrytointi, työsuhteiden hallinta, alihankinta- ja toimittajasuhteiden hallinta tai turvallisuuspalveluiden tuotanto), sekä käsittelyn oikeusperuste (esimerkiksi suostumus, sopimus, lakisääteiset velvoitteet tai oikeutettu etu)
- käsiteltävät henkilötietoryhmät (esimerkiksi nimi, henkilötunnus, yhteystiedot) on suositeltavaa ilmoittaa myös tässä tilanteessa, vaikka tietosuoja-asetus vaatii sitä vain tilanteessa, jossa henkilötiedot on kerätty jostain muualta kuin rekisteröidyltä itseltään

- yrityksen tai kolmannen osapuolen oikeutetut edut, jos käsittely perustuu niihin (esimerkiksi asiakassuhde tai työsuhde)
- yrityksen käsittelemien henkilötietojen vastaanottajat tai vastaanottajaryhmät (esimerkiksi tietyt viranomaiset tai yrityksen kanssa samaan konserniin kuuluvat yritykset)
- tieto siitä, aikooko rekisterinpitäjä siirtää henkilötietoja EU:n ulkopuolelle ja jos, niin minne, sekä lisäksi tieto tietosuojan riittävyyttä koskevan komission päätöksen olemassaolosta tai puuttumisesta, sekä muut artiklassa edellytetyt tiedot asianmukaisista suojatoimista ja dokumentaation saatavuudesta
- käsiteltävien henkilötietojen säilytysaika tai jos se ei ole mahdollista ilmoittaa, niin henkilötietojen säilytysaikojen määrittämiskriteerit
- rekisteröidyn oikeudet:
    - oikeus pyytää yritykseltä pääsy häntä itseään koskeviin henkilötietoihin
    - oikeus pyytää yritystä häntä itseään koskevien henkilötietojen oikaisemiseen, poistamiseen tai käsittelyn rajoittamiseen
    - oikeus vastustaa häntä itseään koskevien henkilötietojen käsittelyä
    - oikeus pyytää yritystä siirtämään häntä itseään koskevat henkilötiedot järjestelmästä toiseen
    - oikeus peruuttaa suostumus milloin tahansa suostumuksen peruuttamisen vaikuttamatta suostumuksen perusteella ennen tämän peruuttamista suoritetun käsittelytoimien lainmukaisuuteen, jos käsittely perustuu rekisteröidyn suostumukseen
    - oikeus tehdä valitus rekisterinpitäjästä valvontaviranomaiselle, jos hän katsoo tietosuoja-asetukseen perustuvia oikeuksiaan loukatun
- ”onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus taikka sopimuksen tekemisen edellyttämä vaatimus sekä onko rekisteröidyn pakko toimittaa henkilötiedot ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset” (esimerkiksi jos rekisteröity ei anna henkilötietojaan ei palvelua voida toimittaa)
- automaattisen päätöksenteon, mukaan lukien sellainen profilointi, jolla on rekisteröityä koskevia oikeusvaikutuksia, sekä ainakin näiden osalta merkitykselliset tiedot käsittelyyn liittyvästä logiikasta, samoin kuin kyseisen käsittelyn merkittävyys ja mahdolliset seuraukset rekisteröidylle (esimerkiksi suoramarkkinoinnin kohdistamiseen)
- tietoja ei tarvitse toimittaa, jos ja siltä osin kuin rekisteröity on jo saanut tiedot

Kun henkilötietoja kerätään muualta kuin rekisteröidyltä itseltään, tulee rekisteröidylle edellä mainittujen tietojen lisäksi antaa seuraavat tiedot kohtuullisessa ajassa, kuitenkin viimeistään yhden kuukauden kuluessa:

- käsiteltävät henkilötietoryhmät (esimerkiksi nimi, henkilötunnus, yhteystiedot)
- mistä henkilötiedot on saatu ja tarvittaessa se, että onko henkilötiedot saatu yleisesti saatavilla olevista lähteistä

Kun yritys on kerännyt henkilötiedot muualta kuin rekisteröidyltä itseltään, sen ei tarvitse antaa tietoja rekisteröidylle seuraavissa erityistapauksissa:

- rekisteröity on jo saanut tiedot
- tietojen toimittaminen rekisteröidylle osoittautuu mahdottomaksi tai se vaatisi kohtuutonta vaivaa
- tietojen hankinnasta ja luovuttamisesta säädetään nimenomaisesti rekisterinpitäjän yritykseen sovellettavassa lainsäädännössä, jossa vahvistetaan asianmukaiset toimenpiteet rekisteröidyn oikeutettujen etujen suojaamiseksi
- tiedot on pidettävä luottamuksellisena, koska niihin koskee soveltuvaan lainsäädäntöön perustuva vaitiolovelvollisuus

Rekisteröidyn tulee tarvittaessa oikeuksiaan käyttäessään toimittaa rekisterinpitäjälle tiedot, jolla rekisterinpitäjä voi todentaa rekisteröidyn henkilöllisyyden ja oikeutensa.

5.1.2 Rekisterinpitäjän informointitavat ja keinot

Tietosuoja-asetuksen mukainen rekisteröityjen informointivelvollisuus ei ole rekisteriperusteinen. Tietosuoja-asetuksessa ei säädetä mistään erityisestä tai tietystä informointi muodosta, eikä edes selosteesta tai viestinnän keinoista. Tiedot käsittelytoimista voidaan antaa rekisteröidylle esimerkiksi sähköpostitse, verkkosivuilla, kirjeenä postitse, paperilla, kuvakeinformaatiolla tai videotiedostona. Informointitapa on vapaa, mutta käytännössä viestintätapa ratkaisee, sekä se, että rekisterinpitäjällä on osoitusvelvollisuus.

Monelle yritykselle on edelleen helpointa ja osoitusvelvollisuuden kannalta tehokkainta kuvata henkilötietojen käsittely rekisteröityjen informaatioksi tietosuojaselosteiden avulla ja edelleen rekisterikohtaisena, vaikka tietosuoja-asetuksessa käytetään rekisterien asemasta henkilötietojen käsittelyn tarkoituksia. Lisäksi yritys voisi miettiä yhdistäisikö se rekisteröityjen informoimiseksi laatiman tietosuojaselosteen valvontaviranomaisen

vaatiman seloste käsittelytoimista kanssa. Selosteratkaisumalliin vaikuttaa yrityksen koko ja palvelutoiminnan monimuotoisuus.

5.2 Tietojenkäsittelysopimukset ja henkilötietojen luovutussopimukset

5.2.1 Tietojenkäsittelysopimuksen laatimisvelvollisuus ja sisältö

Tietosuoja-asetus edellyttää kirjallisen tietojenkäsittelysopimuksen tai vastaavan oikeudellisen asiakirjan tekemistä kaikissa toimeksiannoissa, joissa henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän puolesta ja lukuun. Tietojenkäsittelysopimus voi olla muodoltaan esimerkiksi yksittäinen sopimus tai liite.

Tietojenkäsittelysopimuksessa tulee tietosuoja-asetuksen mukaisesti vahvistaa ja kuvata sopimuksesta ainakin seuraavat asiat:

- henkilötietojen käsittelyn kohde ja kesto (esimerkiksi: sopimuksen osapuolet, kohde ja sopimusaika tai sopimus on toistaiseksi voimassaoleva kolmen kuukauden molemminpuolisella irtisanomisajalla)
- henkilötietojen käsittelyn luonne ja tarkoitus (esimerkiksi: turvallisuuspalveluiden toimittaminen – vartiointi- ja turvasuojaustoiminta, tarvittaessa tarkemmin)
- henkilötietojen tyyppi, eli mitä henkilötietoja käsitellään (esimerkiksi: henkilöiden yksilöinti- ja yhteystiedot, mekaaniset ja sähköiset kulkuoikeustunnisteet, hälytyslaitteiden käyttökoodit, kuvatallenne/videotallenne, turvallisuusjärjestelmien lokitiedot, IP osoitteet, henkilön muut tunnistetiedot, henkilötiedot voivat sisältää arkaluontoisia henkilötietoja ja henkilötietoja rikostuomioista tai rikkomuksista)
- rekisteröityjen ryhmät (esimerkiksi: asiakas, työntekijät, sidosryhmät, toimenpiteiden kohde tai muu mahdollinen kolmas osapuoli)
- rekisterinpitäjän oikeudet ja velvollisuudet (esimerkiksi: viittaus lainsäädäntöön, tarkennus velvoitteiden aiheuttamien kustannusten jakoa ja maksuja koskien)

Tietojenkäsittelysopimuksessa tulee tietosuoja-asetuksen mukaisesti erityisesti sopia seuraavista menettelyistä koskien henkilötietojen käsittelijää:

- henkilötietojen käsittelijä käsittelee tietojenkäsittelysopimuksen tarkoituksessa henkilötietoja ainoastaan ja vain rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti, huomioiden myös turvallisuuspalveluja ohjaava lainsäädäntö

- henkilötietojen käsittelijä varmistaa, että henkilöt, jotka käsittelevät henkilötietoja, ovat dokumentoidusti sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee lakisääteinen salassapitovelvollisuus
- henkilötietojen käsittelijällä on velvollisuus toteuttaa ja varmistaa kaikki tietosuoja-asetuksessa säädetyt käsittelyn turvallisuuteen liittyvät tekniset- ja organisatoriset toimenpiteet
- henkilötietojen käsittelijä ei saa sopimuksen mukaisessa palvelussaan käyttää alihankintaa, eli toista henkilötietojen käsittelijää ilman rekisterinpitäjän antamaa erityistä tai yleistä kirjallista lupaa, lisäksi toiseen henkilötietojen käsittelijään sovelletaan kaikkia samoja vaatimuksia kuin toimeksiannon saaneeseen ensimmäiseen henkilötietojen käsittelijään, toimeksiannon saanut ensimmäinen henkilötietojen käsittelijä vastaa käyttämästään toisesta tai useammasta henkilötietojen käsittelijästä velvoitteiden osalta kuin omistaan
- henkilötietojen käsittelijä sitoutuu auttamaan mahdollisuuksiensa mukaan asianmukaisilla teknisillä- tai organisatorisilla toimenpiteillä rekisterinpitäjää, tämän täyttäessä velvollisuuttaan vastata pyyntöihin, joita rekisteröidyt voivat esittää tietosuoja-asetuksen mukaisten rekisteröityjen oikeuksien perusteella
- henkilötietojen käsittelijän on käsittelyn luonne ja siitä saatavilla olevat tiedot huomioiden autettava rekisterinpitäjää varmistamaan, että rekisterinpitäjän tietyistä velvollisuuksista huolehditaan; näitä ovat:
    - henkilötietojen käsittelyn turvallisuus
    - henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle
    - henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle
    - tietosuojaa koskevan ja edellyttävän vaikutusarvioinnin teettäminen
    - valvontaviranomaisen ennakkokuuleminen
- henkilötietojen käsittelijän on rekisterinpitäjän valinnan mukaan joko poistettava tai palautettava käsittelyyn liittyvien palveluiden päätyttyä kaikki henkilötiedot rekisterinpitäjälle, paitsi jos henkilötietojen käsittelijään sovellettavassa lainsäädännössä vaaditaan säilyttämään henkilötiedot palvelun päättymisen jälkeen
- henkilötietojen käsittelijän on saatettava rekisterinpitäjän saataville kaikki tiedot, jotka ovat tarpeen tietosuoja-asetuksen tai tietojenkäsittelysopimuksen mukaisten velvoitteiden noudattamisen osoittamista varten, sekä sallia rekisterinpitäjän tai tämän valtuutetun suorittamat auditoinnit ja itse osallistuttava niihin

Henkilötietojen käsittelijän on aina ilmoitettava rekisterinpitäjälle jos hän katsoo, että ohjeistus tai muu rikkoo tietosuoja-asetusta, muita tietosuojasäädöksiä tai lainsäädäntöä. Mikäli henkilötietojen käsittelijä rikkoo tietosuoja-asetusta ja tietojenkäsittelysopimusta määrittämällä henkilötietojen käsittelyn tarkoitukset ja keinot, on henkilötietojen käsittelijää pidettävä tämän käsittelyn osalta rekisterinpitäjänä velvollisuuksineen ja vastuineen.

Tietojenkäsittelysopimusten sijaan voidaan käyttää tapauskohtaisesti harkiten komission tai valvontaviranomaisen hyväksymiä vakiosopimuslausekkeita. Suomessa esimerkiksi Teknologiainfo Teknova Oy:n julkaisema IT2018-ehdot on uudistettu ja näihin on sisällytetty henkilötietojen käsittelyä koskevat erityisehdot. Näitä on myös turvasuojauksessa mahdollista hyödyntää sopimuksen liitteinä esimerkiksi videovalvontajärjestelmien sopimusehtoina. Samoin ehtoja voidaan luonnollisesti käyttää IT palveluntoimittajien kanssa.

Myös Taloushallintoliiton TAL2018-ehdot päivityksessä on huomioitu sopimus henkilötietojen käsittelystä rekisterinpitäjän ja henkilötietojen käsittelijän välillä muun muassa kirjanpidossa ja palkanlaskennassa. Mikäli nämä on ulkoistettu esimerkiksi tilitoimistolle ja tilitoimisto käyttää taloushallintoliiton uusia sopimuslomakkeita, sen liitteitä ja sopimusehtoja, niitä on hyvä ja turvallista soveltaa myös tietojenkäsittelysopimuksen myötä. Myös useimmilla taloushallinnon ja HR:n SaaS-ohjelmistopalvelujen tuottajilla on hyvät tietojenkäsittelysopimukset, joita on hyvä hyödyntää sopimusvelvoitteen täyttämiseksi.

5.2.2 Henkilötietojen luovuttaminen, sen perusteet ja luovutussopimukset

Rekisterinpitäjä voi siirtää rekisteröityjensä henkilöiden henkilötietoja kolmansille osapuolille joko käsiteltäviksi tai niin, että tiedot vastaanottaneesta kolmannesta osapuolesta tulee rekisterinpitäjä. Kun tiedot vastaanottanut viranomainen tai yritys on tehdyn siirtämistoimenpiteen jälkeen siirrettyjen henkilötietojen rekisterinpitäjä, on kyseessä henkilötietojen luovutus. Yritys voi rekisterinpitäjänä luovuttaa henkilötietoja vain, jos sekä luovuttajalla että luovutuksensaajalla on laillinen peruste henkilötietojen käsittelyyn.

Henkilötietoja luovutetaan esimerkiksi lakisääteisistä velvoitteista: näitä ovat esimerkiksi työntekijöiden henkilötietojen kohdalla palkkatietojen ilmoittaminen tulorekisteriin, josta veroviranomainen, yrityksen kanssa sopimuksen tehnyt työeläkeyhtiö, yrityksen kanssa sopimuksen tehnyt tapaturma- ja ryhmähenkivakuutusyhtiö ja työllisyysrahasto saavat tarvitsemansa tiedot. Vastaavasti työntekijöiden henkilötietojen kohdalla toimii poliisihallitukselle vuosittain tehtävä turvallisuusalan elinkeinoluvanhaltijan vuosi-ilmoitus, jossa

ilmoitetaan vuoden aikana vartijana, järjestyksenvalvojana, turvasuojaajana, vastaavana hoitajana ja vastaavan hoitajan sijaisena toimineet henkilöt pyydetyillä henkilötiedoilla. Edellä mainitut esimerkit perustuvat yksityisen turvallisuuspalveluyrityksen lakisääteiseen velvollisuuteen, jolloin henkilötietojen luovutuksesta ei ole tarpeen sopia erikseen.

Kun yritys luovuttaa henkilötietoja toiselle yritykselle on laillisen käsittelyperusteen punninnan lisäksi hyvä laatia luovutuksesta kirjallinen henkilötietojen luovutussopimus. Luovutussopimuksen laatimisvelvollisuudesta tai sisällöstä ei ole säädetty tietosuoja-asetuksessa. Luovutussopimuksen tekeminen on kuitenkin asianmukaista ja perusteltua sen varmistamiseksi, että tietosuoja-asetuksen henkilötietojen luovuttamiseen ja osoitusvelvollisuuteen liittyvät vaatimukset tulevat täytetyksi. Luovutussopimuksessa olisi hyvä kirjata ainakin seuraavat asiat:

- tietojen luovuttajan ja vastaanottajan tiedot
- henkilötietojen luovuttaminen rekisterinpitäjältä toiselle rekisterinpitäjälle
- tieto millä perusteella henkilötiedot luovutetaan ja käsittelyn oikeusperuste
- mitä tietoja luovutetaan ja miten tiedot luovutetaan tietoturvallisesti
- milloin tiedot luovutetaan ja mikä on luovutussopimuksen voimassaoloaika
- osapuolet päivittävät tietosuojaselosteensa ja/tai muulla lailla informoivat rekisteröityjä henkilötietojen luovuttamisesta
- osapuolet päivittävät selosteensa käsittelytoimista
- osapuolet hoitavat velvoitteensa rekisteröityjen oikeuksien huomioimisessa
- osapuolet sitoutuvat toimimaan tietosuoja-asetuksen mukaisesti

Henkilötietojen luovuttamisessa ei siis ole kysymyksessä henkilötietojen siirto henkilötietojen käsittelijälle eikä yhteinen rekisteri. Tämä on huomioitava erityisesti samaan konserniin kuuluvien yritysten kesken heidän luovuttaessaan tai siirtäessään henkilötietoja. Kunkin konserniyhtiön rooli henkilötietojen käsittelyssä ratkaisee mikä toimenpide on kyseessä. Henkilötietojen luovuttamisessa niiden vastaanottajasta tulee rekisterinpitäjä.

5.3 Seloste käsittelytoimista

5.3.1 Selosteen tarkoitus ja laatimisvelvollisuus

Tietosuoja-asetuksessa on sekä rekisterinpitäjälle että henkilötietojen käsittelijälle asetettu velvollisuus laatia seloste käsittelytoimista. Seloste tulee olla kirjallisessa sekä sähköisessä muodossa ja se tulee olla pyynnöstä toimitettavissa valvontaviranomaiselle.

Velvollisuus laatia seloste käsittelytoimista ei koske yritystä, jossa on alle 250 työntekijää, paitsi jos yrityksen suorittama henkilötietojen käsittely:

- aiheuttaa todennäköisesti riskin rekisteröidyn oikeuksille ja vapauksille
- ei ole satunnaista
- kohdistuu erityisiin henkilötietoryhmiin eli arkaluontoisiin henkilötietoihin
- kohdistuu rikostuomioita ja rikkomuksia koskeviin henkilötietoihin

Yksityisten turvallisuuspalveluiden näkökulmasta ei ole perusteltua jättää selostetta käsittelytoimista tekemättä. Kun yrityksessä on aktiivista toimintaa, on henkilötietojen käsittely muuta kuin satunnaista, lisäksi vartiointi- ja järjestyksenvalvojatoiminnassa kaikki muutkin kolme edellytyskohtaa täyttyvät ja turvasuojauksessakin täyttyvät kaksi - kolme.

Seloste käsittelytoimista laatimisvelvollisuus on hyväksi rekisterinpitäjälle ja käsittelijälle. Selosteen laatimis- ja ylläpitovelvollisuus edellyttää ajantasaista tietoa siitä, mitä käsittelytoimia yrityksen vastuulla milloinkin on. Selosteen tarkoituksena on toimia yrityksen sisäisenä asiakirjana käsittelytoimien laajuuden tiedostamisessa ja informoimisessa pyydettäessä valvontaviranomaiselle, sekä osoitusvelvollisuusvaatimuksen täyttämiseksi.

5.3.2 Rekisterinpitäjän laatiman selosteen sisältö

Rekisterinpitäjän laatiman ja ylläpitämän selosteen käsittelytoimista dokumentin sisältönä tulee olla seuraavat tiedot:

- rekisterinpitäjä, tämän edustajan ja tietosuojavastaan nimi, sekä yhteystiedot
- henkilötietojen käsittelyn tarkoitukset riittävän yksityiskohtaisesti ja selkeästi (kuvaa selosteessa erikseen kaikki käyttötarkoitukset, esimerkiksi markkinointi- ja viestintä, asiakassuhteiden hallinta, työntekijöiden rekrytointi, työsuhteiden

hallinta tai alihankinta- ja toimittajasuhteiden hallinta), lisäksi selosteessa on hyvä mainita käsittelyperuste, vaikka siitä ei ole tämän selosteen laatimisen osalta säädetty (esimerkiksi suostumus, sopimus, lakisääteiset velvoitteet tai oikeutettu etu)

- kuvaus rekisteröityjen ryhmistä ja henkilötietoryhmistä (rekisteröityjen ryhmistä esimerkiksi: potentiaaliset asiakkaat, asiakkaat, työnhakijat, työntekijät, toimittajat, alihankintayritykset ja henkilötietoryhmistä esimerkiksi: nimi, henkilötunnus, yhteystiedot, pankkitili, veronumero, henkilönumero, valokuva, IP osoite, kulkutunniste, käyttökoodi, videotallenne tai kuvatallenne)
- kuvaus henkilötietojen vastaanottajien ryhmistä, joille henkilötietoja on luovutettu tai luovutetaan (selosteessa tulee kuvata täsmällisesti rekisterinpitäjät, joille henkilötietoja on luovutettu tai luovutetaan, näiden lisäksi tulee mainita yhteisrekisterinpitäjät ja henkilötietojen käsittelijät joille henkilötietoja on luovutettu tai luovutetaan tai siirretty tai siirretään), vastaanottajalla tulee olla lainmukainen peruste henkilötietojen käsittelylle, mikäli luovutetaan kolmansiin maihin, kerro mihin, sekä peruste ja mekanismi mikä mahdollistaa näiden tietojen hyväksytyn luovutuksen
- tarvittaessa kuvaus ja tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainvälisille järjestöille (jos siirretään, kerro mihin maihin tai mille järjestöille, sekä peruste ja mekanismi mikä mahdollistaa näiden tietojen hyväksytyn siirron)
- kuvaus eri tietoryhmien osalta niiden poistamisen määräajoista ja mikäli se ei ole mahdollista niin tietoryhmien poistamisaikoihin sovellettavat kriteerit (jos eri henkilötietoryhmillä tai eri tarkoituksiin käsiteltävillä tiedoilla on erilaiset säilytysajat, kuvaa ne selosteessa erikseen)
- mahdollisuuksien mukaan yleinen kuvaus henkilötietojen käsittelyn turvallisuuteen tarkoitetuista teknisistä- ja organisatorisista toimenpiteistä (kuvaa yleisesti vähintään millä tavoilla tiedot on suojattu organisaation ulkopuolisilta, miten käyttöoikeudet käsittelyyn on rajattu organisaation sisällä, millä tavalla ohjeistus on jalkautettu ja millä tavalla käyttöä valvotaan)

Selostetta käsittelytoimista ei ole tarkoitettu rekisteröityjen informointiin. Käytännössä rekisterinpitäjä voi yhdistää selosteet käsittelytoimista tietosuojaselosteisiin, jotka yrityksen on laadittava rekisteröityjen informointivelvollisuuksia varten. Yhdistämisessä on omat puolensa ja etunsa, niin kuin tavallaan myös erillään pidossa. Myös yrityksen suurempi koko ja toiminnan moninaisuus luo selosteiden yhdistämiselle omat selkeyshaasteensa.

5.3.3 Henkilötietojen käsittelijän laatiman selosteen sisältö

Henkilötietojen käsittelijän laatiman ja ylläpitämän, selosteen käsittelytoimista dokumentin sisältönä tulee olla seuraavat tiedot:

- henkilötietojen käsittelijä (nimeä henkilötietojenkäsittelijä yksilöidysti, tämän mahdollisen edustajan ja mahdollisen tietosuojavastaavan nimi ja yhteystiedot)
- rekisterinpitäjät, joiden lukuun henkilötietojen käsittelijä toimii (nimeä kaikki rekisterinpitäjät yksilöidysti, näiden rekisterinpitäjien mahdolliset edustajat ja mahdolliset tietosuojavastaavat, sekä näiden nimet ja yhteystiedot)
- kunkin rekisterinpitäjän lukuun suoritettujen käsittelyiden ryhmät (kuvaa kunkin rekisterinpitäjän osalta erikseen minkä tyyppistä käsittelyä yrityksessä toteutetaan rekisterinpitäjien lukuun esimerkiksi vartioimistoiminta, järjestyksenvalvojatoiminta, turvasuojaustoiminta, tarvittaessa yksilöidymmin)
- tarvittaessa kuvaus ja tiedot henkilötietojen siirtämisestä kolmanteen maahan tai kansainvälisille järjestöille (jos siirretään, kerro mihin maihin tai mille järjestöille, sekä peruste ja mekanismi mikä mahdollistaa näiden tietojen hyväksytyn siirron)
- mahdollisuuksien mukaan yleinen kuvaus henkilötietojen käsittelyn turvallisuuteen tarkoitetuista teknisistä- ja organisatorisista toimenpiteistä (kuvaa yleisesti vähintään millä tavoilla tiedot on suojattu organisaation ulkopuolisilta, miten käyttöoikeudet käsittelyyn on rajattu organisaation sisällä, millä tavalla ohjeistus on jalkautettu ja millä tavalla käyttöä valvotaan)

Selostetta käsittelytoimista ei ole tarkoitettu rekisteröityjen informointiin. Henkilötietojen käsittelijän ylläpitämää selostetta käsittelytoimista ei voi yhdistää tietosuojaselosteisiin.

5.4 Käsittelytoimien johtaminen turvallisuus- ja riskienhallintalähtöisesti

5.4.1 Sisäänrakennettu ja oletusarvoinen tietosuoja

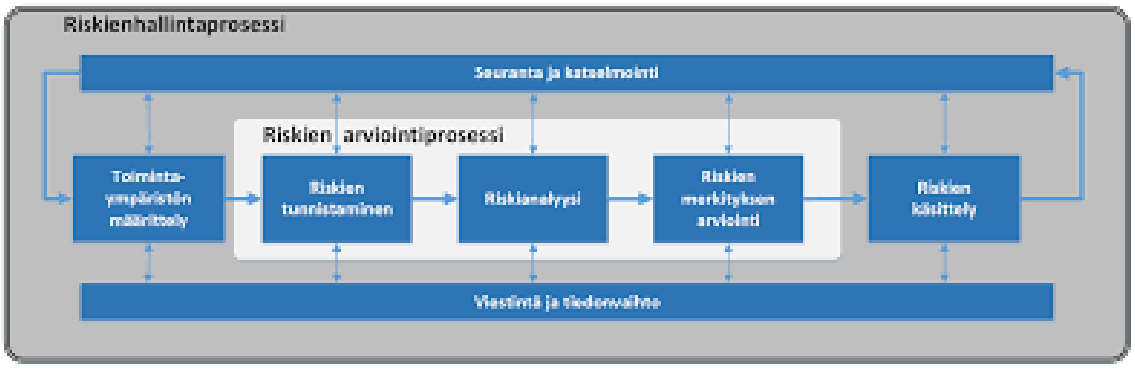
Sisäänrakennettu ja oletusarvoinen tietosuoja tarkoittaa suunnitelmallista lähestymistapaa tietosuoja-asioissa yrityksessä. Tässä tavassa tietosuojaperiaatteet ja kysymykset otetaan huomioon jo alusta alkaen yrityksen suunnitellessa uusia palvelutuotteita tai muutoksia palvelutuotteissaan tai palveluprosesseissaan. Tietosuojakysymykset ovat

esillä yrityksen työstäessä muun muassa palvelunsa henkilötietojen käsittelyä, tietojärjestelmiä, tiedonkäsittelyn turvallisuutta, sekä mahdollisia riskejä ja niihin varautumista.

Tietosuoja tulee siis ottaa huomioon ennakoivasti eli proaktiivisena toimintana. Riskienhallinnassa tai vaikutusten arvioinnissa tunnistetut riskit pyritään ennaltaehkäisemään ja yksityisyyden loukkaukset torjumaan tai ainakin minimoimaan korjailutoimien sijaan. Yksityisyyden suoja on oletusarvo palvelussa ja sen toteuttamisessa käytettävässä järjestelmässä niin, että se ei kuitenkaan heikennä palvelun tai käsittelyn toiminnallisuutta. Luotettavuutta lisää läpinäkyvyys ja avoimuus, sekä käyttäjien yksityisyyden kunnioitus.

5.4.2 Riskienhallintaprosessi

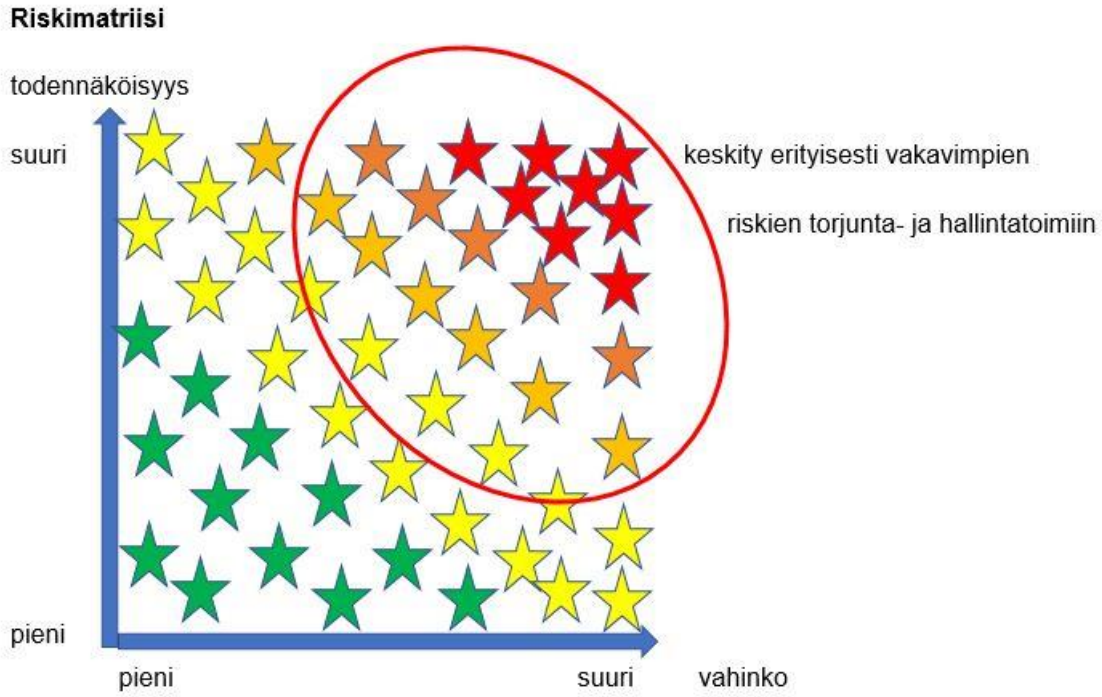
Tietosuoja-asetuksen yhtenä keskeisenä periaatteena on riskiperusteinen lähestymistapa, johon kuuluu riskien arviointi ja sitä kautta ongelmien ennaltaehkäisy. Riskienhallintaprosessia voidaan kuvata selkeästi seuraavan kuvan 2 avulla:



Kuva 2. Riskienhallintaprosessin kuvaus SFS-ISO 31000 mukaisesti.

Yritys tarkastelee kokonaisvaltaisesti riskejä esimerkiksi strategisten riskien, vahinkoriskien, operatiivisten riskien ja taloudellisten riskien näkökulmasta tai yksittäisen projektin tai prosessin tarkastelunäkökulmasta. Tietosuojaan liittyvien riskien tarkastelu ei tästä poikkea. Tunnista toimintaympäristösi, mitä ja miten teet, keiden kanssa toimit ja mitä sidosryhmäriippuvuuksia on olemassa, ja mitä ne tarkoittavat riskienhallinnan kannalta yritykselle ja rekisteröityjen oikeuksille ja vapauksille tietosuojan vaatimusten kannalta. Tietosuojariskien tarkastelussa riskitapahtumat tulee tunnistaa aivan kuten muissakin riskien tarkastelussa ja ne tulee analysoida sekä arvottaa ja riskienhallinnan kannalta käsitellä. Tietosuojariskien tunnistamisessa voidaan lähteä liikkeelle yksinkertaisesti tarkastelemalla henkilötietojen käsittelyn käyttötarkoituksia, rekisteröityjen ryhmiä ja

henkilötietoryhmiä, sekä kenelle yhteistyökumppanille yritys siirtää henkilötietoja käsiteltäväksi ja kenelle se luovuttaa henkilötietoja. Lisäksi tarkastelu voidaan tehdä käytettäviin järjestelmiin ja prosesseihin tietosuojan näkökulmasta. Riskimatriisia voidaan helposti käyttää tähän työvälineenä lueteltujen kohtien ja niiden riskien erillistarkastelussa.



Kuva 3. Riskimatriisin käyttö riskienarvioinnissa.

Matriisissa voi olla tarkasteltavat asiat numeroituina ja ne voidaan viedä riskitaulukkoon.

todennäköisyys					
	4				
	3				
	2				
	1				
		1	2	3	4
	vaikutus				

Taso	Käsittelyn tarve
Kriittinen riski (riskiluku 9-16)	• vaatii yleensä välittömiä toimia • edellyttää jatkuvaa seurantaa
Merkittävä riski (riskiluku 4-8)	• tehtävä suunnitelma riskin pienentämiseksi • seurattava
Kohtalainen riski (riskiluku 3-4)	• ei välttämättä tarvita toimenteitä • seurattava riskiä ja sen mahdollista kehittymistä
Matala riski (riskiluku 1-2)	• ei vaadi akuutteja toimenpiteitä

Riskin nimi	Riskin kuvaus	Riski-luokka	Toden-näköi-syys	Vaikutus	Riskitaso	Käsittelyn tarve	Toimenpiteen kuvaus	Vastuu-henkilö	Aikataulu	Tilanne

Kuva 4. Riskimatriisin ja riskisuunnitelman käyttö riskienhallinnassa (Vahti-ohje).

Riskienarvioinnissa tulee tarkastella tietosuojariskit yrityksen kannalta, mutta myös tietosuoja-asetuksen vaatimuksen mukaisesti rekisteröityjen ihmisten näkökulmasta, joiden henkilötiedoista on käsittelyssä kysymys. Näin esimerkiksi tietoturvariskin vakavuutta arvioitaessa tulisi ottaa huomioon myös se, millaisia vahinkoja ihmisille aiheutuu, jos heidän tietoihinsa ei enää olekaan pääsyä tai heidän yksityiset tietonsa päätyvät vääriin käsiin. Riskeissä rekisteröityjen näkökulma kulkee siis yrityksen näkökulman rinnalla.

Kun tietosuojariskit on tunnistettu, analysoitu ja arvioitu määritellään jatkotoimenpiteet riskien käsittelylle toimenpiteineen, vastuuhenkilöineen ja tavoiteaikatauluineen. Riskien käsittelyvaihtoehtoja voivat olla esimerkiksi:

- riskin torjuminen pidättäytymällä riskiä aiheuttavasta käsittelystä ja toiminnasta
- riskin salliminen eli ottaminen tai jopa lisääminen hyväksytysti esimerkiksi jonkun toiminnallisen mahdollisuuden saavuttamiseksi (riski on myös mahdollisuus)
- riskin aiheuttajalähteen poistaminen tai korjaaminen
- riskin todennäköisyyden muuttaminen riskienhallinnan keinoin
- riskin vaikutusten muuttaminen riskienhallinnan keinoin
- riskin jakaminen toisen osapuolen kanssa tai siirtäminen vakuutuksella
- riskin hyväksyminen

Yhteen riskiin voi kohdentua yksi tai useampi käsittelytoimenpide. Toimenpiteiden tulee olla oikeassa suhteessa riskin suuruuteen nähden ja ne tulee toteuttaa oikealla organisaatiotasolla ja tehtävissä yrityksessä. Merkittävimmät riskit ja niiden riskienhallintatoimenpiteet tulee viedä asianmukaiseksi suunnitelmaksi ja sen seuranta tulee varmistaa. Riskienhallintasuunnitelman seuranta- ja katselmointivaihe ovat tärkeä osa riskienhallintaprosessia, jolla varmistetaan tehdyn suunnitelman loppuun vieminen ja katselmoidaan aika ajoin, miten yritys on onnistunut riskienhallinnassa toimintaympäristössään ja mitä uusia tai muuttuneita riskejä ja niiden hallinnan keinoja, sekä muutostarpeita voi yrityksellä olla edessään. Riskienhallinta on yrityksessä jatkuva prosessi ja osana yrityksen päivittäistä johtamista sen eri tasoilla ja tilanteissa niin lyhyen kuin pitkän aikavälin näkökulmasta tarkasteltuna. Riskienhallintaan sisältyy myös toimiva ja tavoittava viestintä yrityksen sisällä ja sen toimintaympäristössä eri osapuolten välillä, joiden tulee olla niistä tietoisia. Riskienhallinnan viestintään sisältyvät kaikki oleelliset riskit ja käsittelytoimet.

5.4.3 Vaikutusten arviointi ja ennakkokuuleminen

Riskiperusteisen lähestymistavan ja tietosuoja-asetuksessa säädetyn osoitusvelvollisuusvaatimuksen mukaisesti rekisterinpitäjän pitää etukäteen arvioida ja dokumentoida, millaiset riskit henkilötietojen käsittelystä rekisteröidyille eli ihmisille aiheutuu. Tapauksissa, joissa ihmisten oikeuksiin tai vapauksiin kohdistuu korkea riski, rekisterinpitäjän on todetun riskin ja erityisen todennäköisyyden ja vakavuuden arvioimiseksi käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitusten sekä riskin alkuperä huomioon ottaen tehtävä ennen henkilötietojen käsittelyä tietosuojaa koskeva vaikutusten arviointi. Vaikutusten arvioinnissa on erityisesti tarkasteltava suunniteltuja toimenpiteitä, sekä suojatoimenpiteitä ja mekanismeja, joiden avulla vähennetään riskiä ja varmistetaan rekisteröityjen henkilötietojen suoja ja osoitetaan selkeästi, että tietosuoja-asetusta on noudatettu.

Rekisterinpitäjän pitää siis tehdä vaikutustenarviointi, jos henkilötietojen käsittely sen luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen todennäköisesti aiheuttaa rekisteröityjen ihmisten oikeuksien kannalta korkean riskin. Käytännössä tietosuoja-asetuksen säädös velvoittaa kaikkia rekisterinpitäjiä vähintään arvioimaan, onko vaikutustenarviointi tehtävä. Vaikutustenarviointi vaaditaan erityisesti seuraavissa tilanteissa:

- ihmisten henkilökohtaisia ominaisuuksia arvioidaan automaattisen käsittelyn keinoin ja käsittely johtaa päätöksiin, joilla on ihmisiä koskevia oikeusvaikutuksia tai muita merkittäviä vaikutuksia
- suoritetaan laajamittaista käsittelyä, joka kohdistuu erityisiin henkilötietoryhmiin eli arkaluontoisiin tietoihin tai rikostuomioita tai rikkomuksia koskeviin tietoihin
- järjestelmällinen ja laajamittainen yleisölle avoimen alueen valvonta

Vaikutustenarvioinnin toteuttamisesta vastaa aina rekisterinpitäjä, vaikka sen toteutuksesta huolehtisikin jokin muu taho. Myös henkilötietojen käsittelijän tulee avustaa rekisterinpitäjää vaikutustenarvioinnin tekemisessä pyydettäessä muun muassa antamalla kaikki tarvittavat tiedot tämän tekemistä varten. Tietosuojatyöryhmä on lausunut (WP248) vaikutusten arvioinnin tekemisestä turvallisuuspalveluja ja erityisesti toimeksiantajia koskevasti seuraavalla tavalla ”yleisölle avoimen alueen järjestelmällinen valvonta laajamittaisesti” ja ” rikoksentekijöiden tietoja säilyttävä yksityisetsivä” edellyttävät vaikutusten arvioinnin tekemistä. Mielestäni tuhansia asiakkaita valvova hälytys- ja palvelukeskustoiminta olisi myös pitänyt mainita tietosuojatyöryhmän lausunnossa. Vaikutusten arvioinnin on tietosuoja-asetuksen mukaan sisällettävä vähintään seuraavat asiat:

- järjestelmällinen kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista mukaan lukien tarvittaessa rekisterinpitäjän oikeutetut edut
- arvio käsittelytoimien tarpeellisuudesta ja oikeasuhtaisuudesta tarkoituksiin nähden
- arvio niistä rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä, joiden takia vaikutustenarviointi täytyy tehdä
- suunnitellut toimenpiteet riskeihin puuttumiseksi, mukaan lukien suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan, että tietosuoja-asetusta on noudatettu ottaen huomioon rekisteröityjen ja muiden asianomaisten oikeudet ja oikeutetut edut

Vaikutustenarviointi on keskeinen arviointityökalu henkilötietojen käsittelyyn liittyvässä riskienhallinnassa. Arvioinnin tulos on huomioitava määriteltäessä asianmukaisia toimenpiteitä sen osoittamiseksi, että yrityksen henkilötietojen käsittely on tietosuoja-asetuksen mukaista. Aina ei kuitenkaan onnistuta saamaan riskejä pienennettyä riittävän matalalle tasolle kohtuullisin toimenpitein saatavilla oleva tekniikka ja näiden kustannukset huomioon ottaen. Mikäli rekisterinpitäjä ei kykene toteuttamaan riittäviä toimenpiteitä riskien pienentämiseksi on ennen henkilötietojen käsittelyn aloittamista kuultava valvontaviranomaista eli Suomessa tietosuojavaltuutettua. Ennakkokuulemista varten on rekisterinpitäjän toimitettava valvontaviranomaiselle seuraavat tiedot:

- rekisterinpitäjän ja mahdollisten henkilötietojen käsittelijöiden vastuualueet
- kysymyksessä olevan suunnitellun käsittelyn tarkoitus ja keinot
- tehdyt toimenpiteet ja toteutetut suojatoimet
- tietosuojavastaavan yhteystiedot (jos yrityksellä sellainen on)
- vaikutustenarviointi ja muut pyydetyt tiedot

Valvontaviranomaisen on vastattava kuulemispyyntöön määräajassa. Mikäli valvontaviranomainen katsoo, että suunniteltu henkilötietojen käsittely rikkoo tietosuoja-asetusta, erityisesti jos rekisterinpitäjä ei ole riittävästi tunnistanut tai pienentänyt riskiä, valvontaviranomaisen on annettava kirjalliset ohjeet rekisterinpitäjälle tai henkilötietojen käsittelijälle asian korjaamiseksi. Lisäksi valvontaviranomainen voi käyttää tietosuoja-asetuksen mukaisia valtuuksiaan, kuten antamaan lisätietoja, saada pääsy kaikkiin henkilötietoihin, määrätä rekisterinpitäjä tai henkilötietojen käsittelijä saattamaan käsittelytoimet tietosuoja-asetuksen säädösten mukaisiksi sekä asettaa väliaikainen tai pysyvä rajoitus tai kielto henkilötietojen käsittelylle.

5.4.4 Käsittelyn turvallisuus, tekniset ja organisatoriset toimenpiteet

Yrityksen on tietosuoja-asetuksen mukaisesti toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla varmistetaan henkilötietojen asianmukainen turvallisuustaso ottaen huomioon uusin tekniikka ja toteuttamiskustannukset suhteessa tietojenkäsittelyn riskeihin ja suojeltavien henkilötietojen luonteeseen. Henkilötietojen suojaamisesta on huolehdittava käsittelyn kaikissa vaiheissa alkaen aina tietojen keräämisestä ja päättyen niiden tuhoamiseen. Käsittelyyn liittyvät riskit ja henkilötietojen laatu vaikuttavat suojauksen toteutustapaan. Yrityksen tulee tarvittaessa jopa salata ja pseudonymisoida tiedot.

Tietoturva pitää sisällään tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistamisen teknisin ja organisatorisin toimenpitein. Yrityksen tietoturvatoimia ovat esimerkiksi:

- henkilöstön kouluttaminen tietoturva- ja tietosuoja asioissa
- henkilöstölle annetut ohjeet ja määräykset
- tietojen luokittelu ja niiden käsittelyohjeet
- salassapitositoumukset
- tietojen salauskeinot ja salatun sähköpostin käyttö
- tilojen, laitteiden ja ohjelmistojen tilan-, kulun- ja käytönvalvonta
- työasemien-, palvelinten- ja tietoverkon tietoturva, sekä sovellusten turvallisuus
- tietojen sekä järjestelmien suojaaminen viruksilta ja haittaohjelmilta
- tietojen ja järjestelmien ylläpitotoimet, sekä tietojen varmuuskopiointi
- järjestelmien ja ohjelmistojen käyttöoikeuksien määrittely
- käyttäjien todentaminen käyttäjätunnuksin ja turvallisin salasanoin
- tietojen ja järjestelmien luvattoman käytön esto
- käsittelytapahtumien kirjaaminen / lokitiedot
- tietoliikenteen valvonta
- käytännesääntöjen ja sertifikaattien käyttöönotto
- varautuminen tietoturvariskeihin ja palautumissuunnitelmat

Yrityksen tulee säännöllisesti testata, tutkia ja arvioida tehtyjen toimenpiteiden tehokkuutta. Yrityksen pitää varmistaa, että työntekijät, joilla on pääsy henkilötietoihin, käsittelevät niitä ainoastaan ja vain rekisterinpitäjän antamien ohjeiden mukaisesti. Rekisterinpitäjän tulee luoda sisäinen menettely tietoturvatason säännöllistä selvittämistä varten sekä laatia yrityksen sisäinen toimintaohje henkilötietojen turvallisesta käsittelystä.

5.4.5 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tapahtuvaa loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai luvaton pääsy tietoihin. Yrityksen tietoturvan tavoitteiden näkökulmasta katsottuna tietoturvaloukkaus voi olla:

- henkilötietoihin kohdistuva luottamuksellisuuden loukkaus
- henkilötietoihin kohdistuva eheyden loukkaus
- henkilötietoihin kohdistuva saatavuuden eli käytettävyyden loukkaus

Henkilötietoihin kohdistuneen tietoturvaloukkauksen seurauksena on se, että rekisterinpitäjä ei enää pysty vastaamaan rekisteröidyille siitä, että se noudattaisi tietosuoja-asetuksen edellyttämiä henkilötietojen käsittelyn periaatteita. Tietosuoja-asetus lähtee siitä, että jos tietoturvaloukkaukseen ei puututa ja tehdä toimenpiteitä riittävän nopeasti ja tehokkaasti, siitä voi aiheutua rekisteröidyille huomattavia vahinkoja, maineriskejä tai taloudellisia menetyksiä. Myös rekisterinpitäjän maine voi kärsiä tietoturvaloukkauksesta ja yritykselle voi koitua tästä liiketaloudellisia menetyksiä puhumattakaan tietosuoja-asetuksen mahdollistamasta hallinnollisesta sakosta.

Mikäli henkilötietojen tietoturvaloukkaus on tapahtunut, tulee rekisterinpitäjän tehdä asiasta ilmoitus valvontaviranomaiselle, paitsi jos loukkaus ei todennäköisesti aiheuta riskiä rekisteröityjen, eli luonnollisten henkilöiden oikeuksille ja vapauksille. Punninta tässä asiassa jää rekisterinpitäjälle itselleen, mutta päätös tulee pystyä osoitusvelvollisuuden vuoksi todentamaan dokumentoidusti tarvittaessa jälkikäteen. Ilmoituksen henkilötietojen tietoturvaloukkauksesta voi tehdä tietosuojavaltuutetun toimiston verkkosivuilla. Ilmoituksen tulee tehdä aina rekisterinpitäjä, vaikka tieto ja havainto tulisi henkilötietojen käsittelijältä. Henkilötietojen käsittelijän on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä. Rekisterinpitäjän on tehtävä ilmoitus henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta. Mikäli ilmoitusta ei tehdä 72 tunnin kuluessa, rekisterinpitäjän on toimitettava valvontaviranomaiselle hyvin perusteltu selvitys viivästymisen syistä. Tämä ei kuitenkaan poista ilmoituksen tekovelvollisuutta ilman aiheetonta viivytystä. Viivytykseen tulee siis olla perusteltavissa oleva syy, kuten loukkauksen luonne ja haittavaikutukset rekisterinpitäjälle.

Parempi on tehdä ilmoitus määräajassa ja antaa siinä aikataulussa saatavat ilmoitustiedot.

Valvontaviranomaiselle tehtävässä henkilötietojen tietoturvaloukkauksessa rekisterinpitäjän tulee ainakin:

- kuvata henkilötietojen tietoturvaloukkaus sekä antaa tiedot loukkauksen kohteena olevista rekisteröityjen ryhmistä ja henkilötietoryhmistä sekä näiden lukumääristä mahdollisuuksien mukaan
- ilmoittaa tietosuojavastaavan yhteystiedot tai muu yhteystaho lisätietojen saamiseksi
- kuvata todennäköiset seuraukset tapahtuneessa henkilötietojen tietoturvaloukkauksesta
- ilmoittaa ja kuvattava ne toimenpiteet, jotka rekisterinpitäjä on toteuttanut tai joita se on ehdottanut tehtäväksi mahdollisten haittavaikutusten pienentämiseksi

Ilmoitus henkilötietojen tietoturvaloukkauksesta on annettava siis ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa loukkauksen ilmitulosta, mutta mikäli rekisterinpitäjä ei saa kaikkia tietoja toimitetuksi 72 tunnin määräajassa, tiedot voidaan toimittaa osissa ensimmäisestä ilmoituksesta, kuitenkin ilman aiheetonta viivytystä.

Tietoturvaloukkauksissa ilmoitusvelvollisuus rajoittuu vain henkilötietoja sisältäviin ja koskeviin tietoturvaloukkauksiin. Tietoturvaloukkauksen tietojärjestelmän kohde ja sen tietosisältö sekä loukkauksen vaikutukset rekisteröidyille ratkaisevat ilmoitusvelvollisuuden tietosuoja-asetuksen perusteella. Rekisterinpitäjän on kuitenkin dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset mukaan luettuna näihin liittyvät seikat osoitusvelvollisuuden vuoksi, tehtiin ilmoitus valvontaviranomaiselle tai ei. Valvontaviranomaisen on pystyttävä dokumentoinnista todentamaan, noudatettiinko tietosuoja-asetusta. Dokumentaation tulee siksi sisältää ainakin rekisterinpitäjän tiedot tietoturvaloukkauksesta, sen vaikutusten arvioinnista sekä rekisterinpitäjän tekemistä toimenpiteistä.

Rekisterinpitäjä on velvollinen ilmoittamaan henkilötietojen tietoturvaloukkauksesta suoraan myös rekisteröidyille henkilöille, jos loukkaus todennäköisesti aiheuttaa korkean riskin ihmisten oikeuksille ja vapauksille. Ilmoitus on tehtävä ilman aiheetonta viivytystä, mutta tietosuoja-asetuksessa ei ole määriteltyä tuntiperusteista aikarajaa. Rekisterinpitäjän tulee lähtökohtaisesti tehdä ilmoitus suoraan rekisteröidylle itselleen, mutta jos ilmoituksen tekeminen aiheuttaisi kohtuutonta vaivaa rekisterinpitäjälle, ilmoitus voidaan

tehdä perustellusti julkisella ilmoituksella tai muulla vastaavan kaltaisella tehokkaalla tavalla. Henkilötietojen tietoturvaloukkauksen Ilmoituksessa rekisteröidyille tulee ainakin:

- kuvata selkeän yksinkertaisesti henkilötietojen tietoturvaloukkauksen luonne
- ilmoittaa tietosuojavastaan yhteystiedot tai muu yhteystaho lisätietojen saamiseksi
- kuvata todennäköiset seuraukset tapahtuneessa henkilötietojen tietoturvaloukkauksessa
- ilmoittaa ja kuvattava ne toimenpiteet, jotka rekisterinpitäjä on toteuttanut tai joita se on ehdottanut tehtäväksi mahdollisten haittavaikutusten pienentämiseksi

Edellä mainittua ilmoitusta rekisteröidyille ei vaadita tehtäväksi, jos rekisterinpitäjä on toteuttanut sellaiset asianmukaiset tekniset ja organisatoriset suojatoimenpiteet, jonka johdosta tietoja ei voi ulkopuolinen käyttää (esimerkiksi salausta tai vahvaa suojausta) tai se on tehnyt nopeita korjaavia jatkotoimenpiteitä, joilla on varmistettu, ettei vastaavaa korkeaa riskiä rekisteröityjen oikeuksille tai vapauksille enää todennäköisesti tapahdu.

Tietoturvaloukkauksiin reagoimisessa vaaditaan yritykseltä nopeutta ja määrätietoista selkeää ennalta mietittyä ja harjoiteltua toimintaprosessia, sekä työkaluja. Ilmoituksen sisältö tulee olla yksityiskohtainen, oli kyseessä sitten henkilötietojen tietoturvaloukkauksen ilmoitus valvontaviranomaiselle tai rekisteröidyille. Tiedot tulee saada ja antaa nopeasti ja se edellyttää yritykseltä kyvykkyyttä tietoturvaloukkausten havaitsemiseen ja yksityiskohtaiseen todentamiseen, jotta yritys pystyy arvioimaan henkilötietojen tietoturvaloukkauksen todennäköisiä seurauksia rekisteröidyille ja yritykselle itselleen. Hyvin ja riittävin yksityiskohdin tehty riskienarviointi ja vaikutusten arviointi auttavat tässä asiassa.

Kun yrityksessä arvioidaan henkilötietojen tietoturvaloukkaukseen liittyviä riskejä otetaan riskienarvioinnissa huomioon tietoturvaloukkauksesta riskin todennäköisyys ja sen mahdollisesta toteutumisesta arvioitu seuraus. Tietoturvaloukkaukseen liittyy sitä suurempi riski, mitä vakavampi seuraus on yksilön kannalta ja mitä todennäköisemmin tunnistettu riski toteutuu. Tietoturvaloukkauksen seurausten voidaan katsoa olevan erityisen vakavia esimerkiksi silloin, kun seurauksena voi olla henkilön identiteettivarkaus, petos, lavastaminen, julkinen nöyryytys, maineen menetys ja terveyteen vaikuttavaa psyykkistä ahdistusta. Mitä arkaluonteisempaan henkilötietoon tietoturvaloukkaus kohdistuu, sitä suuremmat henkilökohtaiset seuraukset se aiheuttaa loukkauksen kohteena olevalle henkilölle. Merkityksellistä on aina myös se kenen haltuun tiedot päätyvät; väärinkäytöksen todennäköisyys on suurempi jos tiedetään, että tiedot ovat päätyneet rikollisille.

5.4.6 Tietosuojavastaava

Tietosuoja-asetuksessa edellytetään rekisterinpitäjän ja henkilötietojen käsittelijän nimittävän tietosuojavastaavan kun:

- henkilötietojen käsittelyä suorittaa jokin muu julkishallinnon viranomainen tai elin kuin tuomioistuin
- yrityksen ydintehtävät muodostuvat henkilötietojen käsittelytoimista jotka luonteensa, laajuutensa ja/tai tarkoituksensa vuoksi edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa
- yrityksen ydintehtävät muodostuvat laajamittaisesta henkilötietojen käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin, eli arkaluontoisiin henkilötietoihin tai rikostuomioihin ja rikkomuksiin liittyviin henkilötietoihin

Konserniyritys tai viranomainen voivat nimittää yhden ainoan tietosuojavastaavan edellyttäen, että tietosuojavastaavaan voidaan ottaa helposti yhteyttä jokaisesta toimipaikasta ja tehtävän hoitaminen on organisaation rakenne ja koko huomioiden mahdollista. Tietosuojavastaavan henkilövalinnassa ja nimeämisessä on otettava huomioon henkilön ammattipätevyys ja erityisesti asiantuntemus tietosuojalainsäädännöstä ja toimialan käytänteistä sekä henkilön kyvystä ja valmiuksista suoriutua tietosuojavastaavan tehtävistä. Yrityksen on ilmoitettava tietosuojavastaavansa yhteystiedot valvontaviranomaiselle.

Tietosuojavastaava voi olla rekisterinpitäjän tai henkilötietojen käsittelijän palkkalistoilla oleva työntekijä tai tietosuojavastaava voi hoitaa tehtäväänsä toimeksiannosta palvelusopimukseen perustuen. Tietosuojavastaavalla on valvova, konsultoiva ja yhteistyötä koordinoiva rooli yrityksessä sen varmistamisessa, että tietosuojasääntelyä noudatetaan organisaation toiminnassa. Tietosuoja-asetuksen mukaan tietosuojavastaavan tehtävät ovat:

- antaa yritykselle ja sen henkilötietoja käsittelevälle henkilöstölle tietoja ja neuvoja tietosuojasäännösten mukaisista velvollisuuksista
- seurata ja valvoa, että tietosuoja-asetusta sekä kansallisia tietosuojalainsäädöksiä noudatetaan yrityksessä ja yritysten välisissä käsittelyn vastuujaoissa
- henkilötietoja käsittelevien henkilöiden kouluttaminen tietosuoja-asioissa
- suorittaa tarkastuksia henkilötietojen käsittelyyn liittyvissä toiminnoissa
- antaa pyydettäessä konsultaatiota tietosuojaa koskevasta vaikutustenarvioinnista sekä seurata ja valvoa sen toteuttamista tietosuoja-asetuksen mukaisesti

- toimia proaktiivisesti tietosuoja-asioissa yrityksessä ja tehdä yhteistyötä valvontaviranomaisen kanssa
- toimia valvontaviranomaisen yhteyspisteenä henkilötietojen käsittelyyn liittyvissä asioissa ja kysymyksissä
- toimia yhteyskanavana rekisteröidylle siten, että he voivat ottaa yhteyttä asioissa, jotka liittyvät heidän henkilötietojensa käsittelyyn ja heidän oikeuksiinsa
- huomioitava tehtäviä suorittaessaan henkilötietojen käsittelyyn liittyvät riskit ottaen samalla ja yhtä lailla huomioon käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset

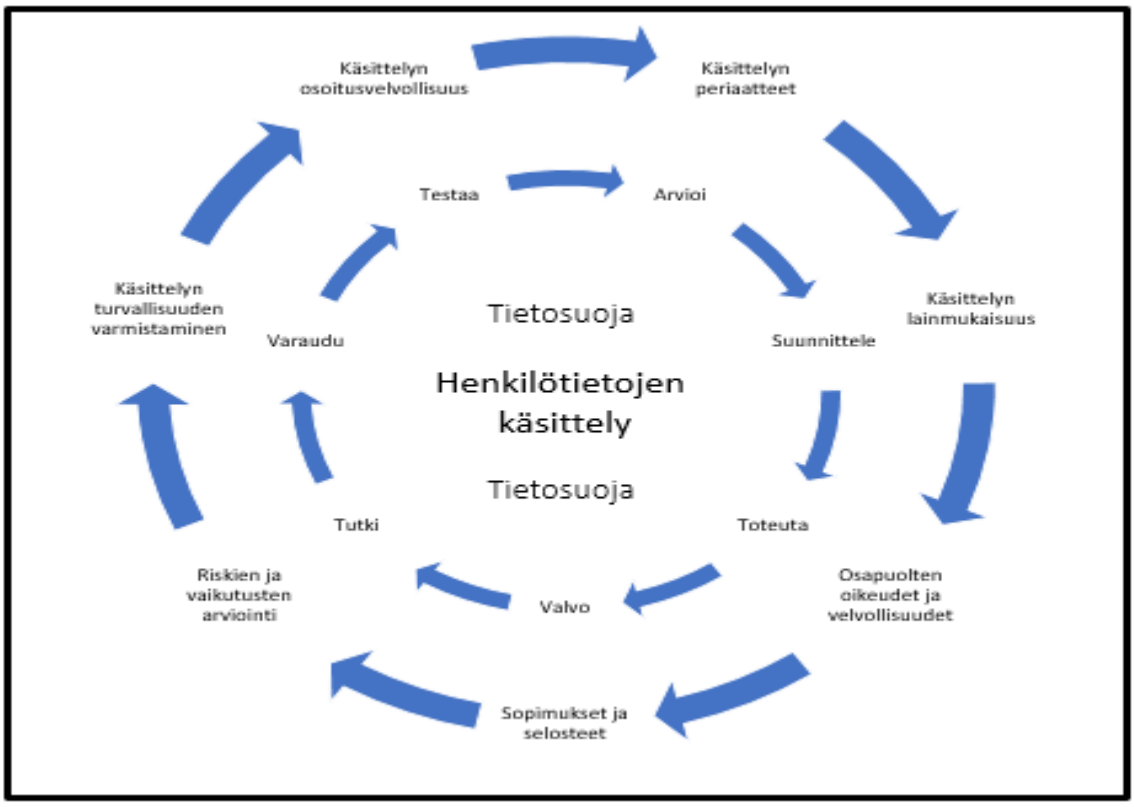
Tietosuojavastaava voi tehdä yrityksessä muitakin tehtäviä. Keskeistä on riippumattomuus, eli tietosuojavastaava ei voi olla samaan aikaan tehtävässä, jossa päätetään henkilötietojen käsittelyn tarkoituksista ja keinoista yrityksessä. Tämä riippumattomuusvelvoite rajaa monta toimenkuvaa pois tietosuojavastaavan muista mahdollisista rooleista yrityksessä. Tietosuojavastaava ei päätä henkilötietojen käsittelyn tarkoituksista ja keinoista yrityksessä vaan se tehtävä on rekisterinpitäjän edustajan. Tietosuojavastaavan rooli on konsultoiva, eräänlainen yrityksen johdon keskustelukumppani tietosuoja asioissa. Rekisterinpitäjän ja henkilötietojen käsittelijän onkin otettava tietosuojavastaava asianmukaisesti sisään työtehtäviensä hoitoon ja tuettava tätä työtehtävässään antamalla resurssit, pääsy henkilötietoihin ja käsittelytoimiin sekä mahdollistettava henkilökohtaisen asiantuntemuksen ylläpito lisäkoulutuksella. Tietosuojavastaava raportoi tehtävästään suoraan ylimmälle johdolle, eikä hän saa ottaa yrityksen sisältä keneltäkään vastaan ohjeita tehtäviensä hoitamiseen. Tietosuojavastaava on parhaimmillaan monissa henkilötietojen käsittelyyn ja sen turvallisuuteen liittyvissä toimissa ja päätöksissä mukana, sekä tekemässä erilaisia sopimuksia, selosteita tai riski- ja vaikutusten arviointeja, mutta tietosuojavastaava ei ole vastuussa henkilötietojen käsittelyn lainmukaisuudesta yrityksessä, vaan näistä vastuussa on rekisterinpitäjä ja henkilötietojen käsittelijä. Tietosuojavastaavaa sitoo salassapitovelvollisuus kaikkien työtehtäviensä hoitamisessa.

Tietosuojatyöryhmä (WP243) on lausunut, että yksityisen turvallisuusalan yritys, joka vastaa useiden yksityisten kauppakeskusten ja julkisten tilojen valvonnasta tulee nimittää tietosuojavastaava. Valvonta on näin yrityksen ydintehtävä ja tähän ydintehtävään liittyy erottamattomasti henkilötietojen käsittely. Näin yksityisen turvallisuusalan yrityksen, joka suorittaa vartiointi- ja järjestyksenvalvojatoimintaa edellä kuvatusti tulee nimittää tietosuojavastaava. Yritys voi rekrytoida tai nimittää tietosuojavastaavan omasta henkilöstöstä tai ostaa sen palveluna yksityiseltä lakitoimistolta tai konsultointiyritykseltä.

6 LOPUKSI

Tutkimuksen yleisenä tavoitteena oli konkretisoida kirjallisesti EU:n tietosuoja-asetuksen ja tietosuojalain keskeiset säädökset turvallisuuspalveluyrityksen näkökulmasta. Toimeksiantajan asettama opinnäytetyötavoite oli selvittää ja dokumentoida EU:n tietosuoja-asetuksen ja tietosuojalain keskeiset säädökset ja käsittelytoimet selkeäksi ja hyödynnettäväksi käsikirjaksi. Teoriatiedon hankkiminen perustui pääasiassa tietosuoja-asetuksen, tietosuojalain ja EU:n tietosuojatyöryhmän lausuntojen lukemiseen ja tutkimiseen, sekä joidenkin tietosuojasta kirjoitettujen kirjallisten tuotosten lukemiseen. Tutkimuksessa hyödynnettiin empiiristä tietoa ja osaamista. Tietosuojasäädöksiä ja käsittelytoimia arvioitiin ja pohdittiin työ- ja yrityselämässä suuressa sekä pienessä yrityksessä.

Tuloksena syntyi tavoitteen mukainen tietosuoja-asetuksen ja tietosuojalain keskeiset säädökset ja käsittelytoimet sisältävä ja avaava käsikirjamainen opinnäytetyö. Opinnäytetyötä voi hyödyntää henkilötietoja käsittelevien henkilöiden koulutuksessa ja tietosuojaoppaana toimialan yrittäjille. Alla oleva kuva 5 ilmentää keskeisimmät asiat tehdystä.



Kuva 5. Henkilötietojen turvallisen käsittelyn keskeiset säädökset ja käsittelytoimet.

Kuva 5 ilmaisee keskeisimmät asiat käsitellystä aiheesta. Aiheena tietosuoja eli henkilötietojen käsittely. Ensimmäinen jatkuva prosessi kuvaa tietosuoja-asetuksen yhtä keskeisintä periaatetta eli riskiperusteista ja turvallisen käsittelyn periaatetta ja vaatimusta. Toinen jatkuva prosessi kuvaa henkilötietojen käsittelyn keskeisimmät säädökset ja käsittelytoimet. Työ vastaa tutkimuskysymykseen, miten huomioida tietosuojaan liittyvät oikeudet ja velvollisuudet tietosuoja-asetuksen ja tietosuojalain säädösten mukaisesti. Tätä opinnäytetyötä voisi jatkaa keskittymällä vain riskien ja vaikutusten arviointityöhön.

EU:n yleinen tietosuoja-asetus annettiin 27.4.2016 ja se tuli voimaan EU:ssa 25.5.2018. Siirtymäaikaa säädöksien velvoitteisiin oli annettu yrityksille noin kaksi vuotta. EU:n tietosuoja-asetuksen edellyttämien velvoitteiden tulkintaan ja vaadittavien dokumenttien tekemiseen ei ole tullut selkeitä ja riittävän tietoperustan kattavia oppaita tai ohjeita yrityksille. Tietosuojavaltuutetun toimiston verkkosivut ovat kehittyneet sisällöltään 2019-2020. EK ja Suomen Yrittäjät ovat antaneet tietosuojasta ohjeistuksia yrityksille yleisluontoisesti. Käytännössä moni asia EU:n tietosuoja-asetuksen voimaantulon jälkeen on odottanut valvontaviranomaisen toimia ja mahdollisia seuraamusmaksuja tietosuojavaatimusten rikkomuksista ja sitä kautta näyttöä valvonnan olemassaolosta ja sen toimivuudesta. Suomessa tietosuojavaltuutetun toimiston seuraamuskollegio määräsi ensimmäiset kolme seuraamusmaksua tietosuojarikkomuksista 18.5.2020. Kaikki kolme seuraamusmaksua tulivat niin sanotusti perustavanlaatuisista rikkomuksista. Seuraamusmaksut olivat yrityksen koosta riippuen 12.500 – 100.000 euroa. Seuraamusmaksut eli hallinnolliset sanktiot annettiin rikkomuksista ”oikeus vastustaa henkilötietojen käsittelyä”, ”vaikutusten arvioinnin tekemisen jättäminen sijaintitiedon käsittelyssä” ja ” yritys keräsi työnhakijoiden ja työntekijöiden henkilötietoja tarpeettomasti”. Tämän opinnäytetyön aikaan päätökset eivät ole vielä lainvoimaisia, koska seuraamuskollegion päätöksistä voi valittaa hallinto-oikeuteen. Kaikki tapaukset on informoitu tietosuojavaltuutetun sivustolla. Seuraamuskollegiolta on tulossa uusia seuraamusmaksuja yrityksille ja ne tulevat ohjaamaan ja terävöittämään yritysten tietosuojatoimintaa jatkossa kaikissa yrityksissä.

Turvallisuusalan elinkeinolupia oli poliisin 9.4.2020 päivätyn rekisterin mukaan 842 kpl. Yhteinen lainsäädäntö yhdistää yrityksiä, mutta yrityksien taloudellisten ja toiminnallisten resurssien, toimintojen, prosessien, käytänteiden, käytettävissä olevien tietojärjestelmien ja ohjelmistojen sekä digitaalisen toiminta- ja palvelualustan osalta on suuria eroja. Yksityisten turvallisuuspalveluiden kannalta katsoisin, että jokainen yritys kiinnittäisi huomiota turvallisen ja riskilähtöisen käsittelyperiaatteen mukaisesti seuraaviin perustavan laatuisiin asioihin, yksityiskohtiin ja kehityskysymyksiin:

- toteuttaa tietosuojaan liittyvä koulutus henkilötietoja käsitteleville henkilöille esimerkiksi tämän opinnäytetyön sisältämän asiankäsittelyn laajuudessa
- laatia henkilöstölle henkilötietojen käsittelyn ohjeet ja yrityksen tietoturvaohjeet
- täyttää osoitusvelvollisuuteen liittyvät käsittelytoimenpiteet säädösten mukaisesti
- varmistaa yrityksen ja sen palvelujen tietoturva teknisin ja organisatorisin keinoin
- siirtyä käyttämään suojattuja ja toiminnallisesti hyväksi todettuja digitaalisia palvelualustoja sekä ohjelmistoja tarkoituksena esimerkiksi vähentää perinteistä paperista tiedonkäsittelyä ja tietojen välittämistä käsittelyn osapuolten välillä
- tapahtumailmoituksen ja rikosilmoituksen laadinnassa sekä näiden tietojen raportointi- ja ilmoitusviestinnässä tiedot tulisi suojata käyttämällä mahdollisuuksien mukaan digitaalisia palvelualustoja tai ohjelmistoja sekä näin minimoida perinteinen paperinen tiedonkäsittely
- huomioitava erityisesti arkaluontoisten tallenteiden ja raporttien säilyttäminen
- mahdollistaa salatun / suojatun sähköpostin käyttö henkilötietoja sisältävissä sähköposteissa
- huomioitava turvasuojaustietojen ja valvonnan toimenpideohjeiden viestinnän turvallisuus esimerkiksi asennus – hälytyskeskus – toimeksiantaja välillä
- varmistua turvasuojauksessa turvallisista salasanoista ja koodeista sekä laitteistojen käytön tietoturvan sekä tietosuojan suojauskäytännöistä ja koulutuksesta
- suorittaa suurissa hälytys- ja palvelukeskuksissa vaikutusten arviointi
- toteuttaa turvalliset toimitilat ja palveluliiketoiminnan infrastruktuuri
- käyttää hallinnon ohjelmistoissa nykyaikaisia ja turvallisia SaaS-ohjelmistoja
- varmistaa että digitaalisten lukitusjärjestelmien, teknisen turvasuojauksen, hälytys- ja palvelukeskustoiminnan ja turvallisuuspalvelujen integraatiot ja näiden palveluratkaisut käyttäjille tulisi aina arvioida niihin sisältyvien riskien osalta sekä myös mahdollisuuksien osalta toiminnan, tietoturvan ja tietosuojan näkökulmasta
- huomioida oletusarvoisesti tietosuoja kehitettäessä uusia palveluratkaisuja
- yksityisten turvallisuuspalveluiden toimialajärjestöt voisivat harkita vakiosopimuslausekkeiden ja käytännesääntöjen laatimista alan tietosuojan kehittämiseksi

Yksityinen turvallisuusala on digitaalisessa murroksessa. Muutos luo uusia mahdollisuuksia, mutta myös uusia haasteita. Tietosuojan näkökulmasta digitalisaatio ennemmin parantaa henkilötietojen suojaa kuin heikentää sitä, kunhan käsittelyn turvallisuudesta huolehditaan asianmukaisesti alkaen heti jo tuotteiden ja palvelujen suunnittelemisesta. Tietosuojan varmistaminen yrityksen toiminnassa on jatkuva ja kaikkia koskeva prosessi.

LÄHTEET

Aalto-Setälä, M. & Viitaila, M. 2019. Tietosuoja pähkinänkuoressa. Tietosuojaopas yrityksille. Helsinki: Keskuskauppakamari. Saatavilla Keskuskauppakamarin www sivuilta.

EU:n tietosuojatyöryhmä WP29 lausunnot. Saatavilla https://tietosuoja.fi/euroopan-tietosuojaneuvoston-ohjeet.

EU:n yleinen tietosuoja-asetus (GDBR). Euroopan parlamentin ja neuvoston asetus (EU) 2016/679. Annettu 27 päivänä huhtikuuta 2016. Saatavilla https://eur-lex.europa.eu/legal-content/FI/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504.

Finnsecurity Ry:n julkaisut. Finnsecurity turvallisuutta osaavalla yhteistyöllä, yleisesite. Yksityisten turvallisuuspalveluiden toimialalla työskentelevien lukumäärä. Saatavilla https://finnsecurity.fi.

ICC Cyber security quide for business. 2015. International Chamber of Commerce (ICC). Tietoturvaopas yrityksille. 2016. Keskuskauppakamari. Saatavilla Keskuskauppakamarin www sivuilta.

Kilpailu- ja kuluttajavirasto, KKV / lähde - yksityisten turvallisuuspalveluiden liikevaihto suomessa. Saatavilla https://www.kkv.fi/globalassets/kkv-suomi/ratkaisut-aloitteet-lausunnot/ratkaisut/kilpailuasiat/2018/yk---ehdolliset/r-2018-10-0121.pdf.

Korpisaari, P.; Pitkänen, O & Lehtinen-Warma, E. 2018. Uusi Tietosuoja Lainsäädäntö. Helsinki: Alma Talent Oy ja tekijät yhteistyössä Lakimiesliiton Kustannus.

Laki yksityisistä turvallisuuspalveluista 21.8.2015/1085. Annettu Helsingissä 21.8.2015. Saatavilla https://www.finlex.fi/fi/laki/ajantasa/2015/20151085.

Laki yksityisyyden suojasta työelämässä 13.8.2004/759. Annettu Helsingissä 13.8.2004. Saatavilla https://www.finlex.fi/fi/laki/ajantasa/2004/20040759.

Poliisi. Poliisin päivittämä ajantasainen luettelo turvallisuusalan elinkeinoluvan haltijoista (opinnäytetyössä päivämäärällä 9.4.2020 (pdf-taulukko). Saatavilla https://www.poliisi.fi/luvat/yksityinen_turvallisuusala/luettelo_turvallisuusalan_elinkeinoluvan_haltijoista.

Rikosasioiden tietosuojadirektiivi. Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016. Saatavilla https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32016L0680.

Rikosasioiden tietosuojalaki. Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 1054/2018. Annettu Helsingissä 5 päivänä joulukuuta 2018. Saatavilla https://www.finlex.fi/fi/laki/alkup/2018/20181054.

Teknologiainfo Teknova Oy IT2018YSE ja Taloushallintoliitto TAL2018 sopimusehdot – maininta.

Tietosuojalainsäädäntö 2019. 2019. Suomen laki. Tietosuojalainsäädännön erillispainoskirja. Helsinki: Alma Talent Oy.

Tietosuojalaki 5.12.2018/1050. Annettu Helsingissä 5.12.2018. Saatavilla https://www.finlex.fi/fi/laki/ajantasa/2018/20181050.

Tietosuojavaltuutetun toimiston www-sivut. Tietosuoja. Saatavilla https://tietosuoja.fi.

Tilastokeskus / PAM - palvelualojen taskutilasto 2019 / työskentelevien vartijoiden lukumäärä

VAHTI-ohjeet. Ohje riskienhallintaan. Valtiovarainministeriön julkaisu 22/2017. Saatavilla https://www.vahtiohje.fi – sisältää SFS-ISO 31000 riskienhallintaprosessin kuvaus kuvan sekä riskimatriisin ja riskisuunnitelman käyttö riskienhallinnassa taulukkokuvan.