TAMPEREEN
AMMATTIKORKEAKOULU

EU:n yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi (DPIA)

Riskit ja niiden vaikutukset luonnollisen henkilön oikeuksiin ja vapauksiin

Paula Himanka

Opinnäytetyö
Toukokuu 2018
Liiketalouden koulutusohjelma
Oikeudellinen asiantuntijuus

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Liiketalouden koulutusohjelma
Oikeudellinen asiantuntijuus

HIMANKA PAULA:
EU:n yleisen tietosuoja-asetuksen mukainen vaikutustenarviointi
Riskit ja niiden vaikutukset luonnollisen henkilön oikeuksiin ja vapauksiin

Opinnäytetyö 97 sivua, joista liitteitä 12 sivua
Toukokuu 2018

EU:n yleistä tietosuoja-asetusta sovelletaan 25.5.2018 alkaen kaikissa EU-maissa. Tietosuoja-asetus korvaa tämänhetkisen henkilötietojen käsittelyä koskevan lainsäädännön kansallista liikkumavaraa lukuun ottamatta. Vielä hallituksen esityksenä oleva kansallinen tietosuojalaki tulee Suomessa vastaamaan yleislakina tähän tarpeeseen.

Kun henkilötietojen käsittely todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin, on rekisterinpitäjän toteutettava tietosuojaa koskeva vaikutustenarviointi eli arvioitava henkilötietojen käsittelyn vaikutukset henkilötietojen suojalle. Arvioinnissa tulee myös puuttua havaittuihin riskeihin toteuttamalla riittävät suojakeinot riskien pienentämiseksi tai poistamiseksi. Tämän lisäksi tietosuoja-asetuksessa on omaksuttu yleinen riskiperusteinen lähestymistapa; tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet tulee suhteuttaa henkilötietojen käsittelystä aiheutuvaan riskiin. Riskiperusteinen lähestymistapa ohjaa rekisterinpitäjiä kokonaisvaltaiseen tietosuojariskien huomiointiin ja tukee osoitusvelvollisuuden toteuttamista.

Opinnäytetyö on tulkintalainopillinen tutkielma, jonka empiirisessä osassa käytettiin laadullisena menetelmänä avoimia haastatteluja. Työn tavoitteena oli perehtyä vaikutustenarviointiin liittyvään sääntelyyn ja ohjaukseen sekä tunnistaa henkilötietojen käsittelyyn liittyviä riskejä ja niiden vaikutuksia luonnollisen henkilön oikeuksiin ja vapauksiin. Työn tarkoituksena oli laatia selkeä ja ymmärrettävä kooste sääntelyn perusteista ja ajanmukaisesta tulkintaohjeistuksesta. Työn oheismateriaalina tuotettiin toimeksiantajan käyttöön ohje vaikutustenarviointien laatimiseksi sekä tietosuojan riski- ja vaikutusanalyysi yleisimmistä riskeistä. Opinnäytetyö sisältyy toimeksiantajan laajempaan prosessiin tietosuoja-asetuksen velvoitteiden implementoimiseksi tämän hallintoon.

Vaikutustenarvioinnin sääntely on uutta. Se antaa raamit, mutta jättää rekisterinpitäjälle laajasti tulkinnanvaraa vaikutustenarviointien käytännön toteuttamisesta. Myös kansallinen lainsäädäntö ja ohjaus ovat vielä keskeneräiset. Yhdessä oikeuskäytännön kanssa ne määrittelevät aikanaan vaikutustenarvioinnin sääntelyn tarkemman tulkinnan. Uudet teknologiat, käytännesäännöt, menetelmät ja toimijoiden väliset yhteistyömuodot tarjoavat monenlaisia lähestymistapoja vaikutustenarviointien tutkimiseen jatkossa.

Asiasanat: GDPR, EU:n yleinen tietosuoja-asetus, DPIA, vaikutustenarviointi

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Administration
Legal Expertise

PAULA HIMANKA:
The Data Protection Impact Assessment (DPIA) in EU's General Data Protection Regulation
Risks and impacts to the rights and freedoms of a data subject

Bachelor's thesis 97 pages, appendices 12 pages
May 2018

The General Data Protection Regulation (GDPR) applies from 25 May 2018 in all EU countries. It replaces the current legislation on processing personal data, with the exception of national margins. In Finland, national Data Protection Act will respond to this need.

Where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the data controller or the data processor should carry out a data protection impact assessment (DPIA) to evaluate the risk. A DPIA must be a genuine risk assessment, which allows data controllers not only to identify, but also to take measures to address the risks. The risk-based approach embodied by the GDPR guides the data controllers to relate the obligations of the GDPR and appropriate safeguards to the risk of processing personal data. The risk-based approach will guide the data controllers to take full account of the data protection risks and support them demonstrating compliance (accountability).

The aim of this thesis was to orient on the regulation and guidance available on DPIAs and to identify the risks related to the processing of personal data and their impacts on the rights and freedoms of natural persons. The purpose of the thesis was to produce a comprehensible summary of the regulation and the latest interpretation guidelines of DPIA. As an appendix to the thesis, the commissioner was provided with a DPIA summary and a simple risk and impact analysis exemplifying the most common risk factors and their impacts on a data subject. The appendices are not to be published. The thesis with the complementary material is part of the commissioner's process of implementing the obligations of the data protection regulation in their administration.

National legislation and guidance or best practices for carrying out DPIAs are not yet available. The regulation offers the framework, but leaves the data controller in charge of the implementation. The national general law with the guidance of the supervisory authority and the case law will determine a more precise interpretation of the regulation in due course. New technologies, codes of conduct, methods and forms of cooperation between actors will provide a wide range of approaches in studying data protection impact assessments in the future.

Key words: GDPR, general data protection regulation, DPIA, data protection impact assessment

SISÄLLYS

LYHENTEET JA TERMIT

anonymisointi	henkilötiedon tunnistettavuuden poistaminen niin, ettei tietoa voi (tai ei voi enää) yhdistää luonnolliseen henkilöön; tällöin EU:n yleinen tietosuoja-asetus ei tule sovellettavaksi
avoin data	julkishallinnolle, organisaatiolle tai yksityiselle kertynyt tieto, jota avataan vapaasti ja maksutta kaikille hyödynnettäväksi; tätä varten datasisällön tulee olla tarkasti kuvattu
DPIA	Data Protection Impact Assessment eli vaikutustenarviointi; tulee tehdä, mikäli henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin luonnollisen henkilön oikeuksille ja vapauksille
erityiset henkilötietoryhmät	aik. arkaluonteiset tiedot; henkilötietojen käsittely, josta ilmenee esim. rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus, seksuaalinen suuntaus tai ammattiliiton jäsenyys; uusina tietoina geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten
GDPR	General Data Protection Regulation; EU:n yleinen tietosuoja-asetus (EU) 2016/679
henkilötieto	tieto, josta luonnollinen henkilö voidaan suoraan tai epäsuorasti tunnistaa; esimerkiksi nimi, henkilötunnus, sijainti- tai verkkotunnistetieto taikka yksi tai useampi henkilölle tunnusomainen fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurillinen tai sosiaalinen tekijä
henkilötietojen käsittelijä, data processor	luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun
henkilötietojen käsittely	toiminto tai toiminnot, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin automaattista tietojenkäsittelyä käyttäen tai manuaalisesti; tietojen kerääminen, tallentaminen, muokkaaminen ja muuttaminen, mutta myös

	haku, kysely, säilyttäminen ja käyttö sekä tietojen luovuttaminen siirtämällä, levittämällä tai asettamalla ne muutoin saataville sekä tietojen yhteensovittaminen tai yhdistäminen, rajoittaminen, poistaminen tai tuhoaminen
henkilötietojen suoja, protection of personal data	
	perustuu luonnollisten henkilöiden suojeluun, perusoikeuksiin ja vapauksiin; ”henkilötietojen oikeaoppinen käsittely”, sisältää myös yksityisyyden suojan (katso myös tietoturva)
IoT	Internet of Things, esineiden internet; muodostuu verkkoon liitettävistä kodinkoneista ja laitteista
kansallinen liikkumavara	direktiivinomainen, tietosuoja-asetuksessa myönnetty mahdollisuus säätää kansallisesti tietosuoja-asetuksen tietyistä kohdista tarkentavasti tai jopa poiketen; esimerkiksi nuoren henkilön ikäraja tai hallinnollisten sakkojen käyttöönotto julkisella sektorilla
lokit, lokittaminen	tietojärjestelmässä, verkossa tai muussa ympäristössä tapahtuvan tiedon dokumentointi; merkintöjen kerääminen automaattisesti tai manuaalisesti tietojärjestelmässä tapahtuneiden lisäysten, muutosten tai pelkän katselun todentamiseksi; käytännössä ainoa mahdollisuus jälkikäteiseen valvontaan
profilointi	henkilötietoja automaattisesti käsittelemällä 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	henkilötietojen käsitteleminen niin, että henkilötietoja ei voida enää suoraan yhdistää luonnolliseen henkilöön käyttämättä lisätietoja - tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu - kuitenkin peruutettavissa oleva toiminto

rekisteri, filing system	jäsennelty henkilötietoja sisältävä tietojoukko, josta tiedot ovat saatavilla tietyin perustein; keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu - looginen rekisteri tarkoittaa samaan käyttötarkoitukseen kerättyjä tietoja
rekisterinpitäjä, data controller	luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; taho, jonka tosiasiallista käyttötarkoitusta varten henkilötietoja kerätään
rekisteröity, data subject	tunnistettu tai tunnistettavissa oleva luonnollinen henkilö, jonka henkilötietoja käsitellään
suostumus	vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla henkilö hyväksyy tietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen
TATTI-työryhmä	oikeusministeriön asettama kansallinen EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmä, jonka tehtävänä oli valmistella lainsäädäntöehdotus mm. kansallisesta liikkumavarasta ja uudesta tietosuojalaista
tietotilinpäätös	organisaation laatima (vapaaehtoinen) raportti sen tietojenkäsittelyn nykytilasta; toimii johdon työkaluna ja osoitusvelvollisuuden toteuttamisen välineenä
tietoturva	eli tietoturvallisuus; tiedon saatavuuden, luotettavuuden ja eheyden takaaminen erilaisin teknisin ja organisatorisin keinoin (katso myös henkilötietojen suoja)
turvakielto	maistraatin myöntämä tietojen luovutusrajoitus, joka perustuu hakijan perusteltuun syyhyn epäillä oman tai perheensä turvallisuuden olevan uhattuna; tällöin henkilön yhteystietoja ei saa luovuttaa useissa tapauksissa viranomaisellekaan
vuosikello	dokumentti, jossa kuvataan tietosuojaorganisaation säännölliset ja määrämuotoiset tehtävät niiden toteuttamisen ja seurannan mahdollistamiseksi; esimerkiksi järjestelmähankkeet ja muutokset, luonnollisilta henkilöiltä ja valvontaviranomaisilta tulleet yhteydenotot, merkittävien tietoturvatapahtumien käsittely, vaikutustenarvioinnit

WP29	Working Party 29; tietosuojaviranomaisista koostuva tietosuojatyöryhmä, jossa on yksi edustaja kustakin EU-maasta ja joka laatii ja julkaisee lisäohjeita tietosuoja-asetuksen tulkitsemiseksi ja noudattamiseksi

1 JOHDANTO

1.1 Opinnäytetyön tausta ja toimeksiantaja

Uudenlaisten tekniikoiden, laitteiden sekä innovatiivisten sähköisten palvelujen ja valvonnan räjähdysmäinen kasvu, kehittyminen ja käyttöönotto ovat arkipäivää. Samaan aikaan kun digikulttuurin myötä asenteemme tietojen luovuttamiseen ja jakamiseen on muuttunut jatkuvasti avoimempaan suuntaan, henkilötiedoista on tullut tärkeää pääomaa ja kauppatavaraa. Luovutamme henkilötietojamme laajasti sekä työ- ja vapaa-ajan, että esimerkiksi julkishallinnon palvelujen käyttöä, omaa asianhoitoamme ja rekisterinpitäjän toimintoja varten. Henkilötietomme toimivat paitsi myyntiartikkeleina ja markkinoinnin lähdemateriaalina, myös profiloinnin kohteena sekä tausta-aineistona suunniteltaessa, kehitettäessä ja tehostettaessa nykyisiä ja uusia tuotteita ja palveluita.

Tietojamme kerätään, jatkojalostetaan, luovutetaan ja siirretään eteenpäin yhä enemmän sekä kansallisesti että rajat ylittäen. Henkilötietojen käsittelyn kansainvälinen sääntely ja soveltaminen ovat kuitenkin olleet hajanaista ja epäyhtenäistä.[1] Informaatiotekniikan nopea kehittyminen, kulttuurillinen muutos ihmisten käyttäytymisessä ja sääntelyn yhdenmukaistamisen tarve ovat myös EU:n yleisen tietosuoja-asetuksen[2] (GDPR, (EU) 2016/679, jäljempänä tietosuoja-asetus) taustalla. Henkilötietojen käsittelyyn – mm. keräämiseen, hallintaan, profilointiin, poistoon tai tietojen luovuttamiseen ja siirtämiseen – tarvitaan nykypäivän teknologian ja kehityksen huomioivaa, ajanmukaista sääntelyä, johon nykyisessä lainsäädännössä ei ole voitu varautua. Tietosuojauudistuksen yhtenä tavoitteena onkin luoda ajanmukainen, yhtenäinen ja kattava tietosuojakehys Euroopan unionille.[3] Keskeisenä tavoitteena kuitenkin on, kuten myös tämänhetkisessä lainsäädännössä, luonnollisten henkilöiden suojelu henkilötietojen käsittelyssä.

Tietosuojaa koskevasta vaikutustenarvioinnista (DPIA, Data Protection Impact Assessment) säädetään tietosuoja-asetuksen 35 artiklassa. Vaikutustenarvioinnilla tarkoitetaan

---

[1] Oikeusministeriö 2017, 98.
[2] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).
[3] HE 9/2018 vp, 4.

ennen henkilötietojen käsittelyn aloittamista tehtävää arviointia suunniteltujen käsittelytoimien vaikutuksista luonnollisten henkilöiden oikeuksiin ja vapauksiin, kun henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin. Vaikutustenarviointia edellytetään erityisesti, kun henkilötietojen käsittelyn taustalla on uudenlaista teknologiaa, kun käsittely on laajamittaista ja erityisiin henkilötietoryhmiin perustuvaa tai kun käsittely perustuu luonnollisten henkilöiden henkilökohtaisten ominaisuuksien järjestelmälliseen ja kattavaan arviointiin. Vaikutustenarviointivelvoitteen ohella tietosuoja-asetuksessa on omaksuttu riskiperusteinen lähestymistapa, joka velvoittaa rekisterinpitäjän suhteuttamaan tekniset ja organisatoriset suojatoimet henkilötietojen käsittelystä aiheutuviin riskeihin.

Opinnäytetyön tilasi Tampereen kaupunki, jossa tietosuoja-asetuksen implementointi kaupunkikonsernin toimintoihin on projektoitu ja tietosuoja-asetukseen sekä tietosuojatyöhön on yleisesti perehdytty syvällisesti ja laajasti. Tietoa jaetaan aktiivisesti sekä kaupunkikonsernin sisällä että erilaisissa yhteistyöryhmissä esimerkiksi suurimpien kaupunkien ja it-palveluntoimittajien kesken. Toimeksiantajan toiminnoissa vaikutustenarviointiprosessin kehitys on osa laajempaa henkilörekisterihallinnon järjestämismallin[4] laatimista ja liittyy tietosuoja-asetuksen vaatimusten toimeenpanoon kaupunkikonsernissa.

Tätä kirjoitettaessa uudistuvaan lainsäädäntöön liittyvä tietosuojatyön organisointi ja toimeenpano organisaatioissa on pääsääntöisesti meneillään. Hyviä käytänteitä etsitään julkishallinnossa yhteistyöperusteisesti eri toimijoiden välillä kansallisen lainsäädännön, laajemman ohjauksen ja oikeuskäytännön vielä puuttuessa. Ajan myötä uudistunut sääntely ja ohjaus toivottavasti täsmentyvät ja vakiintuvat, ja tietosuojan huomioimisesta käsittelytoiminnoissa tulee organisaation omia prosesseja tukeva ja tehostava, luonnollinen osa rekisterinpitäjän toimintaa.

[4] Tampereen kaupunki 2018. Henkilörekisterihallinnon järjestämismalli on kokonaisuus, johon kuuluu konsernitasoisia ohjeita ja prosesseja tietosuojalainsäädännön, erityisesti tietosuoja-asetuksen, implementoimiseksi Tampereen kaupunkikonsernin hallinnossa.

1.2 Työn tutkimusmetodit, tarkoitus ja rakenne

Opinnäytetyön tavoitteena on perehtyä tietosuoja-asetuksen mukaiseen vaikutustenarviointiin ja riskiperusteiseen lähestymistapaan liittyvään sääntelyyn ja ohjaukseen sekä tunnistaa henkilötietojen käsittelyyn liittyviä riskejä ja niiden vaikutuksia luonnollisen henkilön oikeuksiin ja vapauksiin. Tarkoituksena on luoda tämänhetkiseen tietoon perustuva, selkeä ja ymmärrettävä kooste, johon on koottu lainsäädäntöperusteen lisäksi tulkintaa ja esimerkkejä riskeistä ja niiden vaikutuksista. Työn lähestymistapa vaikutustenarviointiin on riskilähtöinen, mutta siinä pyritään antamaan katsaus myös vaikutustenarviointiin kokonaisuutena ja prosessina.

Opinnäytetyön oheismateriaalina tuotetaan toimeksiantajalle ohje vaikutustenarvioinnin laatimisen perusteista sekä tietosuojan riski- ja vaikutusanalyysi, johon kootaan esimerkinomaisesti valmiiksi yleisimpiä ajankohtaisia riskitekijöitä ja niiden vaikutuksia organisaatiolle ja luonnolliselle henkilölle. Tuotokset ovat organisaation sisäisiä materiaaleja, jotka tukevat palvelualueille tarjottavia koulutuksia ja työpajoja, joissa vaikutustenarviointeja laaditaan. Ohjeistuksen ja Excel-pohjan tarkoituksena on auttaa kaupunkikonsernin palvelualueita havaitsemaan vaikutustenarvioinnin tarve henkilötietojen käsittelyssä sekä arvioimaan yksityiskohtaisempia, palvelualueen erityispiirteisiin liittyviä riskitekijöitä, niiden toteutumistodennäköisyyttä, vakavuutta ja vaikutuksia. Kehittämällä laaja ”riskipankki” ja jalkauttamalla oikeaoppisen henkilötietojen käsittelyn ajatusmallia koko henkilöstön tasolle työntekijät oppivat huomioimaan tietoturvaan ja tietosuojaan liittyviä hyvä käytänteitä, tunnistamaan riskitekijöitä omassa työssään ja rohkaistuvat tuomaan niitä aktiivisesti esille, jolloin riskeihin voidaan puuttua pohtimalla keinoja niiden pienentämiseksi tai poistamiseksi. Opinnäytetyö oheismateriaaleineen sisältyy siten laajempaan vaikutustenarviointiprosessin kehittämiseen ja tavoitteeseen edistää tietoturva- ja tietosuojariskien havaitsemista ja hallintaa kaikilla toiminnan tasoilla. Näin toimeksiantaja vastaa myös tietosuoja-asetuksen edellytykseen riskiperusteisen lähestymistavan huomioimisesta henkilötietojen käsittelyssä. Ajan myötä vaikutustenarviointiprosessi liittyy luonnolliseksi osaksi kaupungin laajempaa, jatkuvaa riskienhallintaprosessia.

Tietosuoja-asetuksen artiklat johdanto-osineen muodostavat tärkeimmän viitekehyksen tietosuoja-asetuksen ja vaikutustenarvioinnin perusteisiin ja sisältöön. Luonnollisen henkilön oikeuksille ja vapauksille aiheutuvaa korkeaa riskiä on peilattu myös perustuslain (PL, 731/1999) säännöksiin. Vaikka asetuksen johdanto-osilla ei ole juridisesti sitovaa

oikeusvaikutusta, niillä on kuitenkin oikeudellisia vaikutuksia artiklojen keskeisten säännösten tai määräysten perusteluissa ja näiden tulkinnassa.[5] Lisäksi merkittävänä ”soft law”-oikeuslähteenä[6] on käytetty WP29-tietosuojatyöryhmän antamia lausuntoja ja ohjeita (guidelines). Kansallisen lainsäädännön vielä puuttuessa lähteenä on käytetty myös tietosuojavaltuutetun toimiston linjauksia siltä osin kun niitä on saatavilla, sekä julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) ja julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) tietosuojan yhteishankkeiden luentoja ja luentomateriaaleja.[7] Kirjallisina lähteinä toimivat kotimaiset henkilötietojen käsittelyyn sekä tietoturvaan ja tietosuojaan liittyvät, ajanmukaiset teokset ja vaikutustenarviointiin liittyvät ulkomaiset julkaisut ja artikkelit. Toiminnallista, konstruktiivista, otetta työhön ovat tuoneet avoimet asiantuntijahaastattelut, jotka ovat olleet erinomainen ja tarpeellinen lisä asetustekstin ja WP29- ohjeistuksen tulkinnassa sekä mahdollisimman ajanmukaisen tiedon keräämisessä työhön. Palvelualueiden kanssa tehty yhteistyö on selkiyttänyt tietosuoja-asetuksen soveltamisen ohjeistus- ja koulutustarpeita.

Lainopin tehtävinä on perinteisesti ollut tulkinta ja systematisointi, ja sen tarkoituksena on selvittää voimassaolevien oikeusnormien sisältöä. Tulkintalainoppiin eli käytännölliseen lainoppiin sisältyy oikeusperiaatteiden punninta ja tasapainottaminen.[8] Opinnäytetyössä tulkitaan tietosuoja-asetuksen sääntelyä, ja sen tarkoituksena on hahmottaa lainsäädännön vaatimukset vaikutustenarvioinnin laatimiseen käytännössä. Laadullisia menetelmiä käytetään yleensä silloin, kun tarkoituksena on hankkia suppeasta kohteesta paljon tietoa ja ymmärtää aihetta paremmin ja kokonaisvaltaisemmin. Haastattelu on perinteinen kvalitatiivinen menetelmä.[9] Opinnäytetyö on siis tulkintalainopillinen tutkielma, jonka empiirisessä osassa on käytetty laadullisena menetelmänä avoimia haastatteluja.

Suomessa on poikkeuksellisen laaja henkilötietojen käsittelyä sisältävä erityislainsäädäntö. Palvelualakohtaisen erityislainsäädännön lisäksi henkilötietojen käsittelyssä julkishallintosektorilla tulee erityisesti huomioida myös julkisuuslakiin (JulkisuusL, 621/1999) perustuva julkisuusperiaate osana hyvän hallinnon takeita sekä tietoturvallisuusasetuksen (621/2010) mukaiset tietojen luokitteluperusteet. Työn rajallinen pituus asettaa haasteita erityislainsäädännön huomioimiseen edes pintapuolisesti, joten se on

[5] Euroopan unionin neuvosto 2002, 82 – 83.
[6] Raitio 2016, 206.
[7] Valtiovarainministeriö 2018a.
[8] Hirvonen 2011, 22, 24 – 25.
[9] Ojasalo, Moilanen & Ritalahti 2014, 105.

muutamia huomioita lukuun ottamatta rajattu työn ulkopuolelle. Myös kansallinen tietosuojalainsäädäntö (tietosuojalaki, HE 9/2018 vp) on pääsääntöisesti rajattu työn ulkopuolelle, koska hallituksen esitystä ei vielä tätä kirjoitettaessa ole hyväksytty laiksi.

Vaikutustenarvioinnin hahmottaminen ja riskien kartoittaminen edellyttävät tietosuoja-asetuksen periaatteiden, tavoitteiden ja määritelmien ymmärtämistä, jonka vuoksi tärkeimmät periaatteet sekä muutokset ja tarkennukset nykylainsäädäntöön esitellään lyhyesti pääluvussa 2. Samalla annetaan esimerkkejä riskien vaikutuksista luonnollisen henkilön oikeuksille ja vapauksille tietosuoja-asetuksen periaatteisiin ja laajemmin perusoikeuksiin peilaten. Riskiperusteinen lähestymistapa on koko tietosuoja-asetuksen läpileikkaava teema, jonka sisäistämisessä auttaa yleinen riskienhallinnan osaaminen: tietoturva- ja tietosuojariskien tunnistaminen, luokittelu ja niiden lieventämistoimenpiteiden määrittely. Riskejä ja niiden vaikutuksia käsitellään läpi työn, ja vaikutustenarviointiin perehdytään erityisesti pääluvussa 3, jossa pohditaan myös korkean riskin vaikutuksia luonnolliselle henkilölle WP29-tietosuojatyöryhmän antamien esimerkkien pohjalta.

Tietosuoja-asetuksen suomenkielinen käännös ei kaikilta osin ole täysin onnistunut, ja saattaa aiheuttaa epäselvyyttä sääntelyn tulkinnassa. Näiltä osin ensimmäisellä käsittelykerralla termin yhteyteen on lisätty sulkuihin myös asiaa paremmin kuvaava englanninkielinen termi, vaikka pääsääntöisesti työssä käytetäänkin luettavuussyistä suomenkielisiä käännöksiä. Tietosuoja-asetusta kannattaa tulkita myös muun kieliseen, esimerkiksi englanninkieliseen versioon perustuen.

1.3 Tietosuojan suhde tietoturvaan ja tietojen julkisuusperiaate

Yksityisyyden suoja on perusoikeus, joka rakentuu kahdesta osa-alueesta: henkilötietojen suojasta ja tietoturvasta.[10] Yksityisyyden suojan turvaavia toimenpiteitä ovat esimerkiksi henkilötietojen luottamuksellisuuden säilyttäminen ja valtuudettoman tiedon saannin estäminen sekä henkilötietojen suojaaminen valtuudettomalta tai henkilöä vahingoittavalta käytöltä.[11] Tietosuojalla on perinteisesti tarkoitettu henkilötietojen käsittelyä sääntelevän lainsäädännön huomioimista sekä luonnollisten henkilöiden yksityisyyden suojan ja oikeusturvan varmistamista. Tietosuojan tarkoitus ei ole itse tiedon suojaaminen sinänsä,

[10] Neuvonen 2014.
[11] Valtioneuvosto 2008, 105.

vaan ennemminkin hyvien henkilötietojen käsittelyperiaatteiden soveltaminen.[12] Tietosuojan avulla varmistetaan henkilötietojen oikea, tarkoituksen- ja vaatimustenmukainen käyttö; voidaankin puhua henkilötietojen oikeaoppisesta käsittelystä.[13]

Tietoturva käsittää tekniset ja hallinnolliset toimenpiteet, joilla pyritään turvaamaan luonnollisen henkilön yksityiselämä, edut, oikeudet ja vapaudet sekä tiedon luottamuksellisuus, eheys ja saatavuus ja ehkäisemään näihin liittyviä loukkauksia. Tietoturvatyö tähtää toiminnalle tärkeiden tietojärjestelmien ja -verkkojen häiriöttömyyteen, niiden keskeytymättömään toimintaan, valtuudettoman käytön ja tahattoman tai tahallisen tiedon tuhoutumisen tai vääristymisen estämiseen sekä mahdollisten vahinkojen minimointiin. Tietoturvan keinoin pyritään siis toteuttamaan tietosuojaa[14], esimerkiksi palomuurien, virustorjuntaohjelmistojen, tietojen salauksen sekä henkilöstön ohjeistuksen ja koulutuksen avulla.

Julkishallinnon toiminnassa on tärkeää ymmärtää monipuolisesti hallinnon julkisuuteen ja tietojen salassapitoon ja luokitteluun liittyviä lainsäädäntöperusteita sekä hahmottaa näiden suhde henkilötietojen käsittelyyn liittyvään tietosuojaan.[15] Viranomaisen toiminnan lähtökohtana on julkisuus: toiminnan on oltava avointa ja siitä tulee saada tietoja. Julkisuusperiaate toteutuu käsittelyn julkisuutena, asiakirjajulkisuutena ja tiedottamisena, ja sen vastinparina toimii salassapito. Asiakirja on pidettävä salassa, mikäli laissa on näin säädetty, viranomainen on määrännyt asian salassa pidettäväksi tai jos se sisältää asioita, joista on lailla säädetty vaitiolovelvollisuus. Salassapitovelvollisuus koostuu asiakirjasalaisuudesta ja vaitiolovelvollisuudesta, joka taas tarkoittaa velvollisuutta olla ilmaisematta asiaa, joka on salassa pidettävä.[16] Julkisuuslain 23.3 § mukaisesti vaitiolovelvollisuuteen liittyy myös hyväksikäyttökielto; vaitiolovelvollisuuden piiriin liittyviä tietoja ei saa käyttää omaksi tai toisen hyödyksi tai toisen vahingoksi. Sillä, ettei tieto ole salainen tai että molempia osapuolia sitoo vaitiolovelvollisuus, ei voi perustella henkilötietojen käsittelyä tai ohittaa tietosuojan huomioimista työtehtävissä. Salassa pidettävien tietojen käsittelyyn tulee aina olla myös käsittelijän työrooliin perustuva oikeutus.[17]

[12] Andreasson, Riikonen & Ylipartanen 2017, 20.
[13] Järvinen & Rousku 2017, 18.
[14] Andreasson ym. 2017, 20 – 21.
[15] Andreasson 2017.
[16] Kulla & Koillinen 2014, 4, 66, 68.
[17] Andreasson 2017.

Tietosuoja-asetuksen siirtymäajan puitteissa (24.5.2016 – 24.5.2018) rekisterinpitäjän (data controller) tai henkilötietojen käsittelijän (data processor) vastuulla on ollut selvittää muuttuvan sääntelyn vaikutukset toimintaansa. Tietosuoja-asetus asettaa tietojen suojaamiselle osin henkilötietolakia tarkempia ja yksityiskohtaisempia velvoitteita. Lisäksi tietosuoja-asetuksen yleinen riskiperusteinen lähestymistapa edellyttää riskien ja niiden vaikutusten jatkuvaa käsittelyä; niiden tunnistamista, analysointia ja arviointia sekä riskien pienentämiskeinojen määrittelyä. Vaikutustenarviointi on yksi osa riskienhallintaa.

1.4 Kansallisen tietosuojalainsäädännön nykytila

EU:n henkilötietodirektiivi, jossa säädetään yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, pantiin Suomessa täytäntöön henkilötietolailla (HeTiL, 523/1999). Yleislakina vielä kevään 2018 ajan toimivassa henkilötietolaissa säädetään mm. henkilötietojen käsittelyn yleisistä periaatteista, käsittelytarkoituksista, arkaluonteisten tietojen käsittelystä, tietojen siirrosta sekä rekisteröidyn oikeuksista ja rekisterinpitäjän velvollisuuksista.

Henkilötietolain lisäksi merkittävimpiä kansallisia säädöksiä ovat yksityiselämän suojan takaava perustuslaki (PL, 731/1999), työelämän tietosuojalakina toimiva laki yksityisyyden suojasta työelämässä (YksTL, 759/2004), sähköistä viestintää sääntelevä laki sähköisen viestinnän palveluista (tietoyhteiskuntakaari, 917/2014) sekä kuntasektorilla vaikuttavat kuntalaki (KL, 410/2015), hallintolaki (HL, 434/2003) sekä julkisuuslaki. Lisäksi eri palvelualoilla sovelletaan laajasti alakohtaisia erityislakeja, esimerkiksi sosiaali- ja terveyshuoltoon liittyvien tietojen käsittelyä sääntelevät mm. terveydenhuoltolaki (TervHL, 326/2010), laki sosiaalihuollon asiakkaan asemasta ja oikeuksista (sosiaalihuollon asiakaslaki, 812/2000), laki potilaan asemasta ja oikeuksista (potilaslaki, 785/1992) sekä laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (SähkAsL, 159/2007).

Henkilötietojen käsittelyä koskevien säädösten määrä Suomessa on kansainvälisesti vertailtunakin poikkeuksellisen suuri. Oikeusministeriön helmikuussa 2016 asettama EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmä (TATTI) lausui loppumietinnössään, että Tietosuojasäädösten muutostarve-hankkeessa käytiin läpi lähes 800 säädöstä,

joiden säännösten suhdetta arvioitiin tietosuoja-asetuksen henkilötietojen käsittelyperusteisiin.[18] Lainsäädännön pirstaleisuus voi aiheuttaa epätietoisuutta yksityisyyttä ja julkisuutta koskevan sääntelyn keskinäisistä suhteista sekä hankaloittaa tietosuojalainsäädännön sisällöllistä osaamista ja oikeaa soveltamista.[19]

Henkilötietolain noudattamista ohjaavat ja valvovat tietosuojaviranomaiset eli tietosuojavaltuutettu ja -lautakunta. Tietosuojavaltuutettu antaa suosituksia ja määräyksiä ja voi tarvittaessa asettaa uhkasakon tehostaakseen päätöksensä noudattamista tai määrätä rekisteritoiminnan lopetettavaksi. Käytännössä tietosuojaviranomaisilla on ollut Suomessa lähinnä ohjaava rooli. Merkittävä haaste nykylainsäädännössä sen pirstaleisuuden lisäksi onkin henkilötietojen käsittelyn ohjauksen hajanaisuus sekä puuttuva järjestelmällinen valvonta ja sanktiointi, jonka vuoksi organisaatiot eivät ole välttämättä toteuttaneet henkilötietolain vaatimuksia toimintaprosesseissaan.[20]

Kansallinen lainsäädäntö on monin tavoin murroksessa.[21] TATTI-työryhmä ehdotti 21.6.2017 mietinnössään uutta tietosuojalakia, jolla kumottaisiin henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta sekä säädettäisiin tietosuoja-asetuksen salliman kansallisen liikkumavaran soveltamisesta.[22] Arviointineuvosto antoi 8.2.2018 lausunnon, jossa se katsoi, että hallituksen esitystä tulee korjata ennen sen antamista edelleen eduskunnan käsiteltäväksi.[23] Hallituksen esitys eduskunnalle annettiin 1.3.2018, ja lakimuutokset ehdotettiin tuleviksi voimaan 25.5.2018.[24] Käsittely on kuitenkin viivästynyt, eikä hallituksen esitystä tietosuojalaiksi ole vielä kesäkuun puolivälissä 2018 hyväksytty laiksi. Lainsäädäntömuutosten lisäksi julkishallinnon toimintaan vaikuttavat tällä hetkellä merkittävästi maakunta- ja SOTE-uudistus sekä julkisen toiminnan lisääntyvä yhtiöittäminen.

---

[18] Oikeusministeriö 2018, 27.
[19] Pitkänen, Tiilikka & Warma 2013, 4.
[20] Andreasson 2018.
[21] Valtioneuvosto 2018b. Tutustu muutoksiin: http://valtioneuvosto.fi/artikkeli/-/asset_publisher/vuoden-2018-alusta-voimaan-tulevia-muutoksia-ministerioiden-hallinnonaloilla.
[22] Oikeusministeriö 2017, 13.
[23] Oikeusministeriö 2018, 1.
[24] HE 9/2018 vp, 142.

1.5 Rekisterinpitäjän uhkamaisema

Tietosuoja-asetuksessa korostuu riskilähtöisyys. Henkilötietojen käsittelyyn liittyviä riskejä tulee arvioida paitsi vaikutustenarviointimenettelyssä, myös yleiseen riskiperusteiseen lähestymistapaan perustuen. Tämä edellyttää rekisterinpitäjiltä aiempaa laajempaa riskienhallinnan osaamista.

Riskienhallinnassa riskit on jaoteltu yleisesti organisaation sisäisiin ja ulkoisiin riskeihin tai tarkemmalla tasolla strategisiin, operatiivisiin, taloudellisiin ja vahinkoriskeihin.[25] Tietoturvariskejä voidaan tarkastella myös tiedon luottamuksellisuuden (tahaton tai luvaton tiedon vuotaminen tai pääsy tietoon), eheyden (tahaton tai luvaton tiedon muuttuminen tai muuttaminen) tai saatavuuden (tahaton tai luvaton tietojen saatavuuden estyminen tai tiedon menettäminen) kannalta.[26] Tässä työssä riskejä käsitellään lähtökohtaisesti tietosuoja-asetuksen periaatteiden tai korkean riskin kriteereiden näkökulmasta. Esitellyt riskit ovat yleisiä tietosuoja- ja tietoturvariskejä, jotka ovat merkityksellisiä myös tietosuoja-asetuksen toimeenpanon sekä vaikutustenarvioinnin kannalta.

Johdon tuki ja sitoutuminen tietosuoja-asetuksen toimeenpanossa on rekisterinpitäjän lainmukaisen toiminnan lähtökohta. Tietosuoja-asetuksen velvoitteet edellyttävät kokonaisvaltaista tietojenkäsittelytoimintojen läpikäyntiä ja tarkastelua sekä erilaisten toimintaa ohjaavien prosessien, ohjeiden ja koulutusten laatimista ja päivittämistä, joten riittävien resurssien mahdollistaminen on kriittisen tärkeää. Varsinkin julkishallinnossa ohjeet, määräykset ja politiikat tulisi määritellä korkealla tasolla, etenkin työnkuvauksiin ja tietojärjestelmien pääsynhallintaan ja käyttövaltuushallintaan liittyen. Selkeällä määrittelyllä ehkäistään toimiala- ja yksikkökohtaisten, usein ristiriitaistenkin käytänteiden muodostuminen ja selkiytetään toimintoja ja vastuita.[27]

Yleisiä tietosuoja-asetuksen noudattamiseen liittyviä haasteita ovat sen tulkinnanvaraisuus sekä kansallisen ohjauksen ja oikeuskäytännön puuttuminen. Nämä voivat johtaa siihen, ettei tietosuoja-asetuksen velvoitteita osata toteuttaa tarkoituksenmukaisella tavalla. Velvoitteet saatetaan jättää toteuttamatta odotellen tarkentuvia ohjeita tai mahdol-

[25] Valtiovarainministeriö 2017a, 22.
[26] Andreasson, Koivisto & Ylipartanen 2016, 18.
[27] Andreasson 2017.

lisia sanktioita, tai vaihtoehtoisesti saatetaan ottaa käyttöön velvoitteisiin nähden ylimitoitettuja toimintamalleja ja menetelmiä, joilla saattaa olla laajojakin taloudellisia tai vastuisiin liittyviä vaikutuksia. Myös lainsäädännön ristiriitaisuus voi olla riskitekijä, tietosuojavaltuutettu onkin julkaissut ohjeen myös lainsäädäntölausuntoihin.[28]

Vaikutustenarvioinnin kannalta on huomioitava erityisesti uudet teknologiat ja uusien teknisten tai organisatoristen ratkaisujen innovatiivinen käyttö tai soveltaminen. Korkeita riskejä luonnollisen henkilön oikeuksille ja vapauksille voivat aiheuttaa esimerkiksi sähköistyvät palvelut ja siirtyminen pilvipalveluiden käyttöön, IoT (Internet of Things, esineiden internet), vapaasti maksutta hyödynnettävä avoin data, henkilön omiin henkilötietoihin perustuva omadata (MyData) sekä laajat tietovarannot ja niihin liittyvä profilointi. Erilaisten mobiililaitteiden ja ulkoisten muistitikkujen havaitseminen ja hallinta organisaation sisäisessä verkossa on erityisen tärkeää tietoturvariskien kuten haittaohjelmien, tietomurtojen tai tietoturvaloukkausten ehkäisemiseksi. Viestintäviraston Kyberturvallisuuskeskus julkaisee vuosittain yleisimpiä tietoturvauhkia ja niiden ratkaisuja; vuonna 2017 yleisimmät uhkat olivat päivitysten laiminlyönti, kiristyshaittaohjelmat, huijausviestit ja tietojen kalastelu, ulkoistukset ja laitehankintojen hallinta sekä hyökkäyksillä uhkaaminen.[29]

Tietojärjestelmiin liittyviä riskejä ovat esimerkiksi niiden käyttökatkot, laiteviat, heikot suojaukset ja salaukset, puutteellinen käyttövaltuushallinta, puuttuvat lokikäytänteet, haasteet varmuuskopiointikäytänteissä tai elinkaaren loppuvaiheessa olevat tuotteet, joita ei ehkä ole enää mahdollisuutta tai tarkoituksenmukaista kehittää. Kun tietojärjestelmiin liittyvä käyttöoikeusprosessi määritellään selkeästi, tietojärjestelmien käyttö on hallittua. Roolipohjaiset käyttäjätunnukset mahdollistavat työtehtäviin perustuvan, asiallisen tietojärjestelmän käytön.[30]

Yksi suurimmista henkilötietojen käsittelyn riskeistä on rekisterinpitäjän tai henkilötietojen käsittelijäorganisaation henkilöstön puutteellinen tietosuojaosaaminen. Järjestelmiin tai toimintaprosesseihin liittyvä tietämättömyys, osaamattomuus, välinpitämättömyys tai piittaamattomuus saattavat johtaa tahattomasti tai tahallisesti asiattomaan käyttöön, tieto-

[28] Tietosuojavaltuutetun toimisto 2017d.
[29] Viestintävirasto 2018.
[30] Andreasson, Koivisto & Ylipartanen 2013, 46.

vuotoihin tai yksityiselämää loukkaavan tiedon levittämiseen liittyvien riskien kasvamiseen ja realisoitumiseen, jolloin kyseessä on tiedon luottamuksellisuuden loukkaus. Tästä ovat esimerkkeinä työvälineiden, kuten työasemien ja mobiililaitteiden, huolimaton säilyttäminen ja jättäminen lukitsematta tai valvomatta, heikot salasanakäytänteet, tietojen näyttäminen tai kertominen sivullisille tai jättäminen sivullisten saataville esimerkiksi muistitikkujen tai paperitulosteiden muodossa, tietojen julkaiseminen sosiaalisessa mediassa tai tietoturvapäivitysten laiminlyönti. Yleinen haaste on myös varjo-IT eli tietohallintoyksikön ohjeiden ja hankintaprosessin ohi tilatut tai käyttöönotetut järjestelmät tai työtavat, joiden käyttöönoton myötä tiedon hallinta ja integrointi vaikeutuu.[31] Henkilöstön tietosuojaosaamisen kasvattaminen edellyttää riittävää, selkeää ja yksiselitteistä, lainsäädännön ja toimialueen erityisvaatimukset huomioivaa ohjeistusta ja koulutusta. Henkilöstön tulee myös ymmärtää omat velvoitteensa työntekijänä. Rekisterinpitäjän olisikin hyvä pohtia, millaisista laiminlyönneistä mahdollisesti seuraa työoikeudellisia seuraamuksia tai toimenpiteitä, dokumentoida ne selkeästi ja viestiä niistä henkilöstölle.

Useimmin esillä ollut tiedon luottamuksellisuuteen liittyvä riski on henkilötietojen paljastuminen ulkopuolisille esimerkiksi tietomurron, salassapitorikkomuksen tai asiattoman käytön johdosta. Tällöin rekisterinpitäjään kohdistuvia riskivaikutuksia voivat olla tietovuodosta aiheutuvat taloudelliset seuraukset mm. itse tietovuotoon liittyvän selvitystyön sekä tietosuojaviranomaisen mahdollisesti määräämien hallinnollisten sakkojen, oikeudenkäynnistä johtuvien kulujen ja vahingonkorvausten osalta sekä mahdolliset rikosoikeudelliset seuraamukset. Taloudellisia sanktioitakin merkittävämpi on maineriski, joka voi johtaa laajoihin taloudellisiin ongelmiin[32]. Tietovuodon operatiivinen vaikutus rekisterinpitäjälle on tietosuoja-asetuksen 33 ja 34 artikloissa säädetty velvollisuus tietyissä tapauksissa ilmoittaa henkilötietojen tietoturvaloukkauksesta tietosuojaviranomaiselle ja rekisteröidylle (data subject). Vastuu tietojen vuotamisesta on rekisterinpitäjän, mutta tapahtumalla voi olla myös rekisterinpitäjän työntekijään kohdistuvia työ-, rikos- ja vahingonkorvausoikeudellisia vaikutuksia, jos taustalla on rikos ja tahallisuus.

Kun tieto on virheellinen, muuttunut, puutteellinen tai vanhentunut, on kyseessä tiedon eheyden loukkaus. Tieto voi muuttua esimerkiksi inhimillisen virheen tai sovelluksessa

---

[31] Ros, 2016. Lue lisää varjo-IT:stä: https://www.tivi.fi/Kumppaniblogit/salesforce/varjo-it-on-myrkkya-digitalisaatiolle-6602931.

[32] Ponemon 2017. Lue lisää tietovuodon kustannusvaikutuksista Ponemon-instituutin tutkimuksesta Cost of Data Breach Study, Global analysis: https://www.oasis-open.org/events/sites/oasis-open.org.events/files/Day2-Session4-Allor.pdf.

olevan virheen vuoksi; henkilöiden tietoihin voidaan tehdä vääriä kirjauksia tai tiedot ovat saattaneet vaihtua tai sekoittua. Tiedot voivat muuttua järjestelmävirheen vuoksi myös silloin, kun tietoa siirretään automaattisesti järjestelmästä toiseen tai eri järjestelmissä olevaa tietoa yhdistellään. Se voi johtaa rekisterinpitäjän toiminnassa virheelliseen toimintaan tai päätökseen, viiveisiin ja esimerkiksi määräaikojen ylitykseen. Näissä tilanteissa rekisterinpitäjälle voi koitua taloudellisia kustannuksia paitsi tietojärjestelmän palauttamisen ja kehittämisen osalta, myös tietosuoja-asetuksen velvoitteiden laiminlyönnistä johtuvina vahingonkorvauksina ja mahdollisina hallinnollisina sakkoina.[33]

Pahimmillaan pääsy tietoihin estyy kokonaan esimerkiksi verkkovian, tietojärjestelmään liittyvän häiriön tai käyttökatkon vuoksi tai tieto on voinut kadota tai tuhoutua pysyvästi, jolloin kyseessä on tiedon saatavuuden loukkaus. Jos järjestelmää ei saada syystä tai toisesta palautettua tai palauttaminen viivästyy, se aiheuttaa viivettä tai esteen päätösten teossa. Tieto on voitu tallentaa työaseman kovalevylle automaattisen varmuuskopioinnin ulottumattomiin, jolloin työaseman katoamisen tai särkymisen vuoksi tieto voi olla lopullisesti saavuttamattomissa. Myös nämä aiheuttavat rekisterinpitäjälle edellä mainittuja taloudellisia vaikutuksia, jonka lisäksi käyttöviive voi aiheuttaa tuottavuuden laskua hukattuina työtunteina.[34]

Vaikutustenarvioinnin laatimisen perusteena on rekisteröidyn oikeuksille ja vapauksille aiheutuva todennäköinen, korkea riski. Jotta riskejä voidaan tunnistaa ja käsitellä, on organisaatiossa tiedettävä, mitä ja minkä tyyppisiä (esim. erityisiin henkilötietoryhmiin kuuluvia, luottamuksellisia, salassa pidettäviä) henkilötietoja sen toiminnoissa käsitellään ja kuvattava henkilötietojen käsittelyyn liittyvät tietovarannot ja niiden hallintajärjestelmät sekä näihin liittyvät käyttövaltuudet. Lisäksi tulee hahmottaa varsinaiset käsittelyprosessit ja niihin liittyvät sopimusvastuut esimerkiksi tietojen käsittelyyn tai siirtoihin (lokit, varmuuskopioiden hallinta, luovutukset) liittyen. Kun henkilötiedoista ja niiden käsittelyperusteista ja -tarkoituksista on tehty nykytila-analyysi, voidaan hahmottaa tietojen käsittelyyn liittyviä riskitekijöitä ja suunnitella keinoja riskeihin puuttumiseksi sekä vaikutustenarviointiin että yleiseen riskiperusteiseen lähestymistapaan perustuen.[35]

[33] Valtiovarainministeriö 2018b.
[34] Valtiovarainministeriö 2018b.
[35] Andreasson ym. 2017, 63 – 64; Lambert 2018, 325.

Taulukkoon 1 on koottu esimerkkejä riskeistä, jotka voivat aiheutua tiedon luottamuksellisuuden, eheyden tai saatavuuden ongelmista, sekä niiden vaikutuksia luonnollisen henkilön oikeuksiin ja vapauksiin.

TAULUKKO 1. Riskit ja riskivaikutukset tiedon luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta.

Loukkaus	Esimerkkejä riskeistä	Esimerkkejä riskin vaikutuksista luonnollisen henkilön oikeuksiin ja vapauksiin
Luottamuksellisuuden loukkaus (tahaton tai luvaton tiedon vuotaminen tai pääsy tietoon), esim. viestintäsalaisuuden loukkaus, identiteettivarkaus, tietomurto tai yksityiselämää loukkaavan tiedon levittäminen.	Luottamuksellinen tai salainen tieto paljastuu ulkopuoliselle: henkilötietoja sisältäviä työvälineitä, muistitikkuja tai dokumentteja häviää tai varastetaan; tietoja kerrotaan tai näytetään sivullisille; tietoja, valokuvia tai videoita julkaistaan internetissä; tulosteita katoaa, jää tulostimelle tai tulostetaan väärään paikkaan; tietojärjestelmään on vanhentuneita tai liian laajoja käyttöoikeuksia; palvelimille, tietokantakopioihin tai tallenteisiin on ylimääräisiä oikeuksia tai tietoturvapäivityksiä jätetään tekemättä.	Loukkaus yksityisyyden suojalle. Omien tietojen käsittelyn valvonnan kontrolli heikkenee. Paljastuneesta tiedosta riippuen voi aiheuttaa eritasoista sosiaalista haittaa (maineen vahingoittumista, kiusaamista), syrjintää, taloudellista haittaa (tilaukset, ostot tai luotot toisen nimissä), vaaraa terveydelle ja hengelle (viharikokset, vainoaminen, perheväkivalta, masennus, itsetuhoisuus). Vaikutuksena voi olla myös paljastuneiden tietojen vuotaminen eteenpäin laajemmin (perheessä, sukulaisille, työyhteisössä, paikkakunnalla, julkisuuteen, verkkorikollisille) ja haittojen kumuloituminen.
Eheyden loukkaus (tahaton tai luvaton tiedon muuttuminen tai muuttaminen), esim. tieto on virheellinen, puutteellinen, ristiriitainen tai vanhentunut.	Tieto muuttuu tai sitä muutetaan inhimillisen virheen tai tietojärjestelmän virheen vuoksi, yhdisteltäessä tietoja eri tietojärjestelmistä tai automaattisen päätöksenteon yhteydessä virheellisen päättelyketjun tuloksena.	Kontrolli omiin tietoihin heikkenee; usein rekisteröidyllä ei ole tietoa henkilötietojen virheellisyydestä. Esimerkiksi etuutta, korvausta tai päätöstä haettaessa virheellisiin tietoihin perustuva päätös saattaa olla myös virheellinen (mahdollisen etuuden epääminen, virheelliset tukipäätökset, vahingonkorvauspäätökset tai sakot). Kun terveyden- tai sairaanhoitoon liittyvä tieto on virheellinen tai muuttunut, riskin vaikutuksena voi olla myös uhka terveydelle ja/tai hengelle.
Saatavuuden loukkaus (tahaton tai luvaton tietojen saatavuuden estyminen tai tiedon menettäminen), esim. tietojärjestelmä on (hallitsemattomasti) pois käytöstä, tiedot katoavat tai häviävät tai palvelinlaitteisto, tietokanta tai manuaalinen arkisto tuhoutuu kokonaan. Syy voi olla myös esim. haittaohjelma, joka estää tietoon pääsyn.	Tieto ei ole saatavilla organisaation työntekijälle, esimerkiksi korvaus-/etuuskäsittelijälle, terveydenhuollon ammattihenkilölle, sosiaaliviranomaiselle tai rekisteröidylle.	Kontrolli omiin tietoihin heikkenee. Pääsy tietoihin estyy; henkilö ei voi toteuttaa esim. tarkastusoikeutta. Viiveet valmistelussa ja päätöksenteossa voivat aiheuttaa määräaikojen ylittymisen, kun henkilö ei saa päätöstä ajallaan. Mahdolliset taloudelliset vaikutukset, kun esimerkiksi tuki-/korvauspäätös viivästyy. Myös uhka terveydelle tai hengelle, jos akuuttiin terveyden-, sairauden- tai sosiaalihuollon tietoon ei ole pääsyä.

2 EU:N YLEINEN TIETOSUOJA-ASETUS (GDPR)

2.1 Sääntelyn tausta ja tärkeimmät tavoitteet

Europan parlamentin ja neuvoston keväällä 2016 antama EU:n yleinen tietosuoja-asetus (GDPR) on suoraan sovellettavaa, velvoittavaa lainsäädäntöä kahden vuoden siirtymäajan jälkeen, 25.5.2018 lähtien. Se korvaa vuonna 1995 annetun henkilötietodirektiivin ja tähän perustuvan kansallisen tietosuojalainsäädännön tietosuoja-asetuksen sallimaa kansallista liikkumavaraa lukuun ottamatta.[36] Tietosuoja-asetuksen kanssa rinnakkain tullaan soveltamaan yleislaiksi tarkoitettua kansallista tietosuojalakia, jossa täsmennetään ja täydennetään tietosuoja-asetusta kansallisen liikkumavaran osalta. Lisäksi erityislainsäädännössä voidaan edelleen poiketa tietosuojalain säännöksistä tietosuoja-asetuksen harkintamarginaalin puitteissa. Tietosuojalain voimaan tullessa henkilötietolaki kumotaan.[37] Samaan aikaan tietosuoja-asetuksen kanssa annettiin rikosasioita koskeva tietosuojadirektiivi ((EU) 2016/680), joka on soveltamisalueensa vuoksi rajattu tämän työn ulkopuolelle.

Vaikka henkilötietodirektiivin tavoitteet ja periaatteet ovatkin edelleen päteviä, sen soveltaminen eri jäsenmaissa on ollut hajanaista ja epäjohdonmukaista, joka on osaltaan aiheuttanut oikeudellista epävarmuutta. Erilaiset henkilötietojen käsittelytavat suhteessa erityisesti oikeuteen henkilötietojen suojaan ovat saattaneet estää henkilötietojen vapaan liikkuvuuden unionin alueella ja muodostua esteeksi unionin taloudelliselle toiminnalle, vääristää kilpailua ja estää viranomaisia suorittamasta unionin oikeuden mukaisia velvollisuuksiaan.[38]

Tietosuoja-asetuksen tavoitteena on parantaa henkilötietojen suojaa ja rekisteröityjen oikeuksia sekä yhdenmukaistaa henkilötietojen käsittelyä ja poistaa liikkuvuuden esteet unionin alueella.[39] Sen tarkoituksena on lisätä henkilötietojen käsittelyn avoimuutta ja läpinäkyvyyttä sekä vahvistaa henkilön oikeuksia valvoa tietojensa käsittelyä. Varsinkin

[36] Oikeusministeriö 2018. Kansallisen liikkumavaran sallivista tietosuoja-asetuksen artikloista ja näihin liittyvistä käytön tarpeista ja perusteluista löytyy kattava kuvaus Tatti-työryhmän mietinnöstä 35/2017 (liikkumavarataulukko).
[37] HE 9/2018 vp 1, 31.
[38] Europan komissio 2012a, 6.
[39] Europan komissio 2012a, 6.

lasten henkilötietoja pyritään suojaamaan. Tätä tuetaan rekisterinpitäjälle asetetuilla lisävelvoitteilla sekä tehokkaalla täytäntöönpanolla, mm. hallinnollisilla sakoilla.[40] Tietosuoja-asetus on voimakkaasti kilpailua tukeva instrumentti ja yksi sen tavoitteista on myös edistää digitaalisten sisämarkkinoiden kehittymistä.[41]

Sääntelymuodon vaihtuminen direktiivistä asetukseen on merkittävä lainsäädäntöuudistus. EU-normijärjestelmässä molemmat ovat sekundaarinormeja, mutta siinä missä direktiivit eivät ole suoraan sovellettavia, vaan sitovat jäsenvaltioita vain sisältämänsä lainsäädäntötavoitteen osalta ja käytännössä vaativat aina kansallisia lainsäädäntötoimia, asetukset ovat tosiasiallisesti suoraan sovellettavaa, jäsenvaltioita sitovaa sääntelyä jota ei tarvitse erikseen säätää laeiksi.[42] Nykylainsäädännön direktiiviperusteisuus on todennäköisesti osaltaan vaikuttanut sen epäyhtenäiseen soveltamiseen. Asetuksen onkin katsottu soveltuvan säädöstyypiksi parhaiten nimenomaan suoran sovellettavuutensa vuoksi.[43]

Tietosuoja-asetuksen sallima kansallinen liikkumavara ei mahdollista kokonaisvaltaisen lain säätämistä, mutta mahdollistaa tiettyjen artiklojen tarkentamisen, täsmentämisen tai säätämisen poikkeavasti kansallisessa yleis- tai erityislainsäädännössä.[44] Tämä sekä asetustekstin tulkinnanvaraisuus huomioiden on mahdollista, että kansallisissa säädöksissä tulee edelleen olemaan jossain määrin eroavaisuuksia.

2.2 Soveltamisalue ja -periaatteet tiivistetysti

Tietosuoja-asetuksen 2 artiklan mukaan asetusta sovelletaan lähtökohtaisesti kaikkeen henkilötietojen käsittelyyn, kun tiedot muodostavat rekisterin osan (aineellinen soveltamisala). Sitä sovelletaan yksityisissä yrityksissä, yhteisöissä sekä julkishallinnossa.[45] Tietosuoja-asetus ei ota kantaa henkilötietojen käsittelyn teknologioihin, välineisiin tai laitteisiin, vaan pääsääntöisesti se jättää rekisterinpitäjälle vastuun miettiä keinot lainsäädännön noudattamiseksi.

[40] Tietosuojavaltuutetun toimisto 2017b, 9.
[41] Tietosuojavaltuutetun toimisto 2018e.
[42] Raitio 2016.
[43] Europan komissio 2012a, 6.
[44] HE 9/2018 vp, 5.
[45] Tietosuojavaltuutetun toimisto 2017b, 9.

Tietosuoja-asetuksen myötä henkilötietojen käsittelysäännöt tarkentuvat ja yhdenmukaistuvat kaikissa EU-jäsenmaissa ja laajemminkin. Tietosuoja-asetuksen 4 artiklassa säädetään sen alueellisesta soveltamisalasta; asetusta sovelletaan henkilötietojen käsittelyyn, joka tapahtuu EU-alueella sijaitsevan rekisterinpitäjän tai henkilötietojen käsittelijän toimesta, tapahtuipa itse käsittely EU-alueella tai ei. Tietosuoja-asetus velvoittaa myös unionin ulkopuolelle sijoittautuneita rekisterinpitäjiä, jotka käsittelevät EU-alueella olevien henkilöiden henkilötietoja silloin kun käsittely liittyy tavaroiden tai palvelujen tarjoamiseen tai luonnollisten henkilöiden käyttäytymisen seurantaan, esimerkiksi profilointiin. Tietosuoja-asetusta sovelletaan myös tapauksissa, joissa rekisterinpitäjä toimii paikassa, jossa sovelletaan jonkin EU-jäsenvaltion lakia kansainvälisen julkisoikeuden nojalla.

Alueellinen soveltamisala on laaja, jonka lisäksi tietosuoja-asetuksessa velvoitetaan rekisterinpitäjä sitouttamaan myös henkilötietojen käsittelijöinä toimivat yhteistyökumppanit tietosuoja-asetuksen noudattamiseen sopimalla kirjallisesti henkilötietojen käsittelystä (tietosuoja-asetuksen artikla 28, johdanto-osan kohta 81). Pilvipalvelujen sekä palveluna hankittujen tietojärjestelmien, sovellusalustojen ja infrastruktuurin[46] jatkuvasti yleistyessä tulee näihin liittyvät tietoturva- ja tietosuojariskit huomioida paitsi palvelua käytettäessä, jo sopimusvaiheessa. Käytännössä yksittäisen rekisterinpitäjän on melko mahdotonta pyrkiä muuttamaan suurten, globaalien yritysten palvelutuotantoa sopimusteitse, mutta pienempien yritysten kanssa tämä voi olla mahdollista.

Lähtökohtana EU-lainsäädännössä on taata tietojen vapaa liikkuvuus unionin alueella. Pääsääntöisesti siirrot kolmansiin maihin eli niihin EU:n ulkopuolisiin maihin, joita tietosuoja-asetus ei velvoita, on kielletty. Komissio on kuitenkin julkaissut listan maista, sektoreista ja kansainvälisistä järjestöistä, joiden se katsoo noudattavan riittävää tietosuojan tasoa. Näissä tapauksissa siirrot myös kolmansiin maihin voidaan toteuttaa. Lista julkaistaan Euroopan unionin virallisessa lehdessä ja komission verkkosivustolla.[47] Helmikuussa 2017 päätettiin myös EU:n ja Yhdysvaltojen välisen Privacy Shield-sopimuksen jatkamisesta.[48]

[46] Tällaisia ovat palveluna hankitut tietojärjestelmät (SaaS, Software as a Service), sovellusalustat (PaaS, Platform as a Service) ja infrastruktuuri (IaaS, Infrastructure as a Service).
[47] Euroopan komissio n.d. Katso tarkemmin: https://ec.europa.eu/info/law/law-topic/data-protection_en.
[48] Tietosuojavaltuutetun toimisto 2017c.

Tietosuoja-asetuksen artiklan 4 mukaan tietojen siirtäminen on yksi osa henkilötietojen käsittelyä ja luovuttamista. Se tarkoittaa sopimusperusteista toimintaa, jossa rekisterinpitäjä siirtää esimerkiksi tietojärjestelmän tai palvelualustan hallinnan IT-toimittajalle tai palveluntarjoajalle tai vastaavasti mahdollistaa ulkopuolisen tahon käsittelemään henkilötietoja teknisen yhteyden avulla rekisterinpitäjän organisaatiossa. Yleisimpiä tilanteita ovat ulkoistukset, pilvipalvelujen käyttö sekä siirrot konsernin yhteiseen rekisteriin. Siirtotilanteissa vastuu rekisteristä säilyy rekisterinpitäjällä, ja henkilötietoa käsittelevä taho toimii tietosuoja-asetuksen tarkoittamana henkilötiedon käsittelijätahona. Tietojen luovuttamisen yhteydessä vastaanottajasta tulee rekisterinpitäjä esimerkiksi tilanteissa, joissa henkilötietoja luovutetaan tai myydään toisen yrityksen markkinointitarkoituksia varten.[49] Termien hahmottaminen ja asianmukainen käyttö oikeissa yhteyksissä on erityisen tärkeää varsinkin sopimusvastuiden kannalta, mutta myös henkilötietojen käsittelyperusteen laillisuuden varmistamiseksi.[50] Luovuttaja vastaa tietojen luovuttamisen laillisuudesta.

Tietosuoja-asetuksen periaatteet noudattelevat pääsääntöisesti nykyisen henkilötietolain periaatteita. Tietosuojaperiaatteet määritellään tietosuoja-asetuksen 5 artiklassa ja niitä selvennetään laajasti asetuksen johdanto-osassa. Tietosuojaperiaatteet ovat

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys,
- käyttötarkoitussidonnaisuus (tietoja kerätään tiettyä, lainmukaista tarkoitusta varten, eikä niitä saa myöhemminkään käsitellä näihin tarkoituksiin nähden yhteensopimattomalla tavalla, poislukien yleisen edun mukaiset arkistointitarkoitukset, tilastointitarkoitukset tai tieteelliset tai historialliset tutkimustarkoitukset),
- tietojen minimointi (kerätään vain käyttötarkoituksen kannalta olennaiset tiedot),
- täsmällisyys (tietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä, epätarkat ja virheelliset tiedot tulee pyrkiä poistamaan tai oikaisemaan),
- säilytyksen rajoittaminen (tiedot säilytetään muodossa, josta rekisteröity on tunnistettavissa vain niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten) sekä
- eheys ja luottamuksellisuus (huolehditaan tietoturvasta ja tietosuojasta; suojataan tiedot luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta).

[49] Tietosuojavaltuutetun toimisto 2013, 3.
[50] Kuntaliitto 2017, 3.

Uusia vaatimuksia ovat osoitusvelvollisuus, jota käsitellään sen merkittävyyden vuoksi erikseen kappaleessa 2.3.1, sekä 5 artiklan 1 kohdassa sekä 12 artiklan 1 kohdassa mainittu henkilötietojen käsittelyn läpinäkyvyys, jota on täsmennetty laajasti tietosuoja-asetuksen johdanto-osan kohdassa 39. Rekisteröidylle tulisi olla läpinäkyvää, miten ja missä määrin häntä koskevaa henkilötietoa käsitellään tai on määrä käsitellä. Tämä tarkoittaa käytännössä sitä, että rekisteröityä tulee tiedottaa paitsi henkilötietojen käsittelyn tarkoituksista, myös käsittelyyn liittyvistä riskeistä, säännöistä, suojatoimista ja rekisteröidyn oikeuksista. Tähän liittyy myös vaatimus mahdollisimman lyhyestä tietojen säilytysajasta ja sen ilmoittamisesta rekisteröidylle. Informoinnin on oltava helposti saatavilla ja ymmärrettävää, ja siinä on käytettävä selkeää ja yksinkertaista kieltä. Vaatimus läpinäkyvästä informoinnista on merkittävä uudistus ja edellyttää rekisterinpitäjältä entistä johdonmukaisempaa, selkeämpää ja yksityiskohtaisempaa tiedottamista. Myös WP29-tietosuojatyöryhmä on antanut omat, tarkentavat ohjeensa informoinnin periaatteista[51] sekä automaattisesta päätöksenteosta ja profiloinnista.[52]

Käsittelyn rajoittamisen velvoitetta on täsmennetty tietosuoja-asetuksen johdanto-osan kohdissa 39 ja 49: käsittely tulisi rajoittaa ehdottoman välttämättömään ja oikeasuhtaiseen. Lähtökohtaisesti tulee kerätä vain käsittelyn kannalta välttämättömät tiedot. Käsittelyn rajoittamisen menetelminä mainitaan johdanto-osan kohdassa 67 tietojen siirtäminen toiseen käsittelyjärjestelmään, käyttäjien pääsyn estäminen valittuihin henkilötietoihin tai julkaistujen tietojen väliaikainen poistaminen verkkosivustolta. Automaattisissa rekistereissä käsittelyn rajoittaminen olisi lähtökohtaisesti varmistettava teknisin keinoin niin, ettei henkilötietoja enää voida käsitellä tai muuttaa. Käsittelyn rajoittaminen olisi lisäksi ilmaistava järjestelmässä selvästi.

Vaatimus käsittelyn rajoittamisesta käsittelyn kannalta ehdottoman välttämättömään ja oikeasuhtaiseen yhdistettynä läpinäkyvän informoinnin velvoitteeseen ohjaa rekisterinpitäjiä rajatumpaan tietojen käsittelyyn. Käsittelyn rajoittaminen edellyttää pääsääntöisesti uudenlaisten toiminnallisten ratkaisujen kehittämistä tietojärjestelmiin sekä uudenlaisten tietojenkäsittelyprosessien laatimista ja kouluttamista henkilötietoja käsitteleville.

Sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta käsitellään tietosuoja-asetuksen artiklassa 25 sekä johdanto-osan kohdassa 78. Sisäänrakennetun tietosuojan (data

[51] WP29 2017e.
[52] WP29 2017d.

protection by design) periaate edellyttää, että tietosuojaperiaatteet otetaan tehokkaasti osaksi sekä käsittelytapojen määrittämisessä että henkilötietojen käsittelyn kaikissa vaiheissa.[53] Kehitettäessä, suunniteltaessa, valittaessa ja käytettäessä sovelluksia, palveluja ja tuotteita, jotka sisältävät henkilötietojen käsittelyä, näiden tuottajia olisi kannustettava huomioimaan tietosuoja sekä varmistamaan uusin tekniikka ja toteutuskustannukset huomioiden, että rekisterinpitäjät ja henkilötietojen käsittelijät pystyvät täyttämään tietosuojavelvoitteensa. Palveluntuottajien ja rekisterinpitäjän tulee siis tunnistaa tietosuojaa koskevat kysymykset ja huomioida ne jo siinä vaiheessa, kun henkilötietojen käsittelyä vasta suunnitellaan tai tietojärjestelmiä kehitetään.[54] Sisäänrakennettu tietosuoja tulee huomioida myös julkisten kilpailutusten yhteydessä.

Rekisterinpitäjän velvollisuutena on toteuttaa tarvittavat tekniset ja organisatoriset toimenpiteet asetuksen vaatimusten täyttämiseksi. Osoitusvelvollisuuden todentamiseksi rekisterinpitäjän tulisi hyväksyä sisäisiä menettelytapoja ja toimenpiteitä, jotka vastaavat erityisesti sisäänrakennettua ja oletusarvoista tietosuojaa. Esimerkkeinä toimenpiteistä ovat henkilötietojen käsittelyn minimointi, henkilötietojen pseudonymisointi mahdollisimman pian, tehtävien ja henkilötietojen käsittelyn läpinäkyvyys, rekisteröidyn omien tietojensa valvonnan mahdollistaminen sekä turvaominaisuuksien luominen ja parantaminen. Vahti-raportin mukaan näillä tarkoitetaan myös henkilötietojen kykyä taata järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus; palauttaa saatavuus ja pääsy tietoihin nopeasti teknisen vian sattuessa sekä menettelyä – esimerkiksi auditointia – jolla testataan, tutkitaan ja arvioidaan säännöllisesti toimenpiteiden tehokkuutta.[55] Tietosuojavaltuutetun oppaassa mainitaan edelleen suojatoimenpiteet, esimerkiksi salassapitositoumukset, tilavalvonta (mm. kameravalvonta), omavalvonnan kautta tapahtuva käytönvalvonta eli järjestelmän käytön lokitus, tietojärjestelmien tietoturva, tietojen salaus, etäkäyttöyhteydet, tekniset rajoitukset, tarkastus- ja valvontajärjestelmät, tietotilinpäätösprosessi sekä käytännesääntöjen ja sertifikaattien käyttöönotto.[56]

[53] Tietosuojavaltuutetun toimisto 2017b, 13
[54] Tietosuojavaltuutetun toimisto 2017b 13.
[55] Valtiovarainministeriö 2016, 35.
[56] Tietosuojavaltuutetun toimisto 2017b, 13.

Tietosuojaperiaatteiden huomioimisen lisäksi tietojärjestelmien suunnittelussa ja toteutuksessa tulee ottaa huomioon rekisterinpitäjän velvollisuus toteuttaa rekisteröidyn oikeuksia esimerkiksi tietojen oikaisemiseen, tietopyyntöihin, henkilötietojen käsittelyn rajoittamiseen tai tietojen poistamiseen liittyen. Sisäänrakennetun tietosuojan merkitys on tärkeä myös vaikutustenarvioinnin kannalta; vaikutustenarviointi tulee tehdä etenkin uutta teknologiaa käytettäessä, kun henkilötietojen käsittely todennäköisesti aiheuttaa korkean riskin henkilön oikeuksille ja vapauksille. Sisäänrakennettu tietosuoja tietojärjestelmissä on myös sopimustekninen asia, joka saattaa sisältää merkittävän taloudellisen riskin.

Oletusarvoisen tietosuojan periaate (data protection by default) tarkoittaa, että rekisterinpitäjän tulee oletusarvoisesti käsitellä vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja.[57] Velvollisuus koskee kerättyjen henkilötietojen määrää (kerätään vain käsittelyn kannalta välttämättömät tiedot), käsittelyn laajuutta (ei kerätä suurempia määriä kuin on tarpeen), säilytysaikaa (ei säilytetä kauemmin kuin on välttämätöntä) ja saatavilla oloa (tietoja ei saateta rajoittamattoman henkilömäärän saataville).

Tietosuoja-asetuksen 25 artiklan mukaan rekisterinpitäjän tulee erityisesti varmistaa, että henkilötietoja ei oletusarvoisesti saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta. Tämä edellyttää käytännössä tehokasta käytönvalvontaa. Järjestelmiin tulisi voida määritellä käyttöoikeudet käyttäjän roolin perusteella niin, että käyttäjä näkee ja voi käsitellä vain oman työnsä kannalta tarpeellisia henkilötietoja. Lisäksi järjestelmän käyttöä tulisi pystyä valvomaan ja mahdolliset muutokset jäljittämään jälkikäteen. Myös järjestelmistä kerättäviin lokitietoihin tai järjestelmän tietokantakopioihin tulisi määritellä pääsynhallinta eli tahot, joilla tietoihin on pääsy. Tietojen katselu tulisi, varsinkin käsiteltäessä erityisiin henkilötietoryhmiin kuuluvaa tai salassa pidettävää tietoa, pystyä lokittamaan.[58]

Yksi tietosuoja-asetuksen tavoitteista on tehdä henkilötietojen suojasta erottamaton osa organisaation hallinnollisia menettelyitä ja teknistä kehitystä.[59] Arvioidessaan tietosuoja-

[57] Tietosuojavaltuutetun toimisto 2017b, 11.
[58] Andreasson 2017.
[59] HE 9/2018 vp, 30.

asetuksen edellyttämiä vaikutuksia toimintaansa, organisaation on hahmotettava kokonaiskuva henkilötietojen käsittelyn nykytilasta. Kartoituksen jälkeen tulee selvittää, mitä konkreettisia muutoksia tai toimenpiteitä sääntely organisaation toiminnassa aiheuttaa.[60]

2.3 Merkittävimmät muutokset ja uudistukset

2.3.1 Osoitusvelvollisuus

Osoitusvelvollisuudesta säädetään tietosuoja-asetuksen 5 artiklassa; se on yksi tietosuoja-asetuksen soveltamisperiaatteista. Rekisterinpitäjän vastuulla on luonnollisesti noudattaa lainsäädäntöä, mutta jatkossa myös osoittaa se (accountability) esimerkiksi erilaisten dokumenttien, suunnitelmien, käytännesääntöjen, sertifikaattien tai tietotilinpäätöksen avulla.[61] Rekisterinpitäjän on artiklojen 24 ja 25 mukaan toteutettava tarvittavat tekniset ja organisatoriset eli hallinnolliset toimenpiteet asetuksen vaatimusten täyttämisen varmistamiseksi; näistä on annettu esimerkkejä jo sisäänrakennetun ja oletusarvoisen tietosuojan yhteydessä. Osoitusvelvollisuuden kannalta erityisen tärkeitä ovat henkilötietojen käsittelyyn liittyvät, organisaation sisäiset politiikat, ohjeet ja määräykset, salassapito- ja käyttösitoumukset, henkilöstön koulutusmateriaalit, selosteet (tietosuojaselosteet, selosteet käsittelytoimista) sekä esimerkiksi lomakkeiden ja prosessien dokumentointi rekisteröidyn oikeuksiin kuten henkilötietojen oikaisuun tai tietopyyntöihin liittyen.[62] Osoitusvelvollisuuden tukena toimivat myös erilaiset raportit sekä tietojärjestelmien lokitiedostot. Tietosuojavastaavan nimittäminen on luonnollisesti yksi keino toteuttaa osoitusvelvollisuutta.

Osoitusvelvollisuus on yksi merkittävimmistä muutoksista tietosuoja-asetuksen vaatimusten toimeenpanossa. Siinä missä valvontaviranomaisen rooli on tähän saakka ollut lähinnä neuvova ja ohjaava, tietosuoja-asetuksessa sen rooli muuttuu valvovampaan suuntaan. Jatkossa valvontaviranomainen vastaa tietosuoja-asetuksen noudattamisesta, ja tämä voi tarvittaessa tehdä tarkastuksia tai pyytää dokumentteja rekisterinpitäjiltä näiden velvoitteisiin liittyen (artikla 57). Myös mahdollisten sanktioiden riski kannustaa rekisterinpitäjiä entistä täsmällisempään rekisterinpitoon.

---

[60] Tietosuojavaltuutetun toimisto 2017b, 13.
[61] Andreasson ym. 2017, 26.
[62] Tietosuojavaltuutetun toimisto 2017b, 13.

Osoitusvelvollisuus tuo merkittävästi lisää velvoitteita varsinkin siirtymäajalla, kun nykyisiä toimintamalleja käydään läpi ja uusien velvoitteiden toteuttamiseen valmistaudutaan. Samalla se kuitenkin mahdollistaa nykyisten toimintamallien tarkastelun, tarkentamisen ja järkeistämisen sekä luo uusia toimintamalleja ja toivottavasti näin ryhdistää rekisterinpitoa, vähentää kustannuksia ja lisää organisaation tuottavuutta tulevaisuudessa. Dokumentointi- ja todentamisvelvoite liittyy myös yleiseen riskiperusteiseen lähestymistapaan sekä vaikutustenarviointien laatimiseen, varsinkin näihin liittyvien riskien lieventämistoimien osalta.

Osoitusvelvollisuuteen liittyvä erittäin suuri riski on johdon vähäinen sitoutuminen tietosuoja-asetuksen velvoitteisiin. Tietosuojaa ei välttämättä nähdä asiana, johon kannattaa sijoittaa merkittäviä resursseja, koska sen avulla saavutettavia hyötyjä tai tavoitteita on hankalaa konkreettisesti todentaa ja mitata. Hyötytavoitteina johdolle voidaan esittää esimerkiksi hallinnollisten sakkojen tai oikeustapausten nostamisen riskin minimointi, prosessien sujuvoittamisen kautta hankitut säästöt resursseissa, henkilöstön osaamisen kasvattaminen, positiivinen imagohyöty sekä luonnollisesti lainsäädännöllisten velvoitteiden noudattaminen. Myös toimialaan liittyvän erityislainsäädännön vähäinen tuntemus voi johtaa puutteellisiin ohjeisiin tai prosesseihin ja sitä kautta estää osoitusvelvollisuuden todentamisen. Erittäin suuri riski on myös se, ettei rekisterinpitäjän toiminnoissa tunnisteta korkean riskin henkilötietojen käsittelyä. Nämä voivat johtaa luonnollisen henkilön – asiakkaan, kansalaisen tai työntekijän – oikeuksien ja vapauksien vaarantumiseen tai tietojen päätyminen asiattomien saataville.[63] On erittäin tärkeää, ettei tietosuoja-asetuksen osoitusvelvollisuuden toteuttamista nähdä vain siirtymäaikaan liittyvänä pakollisena projektina, kun sen tavoitteena pitäisi olla toiminnan jatkuvan prosessin kehittäminen.

2.3.2 Riskiperusteinen lähestymistapa

Myös riskiperusteinen lähestymistapa on yksi tietosuoja-asetuksen läpileikkaavista teemoista, vaikkei siitä säädetäkään erillisenä periaatteena. Vaikka riskienhallintamenettely on yleensä kiinteä ja vakiintunut osa suurempien organisaatioiden toimintaa, se saattaa pienemmissä organisaatioissa olla hyvinkin kevyt ja epämuodollinen, lähinnä taloudelli-

[63] Andreasson, 2017.

siin riskivaikutuksiin keskittyvä toiminne, jossa ei todennäköisesti ole huomioitu jatkuvuutta tai henkilötietojen käsittelyyn liittyviä tietosuojariskejä. Tästä syystä kappaleessa esitellään myös riskienhallinnan periaatteita lyhyesti ja pääpiirteittäin.

Riskiperusteinen lähestymistapa tarkoittaa, että tietosuoja-asetuksen velvoitteet ja asianmukaiset suojatoimet suhteutetaan henkilötietojen käsittelystä luonnollisen henkilön oikeuksiin ja vapauksiin aiheutuvaan riskiin; mitä suurempi arvioitu riski on, sitä laajempia tai vahvempia toimenpiteitä tulee toteuttaa, jotta riskin vaikutus voitaisiin minimoida tai riski välttää kokonaan. Toisaalta tarkoituksena on välttää matalariskisen toiminnan ylisääntelyä.[64] Riskilähtöisyys kannustaa organisaatiot ottamaan tietosuojariskit kokonaisvaltaisesti huomioon toiminnassaan ja prosesseissaan ja samalla se ohjaa henkilötietojen käsittelyä ja on tärkeä osa rekisterinpitäjän osoitusvelvollisuuden toteuttamista.[65]

Riskillä tarkoitetaan yleisesti ottaen ei-toivotun tapahtuman uhkaa, jolla on toteutuessaan negatiivisia vaikutuksia. Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä Vahtin ohjeessa riski määritellään poikkeamaksi odotetusta, se voi olla myönteinen tai kielteinen epävarmuuden vaikutus tavoitteisiin.[66] WP29-tietosuojatyöryhmän ohje määrittelee riskin skenaariona, jolla kuvataan tapahtumaa ja sen seurauksia sekä arvioidaan niiden vakavuutta ja todennäköisyyttä.[67] Tietosuoja-asetuksen johdanto-osan kohdassa 75 henkilötietojen käsittelytoimista aiheutuvia riskejä lähestytään luonnollisen henkilön oikeuksille ja vapauksille aiheutuvien riskivaikutusten kautta:

> – – jotka voivat aiheuttaa fyysisiä, aineellisia tai aineettomia vahinkoja, erityisesti jos henkilötietojen käsittely saattaa johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin tai sosiaaliseen vahinkoon tai pseudonymisoinnin luvattomaan kumoutumiseen.

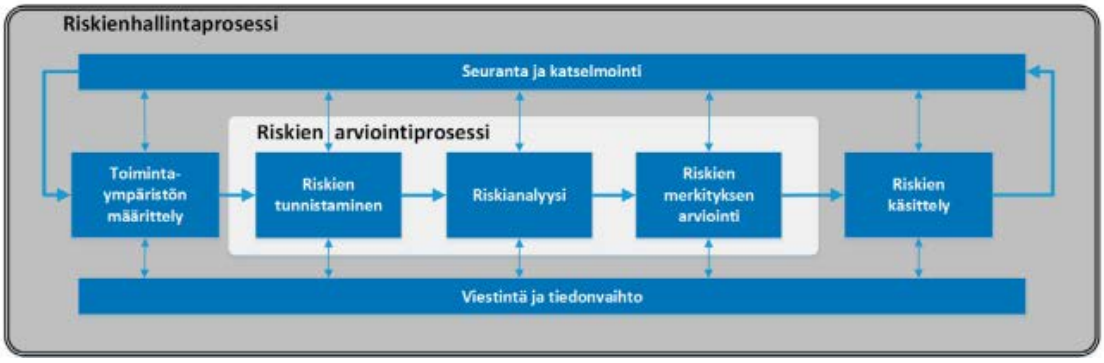
Tietosuoja-asetuksen mukaan riski on korkeampi käsiteltäessä suuria henkilötietomääriä, suurta rekisteröityjen määrää, erityisiin henkilötietoryhmiin kuuluvia tietoja tai heikossa asemassa olevien ja eritystä suojelua tarvitsevien henkilöiden, erityisesti lasten, tietoja. Riski voi olla korkeampi myös silloin, kun arvioidaan henkilökohtaisia ominaisuuksia tai käyttäytymistä esimerkiksi profiloinnin avulla.

---

[64] Tietosuojavaltuutetun toimisto 2017b, 16.
[65] Valtiovarainministeriö 2016, 21; Andreasson ym. 2017, 56.
[66] Valtiovarainministeriö 2017a, 11.
[67] WP29 2017b, 5.

Riskienhallinnan tarkoituksena on pyrkiä hallitsemaan epävarmuuksien vaikutukset organisaation toiminnassa. Riskienhallintaprosessi sisältää kaikki riskeille tehtävät toimenpiteet toimintaympäristön määrittelystä riskien tunnistamiseen, analysointiin ja käsittelyyn, jossa määritellään riskiin kohdistettavat toimenpiteet eli niiden lieventämiskeinot. Riskienhallinnan tulisi olla avointa ja kattavaa, aktiivista ja muutoksiin reagoivaa toimintaa, jota kehitetään määrätietoisesti ja tarkoituksenmukaisesti.[68]

Kuvassa 1 on esitetty ISO31000-laatustandardiin perustuva, julkisen hallinnon digitaalisen turvallisuuden johtoryhmä Vahtin ohjeessa julkaistu riskienhallintaprosessi. Prosessin vaiheet on kuvattu keskellä; jokaiseen vaiheeseen liittyy seuranta ja katselmointi sekä viestintä ja tiedonvaihto.



KUVA 1. Riskienhallintaprosessi.[69]

Myös tietosuoja-asetuksessa korostetaan riskien kokonaisvaltaisen käsittelyn tärkeyttä. Riskien analysoinnin, eli niiden todennäköisyyden ja vaikuttavuuden sekä riskin vaikutusten kartoituksen lisäksi on tärkeää, että kullekin todennetulle riskille suunnitellaan ja toteutetaan lieventämistoimenpiteet, jotta kyseinen riski pienenee tai poistuu kokonaan. Osoitusvelvollisuuden todentamiseksi on tärkeää dokumentoida tehdyt päätökset. On erittäin tärkeää, että henkilötietoja käsittelevät työntekijät organisaation kaikilla tasoilla osaisivat tunnistaa käsittelyyn liittyviä riskejä omassa työssään ja työympäristössään sekä tuoda riskejä aktiivisesti esille ilmoittamalla havainnoistaan esimerkiksi esimiehelleen, it-tukeen tai tietosuojavastaavalle. Tämä luonnollisesti edellyttää riittävää koulutusta, ohjeistusta ja määriteltyä prosessia.

[68] Valtiovarainministeriö 2017a, 13 – 14, 20.
[69] Valtiovarainministeriö 2017a, 18.

Riskienhallintaan ja -kartoitukseen on olemassa monenlaisia työkaluja, joista esimerkkinä Vahti-ohjeen riskienhallinnan Excel-pohja käyttöohjeineen.[70] Excel-taulukosta on kuva myös opinnäytetyön liitteenä 1. Riskin analysointia ja hahmottamista saattaisivat auttaa riskivaikutusten numeerinen arviointi tai kustannusvaikutusluokittelu. Taloudellisia riskivaikutuksia ovat tässä yhteydessä esimerkiksi tietojärjestelmän palauttamisesta ja työskentelyn keskeytymisestä aiheutuvat kulut, mahdolliset hallinnolliset sakot, uhkasakot, oikeudenkäyntikulut, vahingonkorvaukset, organisaation sisäinen työ tai ulkopuolelta ostettu konsultointi liittyen esimerkiksi tietovuodon syiden selvitykseen tai tietojen poistamiseen internetistä.[71]

Jotta tietosuojariskejä voidaan todentaa, tulee rekisterinpitäjän tietää, millaisia henkilötietoja sen toiminnassa käsitellään sekä ymmärtää, millaisista henkilötiedoista todennäköisesti voi aiheutua korkea riski luonnollisen henkilön oikeuksille ja vapauksille, jolloin tulee tehdä erillinen vaikutustenarviointi. Luonnollisesti on tunnettava myös henkilötietojen käsittelytoimintoja, niitä prosesseja ja toimintatapoja, joita henkilötietojen käsittelyyn organisaatiossa kuuluu. On huomioitava, että vaikutustenarviointi on yksi tapa toteuttaa riskiperusteista lähestymistapaa. Ei siis riitä, että organisaatiossa laaditaan vaikutustenarviointi tai todetaan vaikutustenarvioinnin laatiminen tarpeettomaksi; yleinen riskiperusteinen lähestymistapa velvoittaa joka tapauksessa riskien jatkuvaan analysointiin.[72] Tietosuojariskien hallinta kannattaakin liittää osaksi rekisterinpitäjän jo olemassa olevaa riskienhallintaprosessia. Näin tieto merkittävistä riskeistä menee myös ylimmälle johdolle.

2.3.3 Informointi ja seloste käsittelytoimista

Henkilötietolain 10 §:ssä säädetään rekisterinpitäjän velvollisuudesta laatia ja pitää jokaisen saatavilla rekisteriseloste, jossa ilmoitetaan rekisterinpitäjän yhteystiedot ja henkilötietojen käsittelyn tarkoitus, tietojen luovutuskäytänteet sekä rekisterin suojauksen periaatteet. Tietosuoja-asetuksessa ei enää säädetä rekisteriselosteesta, mutta artikloissa 12 –

[70] Valtiovarainministeriö 2017c.
[71] Andreasson 2017.
[72] WP29 2017b, 7.

14 sekä johdanto-osan kohdissa 58 – 64 säädetään rekisteröidyn informoinnista, joka voidaan toteuttaa selosteena ja laatia jo käytössä olevan rekisteri- tai tietosuojaselosteen pohjalta.

Informointivelvoitteella pyritään takaamaan henkilölle riittävät tiedot siitä, mitä tarkoituksia varten ja millä perusteella henkilötietoja kerätään ja käsitellään ja kuka rekisteristä vastaa, jotta rekisteröity voi tarvittaessa olla yhteydessä rekisterinpitäjään tieto-, oikaisu- tai poistopyyntöönsä liittyvissä asioissa. Puutteelliset tai puuttuvat selosteet tai näihin liittyvän prosessin puuttuminen voivat johtaa rekisterinpitäjän toimintojen ruuhkautumiseen, kun tiedusteluja ja pyyntöjä saapuu määritellyn yhteyspisteen sijaan satunnaisiin toimipisteisiin tai yksikköihin. Tietojen selvittäminen ja oikeaan paikkaan ohjaaminen aiheuttavat organisaatiossa resurssihukkaa ja epätietoisuutta ja hidastavat käsittelyä. Lisäksi nämä nakertavat rekisteröidyn luottamusta rekisterinpitäjään. Vastausten viivästyessä rekisteröity voi ilmoittaa asiasta tietosuojaviranomaiselle, joka viime kädessä velvoittaa toimittamaan tiedot.

Informointivelvoitteen lisäksi tietosuoja-asetuksen 30 artiklassa säädetään velvollisuudesta laatia seloste käsittelytoimista. Seloste on organisaation sisäinen, osoitusvelvollisuutta todentava asiakirja, joka toimitetaan pyydettäessä valvontaviranomaiselle. Tietosuojavaltuutettu on maaliskuussa 2018 julkaissut tarkennetut ohjeet ja mallin tietosuojaselosteesta Ajankohtaista-sivullaan.[73]

2.3.4 Rekisteröidyn oikeudet ja rekisterinpitäjän velvollisuudet

Rekisterinpitäjän velvollisuutena on toteuttaa rekisteröidyn oikeuksia huomioimalla ne prosesseissa ja tietojärjestelmien suunnittelussa ja varmistamalla, että näissä noudatetaan tietosuoja-asetuksen vaatimuksia.[74] Rekisterinpitäjän tulee myös tiedottaa avoimesti henkilötietojen käsittelystä jo ennen käsittelyn aloittamista, uusina velvoitteina tähän liittyen ovat henkilötietojen säilytysajan ja tietosuojavastaavan yhteystietojen ilmoittaminen.[75]

[73] Tietosuojavaltuutetun toimisto 2018b.
[74] Tietosuojavaltuutetun toimisto 2017b, 23.
[75] Valtiovarainministeriö 2016, 14.

Tietosuoja-asetuksen tavoitteena on rekisteröityjen oikeuksien lujittaminen. Pääsääntöisesti oikeudet seurailevat henkilötietolain säännöksiä, mutta oikeuksista säädetään nykyistä yksityiskohtaisemmin ja mukana on myös uusia oikeuksia. On huomioitava, että osa oikeuksista on sidoksissa henkilötietojen käsittelyn oikeusperusteeseen. Mikäli rekisteröity katsoo, että häntä koskevien henkilötietojen käsittelyssä on rikottu tietosuoja-asetusta, hänellä on oikeus saattaa asia valvontaviranomaisen käsiteltäväksi. Samoin rekisteröidyllä on oikeus saada korvaus vahingosta, joka hänelle on aiheutunut asetuksen rikkomisesta. Sekä rekisteröidyllä että rekisterinpitäjällä ja henkilötietojen käsittelijällä on oikeus valittaa tietosuojaviranomaisen tekemästä oikeudellisesti sitovasta päätöksestä hallinto-oikeuteen.[76]

Oikeudesta saada pääsy tietoihin säädetään tietosuoja-asetuksen artiklassa 15 ja johdanto-osan kohdissa 63 ja 64; rekisteröidyllä on oikeus saada jäljennös käsiteltävistä henkilötiedoista tai siitä, käsitelläänkö hänen tietojaan ylipäätään rekisterinpitäjän rekistereissä vai ei. Tietopyyntöön on reagoitava pääsääntöisesti yhden kuukauden määräajassa, jona aikana rekisterinpitäjän on joko toimitettava tiedot tai ilmoitettava toimituksen viivästymisestä tai siitä, ettei tietoja pystytä toimittamaan. Tiedot toimitetaan pääsääntöisesti maksutta, joskin asetus jättää mahdollisuuden periä toimittamisesta hallinnollisen maksun. Mikäli pyyntö on perusteeton tai kohtuuton, ei tietoja tarvitse toimittaa, mutta tällöin on perusteettomuus ja kohtuuttomuus pystyttävä osoittamaan ja ilmoitettava asiasta rekisteröidylle.

Tietopyyntöä ei tarvitse enää omakätisesti allekirjoittaa, vaan sen voi tietosuoja-asetuksen johdanto-osan kohdan 59 mukaan esittää sähköisesti, johon rekisterinpitäjän on tarjottava keinot varsinkin niissä tapauksissa, joissa henkilötietoja käsitellään sähköisesti. Tällöin myös tiedot tulee tietosuoja-asetuksen artiklan 15 mukaan toimittaa lähtökohtaisesti sähköisesti, ellei rekisteröity toisin pyydä. Tietosuoja-asetuksen kohdan 64 mukaan rekisterinpitäjän velvollisuutena on käyttää kaikkia kohtuullisia keinoja rekisteröidyn henkilöllisyyden tunnistamiseksi hänen halutessaan saada pääsy tietoihinsa erityisesti verkkopalvelujen ja verkkotunnistetietojen yhteydessä.

Merkittävä uudistus on artiklassa 17 säädetty ja johdanto-osan kohdissa 65 ja 66 selkiytetty oikeus tietyin poikkeuksin tulla unohdetuksi eli saada henkilötietonsa poistetuksi

[76] HE 9/2018 vp, 29 – 30.

rekisteristä ilman aiheetonta viivytystä. Luonnollisella henkilöllä on oikeus virheellisten tietojensa oikaisuun sekä poistamiseen, mikäli tietojen säilyttäminen ei vastaa lainsäädännön vaatimuksia. Erityisesti tiedot tulee poistaa, kun niitä ei enää tarvita sitä käsittelytarkoitusta varten, joita varten ne kerättiin tai tapauksissa, joissa rekisteröity peruuttaa suostumuksensa. Myös lapsen asemaa vahvistetaan: oikeus koskee erityisesti tilanteita, joissa suostumus on annettu lapsena, ja rekisteröity haluaa myöhemmin poistaa tällaiset tiedot erityisesti internetistä. Rekisteröidyllä on oikeus saada myös henkilötietoihin liittyvät linkit tai näiden tietojen jäljennökset tai kopiot poistetuksi, ja rekisterinpitäjä edellytetäänkin - käytössä oleva teknologia ja toteutuskustannukset huomioiden - toteuttamaan kohtuulliset toimenpiteet ilmoittaakseen henkilötietoja käsitteleville rekisterinpitäjille rekisteröidyn poistopyynnöstä.

Oikeus tulla unohdetuksi ei kuitenkaan ole absoluuttinen. Mikäli tietojen säilytys perustuu lakisääteisen velvollisuuden noudattamiseen, yleistä etua koskevan tehtävän suorittamiseen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseen, tiedot voidaan säilyttää kyseistä tarkoitusta varten niin pitkään kuin laissa edellytetään.[77] Tietojen poisto aiheuttaa luonnollisesti uudenlaisia teknisiä vaatimuksia ja haasteitakin tietojärjestelmille. Ei ole selvää, että muihin tietosisältöihin liittyvää, järjestelmäteknisesti ajatellen kriittistä tietoa voidaan yksiselitteisesti poistaa muun tietosisällön eheyden kärsimättä. Myöskään tietojen massapoistot eivät välttämättä ole olleet organisaatioissa vakiintunut käytäntö.[78] Tietojen poistamisen sijaan ne voidaan mahdollisesti siirtää toiseen järjestelmään ja anonymisoida niin, ettei luonnollista henkilöä voida enää tiedon perusteella tunnistaa.

Henkilöllä on myös oikeus tietojensa oikaisemiseen, käsittelyn rajoittamiseen esimerkiksi oikaisu- ja poistopyynnön yhteydessä tai tietojensa käsittelyn vastustamiseen esimerkiksi suoramarkkinoinnin yhteydessä. Näistä löytyy lisätietoja tietosuoja-asetuksen artikloista 16, 18 ja 21. Mikäli henkilö pyytää tietojensa oikaisua, rajoittamista tai poistoa, tulee rekisterinpitäjän ilmoittaa pyynnöstä jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu, paitsi jos tämä osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa (ilmoitusvelvollisuus, artikla 19).

[77] Tietosuojavaltuutetun toimisto 2016.
[78] Tietosuojavaltuutetun toimisto 2015.

Rekisteröidyllä on pääsääntöisesti oikeus saada rekisterinpitäjälle toimittamansa, itseään koskevat henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa sekä oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle, jos käsittely perustuu suostumukseen tai jos käsittely suoritetaan automaattisesti. Oikeudesta siirtää tiedot järjestelmästä toiseen säädetään tietosuoja-asetuksen artiklassa 20. On huomioitava, että oikeutta sovelletaan vain tapauksissa, joissa käsittely perustuu suostumukseen tai sopimukseen. Sitä ei sovelleta julkishallinnossa, mikäli henkilötietojen käsittely perustuu yleistä etua koskevan tehtävän suorittamiseen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseen. WP29-tietosuojatyöryhmä on julkaissut ohjeet tietojen siirrosta joulukuussa 2016.[79]

Profilointia ja automatisoituja päätöksiä käsitellään laajasti tietosuoja-asetuksen artiklassa 22 sekä johdanto-osan kohdassa 71. Lähtökohtaisesti henkilöllä olisi oltava oikeus olla joutumatta henkilökohtaisia ominaisuuksiaan arvioivan, mahdollisesti toimenpiteen sisältävän päätöksen kohteeksi, joka on tehty yksinomaan automaattisen tietojenkäsittelyn perusteella, ja josta hänelle aiheutuu oikeudellisia vaikutuksia tai joka vaikuttaa häneen vastaavalla merkittävällä tavalla. Pääsääntöisesti rekisteröidyllä on siis oikeus vähintään vaatia, että tiedot käsittelee rekisterinpitäjän puolesta luonnollinen henkilö. Henkilötietojen erityisluokitteluun perustuva automaattinen päätöksenteko ja profilointi sallitaan kuitenkin, jos siihen annetaan nimenomainen lupa kansallisessa tai unionin lainsäädännössä tai jos henkilötietojen käsittely perustuu suostumukseen tai sopimukseen. Käsittelyyn tulee aina kohdistaa asianmukaisia suojatoimia; rekisteröidylle on ilmoitettava käsittelystä ja tällä on oikeus vaatia ihmisen osallistumista käsittelyyn. Profilointi edellyttää lähtökohtaisesti vaikutustenarvioinnin tekemistä.

Myös tietosuojavaltuutettu on julkaissut ohjeen, jossa selkiytetään automaattisen päätöksenteon ja profiloinnin käsitettä. Tietosuojavaltuutettu toteaa, että profiloinnin määritelmä riippuu luokittelun tarkoituksesta; jos käsittelyn tarkoituksena on arvioida henkilökohtaisia ominaisuuksia, voi kyse olla profiloinnista. Automaattinen päätöksenteko voi kohdistua minkälaiseen tietoon tahansa, ja se sisältää profiloinnin siltä osin, kun sillä on rekisteröityyn kohdistuvia oikeudellisia tai muuten merkittäviä vaikutuksia. Päätöksiä voidaan siis tehdä automaattisesti ilman profilointia, ja profilointia voidaan tehdä ilman

[79] WP29 2016.

automaattista päätöksentekoa. Riippuen tietojen käyttötavoista, käsittelytoiminto voi sisältää myös molempia. Tietosuojavaltuutettu korostaa, ettei automaattista päätöksentekoa voi kiertää näennäisellä ihmisosallisuudella, vaan osallistumiselta edellytetään aina merkityksellisyyttä päätöksen lopputuloksen kannalta.[80]

Tietosuoja-asetuksen 6 luvussa käsitellään laajasti rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksia ja vastuita, joita tässä työssä käsitellään vain tiivistetysti ja rajatusti. Rekisterinpitäjille tulevaa tiedustelujen ja oikaisu-, poisto- ja tietopyyntöjen määrää voidaan vain arvailla, mutta pyyntöihin on välttämätöntä varautua jo siirtymäaikana luomalla tarvittavat kanavat sekä määrämuotoset prosessit, resursoimalla työaikaa ja kouluttamalla tarvittava henkilöstö erilaisten pyyntöjen ja tiedustelujen käsittelyyn. Myös mahdolliseen sähköiseen asiointiin ja tunnistamiseen on hyvä varautua. Yksi suurimmista ja nopeimmin realisoituvista riskeistä sekä organisaatiolle että rekisteröidyn oikeuksille ja vapauksille onkin se, ettei tietopyyntöjä pystytä prosessien tai resurssien puuttumisen vuoksi joko ollenkaan tai riittävän nopeasti käsittelemään ja toimittamaan. Merkittävä riski on myös rekisteröityjen oikeuksien ja oikeusperusteiden hahmottamisen puute; jos tietoja poistetaan perusteetta laissa säädettyjen säilytysaikojen vastaisesti, voi tästä aiheutua sekä rekisterinpitäjälle että rekisteröidylle merkittäviä haittoja. Varsinkin julkisella sektorilla määrämuotoisen, hallitun prosessin ja henkilöstön koulutuksen merkitys korostuu.

2.3.5 Sopimukset henkilötietojen käsittelijöiden kanssa

Henkilötietojen käsittelijällä tarkoitetaan tietosuoja-asetuksen 4 artiklan mukaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun eli niin, ettei palveluntarjoajalla ole itsenäistä päätösvaltaa henkilötietojen säilytyksen ja käyttämisen suhteen. Henkilötietojen käsittelijä voi olla esimerkiksi sopimus- tai palvelutoimittaja, jolle henkilöstön palkanmaksu tai ittuki on ulkoistettu. Ulkoistamistilanteesta on erotettava ne tilanteet, joissa palveluntarjoaja itse toimii rekisterinpitäjänä tuottaessaan sovittua palvelua; on siis tapauskohtaisesti arvioitava, missä roolissa palvelutuottaja toimii.[81]

[80] Tietosuojavaltuutetun toimisto 2018a.
[81] Kuntaliitto 2017, 3.

Henkilötietojen käsittelijän asemasta ja velvollisuuksista säädetään tietosuoja-asetuksen 28 artiklassa ja sopimusten laatimisesta johdanto-osan kohdassa 81. Rekisterinpitäjä saa valita vain sellaisia henkilötietojen käsittelijöitä, jotka noudattavat hyvää henkilötietojen käsittelytapaa omassa toiminnassaan. Varmistuakseen tästä, rekisterinpitäjän tulee tehdä henkilötietojen käsittelijöiden kassa kirjalliset sopimukset, joissa määritellään mm. henkilötietojen käsittelyn kohde, tarkoitukset ja kesto, henkilötietojen tyyppi ja rekisteröityjen ryhmät sekä vastuut esimerkiksi tietojen luovutuspyyntöihin, käyttöoikeushallintaan, järjestelmiin liittyvien lokitietojen saatavuuteen ja tietojen siirtoihin tai henkilötietojen tietoturvaloukkauksista ilmoittamisiin liittyen. On hyvä myös sopia henkilötietojen käsittelijän velvollisuudesta auttaa vaikutustenarvioinnin laatimisessa sekä rekisterinpitäjän oikeudesta auditoida henkilötietojen käsittelijän suorittama henkilötietojen käsittely sekä näistä aiheutuvien kustannusten jakautumisesta. Sopimuksessa tulee erityisesti huomioida, että henkilötietojen käsittelijä käsittelee henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti (koskien pääsääntöisesti myös siirtoa kolmansiin maihin), joten rekisterinpitäjän tulee huolehtia siitä, että henkilötietojen käsittelijälle toimitetaan tai sillä on pääsy riittäviin ohjeisiin.

Tietojen käsittely on modernissa ICT-toimintaympäristössä laajasti verkottunutta. Rekisterinpitäjällä ei useinkaan enää ole kontrollia vastuullaan olevista henkilötiedoista, mutta se on kuitenkin vastuussa henkilötietojen käsittelystä. On siis rekisterinpitäjän intressi huolehtia myös tietosuojan huomioimisesta sopimuksissa.[82] On tärkeää, että vastuut ja vastuunrajoituslausekkeet määritellään riittävän yksityiskohtaisesti ja selkeästi. Pitkäkestoisissa sopimuksissa kannattaa varautua myös olosuhteiden muuttumiseen.[83] Kuntaliitto on julkaissut Henkilötietojen käsittelyn ehdot-sopimusliitemallin, jossa on huomioitu tietosuoja-asetuksen vaatimukset rekisterinpitäjän ja henkilötietojen käsittelijän vastuissa.[84] Laajasti lisätietoa löytyy myös erillisestä julkisiin hankintoihin tarkoitetusta opasmateriaalista.[85] Tietosuoja-asetuksen vaatimukset on huomioitu myös IT2018-ehdoissa, jotka sisältävät 10 sopimusehtoliitettä ja 9 sopimusmallia.[86] Luonnollisesti osapuolilla on käytössä laajasti myös omiin tarpeisiin räätälöityjä sopimusliitepohjia.

[82] Lång 2017, 134.
[83] Hemmo & Hoppu 2018.
[84] Kuntaliitto 2018.
[85] Kuntaliitto 2017.
[86] Teknologiainfo Teknova 2018.

Kysymys tietosuoja-asetuksen vaatimusten täyttävien (nk. GDPR-valmius, compliancy), järjestelmäteknisten muutoskustannusten jakautumisesta on mielenkiintoinen. Koska osoitusvelvollisuus tietosuoja-asetuksen noudattamisesta on viime kädessä rekisterinpitäjällä, tulee tällä olla laaja ymmärrys paitsi lainsäädäntövaatimuksista, myös organisaation sisäisestä tietojenkäsittelystä ja sen teknisistä vaatimuksista, jotta sopimuksissa voidaan huomioida juuri kyseisessä tietojenkäsittelyssä riittävät ja tarpeelliset keinot osoitusvelvollisuuden todentamiseksi. Sopimuksiin liittyy todellinen ja konkreettinen kustannusriski; it-palveluntarjoajat tarjoavat tällä hetkellä laajasti lisäpalveluja, jotka saattavat olla tai olla olematta oleellisia ja tarpeellisia ao. henkilötietojen käsittelyssä.

2.3.6 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen

Merkittävä uusi rekisterinpitäjän velvollisuus on ilmoittaa henkilötietojen tietoturvaloukkauksesta tietosuojaviranomaiselle ja rekisteröidylle. Ilmoitusvelvollisuudesta säädetään tietosuoja-asetuksen artikloissa 33 ja 34 ja sitä käsitellään laajasti johdanto-osan kohdissa 75 ja 85 – 88. Henkilötietojen tietoturvaloukkaus määritellään artiklassa 4: sillä tarkoitetaan loukkausta, jonka seurauksena on henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. Rekisterinpitäjän on tehtävä ilmoitus valvontaviranomaiselle aina, kun loukkauksesta todennäköisesti aiheutuu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuva riski. Ilmoitus on tehtävä mahdollisimman pian, viimeistään 72 tunnin kuluessa loukkauksen ilmitulosta. Mikäli aiheutuva riski on todennäköisesti korkea, tietoturvaloukkauksesta on ilmoitettava tietyin poikkeuksin myös rekisteröidylle ilman aiheetonta viivytystä. Henkilötietojen käsittelijän on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa.

Ilmoitus rekisteröidylle tulisi tehdä tiiviissä yhteistyössä valvontaviranomaisen kanssa noudattaen valvontaviranomaisen tai muiden asiaankuuluvien viranomaisten, esim. lainvalvontaviranomaisten antamia ohjeita. Myös tietosuojaviranomainen voi vaatia ilmoituksen tekemistä tai päättää, ettei sitä tarvitse tehdä. Ilmoituksessa tulisi kuvata henkilötietojen tietoturvaloukkauksen luonne sekä esittää suosituksia siitä, miten ao. luonnollinen henkilö voi lieventää sen mahdollisia haittavaikutuksia.

On huomioitava, ettei tietoturvaloukkauksesta kuitenkaan tarvitse ilmoittaa valvontaviranomaiselle tai rekisteröidylle, ellei siitä aiheudu riskiä rekisteröidylle. Ilmoitusta ei tarvitse tehdä rekisteröidylle, mikäli rekisterinpitäjä on toteuttanut asianmukaiset suojatoimet, esimerkiksi tietojen salauksen tai anonymisoinnin, joilla voidaan varmistaa, etteivät ao. tiedot ole ymmärrettävässä muodossa. Edelleen, ilmoitusta ei vaadita, kun rekisterinpitäjä on toteuttanut jatkotoimenpiteitä varmistaakseen, ettei rekisteröidyn oikeuksiin ja vapauksiin kohdistuva korkea riski enää todennäköisesti toteudu. Ilmoitusta ei myöskään tarvitse tehdä, mikäli siitä aiheutuisi kohtuutonta vaivaa, tätä arvioidaan tapauskohtaisesti riskien mukaan. Kaikki tietoturvaloukkaukset ja niihin liittyvät seikat, vaikutukset ja toteutetut korjaavat toimenpiteet on kuitenkin dokumentoitava, jotta valvontaviranomainen voi tarkistaa, onko ilmoitusvelvollisuutta noudatettu. Mikäli rekisterinpitäjä ei anna ilmoitusta 72 tunnin kuluessa siitä, kun tietoturvaloukkaus on tullut ilmi, sen on toimitettava tietosuojaviranomaiselle tästä perusteltu selitys.[87]

Ilmoitusvelvollisuuden aikaraja on tiukka. Usein tietoturvaloukkaus paljastuu vasta jälkikäteen jonkun muun kuin rekisterinpitäjän toimesta. Vaikka rekisterinpitäjän aikaraja alkaakin kulua vasta siitä, kun se saa tiedon tietoturvaloukkauksesta henkilötietojen käsittelijältä, on selvä, että se asettaa haasteita ilmoitusvelvollisuuden toteuttamiselle. Toisaalta se myös kannustaa huomioimaan ja toteuttamaan tietoturvaan ja -suojaan liittyviä prosesseja ja menetelmiä entistä tehokkaammin. Ilmoitusvelvollisuus edellyttää kykyä arvioida, minkä tasoinen riski tietoturvaloukkauksesta aiheutuu tietoturvaloukkauksen kohteena olleille henkilöille; tietosuojavaltuutettu on julkaissut ohjeet riskien arvioinnin tueksi.[88] Henkilötietojen tietoturvaloukkaus on merkittävä kustannus- ja maineriski jokaisen rekisterinpitäjän toiminnassa. Mahdollisen tietoturvaloukkauksen varalta onkin järkevää suunnitella jo ennalta prosessikuvaus ja toimintaohjeet, jotta vahingot voidaan minimoida ja toimintakykyisyys palauttaa tehokkaasti.[89]

2.3.7 Valvontaviranomaisen ja tietosuojavastaavan roolit

Tietosuoja-asetuksen myötä valvontaviranomaisen rooli vahvistuu. Kansallinen valvontaviranomainen vastaa kussakin EU-maassa asetuksen yhdenmukaisesta soveltamisesta

[87] Tietosuojavaltuutetun toimisto 2017a.
[88] Tietosuojavaltuutetun toimisto 2017a.
[89] Tietosuojavaltuutetun toimisto 2017b, 33.

ja sen valvonnasta. Valvontaviranomaisen tehtävät ja valtuudet määritellään artikloissa 57 ja 58; se antaa lähtökohtaisesti maksutonta ohjausta ja neuvontaa tietosuoja-asetuksen noudattamisesta ja oikeussuojakeinoista, mutta se voi myös antaa rekisterinpitäjälle tai henkilötietojen käsittelijälle varoituksen tai huomautuksen säännöstenvastaisista käsittelytoimista, määräyksen käsittelytoimien korjaamiseksi tai rekisteröidyn oikeuksien toteuttamiseksi tai asettaa väliaikaisen tai pysyvän käsittelykiellon.

Yksi keskeisistä uudistuksista on valvontaviranomaisen mahdollisuus tehostaa tietosuoja-asetuksen ja antamiensa suositusten noudattamista määräämällä merkittävä hallinnollinen sakko tilanteissa, joissa asetusta rikotaan. Hallinnollisten sakkojen määräämisestä viranomaiselle tai julkisella sektorilla voidaan säätää tarkemmin jäsenvaltion omassa lainsäädännössä hyödyntämällä kansallista liikkumavaraa. Hallituksen esityksessä tietosuojalaiksi on linjattu, ettei hallinnollisia seuraamusmaksuja määrättäisi koskemaan henkilötietojen käsittelyä esimerkiksi valtion tai kunnallisille viranomaisille.[90]

Tietosuojavastaavan nimittämisestä ja toimenkuvasta säädetään yksityiskohtaisesti artiklassa 37 ja johdanto-osan kohdassa 97, lisäksi WP29-tietosuojatyöryhmä on antanut tarkemmat ohjeet asetuksen tulkitsemiseksi. Tietosuojavastaava on henkilö, jolla on tietosuojalainsäädäntöä ja alan käytänteitä koskevaa erityisasiantuntemusta; hän auttaa rekisterinpitäjää toimimalla erityisasiantuntijana ja valvoo, että tietosuoja-asetusta noudatetaan henkilötietojen käsittelyssä. Tietosuojavastaavan nimittäminen on pakollista julkisella sektorilla (tuomioistuimet pois lukien) sekä silloin, kun rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät rekisteröityjen säännöllistä ja järjestelmällistä, laajamittaista seurantaa tai kun ydintehtävät muodostuvat laajamittaisesta, erityisiin henkilötietoryhmiin, rikostuomioihin tai rikkomuksiin kohdistuvasta käsittelystä. Tietosuojavastaava voidaan kuitenkin nimittää aina kun organisaatio kokee sen tarpeelliseksi. Tälläkin hetkellä tietosuojavastaavan nimittäminen on Suomessa pakollista sosiaali- ja terveydenhuollossa, apteekkitoiminnassa sekä Kansaneläkelaitoksen toiminnassa.[91]

[90] HE 9/2018 vp, 57.
[91] Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (2007/159) 20 §; laki sähköisestä lääkemääräyksestä (2007/61) 24 §

Tietosuojavastaavana voi toimia organisaation työntekijä osa-aikaisesti tai kokopäiväisesti tai palvelu voidaan ostaa organisaation ulkopuolelta. Yhtä lailla esimerkiksi konserni voi valita yhteisen tietosuojavastaavan. Tietosuojavastaava on työssään riippumaton, eikä hän saa ottaa vastaan ohjeita tehtäviensä suorittamiseksi. Häntä ei saa rangaista tai erottaa tietosuojavastaavan tehtävien hoitamisen vuoksi, ja hän raportoi suoraan rekisterinpitäjän tai käsittelijän ylimmälle johdolle. Tietosuojavastaavalla on tärkeä yhteistyörooli eri organisaatioiden ja oman organisaation eri yksiköiden välillä, ja hän toimii julkisena yhteyspisteenä valvontaviranomaisten ja rekisteröityjen suuntaan. Tietosuojavastaavalla on merkittävä rooli osoitusvelvollisuuden todentamisessa sekä vaikutustenarvioinnin laatimisessa.

Toisinaan tietosuojavastaavaksi valitaan nimellisesti henkilö, jolla ei ole tarvittavia resursseja tai kompetenssia tehtävän hoitamiseksi. Tietosuojavastaavaan liittyvä, merkittävä riski rekisterinpitäjälle on riittävien resurssien puuttuminen, joka voi johtaa viime kädessä lainsäädännön velvoitteiden rikkomiseen. On huomioitava, että rekisterinpitäjä tai henkilötietojen käsittelijä on organisaationa vastuussa tietosuoja-asetuksen noudattamisesta, ei siis yksittäinen tietosuojavastaava. Organisaation vastuulla on myös huolehtia siitä, että tietosuojavastaava voi hoitaa tehtäväänsä, hänet otetaan riittävän aikaisessa vaiheessa tietosuojakysymysten käsittelyyn ja varsinkin vaikutustenarviointiprosesseihin ja että hän saa riittävät resurssit – aikaa, koulutusta ja ulkopuolista tukea, taloudellisia resursseja ja tarvittaessa henkilöstöä – tehtäviensä noudattamiseksi.

2.4 Henkilötietojen suoja perustuslaillisesta näkökulmasta

Tässä luvussa on käyty läpi vaikutustenarvioinnin kannalta tärkeitä tietosuoja-asetuksen periaatteita ja muutoksia ja esitelty näihin liittyviä riskejä organisaation kannalta. Vaikutustenarvioinnin lähtökohtana on henkilötietojen käsittelystä luonnolliselle henkilölle aiheutuva todennäköinen ja korkea riski. Tässä kappaleessa riskejä ja vaikutuksia hahmotetaan perustuslaillisten oikeuksien ja tietosuoja-asetuksen periaatteiden näkökulmasta.

Tietosuoja-asetuksen johdanto-osien 1 ja 4 mukaan tietosuoja-asetuksen tarkoituksena on tukea luonnollisen henkilön perusoikeuksia ja -vapauksia sekä erityisesti oikeutta henkilötietojen suojaan. Henkilötietojen käsittely tulisi suunnitella ihmistä palvelevaksi. Oikeutta henkilötietojen suojaan tulisi tarkastella suhteessa sen tehtävään yhteiskunnassa ja

sen on oltava suhteessa myös muihin perusoikeuksiin. Oikeus tietosuojaan on kaikilla henkilöillä, joiden tietoja kerätään ja käsitellään, organisaation asiakkaiden lisäksi henkilökunnalla, esimerkkeinä työnhakijat, harjoittelijat, vapaaehtoiset, määräaikaiset tai entiset työntekijät, tai vaikkapa perheenjäsenillä.[92] Rekisteröidyn käsitettä tuleekin tarkastella laajasti.

Perusoikeudet ovat perustuslaissa säädettyjä, kaikille yksilölle yhdenvertaisesti kuuluvia oikeuksia, joille on ominaista erityinen pysyvyys ja oikeudellinen luonne. Ne toimivat oikeusjärjestyksen arvoperustana ja ovat hierarkkisesti tavallisia lakeja ylempänä. Perustuslaillisia oikeuksia on kunnioitettava niin julkisen vallan piirissä kuin lainsäädännössä.[93] Tietosuoja-asetuksen johdanto-osan kohdan 51 mukaan henkilötietoja, jotka ovat erityisen arkaluonteisia perusoikeuksien ja -vapauksien kannalta, on suojeltava erityisen tarkasti, noudattaen huolellisesti tietosuoja-asetuksen yleisiä periaatteita ja sääntöjä. Tällaisten tietojen käsittely on lähtökohtaisesti sallittu vain erityistapauksissa, esimerkiksi julkishallinnossa lakisääteisen velvoitteen noudattamiseksi, yleistä etua koskevan tehtävän suorittamiseksi, rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi tai rekisteröidyn antaman nimenomaiseen suostumukseen perustuen.

Yksityiselämän, kunnian ja kotirauhan suojasta sekä luottamuksellisen viestin salaisuudesta säädetään perustuslain 10 §:ssä. 10.2 §:n mukaan henkilötietojen käsittelystä säädetään tarkemmin lailla; yksityiselämän suoja sisältää siis myös henkilötietojen käsittelysäännökset.[94] Yksityiselämän suoja sisältyy myös Euroopan unionin perusoikeuskirjan (2012/C 326/02) artiklaan 8, jonka mukaan tietojen käsittelyn on oltava asianmukaista, sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn perusteen nojalla. Jokaisella on oikeus tutustua tietoihin, joita hänestä on kerätty ja saada ne oikaistuiksi.

Tietosuojan kannalta merkittäviä perustuslaillisia oikeuksia ovat myös

- syrjinnän kielto (PL 6§), jota voidaan tarkastella myös yhdenvertaisuussäännöksen kannalta. Ihmisiä tulee kohdella yhdenvertaisesti; samanlaisessa tilanteessa

[92] Lambert 2018, 170.
[93] Hallberg 2010.
[94] Viljanen 2011.

samalla tavalla. Syrjintää voi ilmetä varsinkin profiloinnin yhteydessä; mahdolliset väärät päätelmät tai virheet tausta-aineistossa voivat johtaa virheellisiin päätelmiin tai päätöksiin.

- oikeus elämään, henkilökohtaiseen vapauteen ja koskemattomuuteen (PL7 §). Henkilökohtainen koskemattomuus suojaa paitsi fyysistä vapautta, myös tahdonvapautta ja itsemääräämisoikeutta. Oikeuden elämään on katsottu sisältävän myös mm. velvollisuuden tutkia perusteellisesti kuolemaan johtaneet viranomaisoperaatiot ja muut tapahtumat;[95] tältä osin 7 § liittyy myös henkilötietojen käsittelyyn terveydenhuollossa. Lisäksi säännökseen liittyy myös oikeus henkilökohtaiseen turvallisuuteen.
- uskonnon ja omantunnon vapaus (PL 11 §). Siihen liittyy kiinteästi PL 6 §:ssä säädetty syrjinnän kielto, jonka mukaan ketään ei saa ilman hyväksyttävää syytä asettaa eri asemaan esimerkiksi uskonnon, vakaumuksen tai mielipiteen perusteella. Velvoite kohdella tasapuolisesti kaikkia uskonnollisia yhdyskuntia tai maailmankatsomuksellisia suuntauksia koskee erityisesti julkisen vallan käyttöä.[96] Tieto uskonnollisesta tai filosofisesta vakaumuksesta sisältyy tietosuoja-asetuksen mukaisesti erityisiä henkilötietoryhmiä koskevaksi käsittelyksi, joka on lähtökohtaisesti kielletty.
- sananvapaus ja julkisuus (PL 12 §). Viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat lähtökohtaisesti julkisia; jollei julkisuutta ole lailla erikseen rajoitettu, jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta. Sananvapauteen voidaan katsoa sisältyvän oikeus hankkia, välittää, valmistaa, ilmaista, julkaista, levittää ja vastaanottaa tietoja, mielipiteitä ja muita viestejä. Säännös on välineneutraali, sisältäen tekstin, äänen ja kuvallisen esityksen muodossa esitettävät viestit.[97] Tietosuoja-asetuksessa myös esimerkiksi video tai kuvatallenne on määritelty henkilötiedoiksi. Viranomaisen asiakirjat liittyvät henkilötietojen käsittelyyn niiltä osin kuin ne sisältävät henkilötietoja.
- kokoontumis- ja yhdistymisvapaus (PL 13 §) on yksi poliittisista perusoikeuksista[98] ja sallii jokaiselle oikeuden perustaa yhdistyksen, kuulua tai olla kuulu-

[95] Pellonpää 2009.
[96] Ojanen & Scheinin 2010.
[97] Manninen 2011.
[98] Tuori 2009.

matta yhdistykseen ja osallistua yhdistyksen toimintaan. Tietosuoja-asetuksen näkökulmasta perusoikeus vaikuttaa esimerkiksi erityisiin henkilötietoryhmiin kuuluvan poliittisen mielipiteen tai ammattiyhdistystiedon käsittelyrajoitukseen.

- oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä tuomioistuimessa tai muussa viranomaisessa (PL 21 §). Käsittelyn julkisuus sekä oikeus tulla kuulluksi, saada perusteltu päätös ja hakea muutosta samoin kuin muut oikeudenmukaisen oikeudenkäynnin ja hyvän hallinnon takeet turvataan lailla.

Myös hallituksen esityksessä henkilötietolaiksi rekisteröidyn oikeuksia lähestytään nimenomaan itsemääräämisoikeuden kautta; rekisteröidyllä on oikeus valvoa tietojensa käsittelyä ja laatua eli saada virheelliset tietonsa korjatuksi, tarkastaa tietonsa sekä tietyissä tilanteissa määrätä itseään koskevista tiedoista. Suostumuksen lisäksi rekisteröidyllä on kielto-oikeus eli oikeus kieltää henkilötietojensa käsittely esimerkiksi suoramarkkinointitarkoituksissa. Henkilötietojen käsittelystä voi siis aiheutua riski rekisteröidyn oikeuksille siinä tilanteessa, ettei hän saa toteutettua mainittua tarkastus- tai kielto-oikeuttaan.[99] Samoin voidaan ajatella yleisesti tietosuoja-asetuksen periaatteiden osalta; henkilötietojen käsittely vastoin lainsäädännön vaatimuksia rikkoo luonnollisen henkilön oikeuksia ja vapauksia.

Tällä hetkellä erittäin mielenkiintoinen myös tietosuoja-asetuksen periaatteisiin, rekisteröidyn oikeuksiin ja vapauksiin sekä profilointiin liittyvä tapaus on Facebook - Cambridge Analytica, jossa Facebook on tunnustanut vuotaneensa yhteensä jopa 87 miljoonan henkilön tiedot poliittista konsultointia tekevälle data-analyysiyhtiö Cambridge Analyticalle. Asiaton käyttö koskee Euroopan tasolla 2,7 miljoonan ja Suomessa 20 000 henkilön tietoja. Tietoja on hyödynnetty mm. Brexit-kampanjointiin sekä Yhdysvalloissa Donald Trumpin presidentinvaalikampanjointiin. Facebook on juuri julkaissut sovelluksessaan informoinnin, jossa käyttäjä saa tarkemmat tiedot henkilötietojensa käyttöön ja luovutuksiin liittyen. Käyttäjät voivat kieltää esimerkiksi julkaistujen kuvien ja videoiden kasvojentunnistuksen. Tapaus on herättänyt laajaa keskustelua tietosuojasta sekä informoinnin

[99] HE 96/1998 vp, 6 – 7.

läpinäkyvyydestä. Negatiivisesta julkisuudesta huolimatta Facebook on pystynyt kasvattamaan tulostaan vuoden 2018 ensimmäisellä kvartaalilla.[100] Tämä huomioiden voidaan kohtuullisesti ajatella, etteivät palvelujen käyttäjät käytännössä riittävästi ymmärrä henkilötietojen käsittelyn monimuotoisuutta tai hahmota, mihin palvelujen käytön yhteydessä suostuvat. Se ei kuitenkaan saa johtaa henkilötietojen lainvastaiseen käsittelyyn.

Alla olevaan taulukkoon 2 on koostettu esimerkkejä tietosuoja-asetuksen periaatteista ja niihin liittyvistä perustuslaillisista lainkohdista sekä periaatteeseen liittyviä riskejä ja vaikutuksia luonnollisen henkilön oikeuksiin ja vapauksiin. Viimeisessä sarakkeessa esitetään huomioita rekisterinpitäjälle. Taulukko on esimerkinomainen katsaus mahdollisista vaikutuksista, joiden lisäksi useisiin oikeuksiin kohdentuu merkittäviäkin rajauksia tietosuoja-asetuksessa.

TAULUKKO 2. Tietosuoja-asetuksen periaatteet, riskivaikutukset ja huomiot rekisterinpitäjälle.

Tietosuoja-asetuksen periaate sekä perustuslaillinen oikeusperiaate	**Mahdollinen riski ja vaikutus luonnollisen henkilön oikeuksiin ja vapauksiin**	**Huomioita rekisterinpitäjälle**
Käsittelyn lainmukaisuus (esimerkiksi suostumus, sopimus, lakisääteinen velvoite tai julkisen vallan käyttö) ja kohtuullisuus Tietosuoja-asetuksen artiklat 5, 6 PL 10 §	Kerätään ja käsitellään tietoa ilman laillista perustetta tai suostumus ei ole vapaaehtoinen. Rekisteröidyn kontrolli omiin tietoihinsa heikkenee ja mahdollisuus pyytää, oikaista tai poistaa henkilötietonsa estyy.	Henkilötietoja käsitellään vain jos käsittelyn tarkoitusta ei voida muuten kohtuullisesti toteuttaa. Käsittelylle tulee olla oikeudellinen peruste. Suostumuksen osalta huomioidaan sen vapaaehtoisuus, selkeys ja yksinkertainen kieli. Suostumus tulee pystyä todentamaan ja perumaan, ja perumisen on oltava yhtä helppoa kuin suostumuksen antaminen.

[100] Seuraa uutisointia esimerkiksi https://yle.fi/uutiset/18-274254, https://www.bbc.co.uk/search?q=facebook+cambridge ja https://search.cnbc.com/rs/search/view.html?source=CNBC.com&categories=exclude&partnerId=2000&keywords=FACEBOOK%20CAMBRIDGE.

Tietosuoja-asetuksen periaate sekä perustuslaillinen oikeusperiaate	Mahdollinen riski ja vaikutus luonnollisen henkilön oikeuksiin ja vapauksiin	Huomioita rekisterinpitäjälle
Käsittelyn ja informoinnin läpinäkyvyys Tietosuoja-asetuksen artiklat 5, 12 - 15 sekä 21 PL 10 §, PL 21 §	Informointi tai seloste henkilötietojen käsittelystä puuttuu tai on puutteellinen, epäselvä tai vaikeaselkoinen. Henkilö ei saa tietoa henkilötietoihinsa liittyvistä käsittelyperusteista, riskeistä, säännöistä, suojatoimista tai oikeuksistaan, jolloin hän ei myöskään pysty arvioimaan henkilötietojensa käsittelyn oikeutusta.	Luodaan menetelmä ja kanava rekisteröidyn informoimiseksi; informoinnissa huomioidaan käsittelyyn liittyvät riskit, säännöt, suojatoimet sekä rekisteröidyn oikeudet sekä ohjeistus siitä, miten rekisteröidyt voivat käyttää oikeuksiaan. Huomioidaan viestinnässä helppo saatavuus sekä selkeä ja ymmärrettävä kieli, erityisesti kun kyseessä ovat lasten tai muulla tavoin heikossa asemassa olevien henkilötietojen käsittely. Luodaan tietopyyntömallit ja prosessi tietopyyntöjen, oikaisupyyntöjen ja tiedustelujen käsittelemiseksi, huomioidaan prosessissa myös rekisteröityjen tunnistaminen sekä sähköinen asiointi.
Käyttötarkoitussidonnaisuus ja myöhempi käsittely Tietosuoja-asetuksen artiklat 5, 6 PL 10 §, PL 11 §	Tietoja käsitellään muuhun kuin siihen tarkoitukseen, jota varten ne on kerätty. Rekisteröidyn kontrolli omiin tietoihinsa heikkenee ja mahdollisuus pyytää, oikaista tai poistaa henkilötietonsa estyy. Mahdollinen automaattinen päätöksenteko ja profilointi tai tietojen luovutus käyttötarkoitukseen nähden erilaisiin käyttötarkoituksiin saattaa aiheuttaa syrjintää.	Selvitetään alkuperäisen käsittelyn laillisuutta koskevat vaatimukset ja käyttötarkoitukset. Tietoja myöhemmin hyödynnettäessä huomioidaan käsittelyn tarkoitusten väliset yhteydet sekä myöhemmän käsittelyn seuraukset rekisteröidyille ja asianomaisten suojatoimien olemassaolo sekä alkuperäisessä että suunnitellussa käsittelyssä. Tietojen luovutuksissa rajataan sopimusehdoilla tietojen myöhemmästä käytöstä. Tiedon salaaminen tai pseudonymisointi, mikäli tietoja halutaan myöhemmin käyttää esim. tilastointitarkoituksiin.
Käsittelyn rajoittaminen välttämättömään ja oikeasuhtaiseen (tietojen minimointi) Tietosuoja-asetuksen artiklat 5, 6, 10, 22, 39 PL 10 §	Kerätään liikaa tietoa suhteessa käyttötarkoitukseen, esimerkiksi mahdollisia tulevaisuuden tarpeita varten. Kontrolli omiin tietoihin heikkenee. Mikäli tietoja myöhemmin luovutetaan tai yhdistetään toisiin tietosisältöihin, kertyvät rekisteröidystä laajat ja kattavat tiedot, joita tämän on lähes mahdotonta valvoa.	Tiedot säilytetään muodossa, josta rekisteröity on tunnistettavissa vain niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Selvitetään lakisääteiset tietojen säilytysajat ja asetetaan määräajat henkilötietojen (massa)poistoon; ei säilytetä tietoja pidempään kuin tarpeellista. Varmistetaan henkilötietojen asianmukainen turvallisuus ja luottamuksellisuus (esim. pääsynhallinta).

Tietosuoja-asetuksen periaate sekä perustuslaillinen oikeusperiaate	Mahdollinen riski ja vaikutus luonnollisen henkilön oikeuksiin ja vapauksiin	Huomioita rekisterinpitäjälle
Täsmällisyys; tietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä Tietosuoja-asetuksen artiklat 5 ja 16 PL 10 §, PL 21 §	Rekisteri tai osarekisteri sisältää vanhentuneita, epätarkkoja tai virheellisiä tietoja. Virheet rekisterissä voivat estää tai vaikeuttaa rekisteröidyn asian käsittelyä tai johtaa rekisteröityä koskeviin virheellisiin päätöksiin. Esimerkiksi virheelliset tiedot luottotiedoissa voivat estää lainan tai osamaksun saannin, tai virheellinen terveystieto johtaa vääriin hoitopäätöksiin terveydenhuollon tai sairaanhoidon palveluissa.	Oikaisulle ja poistolle luodaan määrämuotoinen prosessi ja menetelmät näiden käsittelemiseksi. Rekisteröidylle informoidaan mahdollisuudesta ja oikeasta kanavasta selvästi. Virheelliset henkilötiedot oikaistaan tai poistetaan viipymättä. Tarpeettomat tai ilmeisen vanhat tiedot poistetaan tarvittaessa myös massapoistoilla.
Säilytyksen rajoittaminen; tietoja saa säilyttää vain rajoitetun ajan muodossa, josta henkilö on tunnistettavissa (pl. tieteelliset tai historialliset tutkimustarkoitukset) Tietosuoja-asetuksen artiklat 5, 6, 9, 21, 25, 89 PL 10 §, PL 21 §	Tietoa säilytetään perusteetta tunnistettavassa muodossa liian pitkiä aikoja tai ei poisteta lainkaan rekisteristä. Rajoittaa henkilön mahdollisuutta kontrolloida tietojaan ja käyttää oikeuksiaan, kuten oikeutta tulla unohdetuksi.	Tietoja saa säilyttää vain rajoitetun ajan muodossa, josta henkilö on tunnistettavissa (pl. tieteelliset tai historialliset tutkimustarkoitukset, arkistointi, tilastointi). Keinoja säilytyksen rajoittamiseen ovat esimerkiksi siirtäminen toiseen käsittelyjärjestelmään, käyttäjien pääsyn estäminen valittuihin henkilötietoihin tai julkaistujen tietojen väliaikainen poistaminen verkkosivustolta.
Eheys ja luottamuksellisuus; henkilötietojen turvaaminen ja suojaaminen luvattomalta tai lainvastaiselta käytöltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta Tietosuoja-asetuksen artikla 5 PL 10 §	Tietoja päätyy ulkopuolisille tai niitä ei ole lainkaan saatavilla. Katso myös taulukko 1 kappaleessa Rekisterinpitäjän uhkamaisema. Loukkaa yksityisyyden suojaa ja saattaa estää rekisteröityä toteuttamasta oikeuksiaan ja vapauksiaan. Mikäli tietoa ei ole saatavilla, ei rekisteröity saa vastinetta tietopyyntöönsä.	Rajoitetaan henkilötietojen käsittely siihen, mikä on ehdottoman välttämätöntä ja oikeasuhtaista. Toteutetaan riittävät tekniset ja organisatoriset suojatoimet, esimerkiksi salaus, pääsynhallinta ja roolipohjaiset käyttöoikeudet järjestelmiin sekä lokien hallinta. Mahdolliset auditointien ja käytännesääntöjen toteutus. Henkilötietojen tietoturvaloukkauksen osalta laaditaan selkeä prosessi.

Tietosuoja-asetuksen periaate sekä perustuslaillinen oikeusperiaate	Mahdollinen riski ja vaikutus luonnollisen henkilön oikeuksiin ja vapauksiin	Huomioita rekisterinpitäjälle
Osoitusvelvollisuus; tietosuoja-asetuksen noudattamisen osoittaminen. Osoitusvelvollisuuden merkitys korostuu riskiperusteisessa lähestymistavassa. Tietosuoja-asetuksen artikla 5	Osoitusvelvollisuus liittyy välittömästi lähinnä rekisterinpitäjän tai henkilötietojen käsittelijän ja valvontaviranomaisen suhteeseen. Välillisesti osoitusvelvollisuus kytkeytyy rekisteröityyn tietosuojaviranomaisen kautta, joka viime kädessä osoitusvelvollisuuden todentamisen eli erilaisen dokumentaation perusteella tekee päätöksen henkilötietojen käsittelyn asianmukaisuudesta esimerkiksi tapauksissa, joissa rekisteröity kääntyy tietosuojaviranomaisen puoleen oikeuksiensa toteuttamiseen tai henkilötietojensa käsittelyyn liittyen.	Henkilötietojen suojatoimenpiteet suhteutetaan henkilötietojen käsittelystä aiheutuvan riskin mukaiseksi. Yleinen dokumentointivelvoite korostuu; auditoinnit, käytännesäännöt, organisaation sisäiset ohjeet, politiikat, prosessit, vuosikello, raportit, tietoturvaloukkaukset. Voitava osoittaa, että suojaustoimet ovat oikeasuhtaiset käsittelyyn liittyviin riskeihin nähden. Ei koske rekisteröidyn oikeuksia; ne on toteutettava riskeistä riippumatta.

2.5 Havaitut haasteet ja johtopäätökset lyhyesti

Tietosuoja-asetuksen tavoitteena on parantaa rekisteröityjen oikeussuojaa ja elinkeinoelämän toimintaedellytyksiä sekä varmistaa velvoitteiden noudattaminen yhdenmukaisella sääntelyllä ja valvonnalla.[101] Kuten edellä on todettu, vaatimukset aiheuttavat rekisterinpitäjän ja henkilötietojen käsittelijän toiminnoissa laajoja teknisiä ja hallinnollisia velvoitteita tietosuoja-asetuksen noudattamiseksi ja noudattamisen todentamiseksi. Vaikka tietosuojalainsäädännön yhdenmukaistamisen on yleisesti ottaen arvioitu tuovan huomattavat säästöt yritysmaailmalle, sen noudattaminen aiheuttaa myös merkittäviä välittömiä (administrative burden) ja välillisiä (compliance costs) kustannuksia. Välittöminä kustannuksina voidaan nähdä esimerkiksi tietosuojavastaavan nimittämisestä tai henkilötietojen tietoturvaloukkauksesta ilmoittamisesta aiheutuvat kulut ja välillisinä kustannuksina esimerkiksi riskienhallinnasta ja hallinnollisista sakoista aiheutuvat kulut.[102] On kuitenkin huomioitava, että uusien velvoitteiden lisäksi tai ohella lainsäädäntöuudistus tuo myös organisaation sille toiminnan tasolle, jolla sen olisi jo nykylainsäädäntö huomioiden pitänyt olla. Mitä hajanaisempaa tai jäsentymättömämpää henkilötietojen käsittely on ollut, sitä enemmän työtä lainsäädäntöuudistus organisaatiossa aiheuttaa.

[101] HE 9/2018 vp, 64.
[102] Euroopan komissio 2012, 71; Valtioneuvosto 2017.

Riskien tunnistamisen ja vaikutustenarviointien kannalta on tärkeää ymmärtää tietosuoja-asetuksen periaatteita ja velvoitteita sekä rekisteröidyn oikeuksia ja näihin liittyviä hallinnollisia tarpeita. Näistä johtuvat puutteet ja epäselvyydet aiheuttavat merkittäviä riskejä varsinkin tietosuoja-asetuksen soveltamisen alkuvaiheessa. Lähtökohta riskien arvioinnille on tunnistaa omat toiminnot ja prosessit, toiminnassa käytettävät tietojärjestelmät ja näiden sisältämät henkilötiedot sekä tietoturvaan ja sopimuksiin liittyvät menettelyt ja erityispiirteet. Yhtä tärkeää on tunnistaa tietosuoja-asetuksen tarkentuneet määritelmät. Henkilötietoa ovat myös kuva, ääni- tai videotallenne, testidata sekä varmuuskopiot ja henkilötiedon käsittelyä myös tiedon haku ja katselu sekä tulosteilta että tietojärjestelmissä. Henkilötietolaista tuttua loogisen rekiterin käsitettä sovelletaan edelleen; rekisterin määrittelee siis henkilötietojen käsittelyperuste, ei esimerkiksi tietojärjestelmä tai käsittelyn menetelmä.

3 VAIKUTUSTENARVOINTI (DPIA)

3.1 Määritelmä ja oikeusperuste

Tietosuojaa koskevasta vaikutustenarvioinnista säädetään tietosuoja-asetuksen 35 artiklassa ja siihen annetaan laajasti tarkentavaa ohjeistusta johdanto-osan kohdissa 75, 84, 89 - 93 ja 95. Lisäksi WP29-tietosuojatyöryhmä on antanut ohjeet erityisesti siitä, missä tilanteissa vaikutustenarviointi täytyy tai ei tarvitse tehdä. 35 artiklan mukaan,

> – – jos tietyntyyppinen käsittely etenkin uutta teknologiaa käytettäessä todennäköisesti aiheuttaa – käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen – luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin, rekisterinpitäjän on ennen käsittelyä toteutettava arviointi suunniteltujen käsittelytoimien vaikutuksista henkilötietojen suojalle.

Vaikutustenarviointia ei ole varsinaisesti määritelty tietosuoja-asetuksessa, mutta WP29-tietosuojatyöryhmän ohjeessa vaikutustenarviointia kuvataan sen sisällön kautta ja antamalla lisäselvitystä luonnollisen henkilön oikeuksiin ja vapauksiin.

> Vaikutustenarvioinnin avulla on tarkoitus kuvata henkilötietojen käsittelyä, arvioida sen tarpeellisuutta ja oikeasuhteisuutta sekä tukea luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvien henkilötietojen käsittelystä aiheutuvien riskien hallintaa arvioimalla riskit ja määrittelemällä toimenpiteet, joilla niihin puututaan. – – Oikeuksilla ja vapauksilla tarkoitetaan ensisijaisesti oikeutta tietosuojaan ja oikeutta yksityisyyteen, mutta se voi käsittää myös muita perusoikeuksia, esimerkiksi sananvapauden, ajatuksenvapauden, liikkumisvapauden, syrjintäkiellon, oikeuden vapauteen sekä omantunnon ja uskonnon vapauden.[103]

Vaikutustenarviointi on siis prosessi, jossa rekisterinpitäjä velvoitetaan yhdessä tietosuojavastaavan ja henkilötietojen käsittelijöiden kanssa arvioimaan henkilötietojen käsittelyä ja sen tarpeellisuutta suhteessa käsittelystä aiheutuviin riskeihin ja luonnollisen henkilön oikeuksiin ja vapauksiin kohdistuviin riskivaikutuksiin. Vaikutustenarviointia ei tule sekoittaa yleiseen riskienhallintamenettelyyn, jossa riskejä arvioidaan organisaation näkökulmasta[104], vaikkakin tietosuojariskien ottaminen osaksi organisaation yleistä riskienhallintamenettelyä on suositeltavaa ja auttaa tuomaan myös näitä riskejä paremmin johdon tietoisuuteen. Vaikutustenarviointi on olennainen osa tietosuoja-asetusta ja sen noudattamista silloin, kun henkilötietojen käsittelyyn liittyy rekisteröidyn kannalta korkea

[103] WP29 2017b, 4, 7.
[104] Bieker, Friedewald, Hansen, Obersteller & Rost 2016, 24.

riski. Sen tavoite on sisäänrakennetun tietosuojan toteutuminen sekä prosesseissa, palveluissa että järjestelmissä.[105] Vaikutustenarvioinnin laatiminen auttaa rekisterinpitäjää noudattamaan tietosuoja-asetuksen vaatimuksia, mutta sen lisäksi se toimii osoitusvelvollisuuden todentamisen välineenä.[106]

Tietosuojaa koskeva vaikutustenarviointi tehdään suunnitteluvaiheessa olevalle järjestelmälle, sovellukselle, palvelulle tai hankkeelle, jossa tullaan käsittelemään henkilötietoja. Arviointi tulee tehdä mahdollisimman aikaisessa vaiheessa ja kartoituksen tulokset dokumentoida määrämuotoisesti.[107] Vaikutustenarvioinnin laatiminen osana tietojärjestelmän suunnittelu- ja testausprosessia tai ennen projektin hyväksymistä toteutukseen mahdollistaa sen, että ainakin osa riskeistä huomataan ja voidaan joko estää tai ainakin lieventää jo ennen varsinaisen käsittelytoimen aloittamista. Tällöin myös muutoksista tai lieventämistoimista aiheutuvat kustannukset ovat pienemmät.[108] Vaikutustenarviointia tulisi myös päivittää hankkeen koko elinkaaren ajan. Tietyntyyppisissä käsittelytoimissa, esimerkiksi työntekijöiden valvonnan ja seurannan aloittamisen yhteydessä, rekisterinpitäjän on pyydettävä myös rekisteröityjen tai näiden edustajien näkemyksiä.[109]

Myös jo käytössä olevista käsittelytoimista tulee pääsääntöisesti tehdä vaikutustenarviointi, kun ne todennäköisesti aiheuttavat korkean riskin luonnollisen henkilön oikeuksille ja vapauksille ja kun niiden sisältämä riski on käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioiden muuttunut. Vaikutustenarviointia ei voi lykätä tai jättää tekemättä sillä perusteella, että käsittely on jo alkanut ja sitä täytyy sen jälkeen päivittää.[110] Kauppakamarin julkaisemassa teoksessa *Henkilötietojen käsittely - EU:n tietosuoja-asetuksen vaatimukset* tulkitaan, ettei vaikutustenarviointia tarvitsisi tehdä, jos käsittelyyn on saatu tietosuojalautakunnan lupa tai jos henkilötietojen käsittelystä on ilmoitettu tietosuojavaltuutetulle, eivätkä käsittelyn riskit ja käytettävä teknologia ole muuttuneet.[111]

Vaikutustenarviointi koskee lähtökohtaisesti vain yhtä tiedonkäsittelytointa. Tietosuoja-asetuksen johdanto-osan kohdan 92 mukaan yhteisen arvioinnin laatiminen voi kuitenkin olla järkevää ja taloudellista esimerkiksi tilanteissa, joissa käsittelyn luonne, asiayhteys,

---

[105] Wright & Raab 2014, 278 – 279; Viemerö 2017.
[106] WP29 2017b, 4.
[107] Valtiovarainministeriö 2016, 21.
[108] Lambert 2018, 327.
[109] WP29 2017b , 17.
[110] WP29 2017b, 15, 17.
[111] Hanninen, Laine, Rantala, Rusi, & Varhela 2017.

tarkoitus ja riskit ovat samankaltaisia, esimerkiksi kun suunnitellaan viranomaisen toiminnassa tai julkishallinnossa yhteistä sovellusta tai käsittelyalustaa tai otetaan käyttöön yhteistä sovellusta useamman rekisterinpitäjän toiminnassa. Yhteisrekisterinpitäjien toiminnassa eli silloin, kun useampi rekisterinpitäjä vastaa samasta henkilörekisteristä, korostuu riskien käsittelemiseksi ja minimoimiseksi asetetuista vastuista sopiminen.[112]

Samaa teknistä tuotetta, laitetta tai ohjelmaa käyttävien rekisterinpitäjien tulee tehdä vaikutustenarviointi oman käsittelyprosessinsa osalta, mutta tuotteen toimittajan tekemästä vaikutustenarvioinnista voisi olla hyötyä myös rekisterinpitäjälle.[113] Käytännössä ajatus toimittajien tekemästä vaikutustenarvioinnista saattaa olla ristiriitainen. Jos tuotteen tai palvelun tarjoaja sijaitseekin kolmannessa maassa, ei tietosuoja-asetuksessa määritellyt vaatimukset vaikutustenarvioinnista velvoita toimittajaa. Tällöin rekisterinpitäjää voisi palvella paremmin yhdenmukaiset vaatimukset täyttävä sertifiointi.[114]

WP29-tietosuojatyöryhmän ohjeessa korostetaan yhteistyön merkitystä, mutta käytännössä jokainen rekisterinpitäjä vastaa kuitenkin vaikutustenarvioinnin laatimisesta itsenäisesti. Parhaaseen ja kattavimpaan tulokseen voitaisiin päästä laatimalla esimerkiksi tietojärjestelmään tai sovellukseen liittyen yksi yhteinen vaikutustenarviointi yhteistyössä rekisterinpitäjän, henkilötietojen käsittelijän ja palvelutoimittajien kanssa. Näin voitaisiin kartoittaa ja huomioida sekä tietojärjestelmissä, käyttöympäristössä että henkilötiedon käsittelyprosesseissa ilmenevät tarpeet ja vaatimukset sekä asiakas- että toimittajanäkökulmasta.[115] Varsinkin julkishallinnossa, jossa käsittelytoimet ovat pitkälti samanlaisia ja kustannusvaikutukset kohdistuvat yhteiskuntaan, voitaisiin pohtia vaikutustenarviointien osittaista yhteiskäyttöä ja hyödyntämistä, huomioiden kunkin organisaation kannalta salassa pidettävät asiat. Konkreettista tukea tietosuoja-asetuksesta, WP29-tietosuojatyöryhmän materiaaleista tai kansallisesta ohjauksesta ei vielä tällä hetkellä ole olemassa. Ajatus DPIA-rekisteristä on kuitenkin mielenkiintoinen.

[112] WP29 2017b, 8 – 9.
[113] WP29 2017b, 9.
[114] Paakkari 2018.
[115] Paakkari 2018.

Kansainvälisesti yksityisyyden suojan riskejä on arvioitu PIA (Privacy Impact Assessment) -arvioinnein[116] jo ennen kuin tietosuoja-asetuksen mukaisesta vaikutustenarvioinnista on säädetty.[117] PIA:ssa vaikutustenarviointi kohdistuu rekisteröidyn yksityisyyteen liittyviin riskeihin, kun taas tietosuoja-asetuksen mukainen vaikutustenarviointi on joidenkin arvioiden mukaan suppeampi konsepti, jossa keskitytään vaatimustenmukaisuuteen ja tiedon suojaamiseen.[118] Tätä tulkintaa tukee määritelmä, jonka mukaan henkilötietojen suoja on osa yksityisyyden suojan kokonaisuutta.[119] Toisaalta taas eroa vaikutustenarviointien ja PIA-arviointien välillä ei tehdä.[120] Jos vertailua tehdään punnitsemalla rekisteröidyn yksityisyyden suojaa ja henkilön oikeuksille ja vapauksille aiheutuvia riskivaikutuksia, on jälkimmäinen laajempi, jolloin riskivaikutuksia tulisikin pohtia laajemmin kuin vain yksityisyyden suojan kannalta. Vaikutustenarvioinnin merkitys ja sisältö aiheuttaa epätietoisuutta; tietosuojaviranomaisen ohjeet ja käytännesäännöt todennäköisesti selkiyttävät jatkossa mahdollista rajausta ja sisältövaatimuksia.

3.2 Milloin vaikutustenarviointia ei tarvitse tehdä?

WP29-tietosuojatyöryhmä katsoo, ettei tietosuojaa koskevaa vaikutustenarviointia vaadita sellaisen käsittelyn osalta

1. jonka yhteydessä ei katsota, että se ”todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin”.
2. jossa hyvin samankaltaiseen käsittelyn liittyen on jo tehty vaikutustenarviointi, huomioiden käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset. Tällaisissa tapauksissa voidaan käyttää jo laaditun vaikutustenarvioinnin tuloksia.
3. jossa valvontaviranomainen on tarkastanut käsittelytoimet ennen toukokuuta 2018, eivätkä olosuhteet ole muuttuneet.
4. kun käsittelytoimella on tietosuoja-asetuksen 6 artiklan 1 kohdan c (lakisääteisen velvoitteen noudattaminen) tai e (yleinen etu tai julkisen vallan käyttö) nojalla oikeusperuste EU:n oikeudessa tai jäsenvaltion lainsäädännössä ja jos tietosuojaa koskeva vaikutustenarviointi on jo tehty kyseisen käsittelyn oikeusperusteen määrittämisen yhteydessä.

---

[116] ICO 2014; CNIL 2017.
[117] Bieker ym. 2016, 22.
[118] Viemerö 2017; Herold n.d.
[119] Neuvonen. 2014; Pitkänen ym. 2013, 15.
[120] Lambert 2018, 218.

5. jossa käsittely sisältyy valvontaviranomaisen laatimaan vapaaehtoisuuden periaatteeseen perustuvaan luetteloon käsittelytoimista. Tällainen luettelo voi sisältää kyseisen viranomaisen määrittelemien ehtojen mukaisia käsittelytoimia. Tällaista luetteloa ei tätä listaa lukuun ottamatta ole vielä julkaistu.

Rekisterinpitäjä vastaa henkilötietojen käsittelystä ja tietosuojan huomioimisesta paitsi yleiseen riskiperusteiseen lähestymistapaan perustuen, myös harkitessaan, onko sen tehtävä vaikutustenarviointi vai ei. On huomioitavaa, ettei vaikutustenarviointi ole pakollinen, ellei riski luonnollisen henkilön oikeuksille ja vapauksille ole todennäköinen ja korkea. Toisaalta saattaa olla myös tilanteita, joissa käsittely ei ole laajamittaista, mutta yrittäjä käsittelee esimerkiksi turvakiellon alaista tai erityisiin henkilötietoryhmiin liittyvää henkilötietoa havaitsematta siihen liittyviä riskejä. Myös näissä tapauksissa olisi tärkeää, että tietoturva- ja tietosuojariskit kartoitetaan ja riskien lieventämistoimet toteutetaan.[121] WP29-tietosuojaryhmä suositteleekin vaikutustenarvioinnin tekemistä tilanteissa, joissa sen tarpeellisuus ei ole selvää; tämä auttaa rekisterinpitäjää noudattamaan tietosuojalainsäädäntöä.[122]

3.3 Milloin vaikutustenarviointi tulee tehdä?

Tietosuoja-asetuksen 35 artiklassa sekä johdanto-osan kohdissa 71, 75 ja 91 annetaan esimerkkejä siitä, missä tapauksissa vaikutustenarviointia erityisesti vaaditaan. WP29-tietosuojatyöryhmän ohjeessa vaikutustenarviointiin esitetään myös esimerkkejä käsittelytoimista, jotka todennäköisesti aiheuttavat – käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset huomioon ottaen – luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin. Alla oleva listaus perustuu WP29-tietosuojatyöryhmän ohjeistukseen.[123]

Todennäköinen, korkea riski voi aiheutua tilanteissa, joissa

1. on kyse luonnollisten henkilöiden henkilökohtaisien ominaisuuksien arvioinnista tai pisteytyksestä, esimerkiksi profiloinnista tai ennakoinnista. Esimerkkeinä käsittelytoimista ovat työsuorituksen, taloudellisen tilanteen, terveyden, mieltymyk-

[121] Paakkari 2018.
[122] WP29 2017b, 9.
[123] WP29 2017b, 10 – 12.

sen tai kiinnostuksen kohteen, luotettavuuden tai käyttäytymisen, sijainnin tai liikkumisen arviointi tai pisteytys, geenitestien tarjoaminen kuluttajille sairaus- tai terveysriskien arvioimiseksi, käyttäytymis- tai markkinointiprofiilien luominen yrityksen verkkosivuston käytön tai sillä liikkumisen perusteella tai some-kanavien julkisten tietojen kerääminen profiilien laatimiseksi.

2. on kyse automaattisesta päätöksenteosta, jolla on oikeusvaikutuksia tai vastaavia merkittäviä vaikutuksia ja jotka voivat mahdollisesti johtaa syrjintään. Automaattinen päätöksenteko saattaa sisältää profiloinnin.
3. on kyse järjestelmällisestä valvonnasta: rekisteröityjen tarkkailuun, seurantaan tai valvontaan käytettävästä tietojenkäsittelystä tai tietojen keräämisestä verkkojen välityksellä tai yleisölle avoimen alueen järjestelmällisestä valvonnasta, esimerkiksi kameravalvonnasta tai henkilöstön työasema- tai internetkäytön järjestelmällisestä seurannasta.
4. käsitellään laajamittaisesti arkaluonteisia tai erityisiin henkilötietoryhmiin kuuluvia tietoja (aik. arkaluonteiset tiedot sekä geneettiset ja biometriset tiedot) tai rikostuomioita tai rikkomuksia koskevia tietoja. Erityisistä henkilötietoryhmistä säädetään artiklassa 9, rikostuomioihin ja rikkomuksiin liittyvien tietojen käsittelystä artiklassa 10. Esimerkkeinä näistä ovat sairaalan potilastiedostot, yksityisetsivien tiedot rikoksentekijöistä, sähköinen viestintä, paikannustiedot ja taloudelliset tiedot.
5. käsitellään huomattavia määriä henkilötietoja tai kun käsittely vaikuttaa huomattavaan määrään rekisteröityjä. Laajamittaista käsittelyä tarkennetaan johdantoosan kohdassa 91; siinä huomioidaan rekisteröityjen lukumäärä lukuna tai osuutena väestöstä, käsiteltävien tietojen tai tietoyksikköjen määrä, tietojenkäsittelytoimien kesto tai pysyvyys sekä käsittelytoimen maantieteellinen ulottuvuus. Järjestelmällinen käsittely tarkoittaa WP29-tietosuojatyöryhmän mukaan jotain järjestelmää noudattaen tapahtuvaa, ennalta järjestettyä, organisoitua tai menetelmällistä, osana tietojenkeruuta koskevaa yleissuunnitelmaa tapahtuvaa tai osana strategiaa toteutettavaa käsittelyä.[124]
6. tietokokonaisuuksia yhteensovitetaan tai yhdistetään, esimerkiksi kun yhdistetään saman rekisterinpitäjän eri rekistereiden tietoja tai eri rekisterinpitäjien tietovarantoja.

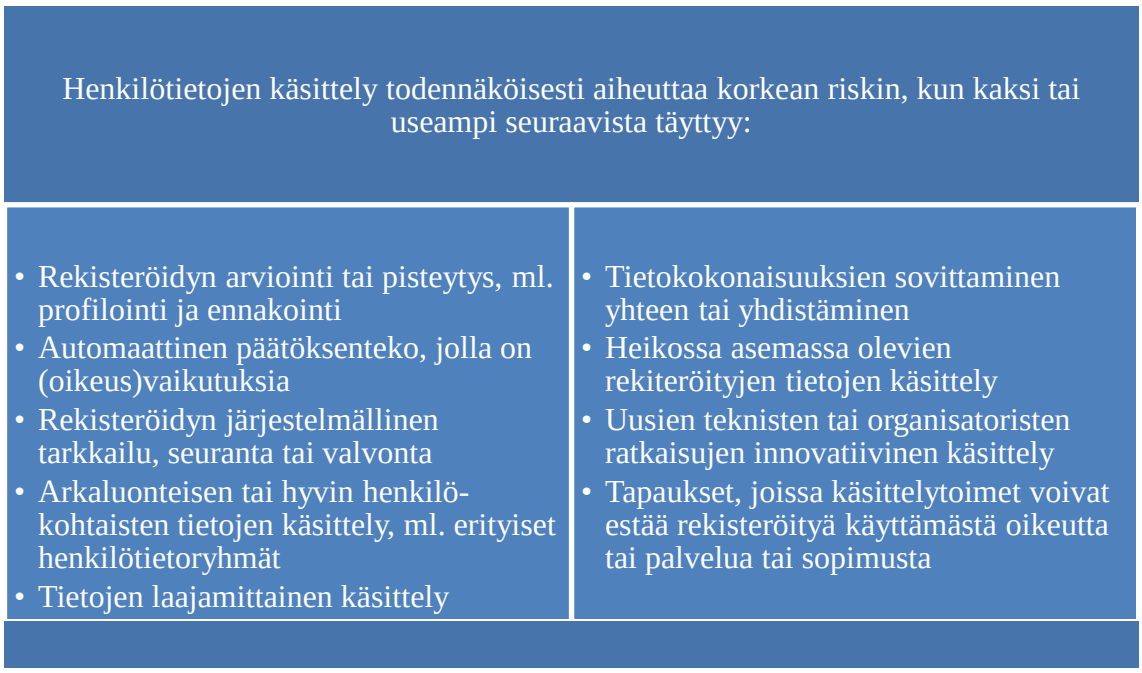
[124] WP29 2017b, 11.

7. on kyse heikossa asemassa olevien henkilöiden tietojen käsittelystä; erityisesti lasten, mutta myös muiden erityistä suojelua tarvitsevien henkilöryhmien (esim. ikääntyneet, potilaat, vammaiset, mielenterveysongelmasta kärsivät tai kun kyseessä on voimasuhteiden epätasapaino).
8. on kyse uusien teknisten tai organisatoristen ratkaisujen innovatiivisesta käytöstä tai soveltamisesta (nk. edistykselliset tietojenkäsittelytavat); esimerkiksi biometristen tietojen hyödyntäminen (sormenjälkien ja kasvojen tunnistus) tai erilaisten sensoreiden käyttö (esim. terveyteen liittyvät) tai IoT-sovellukset.
9. käsittelytoimet estävät rekisteröityjä käyttämästä oikeutta tai palvelua tai sopimusta; esimerkkeinä käsittelytoimet, joiden tavoitteena on sallia tai evätä rekisteröityjen oikeus käyttää palvelua tai tehdä sopimus tai muuttaa kyseistä oikeutta.

Mitä useampi edellä olevista kriteereistä täyttyy, sitä todennäköisempää on, että luonnollisen henkilön oikeuksille ja vapauksille aiheutuu korkea riski ja vaikutustenarviointi tulisi tehdä. Useimmissa tapauksissa kaksi kriteeriä riittää täyttämään edellytykset, mutta voi myös olla, että rekisterinpitäjä katsoo yhdenkin kriteerin täyttymisen velvoittavan vaikutustenarvioinnin laatimiseen. Toisaalta taas käsittelytoimi voi vastata esimerkkejä, mutta rekisterinpitäjä toteaa silti, ettei käsittelytoimi aiheuta ”todennäköistä, korkeaa riskiä”. Tällaisissa tilanteissa tulee vaikutustenarvioinnin tekemättä jättämisen syyt perustella ja dokumentoida ja kirjata näihin tietosuojavastaavan näkemykset.[125]

Kuvassa 2 on esitetty tiivistetty muistilista edellä mainituista kriteereistä todennäköisen, korkean riskin havaitsemisen tueksi. Erilaisia muistilistoja löytyy internetistä myös vaikutustenarvioinnin laatimisen tueksi tai jopa toteuttamiseksi, mutta on huomioitava, ettei itse vaikutustenarviointia ole tarkoitus toteuttaa tarkistuslistanomaisella menetelmällä, vaan se edellyttää erityyppisten ja -tasoisten analyysien laatimista, joihin ei voi vastata kyllä/ei-tyyppisesti.[126]

[125] WP29 2017b, 12 – 14, 16.
[126] Herold n.d.



KUVA 2. Muistilista korkean riskin aiheuttavista käsittelytoimista.

Kuvassa 3 esitetään prosessinomaisesti, millaisia asioita vaikutustenarvioinnin laatimispäätöksen tueksi voidaan huomioida. Lähtökohtana vaikutustenarvioinnin tekemiselle on henkilötietojen käsittelystä todennäköisesti aiheutuva korkea riski luonnollisen henkilön oikeuksille ja vapauksille; mikäli näitä ei havaita, ei vaikutustenarviointia tarvitse tehdä. Päätöksen tueksi voidaan miettiä, käytetäänkö käsittelytoimissa uutta teknologiaa, tehdäänkö profilointia, liittyykö käsittelytoimiin järjestelmällistä valvontaa tai onko käsittely laajamittaista, erityisiä henkilötietoryhmiä sisältävää käsittelyä. Tämän jälkeen tarkistetaan vaatimuksiin liittyvät poikkeukset; esimerkiksi onko kansallinen valvontaviranomainen määritellyt, ettei ao. käsittelytoimeen liittyen tarvitse tehdä vaikutustenarviointia, tai onko sellainen ehkä jo aiemmin tehty. Kun vaikutustenarviointi päätetään laatia, tulee huomioida mahdolliset alakohtaiset käytännesäännöt sekä kuulla tietosuojavastaavaa ja tarvittaessa rekisteröityjä. On huomioitava, ettei vaikutustenarviointi ole kertatoimenpide, vaan käsittelyä tulee myös uudelleenarvioida tarvittaessa. Mikäli vaikutustenarvioinnin riskikartoituksessa jää korkeita jäännösriskejä, tulee vielä kuulla valvontaviranomaista.

KUVA 3. Tietosuoja-asetuksen perusperiaatteet vaikutustenarviointiin liittyen. WP29 2017b, 8.

Tietosuoja-asetuksen 35 artiklan mukaisesti valvontaviranomaisten on laadittava ja julkaistava luettelo käsittelytoimien tyypeistä, joiden yhteydessä vaaditaan tietosuojaa koskeva vaikutustenarviointi. Toisaalta valvontaviranomainen voi laatia luettelon käsittelytoimien tyypeistä, joiden osalta vaikutustenarviointia ei vaadita. Tämänhetkinen sääntely ohjeistuksineen jättää jonkin verran avoimia kysymyksiä vaikutustenarvioinnin toteuttamisesta, joten lisäohjeistus tulee tarpeeseen.

3.4 Todennäköinen ja korkea riski henkilön oikeuksille ja vapauksille

Edellisessä kappaleessa annetaan esimerkkejä käsittelytoimista, joiden yhteydessä rekisteröidyn oikeuksille ja vapauksille todennäköisesti aiheutuu korkea riski. Uudenlaisten teknisten ratkaisujen innovatiiviseen käyttöön voi liittyä seurauksia, joita ei vielä tunneta; esimerkkinä esineiden internet -sovellukset, joilla voi olla huomattava vaikutus yksittäisten henkilöiden arkielämään ja yksityisyyteen.[127] Oikeusvaikutuksia sisältävä automaattinen päätöksenteko voi johtaa rekisteröidyn ulkopuolelle jättämiseen tai syrjintään, kuten myös profilointi, jossa usein yhdistetään laajasti eri tietovarantojen henkilötietoja ja arvioidaan tai pisteytetään rekisteröityjä. Järjestelmällinen valvonta, kameravalvonnan ohella vaikkapa organisaation ajoneuvojen valvonta tai henkilöstön internet-käytön seuranta voi

[127] Pervilä 2018.

aiheuttaa epätietoisuutta siitä, kuka tietoja käsittelee tai mihin tietoja tullaan käyttämään. Esimerkiksi kulunvalvontaraportit tai kameravalvontatallenteet saattavat sisältää arkaluonteista tietoa rekisteröidystä. Tässä kappaleessa pohditaan riskien vaikutuksia luonnolliselle henkilölle.

Tietosuoja-asetuksen johdanto-osan kohdan 75 mukaan henkilötietojen käsittely voi aiheuttaa luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvia riskejä, joiden vaikutukset voivat olla fyysisiä, aineellisia tai aineettomia vahinkoja,

- erityisesti jos käsittely voi johtaa syrjintään, identiteettivarkauteen tai petokseen, taloudellisiin menetyksiin, maineen vahingoittumiseen, salassapitovelvollisuuden alaisten henkilötietojen luottamuksellisuuden menetykseen, pseudonymisoitumisen luvattomaan kumoutumiseen tai aiheuttaa muuta merkittävää taloudellista tai sosiaalista vahinkoa;
- kun rekisteröidyiltä saatetaan evätä heille kuuluvia oikeuksia ja vapauksia tai estää heitä valvomasta omia henkilötietojaan;
- kun käsitellään sellaisia henkilötietoja, jotka koskevat rotua tai etnistä alkuperää, poliittisia mielipiteitä, uskonnollista tai filosofista vakaumusta ja ammattiliittoon kuulumista, tai käsitellään geneettisiä tietoja tai terveyttä ja seksuaalista käyttäytymistä tai rikostuomioita ja rikkomuksia tai niihin liittyviä turvaamistoimenpiteitä koskevia tietoja;
- kun arvioidaan henkilökohtaisia ominaisuuksia, erityisesti jos kyseessä on henkilöprofiilin luomista tai käyttämistä varten suoritettu analyysi tai ennakointi työsuorituksesta, taloudellisesta tilanteesta, terveydestä, henkilökohtaisista mieltymyksistä tai kiinnostuksen kohteista, luotettavuudesta tai käyttäytymisestä, sijainnista tai liikkeistä;
- kun käsitellään heikossa asemassa olevien luonnollisten henkilöiden, erityisesti lasten, henkilötietoja tai kun käsitellään suuria määriä henkilötietoja ja käsittely koskee suurta rekisteröityjen määrää.

Tietosuojavaltuutettu ohjeistaa, että riskien arvioinnissa voidaan huomioida henkilötietojen tyyppi ja luonne, käsittelytoimet, kuten käsittelyn laajamittaisuus, mahdollinen profilointi, yhdistely, tietojen julkaisu ja se, miten henkilötietojen käsittely tulisi mahdollisesti vaikuttamaan rekisteröityyn. Tietojen käsittelyssä tulee huomioida myös sen mahdolliset seuraukset; päätökset, toimet tai tilanteet, joissa henkilötietojen käsittely mahdollisesti johtaa henkilöiden syrjimiseen. Huomioon tulee ottaa myös emotionaaliset vaikutukset,

kuten ärtymys ja mielipaha.[128] Vaikka nämä ohjeet on annettu liittyen rekisterinpitäjän oikeutettuun etuun, ne soveltuvat myös yleisesti riskin ja sen vaikutusten analysointiin.

Rekisteröityä koskevia oikeusvaikutuksia voi sisältyä esimerkiksi päätöksiin, jotka johtavat sopimuksen purkamiseen, lakiin perustuvaan sosiaalietuuden myöntämiseen tai epäämiseen tai maahan pääsyn tai kansalaisuuden epäämiseen. Päätökset voivat aiheuttaa myös muita kuin oikeusvaikutuksia, esimerkiksi kun niiden seurauksena päätöksen kohteena olevan henkilön olosuhteisiin, valintoihin tai käyttäytymiseen aiheutuu merkittäviä vaikutuksia, kun päätöksellä on pitkäkestoisia tai pysyviä seurauksia tai kun päätös johtaa syrjintään tai pois sulkemiseen. Myös kohdennettu markkinointi voi sisältää profilointia, jolla voi olla merkittäviä vaikutuksia rekisteröidylle esimerkiksi tilanteessa, jossa lainaa tarjotaan jo taloudelliseen ahdinkoon joutuneelle henkilölle.[129]

Yksi suurimmista riskeistä rekisteröidyn oikeuksille ja vapauksille on henkilötietojen – varsinkin erityisiin henkilötietoryhmiin kuuluvan tiedon tai salassa pidettävien, arkaluonteisten tai luottamuksellisten tietojen – päätyminen ulkopuolisten saataville. Tietoturvaloukkauksen seurauksena voi olla henkilötietojen valvomiskyvyn menettäminen, maineen vahingoittuminen tai salassa pidettävien asioiden luottamuksellisuuden menettäminen.[130] Yksityisyyden suojan kunnioittaminen on erityisen tärkeää sosiaali- ja terveyspalveluja järjestettäessä[131], myös henkilötiedon käsittelyn osalta. Tähän liittyvät esimerkiksi asianmukainen potilastietojen käsittely tietojärjestelmissä tai asiakirjoina tai vaikkapa kameravalvonta palvelukeskuksissa tai potilaan kotirauhan piirissä ja tallenteisiin liittyvä käyttöoikeushallinta ja luovutuskäytänteet.[132] Riippuen paljastuneen tiedon luonteesta, seuraukset voivat olla jopa kriittiset; esimerkkeinä turvakiellon alaisten tietojen paljastuminen.

Tietovuodot voivat johtaa identiteettivarkauksiin, joissa käyttämällä paljastuneita henkilötietoja voidaan aiheuttaa merkittäviä henkisiä ja sosiaalisia vahinkoja esiintymällä julkisuudessa toisena henkilönä. Taloudellisia vahinkoja voi aiheutua, kun paljastuneita tie-

[128] Tietosuojavaltuutetun toimisto 2018d; Lehtinen 2017.
[129] Tietosuojavaltuutetun toimisto 2018a; Koskinen 2017.
[130] Tietosuojavaltuutetun toimisto 2017a.
[131] Pellonpää 2009.
[132] Tietosuojavaltuutetun toimisto 2014.

toja käytetään lainojen hakemiseen tai tuotteiden ja palvelujen tilaamiseen ja maksamiseen.[133] Tietovuoto aiheuttaa myös käytännön vaivaa, harmia ja mielipahaa asian selvittelyn, rikosilmoituksen tekemisen ja mahdollisen luottokieltopäätöksen hakemisen osalta. Lisäksi jokainen tietovuoto, asiaton pääsy tietoihin tai urkintatapaus aiheuttaa epäluottamusta rekisterinpitäjää kohtaan. Tämä saattaa näyttäytyä niin, ettei rekisteröity halua esittää arkaluonteista asiaansa eri virastojen palveluissa, joka taas voi johtaa uudenlaisiin ongelmiin, esimerkiksi päätösten estymiseen tai virheellisiin päätöksiin. Sama koskee rekisteröidyn asemassa olevaa työntekijää, mikäli työssä esiintyy epäilyjä urkinnasta tai muusta epäasiallisesta tietojen käsittelystä.[134]

Taulukossa 3 esitetään WP29-tietosuojatyöryhmän ohjeeseen perustuvat käsittelytoimet, jotka todennäköisesti aiheuttavat luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin, näistä johtuvia riskivaikutuksia luonnollisen henkilön oikeuksille ja vapauksille sekä kyseiseen käsittelytoimeen liittyviä huomioita rekisterinpitäjälle. Taulukko 3 on esimerkinomainen katsaus mahdollisista vaikutuksista, joiden lisäksi useisiin oikeuksiin voi kohdentua rajauksia tietosuoja-asetuksessa.

TAULUKKO 3. Todennäköisen suuren riskin kriteerit, riskivaikutukset ja huomiot rekisterinpitäjälle.

Kriteeri, joka todennäköisesti aiheuttaa korkean riskin	**Mahdollinen riski ja vaikutus luonnollisen henkilön oikeuksiin ja vapauksiin**	**Huomiot rekisterinpitäjälle**
Arviointi, pisteytys tai profilointi	Rekisteröidyllä on harvoin ymmärrystä tietojensa käsittelyn laajuudesta tai profilointiperusteista ja niiden vaikutuksista rekisteröidylle. Tämä heikentää kontrollia omiin tietoihin. Merkittäviä vaikutuksia voi aiheutua esimerkiksi säännöllisten lainatarjousten kohdentamisesta jo taloudellisessa ahdingossa olevalle, joka voi johtaa lisävelkaantumiseen. Myös kohdennetulla markkinointitarkoituksiin tehtävällä profiloinnilla voi olla merkittäviä vaikutuksia rekisteröidylle, esimerkiksi jos markkinointi on tunkeilevaa (esimerkiksi eri laitteiden ja palveluiden välityksellä	Varmistetaan henkilötietojen käsittelyn lainmukaisuus ja muiden periaatteiden toteutuminen henkilötietojen käsittelyssä. Suostumukseen perustuvan käsittelyn yhteydessä huomioidaan kriteerien täyttyminen myös vapaaehtoisuuden ja peruuttamisen osalta. Rekisteröidyllä on oikeus saada tietoa profiloinnista ja siihen käytetyistä tiedoista, sen logiikasta ja seurauksista rekisteröidylle. Rekisteröidyllä on oikeus oikaista ja poistaa paitsi lähtötiedot, myös itse profiili ja siihen liittyvä pisteytys.

[133] Rousku 2014, 16.
[134] Andreasson 2018.

Kriteeri, joka todennäköisesti aiheuttaa korkean riskin	Mahdollinen riski ja vaikutus luonnollisen henkilön oikeuksiin ja vapauksiin	Huomiot rekisterinpitäjälle
	seuraaminen, erityisen haavoittuvan hetken tai ajankohdan määrittäminen profiloinnin perusteella).	Rekisteröidyllä on oikeus saada pääsy tietoihin sekä vastustaa käsittelyä, josta on myös informoitava. Profiloinnin yhteydessä saattaa muodostua erityisiin henkilötietoryhmiin liittyvää tietoa, vaikkei sitä tarkoituksella kerättäisi. Näiden käsittely on sallittua vain kun itse käsittelykin on sallittua. Edellyttää lähtökohtaisesti vaikutustenarvioinnin tekemistä.
Automaattinen päätöksenteko, jolla on (oikeus)vaikutuksia	Rekisteröidyllä on harvoin tietoa arvioinnin perusteista ja automaattisen päätöksenteon vaikutuksista. Tämä heikentää kontrollia omiin tietoihin. Esimerkiksi sähköisen rekrytoinnin käytänteet saattavat olla syrjiviä, mikäli tietyn ominaisuuden perusteella osa hakijoista suljetaan pois rekrytoinnista. On line -luottohakemusten tai erilaisten etuuksien automaattinen epääminen, joka voi johtaa sopimuksen purkamiseen. Automaattiseen päätöksentekoon perustuva potilaan hoitoonohjaus väärin perustein, jolloin hoitoonohjaus estyy tai viivästyy. Seurauksena voi olla väärä diagnoosi tai potilaan terveydentilan heikkeneminen.	Harkittava, onko automaattinen päätöksenteko välttämätöntä käsittelyn tarkoituksen saavuttamiseksi. Rekisteröidyllä on oikeus vaatia henkilön osallistumista käsittelyyn. Rekisteröidyllä on oikeus esittää kantansa ja saada selvitys arvioinnin jälkeen tehdystä päätöksestä sekä oikeus riitauttaa päätös. Näennäinen ihmisen osallistuminen käsittelyyn ei riitä poistamaan automatisointia. On sallittua tietyin käsittelyperustein (mm. suostumus, sopimus). Ei saa lähtökohtaisesti soveltaa lapsiin. Edellyttää lähtökohtaisesti vaikutustenarvioinnin tekemistä.
Järjestelmällinen tarkkailu, seuranta tai valvonta	Epätietoisuus valvonnan käsittelyperusteista tai tietojen käyttötarkoituksista sekä siitä, kenellä tietoihin on pääsy. Asiakkaan tai työntekijän kontrolli omiin tietoihinsa heikkenee, tähän saattaa kohdistua kiusaamista ja muita sosiaalisia haittoja kuten maineen menetys.	Edellyttää yt-neuvotteluja tai rekisteröidyn / työntekijän suostumusta. Kun järjestelmällinen tarkkailu on rekisterinpitäjän ydintehtävä, on tällä velvollisuus nimittää tietosuojavastaava. Edellyttää lähtökohtaisesti vaikutustenarvioinnin tekemistä.

Kriteeri, joka todennäköisesti aiheuttaa korkean riskin	Mahdollinen riski ja vaikutus luonnollisen henkilön oikeuksiin ja vapauksiin	Huomiot rekisterinpitäjälle
Erityisiin henkilötietoryhmiin liittyvän tiedon käsittely	Erityisiin henkilötietoryhmiin liittyviä tietoja saattaa paljastua profiloinnin tai tietojen laajamittaisen käsittelyn tai tietojen yhdistämisen kautta, vaikkei niitä lähtökohtaisesti erityisesti kerättäisi, tai vaikkei käsittelyperuste edellyttäisi näiden käsittelyä. Tämä heikentää rekisteröidyn mahdollisuutta valvoa omien tietojensa käsittelyä. Myös rekisteröidyn oikeuksien toteuttaminen estyy, mikäli käsittelystä ei selkeästi informoida. Erityisiin henkilötietoryhmiin liittyvän tiedon käsittelyssä luottamuksellisuuden takaaminen on tärkeää. Tietojen paljastuminen sivullisille saattaa aiheuttaa mm. sosiaalista vahinkoa (esim. kiusaaminen), maineen menettämisen, mahdollisen uhkan terveydelle tai hengelle (esim. seksuaalirikostuomiot, turvakiellon alaiset tiedot, vainoaminen).	Erityisiin henkilötietoryhmiin liittyvien tietojen käsittely on lähtökohtaisesti kielletty. Käsittelyssä tulee olla erityisen huolellinen. Suojatoimien (esim. pääsykontrolli tai tietojen lokitus myös katselun osalta) tärkeys tietojärjestelmissä korostuu. Esimerkiksi sosiaali- ja terveydenhuollon tietojen käsittelyyn liittyy laajasti erityislainsäädäntöä. Tällaisia tietoja saattaa muodostua myös tietojen käsittelyn, esimerkiksi profiloinnin yhteydessä, jolloin käsittelyperusteesta ja käsittelyn lainmukaisuudesta on erityisesti huolehdittava. Laajamittainen käsittely yhdistettynä erityisten henkilötietoryhmien tietojen käsittelyyn edellyttää lähtökohtaisesti vaikutustenarvioinnin tekemistä.
Tietojen laajamittainen käsittely	Laajat kansalliset tai ylikansalliset tietovarannot voivat heikentää rekisteröidyn mahdollisuutta valvoa tietojensa käyttöä ja toteuttaa oikeuksiaan, varsinkin mikäli käsittelyyn liittyy profilointia ja tietojen luovuttamista.	Kun rekisterinpitäjän ydintehtävänä on laajamittainen käsittely, tulee nimittää tietosuojavastaava. Saattaa edellyttää vaikutustenarvioinnin tekemistä.
Tietokokonaisuuksien yhteensovittaminen tai yhdistäminen	Kuten edellä. Tietokokonaisuuksien sähköisesti yhdistäminen on myös riski tietojen eheydelle; lisäksi saattavat tulla kyseeseen mahdollisten virheiden aiheuttamat vaikutukset rekisteröidyn oikeuksille ja vapauksille.	Saattaa edellyttää vaikutustenarvioinnin tekemistä.
Heikossa asemassa olevien rekisteröityjen tietojen käsittely	Esimerkiksi laajat terveydenhuollon, sairaanhoidon tai sosiaalitoimen järjestelmät, joissa tietoja mahdollisesti luovutetaan viranomaiselta toiselle ja saadaan näin kattava profiili rekisteröidyn varsinkin erityisiin henkilötietoryhmiin sekä muuten arkaluonteisen tiedon osalta.	Huomioitava rekisteröidyn lähtökohtaisesti alhaisempi kyky kontrolloida omia tietojaan ja toteuttaa tai valvoa oikeuksiaan. Informoinnin selkeys ja läpinäkyvyys korostuvat. Yhdistettäessä laajamittaiseen käsittelyyn, edellyttää vaikutustenarvioinnin tekemistä.

Kriteeri, joka todennäköisesti aiheuttaa korkean riskin	Mahdollinen riski ja vaikutus luonnollisen henkilön oikeuksiin ja vapauksiin	Huomiot rekisterinpitäjälle
Uusien teknisten tai organisatoristen ratkaisujen käyttöönotto	Palvelujen digitalisoituminen mahdollistaa yhä laajemmat tietovarannot. Rekisteröidyn kontrolli omiin tietoihin heikkenee. Esimerkiksi IoT-laitteet ja yhteisöpalvelut keräävät ja tallentavat laajasti tietoja käyttäjästä. Suostumuksen peruuttaminen saattaa johtaa palvelun käytön estymiseen. Kerättyä tietoa profiloidaan, muokataan, siirretään ja luovutetaan eteenpäin.	Huomioitava erityisesti henkilötietojen suoja teknologioita, tuotteita ja palveluita kehitettäessä. Edellyttää lähtökohtaisesti vaikutustenarvioinnin tekemistä.
Käsittelytoimet voivat estää rekisteröityä käyttämästä oikeutta, palvelua tai sopimusta	Tiedon saatavuuden ongelmat; henkilö ei saa ajallaan hänelle kuuluvaa päätöstä esimerkiksi etuuteen liittyen. Virheelliset tai puuttuvat tiedot. Esimerkiksi kameravalvontatallenteen puuttuminen (rikoksen todentaminen, uhrin oikeuksien puolustaminen estyy). Aiheuttaa mahdollisesti myös taloudellisia vaikutuksia.	Rekisteröidyllä on oikeus saada korvaus vahingosta, joka hänelle on aiheutunut asetuksen rikkomisesta.

3.5 Vaikutustenarviointi käytännössä

Tietosuojaa koskevan vaikutustenarvioinnin vähimmäisvaatimukset määritellään 35 artiklan 7 kohdassa sekä johdanto-osan kohdissa 84 ja 90. Arvioinnin tulee sisältää vähintään

- järjestelmällinen kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista sekä oikeutetusta edusta, mikäli käsittely perustuu oikeutettuun etuun
- arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden
- arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä sekä
- suunnitellut toimenpiteet riskeihin puuttumiseksi, mukaan lukien suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan, että tätä asetusta on noudatettu huomioiden rekisteröityjen ja muiden asianomaisten oikeudet ja oikeutetut edut.

Riskejä hallinnoidaan yleisesti erilaisilla Excel-pohjilla. Riskikartoituksen lisäksi tulee pohtia kunkin riskin todennäköisyyttä ja vaikuttavuutta, sitä, millä todennäköisyydellä tunnistettu riski voi realisoitua ja kuinka vakava tai laaja sen vaikutus on toteutuessaan

rekisteröidyn oikeuksille ja vapauksille. Todennäköisyyden kartoittamisessa voidaan huomioida esimerkiksi organisaation tietoturvakäytänteitä, kuten käytössä olevia suojauskeinoja ja -mekanismeja, salaus- ja varmuuskopiokäytänteitä, häiriötilanteiden hallintaprosessia tai toipumissuunnitelmaa. Vaikuttavuuden osalta voidaan pohtia esimerkiksi sitä, millainen kyvykkyys organisaatiolla on tunnistaa henkilötietojen tietoturvaloukkaus ja ilmoittaa siitä määräajan puitteissa. Vaikuttavuuteen liittyy myös esimerkiksi se, minkä tyyppisiä (erityisiin henkilötietoryhmiin kuuluvia, salassa pidettäviä) tietoja käsitellään. Korkea riski voi aiheutua mahdollisen riskin todennäköisyydestä tai vakavuudesta tai näiden yhdistelmästä.[135]

Yhtä lailla keskiössä ovat myös henkilötiedon käsittelyyn tai käsittelyprosessiin liittyvät riskit ja varsinkin niissä tapahtuvat muutokset. Konkreettisia ja ajankohtaisia riskejä julkishallinnossa ovat muutokset rekisterinpitäjän hallinnossa, esimerkiksi tehtävien uudelleen vastuuttaminen, palvelujen ulkoistustilanteet tai tilanteet, joissa rekisterinpitäjälle osoitetaan uusia lainsäädäntöön tai valtionhallintoon perustuvia velvoitteita. Riskikartoituksessa tulisi myös huomioida avainhenkilömuutoksiin liittyvän prosessin laatiminen. Tällaisten muutosten vaikutusten etukäteinen arviointi tietoturvamielessä on erittäin haastavaa.[136]

WP29-tietosuojatyöryhmä painottaa ohjeessaan, että vaikutustenarvioinnin on oltava muodosta riippumatta riskien todellinen arviointi, jonka avulla rekisterinpitäjän on mahdollista puuttua riskeihin.[137] Riskien vakavuuden, luonteen ja toteutumistodennäköisyyden selvittämisen lisäksi tulee siis kartoittaa ja toteuttaa toimenpiteitä, joilla riskiä voidaan vähentää tai poistaa. Saman riskin minimoimiseksi voi olla useitakin erilaisia, vaihtoehtoisia ja osittain päällekkäisiä toimintatapoja, joista rekisterinpitäjän tulee valita omaan liiketoimintaansa ja toimintaprosesseihinsa soveltuvat suojatoimet ja mekanismit, jotka – saatavilla oleva tekniikka ja toteutuskustannukset huomioiden – ovat järkeviä ja riittäviä kulloisenkin riskin kohdalla. On huomioitava, että vaikka tässä työssä vaikutustenarviointia tarkastellaankin pääsääntöisesti riskilähtöisesti, ei pelkkä riskienarviointi sellaisenaan riitä täyttämään vaikutustenarvioinnin sisältövaatimuksia. Vaikutustenarvi-

[135] ICO 2018, 16.
[136] Andreasson 2017.
[137] WP29 2017b, 20.

ointi voidaan tehdä erillisenä lomakemuotoisena dokumenttina, jonka lisäksi riskejä voidaan hallinnoida esimerkiksi Excel-pohjilla. Vastaavasti voidaan käyttää sovellusta, johon tiedot täytetään ja josta voidaan tulostaa valmis vaikutustenarviointiraportti.

Vaikutustenarvioinnin viitekehyksenä toimivat tietosuoja-asetuksen vaatimukset. Tarkkaa ohjeistusta sen rakenteelle ja muodolle tai valmista, kaikille yhteistä menetelmää tai mallipohjaa tietosuoja-asetus ei tarjoa, vaan kunkin rekisterinpitäjän tulee sovittaa vaikutustenarvioinnin laatiminen omiin toimintatapoihinsa ja ehkä jo käytössä oleviin menetelmiinsä sopivaksi. WP29-tietosuojatyöryhmä antaa kuitenkin vaikutustenarviointia koskevan ohjeensa liitteessä 1 esimerkkejä jo olemassa olevista viitekehyksistä. Rekisterinpitäjän tulee menetelmää valitessaan huolehtia siitä, että käytetty viitekehys tai menetelmä on tietosuojatyöryhmän ohjeen liitteen 2 hyväksymiskriteerien mukainen.[138] Annetut esimerkkikehykset ja hyväksymiskriteerit on julkaistu tämän työn liitteinä 2 ja 3.

Esimerkkinä yleisesti käytössä olevasta järjestelmästä toimii Ranskan tietosuojavaltuutetun CNIL:n[139] julkaisema avoimen lähdekoodin PIA-sovellus, joka on saatavissa myös englanninkielisenä.[140] Kotimaisista palveluntarjoajista esimerkiksi Agendiumilla on Tietosuojamalli-digityökalu tietosuojaan ja vaikutustenarviointiin liittyvien riskien hallintaan ja dokumentointiin. Myös Granitella on oma PIA (Privacy Impact Assessment) -työkalunsa. Opinnäytetyön liitteenä 4 on ICO:n julkaisema selkeä ja helppokäyttöinen DPIA-mallipohja, jota voidaan hyödyntää esimerkkipohjana tehtäessä vaikutustenarviointia lomaketyyppisesti.[141]

Rekisterinpitäjä on vastuussa vaikutustenarvioinnin tekemisestä, vaikka se tehtäisiin organisaation ulkopuolella. Artiklassa 35 velvoitetaan rekisterinpitäjä pyytämään neuvoja tietosuojavastaavalta, jos sellainen on nimitetty, ja nämä sekä rekisterinpitäjän tekemät päätökset tulisi dokumentoida vaikutustenarviointiin. Jos henkilötietojen käsittelyn suorittaa kokonaan tai osittain henkilötietojen käsittelijä, tämän olisi autettava rekisterinpitäjää vaikutustenarvioinnin tekemisessä tarjoamalla tälle kaikki tarpeelliset tiedot.[142] Rekisterinpitäjän olisi myös tarpeen mukaan pyydettävä rekisteröityjen tai näiden edustajien näkemyksiä suunnitelluista käsittelytoimista. WP29-tietosuojatyöryhmän näkemyksen

[138] WP29 2017b, 20, 23.
[139] Commission Nationale de l'Informatique et des Libertés.
[140] IAPP 2017; CNIL 2018.
[141] Information Commissioner’s Office, UK.
[142] WP29 2017b, 16 – 17.

mukaan näkemyksiä voidaan pyytää tapauksesta riippuen eri tavoin, esimerkiksi yleisellä tutkimuksella tai kyselyllä. Suostumuksen osalta on huomioitava, ettei suostumuksen pyytäminen käsittelyyn tarkoita näkemysten pyytämistä.[143] Esimerkkinä työntekijöiden kuulemisesta on työntekijöihin kohdistuvan kameravalvonnan aloittaminen, joka tulee käsitellä yhteistoimintamenettelyssä työntekijöiden suostumuksen saamiseksi ja käsittelyn läpinäkyvyyden takaamiseksi.[144]

Rekisterinpitäjän vastuulle jää siis vaikutustenarvioinnin käytännön toteutuksen hallinta. Rekisterinpitäjän toiminnasta riippuen jää harkittavaksi, millaisella menetelmällä ja prosessilla vaikutustenarviointeja jatkossa hallinnoidaan. Erilliset lomakkeet ja taulukkomuotoiset tiedostot riittänevät osoitusvelvollisuuden todentamiseksi, mutta rekisterinpitäjän toiminnoissa prosessin hallinta saattaisi olla helpompaa jonkin tietojärjestelmän tai sovelluksen avulla. Arvioitavaksi tulee myös, missä määrin jo olemassa olevista käsittelytoimista tulisi tehdä arviointi ja mikä on oikea taso arvioinnin pohjaksi; tehdäänkö se organisaatioon, palvelualaan tai toimintaan vai käsittelytoimeen tai -prosessiin perustuen. Erittäin tärkeää on miettiä ja kuvata, kuka hyväksyy vaikutustenarvioinnissa määriteltyjen riskien lieventämistoimenpiteet ja -menetelmät sekä vaikutustenarvioinnin kokonaisuudessaan. On myös sovittava siitä, mikä taho konkreettisesti valvoo toimenpiteiden toteuttamista ja vaikutustenarvioinnin seurantaa eli katselmointia ja millä aikataululla katselmointeja toteutetaan. Vaikutustenarvioinnin hahmottaminen vaiheistettuna prosessina saattaa helpottaa sen laatimista.

Rekisterinpitäjä päättää vaikutustenarvioinnin mahdollisesta julkaisemisesta. Se on joka tapauksessa toimitettava kokonaisuudessaan valvontaviranomaiselle ennakkokuulemistapauksessa tai tietosuojaviranomaiselle pyydettäessä. Yhteenvedon tai päätelmien julkaiseminen voi herättää luottamusta, jonka vuoksi julkaisemista suositellaan harkittavaksi. Luotettavuuden ja läpinäkyvyyden osoittamiseksi julkaiseminen olisi erityisen hyvän käytännön mukaista silloin, kun käsittelytoimi vaikuttaa yksittäisiin kansalaisiin, erityisesti tapauksissa, joissa vaikutustenarvioinnin tekee viranomainen.[145]

---

[143] WP29 2017b, 17. Ohjeen suomenkielisessä versiossa lause ”Although it should be noted that consent to processing is obviously not a way for seeking the views of the data subjects” on käännetty ”On kuitenkin huomattava, ettei käsittelyyn annettu suostumus ole ilman muuta suostumus näkemysten antamiseen.”
[144] Tietosuojavaltuutetun toimisto 2014; WP29 2017c, 8.
[145] WP29 2017b, 21.

3.6 Valvontaviranomaisen ennakkokuuleminen

Vaikutustenarvioinnissa tulee tarkastella erityisesti suunniteltuja toimenpiteitä sekä suojatoimia ja mekanismeja, joiden avulla käsittelyyn kohdistuvaa riskiä voidaan lieventää. Ennakkokuulemisvelvoite tarkoittaa siirtymistä henkilötietolain mukaisesta yleisestä ilmoitusvelvollisuudesta (rekisteri-ilmoitus, toimintailmoitus ja ilmoitus henkilötietojen luovuttamisesta ulkomaille) tietosuoja-asetuksen mukaiseen, riskiperusteiseen ilmoitusvelvollisuuteen.[146]

Valvontaviranomaisen ennakkokuulemisesta säädetään tietosuoja-asetuksen 36 artiklassa sekä johdanto-osan kohdissa 94 – 96. Jos vaikutustenarvioinnin perusteella riskin taso on korkea, eikä rekisterinpitäjä pysty riittävästi puuttumaan tunnistettaviin riskeihin joko sen vuoksi, ettei toimenpiteitä riskin pienentämiseksi ole toteutettu tai jäännösriski on toimenpiteistä huolimatta edelleen korkea, on rekisterinpitäjän kuultava valvontaviranomaista ennen käsittelyn aloittamista.[147] Ennakkokuulemistarve jää siis rekisterinpitäjän harkinnan ja aloitteen varaan; rekisterinpitäjän on itse tunnistettava, milloin riskit tai jäännösriskit jäävät sille tasolle, että valvontaviranomaisen kuuleminen on tarpeen.

Esimerkkinä liian korkeasta jäännösriskistä mainitaan tapaukset, joissa rekisteröidyt voivat joutua kärsimään huomattavista tai jopa peruuttamattomista seurauksista, joita he eivät välttämättä pysty torjumaan. Tällaisia tilanteita ovat esimerkiksi laiton tietoihin pääsy, joka johtaa rekisteröityjen henkeä uhkaavaan vaaraan, irtisanomiseen tai taloudelliseen uhkaan. Riskin ilmeneminen voi konkretisoitua tilanteissa, joissa ei pystytä vähentämään niiden henkilöiden lukumäärää, joilla on pääsy tietoihin tietojen jakamis-, käyttö- tai levitystapojen vuoksi tai kun tiedossa olevaa haavoittuvuutta ei pystytä korjaamaan. Tällaisissa tapauksissa eräinä keinoina riskin torjumiseksi ovat pseudonymisointi ja salaus. On kuitenkin huomioitava, että tarvittavat toimenpiteet määräytyvät aina käsittelytoimen ja asiayhteyden mukaan.[148]

---

[146] Tietosuojavaltuutetun toimisto. 2010, 3; Tietosuojavaltuutetun toimisto 2017b, 18.
[147] WP29 2017b, 22.
[148] WP29 2017b, 22.

3.7 Vaikutustenarviointi jatkuvana prosessina

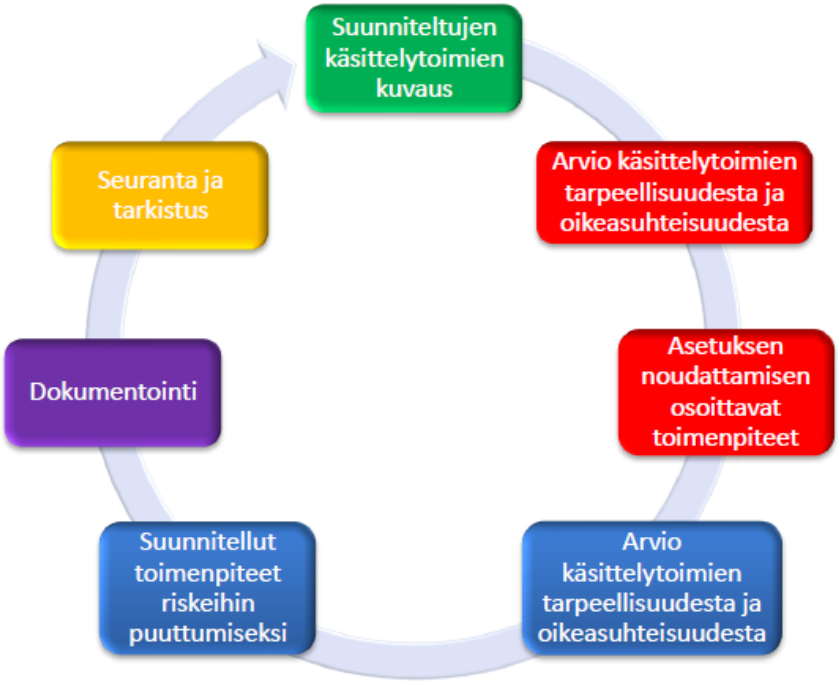
Vaikutustenarviointia tulee tarkastella yksittäisen projektin sijaan jatkuvana prosessina, jota ylläpidetään tietojen käsittelyssä tai tietojärjestelmien toiminnoissa tapahtuneiden muutosten perusteella, erityisesti jos käsittelytoimi on dynaaminen. Tietojenkäsittelytoimet saattavat muuttua nopeastikin korkeiksi esimerkiksi henkilötietojen käsittelytarkoituksen muuttuessa, tai kun käsittelytoiminnan asiayhteys muuttuu, esimerkiksi kun automatisoitujen päätösten vaikutus on kasvanut tai uusista rekisteröityjen ryhmistä on tullut alttiita syrjinnälle.[149] Riski voi nousta myös tilanteissa, joissa otetaan käyttöön uudenlaista teknologiaa, kun rekisteröidyistä kerätään uutta tietoa tai kun uusille henkilöryhmille tai organisaatioille mahdollistetaan pääsy tietoihin. Riskien lisäksi on tärkeää selvittää myös niiden taustat ja juurisyyt.[150] Vaikkei vaikutustenarviointi tulisikaan tällä hetkellä tehtäväksi, yleinen riskiperusteinen lähestymistapa velvoittaa rekisterinpitäjän jatkuvaan riskien hallintaan eli niiden säännölliseen tarkasteluun, käsittelyyn ja lieventämiseen.[151] On huomioitava, ettei mahdollisten vakuutusten ottaminen riskien varalta vapauta rekisterinpitäjää vaikutustenarvioinnin laatimisen, seurannan tai yleisemmin riskiperusteisen lähestymistavan mukaisesta riskien hallinnan vastuusta.[152]

Toisaalta jo tehdyn vaikutustenarvioinnin perusteella suoritetut toimenpiteet riskien lieventämiseksi tai muuten muuttuneet olosuhteet voivat myös pienentää käsittelytoimesta aiheutunutta riskiä. Automatisoidun päätöksenteon tai järjestelmällisen valvonnan kriteerit eivät ehkä enää täyty, jolloin jo tehdyn riskianalyysin uudelleentarkastelu voi osoittaa, ettei tietosuojaa koskevaa vaikutustenarviointia enää vaadita. Vaikutustenarviointia ja sen tarvetta olisikin tarkistettava jatkuvasti ja riskejä arvioitava uudelleen.[153]

Kuva 4 esittää vaikutustenarvioinnin iteratiivista eli toistuvaa menettelyä. Tietosuojatyöryhmä WP29 toteaa ohjeessaan, että vaikutustenarvioinnin tarkastelu eli katselmointi säännöllisesti olisi hyvän käytännön mukaista. Päivittämällä vaikutustenarviointia koko hankkeen elinkaaren ajan voidaan varmistaa tietosuojan ja yksityisyyden huomiointi sekä tukea sellaisten ratkaisujen kehittämistä, jotka noudattavat tietosuoja-asetuksen vaatimuksia. Teknisten ja organisatoristen toimenpiteiden valinta saattaa vaikuttaa käsittelyyn

[149] WP29 2017b, 16.
[150] Lambert 2018, 318 – 319, 327.
[151] WP29 2017b, 7.
[152] WP29 2017b, 7.
[153] WP29 2017b, 16.

liittyvien riskien vakavuuteen ja todennäköisyyteen, joten yksittäisten vaiheiden arvioinnin kertaaminen kehitysprosessin edetessä saattaa olla tarpeen. Onkin todennäköistä, että kuhunkin vaiheeseen palataan useamman kerran ennen vaikutustenarvioinnin valmistumista.[154]

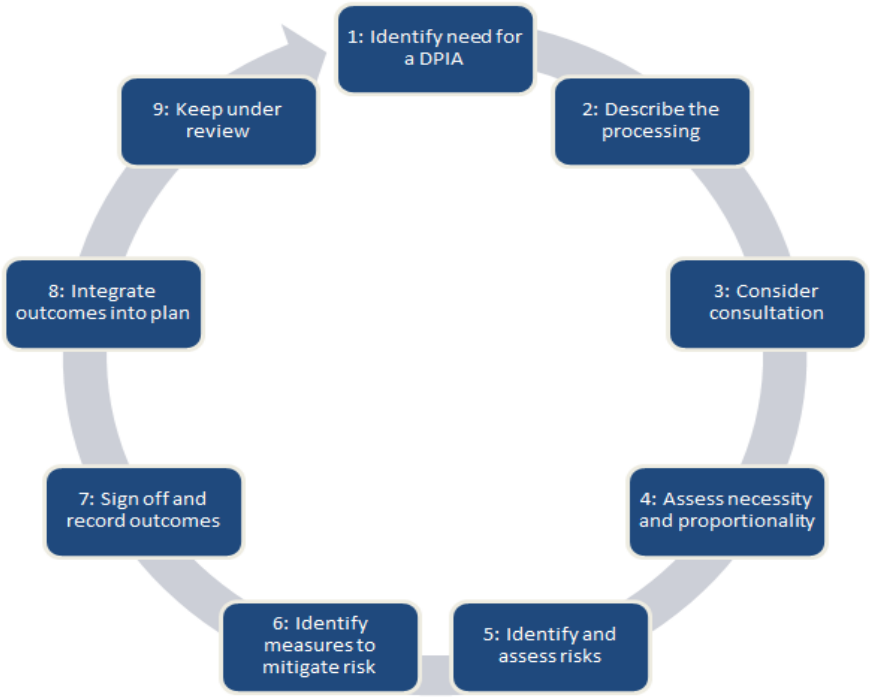


KUVA 4. Vaikutustenarvioinnin iteratiivinen menettely. WP29 2017b, 19.

Myös ICO on kuvannut DPIA-mallipohjan (ks. liite 4) vaiheet prosessina, joka on suunniteltu joustavaksi ja skaalautuvaksi. Prosessin kohdissa 1 – 3 kuvataan vaikutustenarvioinnin perustana olevaa hanketta ja mahdollista vaikutustenarvioinnin tarvetta; hankkeen tavoitteita, henkilötietojen käsittelyn laajuutta, siihen liittyviä tietovirtoja, tietojen luovutuksia ja tietojen elinkaaren hallintaa sekä hankkeen sidosryhmiä, yhteistyömenetelmiä ja niitä tahoja, joiden konsultaatiota ja arvioita hankkeen tai vaikutustenarvioinnin kannalta tullaan tarvitsemaan. Kohdassa 4 keskitytään käsittelyn lainmukaisen perusteen ja vaatimustenmukaisuuden arviointiin tietosuoja-asetuksen periaatteisiin pohjautuen, ja kohdat 5 – 6 keskittyvät riskien tunnistamiseen, arviointiin ja lieventämistoimien määrittelyyn. Kohdassa 7 arvioidaan ja hyväksytetään vaikutustenarvioinnin tulokset, lieventämistoimet ja jäännösriskit sekä kirjataan yhteistyötahojen kuten tietosuojavastaavan kannanotot

[154] WP29 2017b, 16 – 17.

sekä määritellään katselmointiajankohdat. Lisäyksenä DPIA-mallipohjan kohtiin prosessissa kuvataan kohdat 8 ja 9, joissa vaikutustenarvioinnin tulokset toimeenpannaan suunnitelmaksi ja vaikutustenarviointia katselmoidaan ja tarkastellaan säännöllisesti.



KUVA 5. How do we carry out a DPIA?[155]

[155] ICO n.d.

4 JOHTOPÄÄTÖKSET JA POHDINTA

Tietosuoja-asetus asettaa uusia ja tarkentuneita vaatimuksia rekisterinpitäjille samaan aikaan kun rekisteröityjen oikeudet laajenevat ja valvontaviranomaisen rooli vahvistuu. Vaikutukset rekisterinpitäjän toimintaan ja prosesseihin ovat kokonaisvaltaisia ja aiheuttavat merkittäviä resurssitarpeita. Viime kädessä rekisterinpitäjä vastaa henkilötietojen käsittelystä, vaikka sitä suorittaisi henkilötietojen käsittelijä rekisterinpitäjän lukuun tai vaikka vaatimukset rekisteröityjen oikeuksien toteuttamiseksi edellyttäisivät tietojärjestelmiin tehtäviä teknisiä uudistuksia. Sopimusosaamisen merkitys laajan tietosuojalainsäädännön hallinnan ohella korostuu. Dokumentointi on kaikissa prosesseissa tärkeää osoitusvelvollisuuden todentamiseksi. Tietosuoja-asetuksen saaman runsaan julkisuuden myötä rekisteröidyt ovat hyvin valveutuneita oikeuksistaan, ja onkin todennäköistä, että tietopyyntöjen ja erilaisten tiedustelujen määrä ainakin hetkellisesti nousee.

Tietosuoja-asetusta on kritisoitu vaikeaselkoiseksi. Sääntely on joustavaa, mutta kääntöpuolena se jättää rekisterinpitäjälle laajasti tulkinnanvaraa sekä sen noudattamisen että osoitusvelvollisuuden riittävyyden osalta. Sen lisäksi, että tietosuoja-asetuksen suomenkieliseen käännökseen sisältyy kohtia, joiden tarkoitusperä käy paremmin ilmi muun kielisestä versiosta, myös terminologiaan liittyy kansallisia piirteitä esimerkiksi rekisterinpidon, rekisterinpitäjän ja rekisteröidyn käsitteiden osalta. Tietosuoja-asetuksen englanninkielisessä versiossa, kuten myös henkilötietodirektiivissä, käsitteinä ovat rekisterinpidon sijaan henkilötietojen käsittely, rekisteröidyn sijaan pääsääntöisesti luonnollinen henkilö (data subject) ja rekisterinpitäjän sijaan taho, joka kontrolloi henkilötietojen käsittelyä (data controller).

Tietoja kerätään usein laajasti. Käsittelytoimissa saatetaan kerätä – tai rekisteröity itse saattaa luovuttaa vapaaehtoisesti ja pyytämättä – tietoja myös lähiomaisistaan, jolloin myös näistä voi tulla rekisteröityjä. Toisaalta, vaikka näiden tietoja ei käsiteltäisikään rekisterinpitäjän toiminnoissa, rekisteröidyn perheenjäsenen tai lähiomaisen oikeuksiin ja vapauksiin voi aiheutua merkittäviä vaikutuksia rekisteröityyn liittyvän, esimerkiksi turvakiellon alaisen, geneettisen tai terveydellisen tiedon paljastumisesta. Termistön riittävän laajalla tulkinnalla saattaa olla merkitystä mietittäessä riskien vaikutuksia luonnollisen henkilön oikeuksiin ja vapauksiin.

Tietosuoja-asetus asettaa merkittävän haasteen myös riskiperusteisen lähestymistavan edellyttämän yleisen riskienhallintaosaamisen muodossa. Riskien tunnistamisen ja arvioinnin lisäksi tulee määritellä ja toteuttaa keinot niiden pienentämiseksi ja poistamiseksi, ja riskienhallintaa – kuten vaikutustenarviointiakin – tulee toteuttaa kertaluonteisen toiminnon sijaan prosessina, jossa valvotaan hyväksyttyjen suojatoimien toteuttamista. Suojakeinot tulee suhteuttaa riskeistä aiheutuviin vaikutuksiin. Tietosuoja-asetuksen sääntelyä ei tule jättää vaille riittävää huomiota, mutta ylireagointiinkaan ei ole syytä.

Vaikutustenarviointia on pidetty yhtenä tietosuoja-asetuksen vaikeimmin tulkittavista menettelyistä. Vaikutustenarvioinnissa riskejä tulee tarkastella luonnollisen henkilön oikeuksille ja vapauksille aiheutuvien riskivaikutusten näkökulmasta. Opinnäytetyön tavoitteena oli perehtyä vaikutustenarviointiin ja riskiperusteiseen lähestymistapaan liittyvään sääntelyyn ja ajanmukaiseen kansalliseen ohjaukseen sekä tunnistaa ja tuoda esille henkilötietojen käsittelyyn liittyviä riskejä ja riskivaikutuksia. Vaikutustenarvioinnin hahmottamisen kannalta on tärkeää ymmärtää laajasti tietosuoja-asetuksen perusteita ja periaatteita sekä rekisteröidyn oikeuksia ja rekisterinpitäjän velvollisuuksia, sillä varsinkin tietosuoja-asetuksen soveltamisen alkuvaiheessa näistä saattaa aiheutua merkittäviä riskejä. Opinnäytetyön johdanto-osassa kuvataan yleisimpiä tietoturvaan ja tietosuojaan liittyviä riskejä tiedon luottamuksellisuuden, eheyden ja saatavuuden näkökulmasta. Luvussa 2 esitellään tietosuoja-asetuksen periaatteita ja niihin liittyviä riskejä, joita peilataan myös luonnollisen henkilön perustuslaillisiin oikeuksiin. Luvussa 3 esitellään WP29-tietosuojatyöryhmän ohjeen[156] mukaisia käsittelytoimia, joista todennäköisesti aiheutuu korkea riski luonnollisen henkilön oikeuksiin ja vapauksiin, sekä näihin liittyviä riskivaikutuksia. Työssä on pyritty esittämään huomioita myös rekisterinpitäjälle, vaikka työn pääasiallinen tavoite olikin käsitellä riskejä nimenomaan kuvaamalla monipuolisesti niiden vaikutuksia luonnollisen henkilön oikeuksiin ja vapauksiin. Työ lähestyy vaikutustenarviointia riskiperusteisesti, joskin luvussa 3 kuvataan vaikutustenarviointia myös laajemmin prosessina.

Henkilötietojen käsittelyyn liittyvien riskien ja luonnollisen henkilön oikeuksille ja vapauksille aiheutuvien vaikutusten määrittely edellyttää lainsäädäntöosaamisen lisäksi toimialan, oman toiminnan ja varsinkin henkilötietojen ja niiden käsittelytoimintojen tunte-

[156] WP29 2017b.

mista. Riskin, sen juurisyyn tai vaikutusten erottaminen ja toisaalta riittävän pitkälle menevien vaikutusten arviointi saattaa edellyttää pitkällistäkin pohdintaa. Viime kädessä realisoituneen riskin vaikuttavuus on subjektiivinen, kyseisen luonnollisen henkilön kokemus, jolle määritellään syvyys ja taloudellinen painoarvo vasta oikeuskäytännössä. Taulukkoa, josta voitaisiin helposti tarkistaa luonnolliselle henkilölle tietynlaisesta käsittelytoimesta tai spesifin tiedon paljastumisesta aiheutuvat vaikutukset, ei ole olemassa.

Perinteisesti organisaatioissa on totuttu huolehtimaan lähinnä teknisestä tietoturvasta. Suurin riskitekijä henkilötietojen käsittelyssä on kuitenkin yksittäisten henkilöiden toiminta tietoja käsiteltäessä ja varsinaiset arkipäivän työssä ilmenevät riskitilanteet saattavat olla hyvinkin helposti korjattavissa. Selkeät ohjeet, politiikat ja jatkuva koulutus ovat tarpeen, mutta organisaation tulisi tarvittaessa myös varautua puuttumaan väärinkäytöksiin tehokkaasti sisäisillä menettelyillä. Riskiperusteisen lähestymistavan ja vaikutustenarvioinnin nostaminen keskeiseksi osaksi tietosuoja-asetuksen noudattamista ja osoitusvelvollisuutta vahvistaa henkilön oikeuksien ja vapauksien huomiointia ja tuo rekisteröidyn oikeudet henkilötietojen käsittelyssä perinteisen teknologialähtöisyyden rinnalle. On tärkeää, että tietosuojan huomioinnista tulee kiinteä osa organisaation toimintakulttuuria henkilötietoja käsiteltäessä.

Kansallisen tietosuojaviranomaisen tehtävänä on paitsi ohjata, myös valvoa tietosuoja-asetuksen noudattamista. Ohjeiden ja neuvojen lisäksi se voi antaa varoituksia ja huomautuksia toimintatapojen muuttamiseksi ja rekisteröidyn oikeuksien toteuttamiseksi sekä viime kädessä asettaa käsittelylle väliaikaisen tai pysyvän käsittelykiellon tai määrätä hallinnollisen sakon. Hallinnolliset sakot ovat saaneet julkisuudessa suhteettoman suuren painoarvon, vaikka kyseessä on viimesijainen keino rekisterinpitäjän kannustamiseksi tietosuoja-asetuksen noudattamiseen. On kuitenkin totta, että vaikka hallinnollisia sakkoja ei julkishallintoon sovellettaisikaan, se ei poista uhkasakkojen, valitusprosessin, oikeudenkäyntien tai vahingonkorvausten kustannusriskiä, maineriskin vaikutuksista puhumattakaan. On siis vahvasti rekisterinpitäjän oman edun mukaista – nimenomaisesti muutkin taloudelliset riskit huomioiden – huolehtia tietosuoja-asetuksen noudattamisesta. On selvää, että haasteiden ja avointen kysymysten ohella uusi lainsäädäntö myös selkeyttää ja ryhdistää rekisterinpitoa niiltä osin, joilta toimintatavat tähän asti ovat, sääntelystä huolimatta, olleet puutteellisia. Tietosuojatyön jalkauttamisessa organisaation kaikille tasoille osaava tietosuojavastaava ei ole kulu, vaan sijoitus.

Tämän opinnäytetyön tarkoituksena oli luoda selkeä ja mahdollisimman ajanmukainen kooste vaikutustenarvioinnin perusteista riskien ja niiden vaikutusten näkökulmasta. Oheismateriaalina tuotetusta, toimeksiantajan sisäiseen käyttöön tarkoitetusta riski- ja vaikutusanalyysistä on saatu yhteistyöryhmissä hyvää palautetta. Riskianalyysiä sekä tämän työn pohjalta laadittua vaikutustenarviointiohjetta käytetään työpajoissa koulutusten tukena vaikutustenarviointeja laadittaessa, kun taas opinnäytetyö kokonaisuudessaan soveltuu parhaiten tietosuojatyötä tekevän tai vaikutustenarviointeja laativan henkilön tukimateriaaliksi. Vaikutustenarvioinnin sääntely on uutta, eikä siitä vielä löydy juurikaan kansallista ohjausta tai tulkintaa, johon tutkimusta tai lopullisia ohjeita voisi perustaa.

Opinnäytetyön toimeksiantajan toiminnoissa vaikutustenarvioinnit ja niihin liittyvät ohjeet riskianalyyseineen kehittyvät ja tarkentuvat kansallisen ohjauksen, käytännesääntöjen, yhteistyön mukanaan tuomien hyvien käytänteiden sekä oman toiminnan kehittymisen myötä. Vaikutustenarviointien pohjatyönä tehdyt tietoinventaarit eri tietojärjestelmien sisältämistä tiedoista, selosteiden läpikäynti ja rekisteröityjen oikeuksien toteuttamiseksi suunnitellut prosessit ovat tuoneet esille riskejä sekä muutos- ja kehitystarpeita esimerkiksi tietojärjestelmien toiminnoissa, tietojärjestelmien tietojen, tietovirtojen ja elinkaaren dokumentoinnissa, ohjeiden täsmentämisessä ja koulutustarpeiden määrittelyssä. Muutokset tehostavat toimintoja ja prosesseja, selkiyttävät toimintatapoja ja tuovat aikanaan myös kustannussäästöjä. Jatkuvalla koulutuksella taataan hyvien käytänteiden entistä laajempi omaksuminen ja toiminnan kehittyminen. Yhteistyön syventäminen toimijoiden välillä on tärkeää, jotta vaikutustenarviointi saadaan osaksi yleistä riskienhallintaprosessia.

Vaikutustenarviointi ja riskiperusteinen lähestymistapa tarjoavat runsaasti mahdollisuuksia toiminnan kehittämiseen ja sen tutkimiseen paitsi organisaation sisällä, myös laajemmin. Uudet teknologiat kuten big data, IoT, keinoäly tai robotiikka tarjoavat useita mielenkiintoisia näkökulmia tutkimukseen. Kansallisen ohjauksen ja käytännesääntöjen myötä tarkempaa ja yksityiskohtaisempaa tutkimusta voitaisiin tehdä myös esimerkiksi vaikutustenarviointiprosessin mallinnuksesta ja kehittämisestä, vaikutustenarviointien yhteiskäytöstä organisaation sisällä tai julkishallinnon eri organisaatioissa tai rekisterinpitäjän ja palvelun toimittajan välisen yhteistyön näkökulmasta. Olisi tärkeää kehittää laaja-alaista yhteistyötä kansallisten, yhtenäisten toimintatapojen ja käytänteiden saavuttamiseksi esimerkiksi organisaatiomuutoksiin, palvelujen ulkoistuksiin tai rekisterinpitä-

jiä koskeviin lainsäädännön muutoshankkeisiin liittyen. Määrämuotoiset arvioinnit auttaisivat arviointien laatimisessa ja vertailussa esimerkiksi SOTE-sektorin tietojärjestelmähankintoihin liittyen.[157]

Aloitin opinnäytetyöni perustelemalla uudistuneen lainsäädännön tarvetta uudenlaisten tekniikoiden, laitteiden sekä sähköisten palvelujen ja valvonnan kasvulla sekä digikulttuurin muutoksella. Kehitystä ei voi eikä pidä pysäyttää. Toisaalta oikeutta tietosuojaan ei myöskään saa sivuuttaa pyrkimyksessä luoda ja kehittää uudenlaisia menetelmiä, tuotteita ja palveluita. Rekisteröidyn informointiin ja sen läpinäkyvyyteen tulee kiinnittää huomiota, jotta rekisteröidyllä on aidosti mahdollisuus valvoa henkilötietojensa käsittelyä. Valvontaviranomaisen rooli on tärkeä paitsi rekisteröityjen oikeuksien suojaamisen ja tietosuoja-asetuksen soveltamisen valvonnan kannalta, myös ohjauksen ja linjauksen sekä tarvittaessa rikkeisiin puuttumisen näkökulmasta. On erityisen tärkeää löytää tasapaino toiminnan ja palveluiden kehittämisestä aiheutuvien riskivaikutusten ja riskien pienentämiseksi toteutettavien suojatoimien välillä. On huomioitava, että vaikka riskejä havainnoidaan, arvioidaan ja lievennetään yksittäin, vaikutustenarviointien kannalta – kuten riskienhallinnan kannalta yleisestikin ottaen – kyseessä on kuitenkin kokonaistilanne: monen yksittäisen riskin toteutumistodennäköisyyden ja vaikutuksen yhteissumma. Rekisterinpitäjä vastaa riskin arvioinnista ja suojatoimien riittävyydestä oman harkintansa, riskinottokyvykkyytensä ja -halukkuutensa mukaisesti.

[157] Andreasson 2018.

LÄHTEET

Andreasson, A. Tietosuojavastaava. 2017. Haastattelu 29.11.2017. Haastattelija Himanka, P. Tampere.

Andreasson, A. Tietosuojavastaava. 2018. Haastattelu 23.1.2018. Haastattelija Himanka, P. Tampere.

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

Andreasson A., Koivisto J. & Ylipartanen A. 2016. Tietosuojakäsikirja johdolle. Helsinki: Tietosanoma.

Andreasson A., Riikonen J. & Ylipartanen A. 2017. Osaava tietosuojavastaava. Helsinki: Tietosanoma.

Bieker F., Friedewald M., Hansen M, Obersteller H. & Rost, M. 2016. A Process for Data Protection Impact Assessment Under the European General Data Protection Regulation. Karlsruhe, Germany: Fraunhofer Institute for Systems and Innovation Research ISI. Luettu 15.3.2018.

CNIL. 2018. Commission Nationale de l'Informatique et des Libertés. The open source PIA software helps to carry out data protection impact assessment. 20.1.2018. Luettu 10.3.2018.
https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

Euroopan komissio. 2012a. Ehdotus yleiseksi tietosuoja-asetukseksi. [COM(2012) 11 final, 2012/0011 (COD)] 25.1.2012. Tulostettu 14.3.2018.
https://eur-lex.europa.eu/legal-content/FI/ALL/?uri=CELEX%3A52012PC0011

Euroopan komissio. 2012b. Impact Assessment. SEC(2012) 72/2. Tulostettu 20.2.2018.
http://ec.europa.eu/transparency/regdoc/rep/2/2012/EN/SEC-2012-72-2-EN-MAIN-PART-1.PDF

Euroopan komissio. n.d. Riittävän tietosuojatason maat. Päivittyvä. Luettu 12.2.2018.
https://ec.europa.eu/info/law/law-topic/data-protection_en

Euroopan unionin neuvosto. 2002. Euroopan unionin neuvoston säädöskäsikirja. Luxemburg: Euroopan yhteisöjen virallisten julkaisujen toimisto. Tulostettu 15.2.2018.
https://publications.europa.eu/en/publication-detail/-/publication/431ccffd-00c2-491a-b423-ce709af0d6c3/language-fi

Hallberg, P. 2004. Perusoikeusjärjestelmä. Teoksessa Hallberg P., Karapuu H., Ojanen T., Scheinin, M., Tuori K. & Viljanen V-P. Perusoikeudet. 2004, päivittyvä. Päivitetty 6.4.2010. Helsinki: Alma Talent Oy. E-kirja. Luettu 2.4.2018.

Hanninen, M., Laine, E., Rantala, K., Rusi, M. & Varhela, M. 2017. Henkilötietojen käsittely. EU-tietosuoja-asetuksen vaatimukset. Vantaa: Hansaprint Oy. E-kirja. Luettu 3.4.2018.

HE 9/2018 vp. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Julkaistu 1.3.2018. Tulostettu 1.4.2018. https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_9+2018.aspx

Hemmo M. & Hoppu K. 2018. Sopimusoikeus. Helsinki: Alma Talent Oy. E-kirja. Luettu 20.1.2018.

Herold, R. n.d. GDPR: What a Data Protection Impact Assessment is and isn't. ISACA Now Blog. Luettu 14.3.2018. https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=864

Hirvonen A. 2011. Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja 17. Helsinki. Tulostettu 23.4.2018. https://www.helsinki.fi/sites/default/files/atoms/files/hirvonen_mitka_metodit.pdf

IAPP. 2018. The International Association of Privacy Professionals. CNIL releases PIA software for the GDPR: Here's how it works. 28.11.2017. Luettu 15.3.2018. https://iapp.org/news/a/cnil-releases-pia-software-for-the-gdpr-heres-how-it-works/

ICO. 2014. Information Commissioner’s Office, UK. Conducting privacy impact assessments code of practice. Data protection act. 25.2.2014. Version: 1.0. Luettu 14.3.2018. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

ICO. n.d. Information Commissioner’s Office, UK. n.d. Data protection impact assessments. Tulostettu 20.4.2018. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

ICO. 2018. Information Commissioner’s Office, UK. 2018. Sample DPIA template. 9.2.3018. Tulostettu 20.4.2018. https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

Järvinen P. & Rousku K. 2017. Työpaikan tietoturvaopas. Helsinki: Alma Talent Oy.

Koskinen I. 2017. Koneoppiminen EU:n yleisen tietosuoja-asetuksen valossa - etenkin automaattisen päätöksenteon näkökulmasta. Pro gradu-tutkielma. Helsingin yliopisto. Oikeustieteellinen tiedekunta. Luettu 27.2.2018. https://helda.helsinki.fi/handle/10138/229709

Kulla H. & Koillinen M. 2014. Julkisuus ja henkilötietojen suoja viranomaistoiminnassa. Turku: Painosalama Oy.

Kuntaliitto. 2017. Tietosuoja-asetuksen huomioiminen kilpailutettaessa julkisia hankintoja. 05/2017, versio 1.0. Tulostettu 14.42018. http://shop.kunnat.net/product_details.php?p=3362

Kuntaliitto. 2018. Tietosuoja-asetus. Henkilötietojen käsittelyn ehdot 4/2018. Tulostettu. 14.4.2018. https://www.kuntaliitto.fi/asiantuntijapalvelut/laki/julkisuus-ja-tietosuoja/tietosuoja-asetus

Lambert, P. 2018. Understanding the New European Data Protection Rules. Florida, US: CRC Press, Taylor & Francis Group. E-kirja. Luettu 20.4.2018.

Lehtinen, E. 2017. Rekisterinpitäjän oikeutettu etu henkilötietojen käsittelyn oikeusperusteena tietosuoja-asetuksessa ja tietosuojalautakunnan ratkaisukäytännössä. Pro gradu-tutkielma. Helsingin yliopisto. Oikeustieteellinen tiedekunta. Luettu 20.4.2018. https://helda.helsinki.fi/handle/10138/229721

Lång, J. 2017. Tietosuoja ja sopimukset. Teoksessa Andreasson A., Riikonen J. & Ylipartanen A. 2017. Osaava tietosuojavastaava. Helsinki: Tietosanoma, 124 – 136.
Manninen, S. 2004. Sananvapaus ja julkisuus (PL 12 §). Teoksessa Hallberg P., Karapuu H., Ojanen T., Scheinin, M., Tuori K. & Viljanen V-P. Perusoikeudet. 2004, päivittyvä. Päivitetty 18.1.2011. Helsinki: Alma Talent Oy. E-kirja. Luettu 2.4.2018.

Neuvonen, R. 2014. Yksityisyyden suoja Suomessa. Helsinki: Helsingin kamari Oy. E-kirja. Luettu 12.3.2018.

Oikeusministeriö. 2017. EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö 35/2017. 21.6.2017. Tulostettu 15.11.2017.

Oikeusministeriö. 2018. EU:n yleisen tietosuoja-asetuksen täytäntöönpanoryhmän (TATTI) loppumietintö 8/2018. 8.3.2018. Tulostettu 20.3.2018.

Ojanen, T. & Scheinin, M. 2004. Uskonnon ja omantunnon vapaus (PL 11 §). Teoksessa Hallberg P., Karapuu H., Ojanen T., Scheinin, M., Tuori K. & Viljanen V-P. Perusoikeudet. 2004, päivittyvä. Päivitetty 23.2.2010. Helsinki: Alma Talent Oy. E-kirja. Luettu 2.4.2018.

Ojasalo K., Moilanen T. & Ritalahti J. 2014. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Helsinki: Sanoma Pro Oy.

Paakkari, I. Tietosuojakonsultti. 2017, 2018. Haastattelut 29.1.2018 ja 17.4.2018. Haastattelija Himanka, P. Tampere.

Pellonpää, M. 2004. Henkilökohtainen koskemattomuus. Teoksessa Hallberg P., Karapuu H., Ojanen T., Scheinin, M., Tuori K. & Viljanen V-P. Perusoikeudet. 2004, päivittyvä. Päivitetty 17.7.2009. Helsinki: Alma Talent Oy. E-kirja. Luettu 2.4.2018.

Pervilä, M. 2018. Tivi. Iot:n tietoturva mättää, ja seuraukset ovat vakavia: ”Tämä ei ole enää teoriaa”. [Artikkeli]. Julkaistu 30.1.2018. Luettu 15.4.2018.

Pitkänen O., Tiilikka P. & Warma E. 2013. Henkilötietojen suoja. Helsinki: Alma Talent Oy.

Ponemon Institute 2017. Cost of Data Breach Study. Global Overview. June 2017. Luettu 14.4.2018.
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN

Raitio J. 2016. Euroopan unionin oikeus. Helsinki: Alma Talent Oy.

Ros, P. 2016. Tivi. Varjo-IT on myrkkyä digitalisaatiolle. [Tivin kumppaniblogit]. Julkaistu 30.11.2016. Luettu 15.4.2018.
https://www.tivi.fi/Kumppaniblogit/salesforce/varjo-it-on-myrkkya-digitalisaatiolle-6602931

Tampereen kaupunki 2018. Henkilötietojen käsittelyohje. Luettu 15.4.2018. Saatavilla Tampereen kaupungin intranetissä.

Teknologiainfo Teknova. 2018. IT2018. Tutustu IT-ehtoihin. Luettu 2.4.2018.
http://www.it-ehdot.fi/tutustu-ehtoihin

Tietosuojavaltuutetun toimisto, 2010. Henkilötietolain mukainen ilmoitusvelvollisuus. Päivitetty 27.7.2010. Luettu 12.3.2018.
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6Jfpr4Tsl/Henkilotietolain_mukainen_ilmoitusvelvollisuus.pdf

Tietosuojavaltuutetun toimisto, 2013. Henkilötietojen siirto ulkomaille henkilötietolain mukaan. Päivitetty 1.8.2013. Luettu 12.2.2018.
http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2017/02/privacyshield-sopimuksensoveltamistajatketaan.html

Tietosuojavaltuutetun toimisto 2014. Kotihoidon kameravalvonta. Julkaistu 24.10.2014. Luettu 2.4.2018.
http://www.tietosuoja.fi/fi/index/ratkaisut/kotihoidonkameravalvonta.html

Tietosuojavaltuutetun toimisto. 2015. Julkishallinnon tietojen hallinnassa vakavia puutteita. Lehdistötiedote. Julkaistu 28.1.2015. Luettu 20.4.2018.
http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/2015/01/julkishallinnontietojenhallinnassavakaviapuutteita.html

Tietosuojavaltuutetun toimisto. 2016. Kysymyksiä ja vastauksia tietosuojauudistuksesta. Julkaistu 7.4.2016. Luettu 15.3.2018.
http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/kysymyksiajavastauksia.html

Tietosuojavaltuutetun toimisto. 2017a. Henkilötietojen tietoturvaloukkaukset. Julkaistu 5.12.2017. Luettu. 5.2.2018.

Tietosuojavaltuutetun toimisto. 2017b. Selvityksiä ja ohjeita 4/2017. Miten valmistautua EU:n tietosuoja-asetukseen? Julkaistu 27.1.2017. Tulostettu 15.12.2017.
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf

Tietosuojavaltuutetun toimisto. 2017c. Privacy Shield -sopimuksen soveltamista jatketaan. 14.2.2017.

Tietosuojavaltuutetun toimisto. 2017d. Tietosuojavaltuutetun toimiston ohje lainsäädäntölausuntoihin. 16.10.2017, versio 1.0. Luettu 10.2.2018.
http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6OUObDjzr/Tietosuojavaltuutetun_toimiston_ohje_lainsaadantolausuntoihin_versio_1.0.pdf

Tietosuojavaltuutetun toimisto. 2017e. Tietosuojavaltuutetun blogi. Päivittyvä. Luettu 15.1.2018
http://www.tietosuoja.fi/fi/index/blogi/6IUtCELFH/2017/Qn5jFmw7z.html.stx

Tietosuojavaltuutetun toimisto. 2018a. Automaattinen päätöksenteko ja profilointi. Julkaistu 27.4.2018. Luettu 27.4.2018.
http://www.tietosuoja.fi/fi/index/euntietosuojauudistus/ohjeitarekisterinpitajalle/automaattinenpaatoksentekojaprofilointi.html

Tietosuojavaltuutetun toimisto. 2018b. Rekisteri- ja tietosuojaselosteet. Julkaistu 4.4.2018. Luettu 4.4.2018.
http://www.tietosuoja.fi/fi/index/materiaalia/lomakkeet/rekisteri-jatietosuojaselosteet.html

Tietosuojavaltuutetun toimisto. 2018c. Konsultilta opittua – kuinka yritysjohtajat herätetään valmistautumaan tietosuoja-asetukseen? Tietosuojavaltuutetun blogi. Julkaistu 1.12.2017. Luettu 13.12.2018.
http://www.tietosuoja.fi/fi/index/blogi/6IUtCELFH/2017/Qn5jFmw7z.html.stx

Tietosuojavaltuutetun toimisto. 2018d. Rekisterinpitäjän oikeutettu etu henkilötietojen käsittelyperusteena – varmista tasapainotestillä. Julkaistu 9.4.2018. Luettu 25.4.2018.
http://www.tietosuoja.fi/fi/index/ajankohtaista/tiedotteet/on/04/rekisterinpitajanoikeutettuetuhenkilotietojenkasittelyperusteena8210varmistatasapainotestilla.html

Tuori, K. 2004. Kokoontumis- ja yhdistymisvapaus (PL 13 §). Teoksessa Hallberg P., Karapuu H., Ojanen T., Scheinin, M., Tuori K. & Viljanen V-P. Perusoikeudet. 2004, päivittyvä. Päivitetty 1.8.2009. Helsinki: Alma Talent Oy. E-kirja. Luettu 2.4.2018.

Valtioneuvosto. 2017a. EU:n tietosuoja-asetuksen yritysvaikutukset. Policy Brief 10/2017. Luettu 4.4.2018.
http://tietokayttoon.fi/documents/1927382/2116852/10_2017_+EUn+tietosuoja-asetuksen+yritysvaikutukset/7f043abc-2068-45f2-8470-0b2df19f7189?version=1.0 sekä
http://tietokayttoon.fi/documents/10616/3866814/41_2017_Tietosuojas%C3%A4%C3%A4d%C3%B6sten+muutostarve/2c4ad983-8d90-480e-9b05-e3de9c9297c4?version=1.1

Valtioneuvosto. 2017b. Vuoden 2018 alusta voimaan tulevia muutoksia ministeriöiden hallinnonaloilla. Julkaistu 20.12.2017. Luettu 25.2.2018.
http://valtioneuvosto.fi/artikkeli/-/asset_publisher/vuoden-2018-alusta-voimaan-tulevia-muutoksia-ministerioiden-hallinnonaloilla

Valtioneuvosto. 2018. Arviointineuvosto tietosuojalaista: Hallituksen esitysluonnoksessa merkittäviä puutteita. 8.2.2018. Luettu 8.2.2018.
http://valtioneuvosto.fi/artikkeli/-/asset_publisher/10616/arviointineuvosto-tietosuojalaista-hallituksen-esitysluonnoksessa-merkittavia-puutteita

Valtioneuvoston kanslia. 2018. Lainsäädännön arviointineuvoston lausunto luonnoksesta hallituksen esitykseksi eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi yleiseksi lainsäädännöksi Dnro: VNK/133/32/2018. Julkaistu 8.2.2018. Luettu 9.2.2018. http://valtioneuvosto.fi/documents/10616/6601425/Lausunto+luonnoksesta+hallituksen+esitykseksi+eduskunnalle+EUn+yleist%C3%A4+tietosuoja-asetusta+t%C3%A4ydent%C3%A4v%C3%A4ksi+yleiseksi+lains%C3%A4%C3%A4d%C3%A4nn%C3%B6ksi+8.2.2018/219b9497-da3b-4d23-a5f9-a0bb3d01f47f

Valtiovarainministeriö. 2008. Valtionhallinnon tietoruvasanasto 8/2008. Tulostettu 15.4.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=7e2220f1-cc93-4ba6-8c70-a67869c526cc&groupId=10229

Valtiovarainministeriö. 2016. Vahti-raportti 1/2016. EU-tietosuojan kokonaisuudistus. Hyväksytty 3.5.2016. Tulostettu 20.1.2018. https://www.vahtiohje.fi/c/document_library/get_file?uuid=ddb05959-40d1-435f-af23-fd20fc21d63f&groupId=10229

Valtiovarainministeriö. 2017a. Ohje riskienhallintaan, VM 22/2017. Julkaistu 5.6.2017. Tulostettu 2.3.2018. http://julkaisut.valtioneuvosto.fi/handle/10024/80013

Valtiovarainministeriö. 2017b. VM 22/2017. Ohje riskienhallintaan - Liitteet 1-6. Tulostettu 2.3.2018. http://julkaisut.valtioneuvosto.fi/handle/10024/80013

Valtiovarainministeriö. 2017c. Riskienhallintatyökalu - Excel - perusversio. Julkaistu 2.6.2017. Tulostettu 2.3.2018. https://www.vahtiohje.fi/web/guest;jsessionid=DD46A1FD4E98321AF83986975D1348F8872E6A54CAC9FF390BF08ABC03F41CB35255964FD037E57BD9022A

Valtiovarainministeriö. 2018a. Yhteishankkeiden materiaalit. http://vm.fi/juhta-vahti-yhteishankkeiden-materiaalit

Valtiovarainministeriö. 2018b. Työpaja #4. Rekisterinpitäjän velvollisuuksien toteuttaminen, riskienhallinta. Riskienhallinta osa 4, tietosuojanäkökulma. [Työpaja 28.9.2017, luentomateriaali]. Tulostettu 17.11.2017. http://vm.fi/juhta-vahti-yhteishankkeiden-materiaalit

Viemerö, M. CIPP/E, CIPM, CIPT, CISA, CISM. 2017. Tietosuojan vaikutustenarvioinnit (”Data Protection Impact Assessment” / ”DPIA”). Arjen tietosuoja-työpaja: Vaatimusten huomioiminen uusia palveluita ja tietojärjestelmiä kehitettäessä. 25.10.2017. Helsinki.

Viestintävirasto. 2018. Organisaatioiden 5 yleisintä tietoturvauhkaa ja ratkaisua vuonna 2017. 16.1.2018. Luettu 20.2.2018. https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn201801161310.html

Viljanen, V-P. 2004. Yksityiselämän suoja (PL 10 §). Teoksessa Hallberg P., Karapuu H., Ojanen T., Scheinin, M., Tuori K. & Viljanen V-P. Perusoikeudet. 2004, päivittyvä. Päivitetty 9.2.2011. Helsinki: Alma Talent Oy. E-kirja. Luettu 2.4.2018.

WP29. 2016. Oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevat ohjeet. Annettu 13.12.2016. Päivitetty 5.4.2017. Tulostettu 12.11.2017. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233

WP29. 2017a. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. Annettu 4.4.2017. Päivitetty 4.10.2017. Tulostettu 21.11.2017. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

WP29. 2017b. Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu "korkea riski". 2017. Tietosuojatyöryhmä. Annettu 4.4.2017. Päivitetty 4.10.2017. Tulostettu 10.11.2017. http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/ibVehxmcp/Ohjeet_tietosuojaa_koskevasta_vaikutustenarvioinnista.pdf

WP29. 2017c. Opinion 2/2017 on data processing at work. Annettu 8.6.2017. Tulostettu 10.11.2017. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169

WP29. 2017d. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Annettu 3.10.2017. Päivitetty 6.2.2018. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

WP29. 2017e. Guidelines on transparency under Regulation 2016/679. Annettu 29.11.2017. Päivitetty 11.4.2018. Tulostettu 20.4.2018. http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Wright, D. & Raab, C. 2014. Privacy principles, risks and harms. International Review of Law, Computers & Techology, vol. 28, no. 3, pp. 277-298. [Academic Journal]. School of Social and Political Science, University of Edinburgh, Edinburgh, UK. Luettu 12.2.2018.

LIITTEET

Liite 1. Riskienhallintatyökalu, Excel perusversio.[158]

Riskien tunnistaminen				Riskianalyysi		Riskin merkityksen arviointi		Riskin käsittely				Lisätietoja
Riskin tunniste	Riskiluokka	Riski (riskin nimi)	Riskin kuvaus (mistä riski johtuu, mitä voi tapahtua toteutuessa):	Todennäköisyys	Vaikutus	Riskin suuruus (T x V)	Toimenpidetarpeet riskin	Toimenpide-ehdotukset riskin	Toimenpiteiden vapaamuotoinen (sanallinen) kuvaus	Vastuu henkilö	Tavoiteaikataulu (mihin mennessä	
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0	Ei arvioitu	0	Ei			
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0	Ei arvioitu	0	Ei			
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0	Ei arvioitu	0	Ei			
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0	Ei arvioitu	0	Ei			
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0	Ei arvioitu	0	Ei			
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0	Ei arvioitu	0	Ei			
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0	Ei arvioitu	0	Ei			
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0	Ei arvioitu	0	Ei			
	Täytä arvo 1-4			Ei arvioitu	Ei arvioitu	0	Ei arvioitu	0	Ei			

[158] Valtiovarainministeriö 2017c.

Liite 2. Esimerkkejä vaikutustenarvioinnin kehyksistä

WP29 2017b, liite 1.

Tietosuoja-asetuksessa ei määritellä, mitä menettelyä on käytettävä tietosuojaa koskevan vaikutustenarvioinnin tekemiseen. Sen sijaan siinä annetaan rekisterinpitäjille mahdollisuus ottaa käyttöön kehys, jolla täydennetään niiden olemassa olevia toimintatapoja edellyttäen, että niissä otetaan huomioon 35 artiklan 7 kohdassa mainitut osatekijät. Tällainen kehys voi olla rekisterinpitäjän tarpeisiin suunniteltu tai tietylle toimialalle yhteinen. Alla on esimerkkejä EU:n tietosuojaviranomaisten kehittämistä aiemmin julkaistuista kehyksistä ja EU:n alakohtaisista kehyksistä.

Esimerkkejä EU:n yleisistä kehyksistä:

- DE: Standardoitu tietosuojamalli V.1.0 – Testiversio, 2016. https://www.datenschutzzentrum.de/sdm/
- ES: Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf
- FR: Privacy Impact Assessment (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/en/privacy-impact-assessment-pia
- UK: Conducting privacy impact assessments code of practice, Information Commissioner's Office (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

(jatkuu)

Esimerkkejä EU:n alakohtaisista kehyksistä:

- Kehys RFID-sovellusten yksityisyyden suojaa koskevien ja tietosuojavaikutusten arvioinnille32.
    - Katso myös komission suositus, annettu 12 päivänä toukokuuta 2009, yksityisyyden suojaa ja tietosuojaa koskevien periaatteiden toteuttamisesta radiotaajuustunnistusta käyttävissä sovelluksissa: https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-12-may-2009-implementation-privacy-and-data-protection-principles
    - Katso myös lausunto 9/2011 elinkeinoelämän ehdottamasta tarkistetusta kehyksestä RFID-sovellusten yksityisyyden suojaa ja tietosuojaa koskeville vaikutustenarvioinneille: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf
- Älykkäiden verkkojen ja älykkäiden mittausjärjestelmien tietosuojaa koskevan vaikutustenarvioinnin laadintamalli: https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf
    - Katso myös lausunto 07/2013 komission älykkäitä verkkoja käsittelevän erityisryhmän alaisen asiantuntijaryhmän 2 kehittämästä älykkäiden verkkojen ja älykkäiden mittausjärjestelmien tietosuojaa koskevan vaikutustenarvioinnin laadintamallista. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_fi.pdf

Liite 3. Tietosuojaa koskevan vaikutustenarvioinnin hyväksymiskriteerit

WP29 2017b, liite 2.

Tietosuojatyöryhmä ehdottaa seuraavia kriteerejä, joita rekisterinpitäjät voivat käyttää arvioidessaan, onko tietosuojaa koskeva vaikutustenarviointi tai sen tekemiseen käytettävä menetelmä riittävän kattava yleisen tietosuoja-asetuksen noudattamiseksi:

☐ järjestelmällinen kuvaus käsittelystä annetaan (35 artiklan 7 kohdan a alakohta):
- ☐ käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset otetaan huomioon (johdanto-osan 90 kappale)
- ☐ henkilötiedoista, vastaanottajista ja henkilötietojen säilytysajasta pidetään kirjaa
- ☐ toiminnallinen kuvaus käsittelytoimesta esitetään
- ☐ henkilötietojen käsittelyyn käytettävät resurssit (laitteistot, ohjelmistot, verkostot, ihmiset, asiakirjat tai asiakirjojen välittämiseen käytettävät kanavat) yksilöidään
- ☐ hyväksyttyjen käytännesääntöjen noudattaminen otetaan huomioon (35 artiklan 8 kohta)

☐ tarpeellisuus ja oikeasuhteisuus arvioidaan (35 artiklan 7 kohdan b alakohta):
- ☐ suunnitellut toimenpiteet asetuksen noudattamiseksi määritellään (35 artiklan 7 kohdan d alakohta ja johdanto-osan 90 kappale) ottaen huomioon
  - ☐ käsittelyn oikeasuhteisuutta ja tarpeellisuutta edistävät toimenpiteet, joiden perustana on/ovat
    - ☐ yksi tai useampi tietty, nimenomainen ja laillinen tarkoitus (5 artiklan 1 kohdan b alakohta)
    - ☐ käsittelyn lainmukaisuus (6 artikla)
    - ☐ tiedot, jotka ovat asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista (5 artiklan 1 kohdan c alakohta)
    - ☐ rajoitettu säilytysaika (5 artiklan 1 kohdan e alakohta)

(jatkuu)

☐ rekisteröityjen oikeuksia edistävät toimenpiteet:

- ☐ rekisteröidylle annettavat tiedot (12, 13 ja 14 artikla)
- ☐ oikeus saada pääsy tietoihin ja siirtää tiedot järjestelmästä toiseen (15 ja 20 artikla)
- ☐ oikeus tietojen oikaisemiseen ja poistamiseen (16, 17 ja 19 artikla)
- ☐ vastustamisoikeus ja oikeus käsittelyn rajoittamiseen (18, 19 ja 21 artikla)
- ☐ suhteet henkilötietojen käsittelijöihin (28 artikla)
- ☐ kansainvälisiin henkilötietojen siirtoihin liittyvät suojatoimet (V luku)
- ☐ ennakkokuuleminen (36 artikla).

☐ <u>rekisteröityjen oikeuksiin ja vapauksiin kohdistuvia riskejä hallitaan</u> (35 artiklan 7 kohdan c alakohta):

- ☐ riskien alkuperä, luonne, erityisluonne ja vakavuus arvioidaan (ks. johdanto-osan 84 kappale) tai tarkemmin ottaen kunkin riskin (laiton tietoihin pääsy, tietojen asiaton muuttaminen ja tietojen katoaminen) osalta erikseen rekisteröityjen näkökulmasta:
  - ☐ riskien alkuperä otetaan huomioon (johdanto-osan 90 kappale)
  - ☐ rekisteröityjen oikeuksiin ja vapauksiin kohdistuvat mahdolliset vaikutukset tunnistetaan sellaisten tapahtumien osalta, joihin kuuluu laiton tietoihin pääsy, asiaton muuttaminen ja tietojen katoaminen
  - ☐ tunnistetaan uhat, jotka voivat johtaa laittomaan tietoihin pääsyyn, asiattomaan muuttamiseen ja tietojen katoamiseen
  - ☐ todennäköisyys ja vakavuus arvioidaan (johdanto-osan 90 kappale)
- ☐ riskien käsittelyyn suunnitellut toimenpiteet määritellään (35 artiklan 7 kohdan d alakohta ja johdanto-osan 90 kappale)

☐ <u>Sidosryhmät otetaan mukaan seuraavasti</u>:

- ☐ pyydetään tietosuojavastaavalta neuvoja (35 artiklan 2 kohta)
- ☐ tarvittaessa pyydetään rekisteröityjen tai heidän edustajiensa näkemyksiä (35 artiklan 9 kohta).

Liite 3. ICO: Sample DPIA template

Sample DPIA template

This template is an example of how you can record your DPIA process and outcome. It follows the process set out in our DPIA guidance, and you should read it alongside that guidance and the Criteria for an acceptable DPIA set out in European guidelines on DPIAs.

Start to fill out the template at the beginning of any major project involving the use of personal data, or if you are making a significant change to an existing process.

Integrate the final outcomes back into your project plan.

Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
.

(jatkuu)

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

(jatkuu)

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

(jatkuu)

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

(jatkuu)

Step 5: Identify and assess risks

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
	Remote, possible or probable	Minimal, significant or severe	Low, medium or high

(jatkuu)

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
		Eliminated, reduced or accepted	Low, medium or high	Yes/no

(jatkuu)

Step 7: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		
This DPIA will be kept under review by:		The DPO should also review ongoing compliance with DPIA